CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 1

CCIE SCv4 Lab 1 Introduction

Lab Guidelines

The following scenarios are practice labs designed to test your readiness for the Cisco Systems CCIE Security Lab Exam. However, remember that in addition to being designed as a simulation of the actual CCIE lab exam, these practice labs should be used as a learning tool. Instead of rushing through the labs to complete all the configuration steps, take the time to research the networking technology and gain a deeper understanding of the principles behind its operation. For each lab of the CCIE Security Practice Labs Workbook, follow these guidelines:

- Read the entire lab exam before starting the configuration, and correlate tasks within a section to get a complete overview of the lab objectives.
- There are dependencies between tasks of the same section and between tasks from different sections. Carefully read throughout the lab to identify and make notes of it
- The lab consists of six sections that don't necessarily need to be completed in the presented order. However some tasks must be completed before others (such as initialization of ASA firewalls).
- All sections total 100 points, and you must earn a minimum of 80 points to receive a passing grade. To earn the points assigned to each task, you must fulfill all requirements and conform to all restrictions.
- No partial credit is awarded. You will earn all points or zero points for each task; if multiple solutions are available for a task, choose the one that technically best meets the requirements.
- Some tasks present a set of requirements for implementing a technology, and some tasks present outputs to be matched.
- Labs include both configuration and troubleshooting tasks; the number of faults relevant to each troubleshooting task may or not be specified.
- Before starting the exam, verify that all equipment is functional, powered up and that you can access it at the console.
- Routers and switches are preconfigured, do not change it unless specifically allowed

https://t.me/learningnets

by the task. On troubleshooting tickets, you may change any of the initial configurations.

- IPv4/IPv6 static and default routes are allowed to complete any task, but only if this is the only available option, and unless otherwise stated in any task.
- Make sure you do not to lock yourself out of any device, because password recovery or device reset is not available in the lab.
- At the end of the exam, ensure that all devices are accessible at the console by using preconfigured credentials or the ones from specific task requirements.
- For IPv4/IPv6 addressing configuration, the following variables will be used as a reference:
  - **X** is the rack number; the value for **Rack1** will be **1**.
  - **Y** is the device number, with routers ranging from one (1) to seven (7), switches from nine (9) to fourteen (14), and ASA firewalls from fifteen (15) to eighteen (18); the value for **Router1** will be **1**, **Switch1** will be **9**, and **ASA1** will be **15**.

All routers and switches are accessible at the console without requiring any authentication; do not change this. To access other devices within the lab, use the following tables as a reference:

Device	Username	Password
TESTPC-A	ineadmin	ciscoccie
TESTSRV-A	Administrator	Cisco1234
TESTPC-B	ineadmin	ciscoccie
TESTSRV-B	Administrator	Cisco1234
TESTPC-WIFI	ineadmin	ciscoccie

Device	Username	Password
WSA CLI&GUI	admin	default1A

https://t.me/learningnets

Device	Username	Password
ACS1 CLI	admin	default1A
ACS1 GUI	acsadmin	default1A
ACS2 CLI	admin	default1A
ACS2 GUI	acsadmin	default1A
ISE1 CLI&GUI	admin	default1A
ISE2 CLI&GUI	admin	default1A
WLC CLI&GUI	admin	default1A
LAP CLI	cisco	Cisco
IPS CLI&GUI	cisco	ciscoips4240

Lab Instructions

Before you begin, make sure that the initial configuration scripts for each lab have been applied. If you have any questions related to the scenario solutions, visit our CCIE support forum at http://IEOC.com. Refer to the attached physical and logical diagrams on each lab for interface and protocol assignments; you may access these by clicking the **Resources** button in the upper-right corner. Upon lab completion, end-to-end IPv4/IPv6 connectivity is not a requirement unless specifically asked for, but you are required to meet task requirements and restrictions.

Lab Restrictions

Each lab scenario contains explicit general restrictions that you must conform to while configuring the lab. These restrictions are defined in the introductory section for each scenario. Examples of such restrictions include, but are not limited to, not adding additional IP addressing, not changing the default authentication methods,

https://t.me/learningnets

etc. There may also be certain restrictions for particular tasks within a lab scenario. Examples of these restrictions include, but are not limited to, not issuing a particular configuration command, not using the legacy configuration for a technology, etc.

TIP

You may do whatever is necessary to complete a task unless the general requirements for the lab scenario or the specific requirements for the task explicitly prohibit you from doing so. This may include using static routing, NAT statements, ACL exceptions, IPsec/GRE tunneling, etc.

Difficulty Rating

Each lab scenario has been assigned a difficulty rating. Ratings are on a scale of one (1) to ten (10), with 10 being the most difficult. Labs are designed to be more technically challenging than the actual CCIE Security Lab Exam. Do not be discouraged if you score low or do not understand a particular set of technologies. If you are having trouble with a certain area, do not hesitate to read the explanation contained within the solutions guide and study the respective technology using the Technologies Workbook or the Advanced Technologies video course. Remember that these labs are designed to teach you required skills for implementing and troubleshooting a complex network with several technologies mixed together, just as much as they are intended to test your current technical knowledge.

Point Values

As in the actual CCIE Lab exam, each task within a lab is assigned a specific point value. Points are awarded only if the presented solution meets all the given requirements and does not violate any restrictions. No partial credit is awarded for any task. A minimum score of 80 points is required to pass a particular scenario. Some tasks have multiple solutions; as long as the presented solution meets the given requirements, points will be awarded for that task. However, certain solutions may negatively affect previous or future tasks. Make sure that you carefully read all presented requirements and try your best to come up with a technically appropriate solution.

TIP

https://t.me/learningnets

Points will never be awarded for a task in which you have violated the requirements. However, remember the relative point value of the task in question as compared to future tasks. If you cannot find an appropriate solution for a particular task, it is advisable to solve the task by whatever means necessary to complete the future tasks that depend on it.

Loading Initial Config

Each lab contains a set of initial configuration scripts for routers and switches. These configuration scripts include basic Layer 2 and Layer 3 routing connectivity (as well as possible more advanced functionalities for troubleshooting tickets), and must be loaded on your rack before beginning the configuration of the scenario. These are available to be loaded from the Rack Rental Control Panel, or if you are using your own rack, they are attached to each individual lab and available for download. Initial configurations and physical and logical diagrams of each lab are attached to this Introduction; you may access these by clicking the **Resources** button in the upper-right corner.

Rack Rentals

INE has designed the CCIE Security Practice Labs Workbook based around the publicly stated hardware specification used in the actual CCIE Lab exam. To eliminate the cost of buying all the equipment used in the workbook, INE offers cost-effective equipment rentals specifically designed to be used with this and other self-paced training product lines. For more information on rack rentals. visit http://INE.com.

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 1

CCIE SCv4 Lab 1 Tasks

1. Perimeter Security and Services
2. Intrusion Prevention and Content Security
3. Confidentiality and Secure Access
4. Identity Management
5. System Hardening and Availability
6. Threat Identification and Mitigation

Difficulty Rating (10 highest): 8

Point Values

The point values for each section are as follows:

Section	Point Value
Perimeter Security and Services	24
Intrusion Prevention and Content Security	17
Confidentiality and Secure Access	19
Identity Management	16
System Hardening and Availability	14

https://t.me/learningnets

Section	Point Value
Threat Identification and Mitigation	10

GOOD LUCK!

TIP

When taking the CCIE lab exam, you will be provided with a few sheets of scratch paper for notes and diagrams. You should create two diagrams at a minimum: one for the logical Layer 2 topology and one for the logical Layer 3 topology. Note that the physical diagram and the logical Layer 2 diagram are not the same.

Although you are provided with the logical Layer 3 diagram in the lab, it will be in electronic format, which means that you cannot add notes to it and may need to switch between windows to see it on the computer. By having your own diagram, you will be able to take notes on it and quickly reference it as you work through the configuration section. Finally, drawing the Layer 2 and Layer 3 topologies will help you become familiar with a complex network toplogy at first sight.

---

1. Perimeter Security and Services

1.1 ASA Routed Mode (3 points)

- Configure ASA1 in routed single mode with a hostname of **ASA12**, using the information from the table:

Interface	Nameif	Security Level	IPv4 Address
E0/0.43	DMZ1	60	140.1.45.Y/24
E0/0.73	DMZ2	50	140.1.71.Y/24

https://t.me/learningnets

Interface	Nameif	Security Level	IPv4 Address
E0/1.40	INSIDE	100	172.16.3.1/24
E0/1.91	OUTSIDE	0	140.1.91.Y/24

- Configure ASA1 for EIGRP in AS 200; do not advertise VLAN 40 prefix.

1.2 ASA Active-Standby Failover (3 points)

- Configure ASA1 and ASA2 in for active-standby failover, matching the following output from ASA1:

```
ASA12# show failover

    Failover On
    Failover unit Primary
    Failover LAN Interface: FAILOVER Ethernet0/2 (up)
    Unit Poll frequency 500 milliseconds, holdtime 2 seconds
    Interface Poll frequency 5 seconds, holdtime 25 seconds
    Interface Policy 2
    Monitored Interfaces 4 of 110 maximum
    Version: Ours 8.2(5), Mate 8.2(5)
    Last Failover at: 16:09:56 UTC Mar 25 2014
            This host: Primary - Active
                    Active time: 257 (sec)
                    slot 0: ASA5510 hw/sw rev (1.1/8.2(5)) status (Up Sys)
                      Interface DMZ1 (140.1.45.15): Normal
                      Interface DMZ2 (140.1.71.15): Normal
                      Interface INSIDE (172.16.3.1): Normal
                      Interface OUTSIDE (140.1.91.15): Normal
                    slot 1: empty
            Other host: Secondary - Standby Ready
                    Active time: 66 (sec)
                    slot 0: ASA5510 hw/sw rev (2.0/8.2(5)) status (Up Sys)
                      Interface DMZ1 (140.1.45.16): Normal
                      Interface DMZ2 (140.1.71.16): Normal
                      Interface INSIDE (172.16.3.2): Normal
                      Interface OUTSIDE (140.1.91.16): Normal
```

https://t.me/learningnets

```
                    slot 1: empty

    Stateful Failover Logical Update Statistics
            Link : Unconfigured.
```

1.3 ASA Routed Mode (3 points)

- Configure ASA3 in routed single mode with a hostname of **ASA3**, using the information from the table:

Interface	Nameif	Security Level	IPv4 Address
Gi0/0	INSIDE	100	172.16.6.1/24
Gi0/1.38	OUTSIDE	0	140.1.38.Y/24
Gi0/1.63	WLC	40	172.16.5.1/241

- Configure ASA3 to advertise all its connected prefixes into EIGRP AS 200.
- Disable EIGRP packet processing on VLAN 63.

1.4 ASA Transparent Mode (3 points)

- Configure ASA4 in transparent single mode with a hostname of **ASA4**, using the information from the table:

Interface	Nameif	Security Level	Bridge-Group
Gi0/0.71	DMZ1	30	77
Gi0/0.74	INSIDE	100	77
Gi0/1.72	OUTSIDE	0	77

https://t.me/learningnets

Interface	Nameif	Security Level	Bridge-Group
Gi0/1.73	DMZ2	80	77

- Ensure that EIGRP is functional between ASA1, R2, and SW2 using the minimum required commands.
- Use the IPv4 address 140.1.71.Y/24, and allow IPv6 packet forwarding according to security levels without configuring any IPv6 global unicast address.

1.5 CBAC Transparent Mode (2 points)

- Configure CBAC on R3, considering VLAN 93 as the untrusted interface.
- All IPv4 UDP/TCP/ICMP traffic should be inspected as it exits the untrusted interface.

1.6 CBAC Transparent Mode (3 points)

- Configure CBAC on R3, considering VLAN 83 as the untrusted interface.
- Both router-originated and transit IPv4 TCP/UDP/ICMP traffic should be inspected.
- R3 should log a message for ICMP sessions and delete the entry from state table after 30 seconds.

1.7 Traffic Policy (3 points)

- Configure the network to match the following outputs:

```
ASA12# traceroute 150.1.1.1

    Type escape sequence to abort.
    Tracing the route to 150.1.1.1

     1  140.1.91.9 0 msec 0 msec 10 msec
     2  140.1.38.3 0 msec 0 msec 10 msec
     3  140.1.38.1 0 msec *  0 msec

SW1#traceroute 150.1.1.1


    Type escape sequence to abort.
```

https://t.me/learningnets

```
Tracing the route to 150.1.1.1

  1 172.16.6.1 8 msec *  0 msec
  2 140.1.38.3 0 msec 8 msec 0 msec
  3 140.1.38.1 8 msec *  0 msec
```

1.8 ASA NAT (4 points)

- Configure ASA3 to statically NAT R4's Loopback0 into 172.16.6.4 on its **INSIDE** interface.
  - Allow telnet and ping traffic to SW1's Loopback0 interface for testing.
  - NAT rule should restrict traffic from being initiated in the reverse direction.

- Using auto-nat, configure ASA3 to NAT R1's Loopback0 into its **INSIDE** interface.
  - Allow telnet and ping traffic to SW1's Loopback0 interface for testing.

2. Intrusion Prevention and Content Security

2.1 IPS Initialization (2 points)

- Initialize the IPS using the information from the table:

Variables	Values
Hostname	IPS
IPv4 Address	140.1.57.100/24
Default Gateway	140.1.57.9
Telnet	Enabled
Login Banner	This is IPS from CCIE Lab Exam

https://t.me/learningnets

Variables	Values
Management Access	140.1.71.0/24

- Ensure that ping and telnet from the default gateway are allowed by the IPS.
- Ensure that administrators from VLAN 71 can manage the IPS through both telnet and HTTPS.

2.2 IPS Inline Interface-Pair (2 points)

- Configure IPS inline between VLAN 43 and VLAN 45 using the interfaces from the diagram.
- Ensure that traffic between these VLANs is inspected by the IPS.

2.3 IPS Custom Signature (3 points)

- Configure a custom signature to match relevant parts of the output:

```
sensor# show events


    evIdsAlert: eventId=1395295337431000769 severity=medium vendor=Cisco alarmTraits=32768
      originator:
        hostId: IPS
        appName: sensorApp
        appInstanceId: 1202
      time: 2014/03/26 06:15:08 2014/03/26 06:15:08 UTC
      signature: description=My Sig id=60001 created=20000101 type=other version=custom
        subsigId: 0
        sigDetails: My Sig Info
      interfaceGroup: vs0
      vlan: 0
      participants:
        attacker:
          addr: locality=OUT 140.1.45.11
        target:
          addr: locality=OUT 224.0.0.10
          os: idSource=unknown relevance=relevant type=unknown
      triggerPacket:
    000000  01 00 5E 00 00 0A 44 D3  CA 63 99 C1 08 00 45 C0  ..^...D..c....E.
```

https://t.me/learningnets

```
000010  00 3C 00 00 00 00 02 58  1E 94 8C 01 2D 0B E0 00  .<.....X....-...
000020  00 0A 02 05 F1 0A 00 00  00 00 00 00 00 00 00 00  ................
000030  00 00 00 00 00 C8 00 01  00 0C 01 00 01 00 00 00  ................
000040  00 0F 00 04 00 08 07 00  03 00                    ..........
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 66
  threatRatingValue: 66
  interface: ge0_0
  protocol: IP protocol 88
```

2.4 WSA Initialization (4 points)

- Initialize the WSA using the information from the table:

Variables	Values
Hostname	wsa.inelab.local
DNS Server	150.1.4.4
NTP Server	150.1.4.4
Proxy Ports	P1
M1 IPv4 Address	172.16.6.100/24
M1 Default Gateway	172.16.6.1
P1 Default Gateway	140.1.91.9
Admin Password	default1A
Email Address	ccielab@inelab.local

https://t.me/learningnets

Variables	Values
Senderbase Participation	Minimum

- Assign **TEST-PC-B** the IPv4 address of 140.1.71.100/24 for this scope with a default gateway of ASA1.
- Ensure that **TEST-PC-B** can manage the WSA through HTTPS.
- Do not make any configuration changes on SW1 for this task.

2.5 WSA WCCP Integration (3 points)

- Configure SW1 to redirect all HTTP traffic received inbound on its VLAN 91 interface to the WSA.
- Secure the communication and match the output:

```
SW1#show ip wccp 91 detail

    WCCP Client information:
            WCCP Client ID:          140.1.91.100
            Protocol Version:        2.0
            State:                   Usable
            Redirection:             L2
            Packet Return:           L2
            Packets Redirected:    0
            Connect Time:          00:04:21
            Assignment:            MASK
```

2.6 WSA Traffic Policies (3 points)

- Configure the WSA to do caching for as much content as possible.
- Configure the WSA so that access to **wwww.gunbroker.com** is disallowed; the URL resolves to SW1's Loopback0 IPv4 address.
- Users should accept the company Internet access usage policy if idle for two hours.
- Ensure that tests from **VLAN 73** can be performed to verify configured policies.

https://t.me/learningnets

3. **Confidentiality and Secure Access**

3.1 IKEv2 LAN-to-LAN (4 points)

- Configure IKEv2 LAN-to-LAN IPsec VPN between R1 and ASA3 to protect traffic between R1's and SW1's Loopback0 subnets:
  - use the default algorithms on ASA3.
  - modify the smart defaults on R1 accordingly.
  - use symmetric PSK authentication.

3.2 ASA Remote Access (4 points)

- Ensure that users from VLAN 71 can establish IKEv1 IPsec sessions to ASA3:
  - allocate IPv4 addresses from subnet 140.1.50.0/24.
  - do not configure any IPv4 static routes.
  - only traffic destined to R1's Loopback0 should be protected.
  - only ICMP traffic should be allowed through the IPsec tunnel.
  - use **testpcb** for any required password.

- Identify all required parameters from the following output:

```
ASA3# show vpn-sessiondb detail ra-ikev1-ipsec


    Session Type: IKEv1 IPsec Detailed

    Username     : testpcb               Index        : 28
    Assigned IP  : 140.1.50.1            Public IP    : 140.1.71.100
    Protocol     : IKEv1 IPsecOverTCP
    License      : Other VPN
    Encryption   : 3DES                  Hashing      : MD5
    Bytes Tx     : 0                     Bytes Rx     : 0
    Pkts Tx      : 0                     Pkts Rx      : 0
    Pkts Tx Drop : 0                     Pkts Rx Drop : 0
    Group Policy : testpcb               Tunnel Group : TEST_PC_B
    Login Time   : 13:49:39 UTC Thu Mar 27 2014
    Duration     : 0h:02m:42s
    Inactivity   : 0h:00m:00s
    NAC Result   : Unknown
```

https://t.me/learningnets

```
    VLAN Mapping : N/A                    VLAN         : none

    IKEv1 Tunnels: 1
    IPsecOverTCP Tunnels: 1

    IKEv1:
      Tunnel ID    : 28.1
      UDP Src Port : 5211                 UDP Dst Port : 500
      IKE Neg Mode : Aggressive           Auth Mode    : preSharedKeys
      Encryption   : 3DES                 Hashing      : MD5
      Rekey Int (T): 86400 Seconds        Rekey Left(T): 86241 Seconds
      D/H Group    : 2
      Filter Name  : VPN_FILTER
      Client OS    : WinNT                Client OS Ver: 5.0.07.0410

    IPsecOverTCP:
      Tunnel ID    : 28.2
      Local Addr   : 0.0.0.0/0.0.0.0/0/0
      Remote Addr  : 140.1.50.1/255.255.255.255/0/0
      Encryption   : 3DES                 Hashing      : MD5
      Encapsulation: Tunnel               TCP Src Port : 5211
      TCP Dst Port : 80
      Rekey Int (T): 28800 Seconds        Rekey Left(T): 28639 Seconds
      Idle Time Out: 30 Minutes           Idle TO Left : 27 Minutes
      Bytes Tx     : 0                    Bytes Rx     : 0
      Pkts Tx      : 0                    Pkts Rx      : 0

    NAC:
      Reval Int (T): 0 Seconds            Reval Left(T): 0 Seconds
      SQ Int (T)   : 0 Seconds            EoU Age(T)   : 161 Seconds
      Hold Left (T): 0 Seconds            Posture Token:
      Redirect URL :
```

3.3 IPv6 VRF-Aware DMVPN Troubleshooting (4 points)

- The VRF named **DMVPN** has been configured on R2, R5, and R6.
- IPv6 VRF-aware DMVPN has been configured on all three routers, with R6 being the hub.
- EIGRP is the routing protocol used to advertise Loopback256 prefixes.
- Fix the configuration errors so that you match the following outputs:

https://t.me/learningnets

```
R2#ping vrf DMVPN 2001::66 source loopback256
    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 2001::66, timeout is 2 seconds:
    Packet sent with a source address of 2001::22%DMVPN
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R2#ping vrf DMVPN 2001::55 source loopback256

    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 2001::55, timeout is 2 seconds:
    Packet sent with a source address of 2001::22%DMVPN
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

3.4 IPv4 GETVPN Troubleshooting (4 points)

- GET VPN is configured between R1, R4, and R6, with R6 being the KS and R1/R4 the GMs.
- GRE tunnels between R1/R4 and R6 have been configured for the registration process.
- Traffic between R1 and R4 Loopback0 prefixes must be protected.
- Fix the configuration errors so that you match the following output:

```
R6#show crypto gdoi ks members | i ID

    Group Member ID    : 16.16.16.1
     Group ID          : 146
     Key Server ID     : 6.6.6.6
    Group Member ID    : 46.46.46.4
     Group ID          : 146
     Key Server ID     : 6.6.6.6
```

3.5 WLC Security (3 points)

- Configure the network so that CAPWAP UDP ports are allowed between VLAN 12 and WLC, so LAP can join the WLC.
- Ensure that WLC can be managed through HTTPS by administrators in VLAN 71.

https://t.me/learningnets

- Configure a rogue malicious rule named **MALICIOUS_FIRST** that is true when both of the following conditions are matched:
  - SSID named **CCIELAB**.
  - RSSI value of -50 or stronger.

4. Identity Management

4.1 IOS TACACS+ (5 points)

- Configure R5 to be configured via HTTP on port 8080.
- Authenticate users against the ACS server and test with username **WEB_USER** and the password **CISCO**.
- Source the TACACS session off R5's Loopback0 interface and use a shared key of **CISCO**.

4.2 IOS TACACS+ (5 points)

- Configure R2 to authenticate telnet sessions against the ACS server.
- Source the TACACS session off R5's Loopback0 interface and use a shared key of **CISCO**.
- When user **TEST1** is authenticated, the command **show ip interface brief** should be automatically executed without being disconnected.
- User **TEST1** should be authorized for all commands, and user **TEST2** should be given access to all **debug** and **undebug all** commands.
- Both users should be automatically placed into privilege level 15 and use a password of **CISCO**.

4.3 ISE Central Web Authentication (6 points)

https://t.me/learningnets

- Configure SW3 and ISE1 to authenticate **TEST-PC-B** through ISE Web Portal.
  - Test by accessing R6's Loopack0 on port 80.
- Assume that **TEST-PC-B** can have any IPv4 address in VLAN 71 and is configured with a DNS server of 150.1.4.4.
- For testing purposes, configure ISE with a username of **TEST-PC-B** and a password of **Cisco123**.
- Source the RADIUS session off SW3's Loopback0 interface.
- No static routes are allowed for this task.

5. System Hardening and Availability

5.1 Control Plane Security (3 points)

- Configure R6 to drop any packets destined to closed TCP/UDP ports, but ensure that the remote users may still connect to port numbers 3001 and 5001.
- To minimize the impact of packet floods on R6's CPU, limit the aggregate rate of control-plane traffic to 20 Kpps.
- Make sure that the above policing does not affect BGP and EIGRP routing protocols.

5.2 SNMP Security (3 points)

- Configure R2 to inform **TEST-SRV-B** about issues related to environmental temperature via SNMP.
- Ensure the reliable delivery of the messages sourced from Loopback0 and encrypt it using 3DES cipher with the string of **CISCO**.
- Use the most secure authentication algorithm with the string of **CISCO**.

5.3 SSH Access (2 points)

- Configure R6 to be managed via SSH with a username of **ssh** and password of **cisco** .
- Activate version 2 of the SSH server and log a message for each failed or successful VTY session.
- Without affecting the telnet service, ensure that SSH is allowed only from 150.1.0.0/16 sources.

https://t.me/learningnets

5.4 BGP Troubleshooting (4 points)

- R6 and SW1 are configured for authenticated eBGP peering.
- Fix the configuration errors so that eBPG session can be successfully established.

5.5 Device Hardening (2 points)

- To protect R2 from known vulnerabilities and DoS attacks, secure it as follows:
  - disable proxy-arp on its VLAN 2 interface.
  - disable BOOTP and DHCP service.
  - rate-limit ICMP unreachable messages to one per second.
  - display a banner message to all authenticating lines: **Unauthorized access to this device is prohibited**.

6. **Threat Identification and Mitigation**

6.1 Preventing DoS Attacks (2 points)

- Configure R5 to limit inbound ICMP traffic on its VLAN 5 interface to 64 Kbps.
- Allow traffic bursts up to 25% of the configured limit.
- Do not use MQC syntax for this task.

6.2 Preventing CAM Attacks (2 points)

- Configure SW1 so that it allows a single MAC address to be learned on its Fa1/0/4 interface.
- Statically define the MAC address, but allow SW1 to learn new MAC addresses after 10 minutes of no traffic from the configured MAC address.
- SW1 should silently drop traffic in case of policy violation.

6.3 Preventing TCP Attacks (3 points)

- Configure ASA1 to prevent TCP attacks against ISE, received on its VLAN 43 interface:
  - limit the number of TCP open and half-open sessions to 5000 and 1000, respectively.

https://t.me/learningnets

- ensure data integrity for TCP segments.
- ensure that no data payload is carried in connection-establishment segments.
- explicitly permit TCP Echo and Echo Reply options.
- ensure that any reserved bits in TCP headers are cleared.

6.4 Mitigating WORM Attacks (3 points)

- A new worm has been detected that sends the string **root.exe** in the URL to a web server on TCP port 80 and 8080.
- Configure R5 to drop all such HTTP sessions inbound on its VLAN 5 interface.

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 1

CCIE SCv4 Lab 1 Solutions Section 1

1. Task 1.1 Solution
2. Task 1.2 Solution
3. Task 1.3 Solution
4. Task 1.4 Solution
5. Task 1.5 Solution
6. Task 1.6 Solution
7. Task 1.7 Solution
8. Task 1.8 Solution

Task 1.1 Solution

SW1:

```
interface FastEthernet1/0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 40,91
 no shutdown
```

SW2:

```
interface FastEthernet1/0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 43,73
 no shutdown
```

ASA1:

```
hostname ASA12
!
interface Ethernet0/0
 no shutdown
!
interface Ethernet0/0.43
```

https://t.me/learningnets

```
 vlan 43
 ip address 140.1.45.15 255.255.255.0
 nameif DMZ1
 security-level 60
!
interface Ethernet0/0.73
 vlan 73
 ip address 140.1.71.15 255.255.255.0
 nameif DMZ2
 security-level 50
!
interface Ethernet0/1
 no shutdown
!
interface Ethernet0/1.40
 vlan 40
 ip address 172.16.3.1 255.255.255.0
 nameif INSIDE
 security-level 100
!
interface Ethernet0/1.91
 vlan 91
 ip address 140.1.91.15 255.255.255.0
 nameif OUTSIDE
 security-level 0
 authentication key eigrp 200 ***** key-id 1
 authentication mode eigrp 200 md5
!
router eigrp 200
 no auto-summary
 network 140.1.45.0 255.255.255.0
 network 140.1.71.0 255.255.255.0
 network 140.1.91.0 255.255.255.0
```

Task 1.1 Verification

Verify that ports on switches are in trunking mode:

```
SW1#show interfaces fastEthernet1/0/13 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/13    on               802.1q         trunking      1

Port        Vlans allowed on trunk
```

https://t.me/learningnets

```
Fa1/0/13    40,91

Port        Vlans allowed and active in management domain Fa1/0/13    40,91

Port        Vlans in spanning tree forwarding state and not pruned
Fa1/0/13    40,91
!
!SW2#show interfaces fastEthernet1/0/12 trunk


Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/12    on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa1/0/12    43,73

Port        Vlans allowed and active in management domain Fa1/0/12    43,73


Port        Vlans in spanning tree forwarding state and not pruned
Fa1/0/12    43,73
```

Verify security-level, nameif, and IPv4 addressing:

https://t.me/learningnets

```
ASA12# show nameif

Interface               Name                    Security
Ethernet0/0.43          DMZ1                     60
Ethernet0/0.73          DMZ2                     50
Ethernet0/1.40          INSIDE                  100
Ethernet0/1.91          OUTSIDE                   0
!
!ASA12# show ip address

System IP Addresses:
Interface               Name                    IP address      Subnet mask     Method
Ethernet0/0.43          DMZ1                    140.1.45.15     255.255.255.0   manual
Ethernet0/0.73          DMZ2                    140.1.71.15     255.255.255.0   manual
Ethernet0/1.40          INSIDE                  172.16.3.1      255.255.255.0   manual
Ethernet0/1.91          OUTSIDE                 140.1.91.15     255.255.255.0   manual
Current IP Addresses:
Interface               Name                    IP address      Subnet mask     Method
Ethernet0/0.43          DMZ1                    140.1.45.15     255.255.255.0   manual
Ethernet0/0.73          DMZ2                    140.1.71.15     255.255.255.0   manual
Ethernet0/1.40          INSIDE                  172.16.3.1      255.255.255.0   manual
Ethernet0/1.91          OUTSIDE                 140.1.91.15     255.255.255.0   manual
```

Verify that EIGRP adjacency between ASA1 and SW1 is authenticated:

```
ASA12# show eigrp interfaces detail OUTSIDE

EIGRP-IPv4 interfaces for process 200

                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
OUTSIDE            1        0/0         1       0/1           50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 4/14
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 4  Out-of-sequence rcvd: 0
  Topology-ids on interface - 0  Authentication mode is md5,  key is "<removed> key-id 1"
!
!EIGRP-IPv4 neighbors for process 200
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   140.1.91.9              Et0/1.91          14  00:09:25 1    200   0   6
```

https://t.me/learningnets

```
!
!ASA12# show route OUTSIDE


Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
D     140.1.57.0 255.255.255.0 [90/3072] via 140.1.91.9, 0:09:40, OUTSIDE
C     140.1.91.0 255.255.255.0 is directly connected, OUTSIDE
D     172.16.6.0 255.255.255.0 [90/3072] via 140.1.91.9, 0:09:40, OUTSIDE
D     150.1.9.9 255.255.255.255 [90/130816] via 140.1.91.9, 0:09:40, OUTSIDE
```

Task 1.2 Solution

```
SW1:
interface FastEthernet1/0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 40,91
 no shutdown

SW2:
interface FastEthernet1/0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 43,73
 no shutdown
!
interface range FastEthernet1/0/13 , FastEthernet1/0/15
 switchport mode access
 no shutdown

ASA1:
interface Ethernet0/2
 no shutdown
!
failover lan unit primary
```

https://t.me/learningnets

```
failover lan interface FAILOVER Ethernet0/2
failover polltime unit msec 500 holdtime 2
failover interface-policy 2
failover interface ip FAILOVER 140.1.200.15 255.255.255.0 standby 140.1.200.16
failover
!
monitor-interface DMZ1
monitor-interface DMZ2
monitor-interface INSIDE
monitor-interface OUTSIDE
!
interface Ethernet0/0.43
 ip address 140.1.45.15 255.255.255.0 standby 140.1.45.16
!
interface Ethernet0/0.73
 ip address 140.1.71.15 255.255.255.0 standby 140.1.71.16
!
interface Ethernet0/1.40
 ip address 172.16.3.1 255.255.255.0 standby 172.16.3.2
!
interface Ethernet0/1.91
 ip address 140.1.91.15 255.255.255.0 standby 140.1.91.16
```

ASA2:

```
interface Ethernet0/2
 no shutdown
!
failover lan unit secondary
failover lan interface FAILOVER Ethernet0/2
failover polltime unit msec 500 holdtime 2
failover interface-policy 2
failover interface ip FAILOVER 140.1.200.15 255.255.255.0 standby 140.1.200.16
failover
```

Task 1.2 Verification

Verify that requested output is being matched. Stateful failover is not enabled, all interfaces are monitored but failover policy requires two interface failures; unit level hello and holdtime have been modified. Also, failover interface IPv4 addressing is irrelevant, as long as it is an unused subnet.

```
ASA12# show failover
```

https://t.me/learningnets

```
Failover On Failover unit Primary

Failover LAN Interface: FAILOVER Ethernet0/2 (up)
Unit Poll frequency 500 milliseconds, holdtime 2 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 2
Monitored Interfaces 4 of 110 maximum
Version: Ours 8.2(5), Mate 8.2(5)
Last Failover at: 16:09:56 UTC Mar 25 2014
        This host: Primary - Active
                Active time: 257 (sec)
                slot 0: ASA5510 hw/sw rev (1.1/8.2(5)) status (Up Sys)
                  Interface DMZ1 (140.1.45.15): Normal
                  Interface DMZ2 (140.1.71.15): Normal
                  Interface INSIDE (172.16.3.1): Normal
                  Interface OUTSIDE (140.1.91.15): Normal
                slot 1: empty
        Other host: Secondary - Standby Ready
                Active time: 66 (sec)
                slot 0: ASA5510 hw/sw rev (2.0/8.2(5)) status (Up Sys)
                  Interface DMZ1 (140.1.45.16): Normal
                  Interface DMZ2 (140.1.71.16): Normal
                  Interface INSIDE (172.16.3.2): Normal
                  Interface OUTSIDE (140.1.91.16): Normal
                slot 1: empty
Stateful Failover Logical Update Statistics
Link : Unconfigured.
!
!ASA12# show ip address Ethernet0/2
System IP Address:
Interface                Name                   IP address      Subnet mask     Method
Ethernet0/2              FAILOVER               140.1.200.15    255.255.255.0   unset
Current IP Address:
Interface                Name                   IP address      Subnet mask     Method
Ethernet0/2              FAILOVER               140.1.200.15    255.255.255.0   unset
!
!ASA12# show ip address Ethernet0/2

System IP Address:
Interface                Name                   IP address      Subnet mask     Method
Ethernet0/2              FAILOVER               140.1.200.15    255.255.255.0   unset
Current IP Address:
Interface                Name                   IP address      Subnet mask     Method
Ethernet0/2              FAILOVER               140.1.200.16    255.255.255.0   unset
```

https://t.me/learningnets

Task 1.3 Solution

SW1:

```
interface FastEthernet1/0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 38,63
 no shutdown
```

SW2:

```
interface FastEthernet1/0/16
 switchport mode access
 switchport access vlan 93
 no shutdown
```

ASA3:

```
hostname ASA3
!
interface GigabitEthernet0/0
 ip address 172.16.6.1 255.255.255.0
 nameif INSIDE
 security-level 100
 no shutdown
!
interface GigabitEthernet0/1
 no shutdown
!
interface GigabitEthernet0/1.38
 vlan 38
 ip address 140.1.38.17 255.255.255.0
 nameif OUTSIDE
 security-level 0
!
interface GigabitEthernet0/1.63
 vlan 63
 ip address 172.16.5.1 255.255.255.0
 nameif WLC
 security-level 40
!
router eigrp 200
 no auto-summary
 network 172.16.5.0 255.255.255.0
```

https://t.me/learningnets

```
 network 172.16.6.0 255.255.255.0
 network 140.1.38.0 255.255.255.0
 passive-interface WLC
```

Task 1.3 Verification

Verify security-level, nameif, and IPv4 addressing:

```
ASA3# show nameif
Interface                Name                    Security
GigabitEthernet0/0       INSIDE                  100
GigabitEthernet0/1.38    OUTSIDE                   0
GigabitEthernet0/1.63    WLC                      40
!
!ASA3# show ip address

System IP Addresses:
Interface                Name                    IP address      Subnet mask     Method
GigabitEthernet0/0       INSIDE                  172.16.6.1      255.255.255.0   manual
GigabitEthernet0/1.38    OUTSIDE                 140.1.38.17     255.255.255.0   manual
GigabitEthernet0/1.63    WLC                     172.16.5.1      255.255.255.0   manual
Current IP Addresses:
Interface                Name                    IP address      Subnet mask     Method
GigabitEthernet0/0       INSIDE                  172.16.6.1      255.255.255.0   manual
GigabitEthernet0/1.38    OUTSIDE                 140.1.38.17     255.255.255.0   manual
GigabitEthernet0/1.63    WLC                     172.16.5.1      255.255.255.0   manual
```

Verify that ASA3 is EIGRP neighbor with both SW1 on its VLAN 93 interface and R3 on its VLAN 38 interface:

```
ASA3# show eigrp neighbors

EIGRP-IPv4 neighbors for process 200
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   140.1.38.3              Gi0/1.38         12  00:08:06 2    200   0   5
0   172.16.6.9              Gi0/0            12  00:11:30 3    200   0   21
!
!ASA3# show route | b Gateway
Gateway of last resort is not set
 D EX 140.1.12.0 255.255.255.0 [170/51456] via 140.1.38.3, 0:10:32, OUTSIDE
D    140.1.45.0 255.255.255.0 [90/3328] via 172.16.6.9, 0:13:57, INSIDE
```

https://t.me/learningnets

```
C    140.1.38.0 255.255.255.0 is directly connected, OUTSIDE
D    140.1.57.0 255.255.255.0 [90/3072] via 172.16.6.9, 0:13:57, INSIDE
D    140.1.71.0 255.255.255.0 [90/3328] via 172.16.6.9, 0:13:57, INSIDE
D    140.1.91.0 255.255.255.0 [90/3072] via 172.16.6.9, 0:13:57, INSIDE
C    172.16.5.0 255.255.255.0 is directly connected, WLC
C    172.16.6.0 255.255.255.0 is directly connected, INSIDE
D EX 150.1.4.4 255.255.255.255 [170/51456] via 140.1.38.3, 0:10:22, OUTSIDE
D EX 150.1.1.1 255.255.255.255 [170/51456] via 140.1.38.3, 0:10:32, OUTSIDE
D EX 150.1.3.3 255.255.255.255 [170/51456] via 140.1.38.3, 0:10:33, OUTSIDE
D    150.1.9.9 255.255.255.255 [90/130816] via 172.16.6.9, 0:13:57, INSIDE
```

Verify that VLAN 63 interface is EIGRP passive; it's not displayed as EIGRP interface:

```
ASA3# show eigrp interfaces

EIGRP-IPv4 interfaces for process 200

                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
INSIDE             1        0/0         3       0/1           50           0
OUTSIDE            1        0/0         2       0/1           50           0
```

Task 1.4 Solution

```
SW1:
interface FastEthernet1/0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 72,73
 no shutdown

SW2:

interface FastEthernet1/0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 71,74
 no shutdown


ASA4:
firewall transparent
```

https://t.me/learningnets

```
!
hostname ASA4
!
interface GigabitEthernet0/0
 no shutdown
!
interface GigabitEthernet0/0.71
 vlan 71
 nameif DMZ1
 security-level 30
 bridge-group 77
!
interface GigabitEthernet0/0.74
 vlan 74
 nameif INSIDE
 security-level 100
 bridge-group 77
!
interface GigabitEthernet0/1
 no shutdown
!
interface GigabitEthernet0/1.72
 vlan 72
 nameif OUTSIDE
 security-level 0
 bridge-group 77
!
interface GigabitEthernet0/1.73
 vlan 73
 nameif DMZ2
 security-level 80
 bridge-group 77
!
interface Bvi77
 ip address 140.1.71.18 255.255.255.0
 ipv6 enable
!
access-list GLOBAL_ACL permit eigrp any any
access-group GLOBAL_ACL global
```

Task 1.4 Verification

Verify firewall mode and bridge-group configuration:

https://t.me/learningnets

```
ASA4# show firewall
 Firewall mode: Transparent

!
!ASA4# show bridge-group

Static mac-address entries:  0 (in use), 65535 (max)
Dynamic mac-address entries: 4 (in use), 65535 (max)
 Bridge Group: 77
  Interfaces:  GigabitEthernet0/0.71
GigabitEthernet0/0.74
GigabitEthernet0/1.72
GigabitEthernet0/1.73



  Management System IP Address:  140.1.71.18 255.255.255.0
  Management Current IP Address: 140.1.71.18 255.255.255.0
  Management IPv6 Global Unicast Address(es):
     N/A
  Static mac-address entries:  0
  Dynamic mac-address entries: 4
```

Verify that link-local IPv6 addressing has been configured:

```
ASA4# show ipv6 interface brief | e Gi|Ma|unas
DMZ1 [up/up] fe80::a693:4cff:feaa:f78a
INSIDE [up/up] fe80::a693:4cff:feaa:f78a
OUTSIDE [up/up] fe80::a693:4cff:feaa:f787
DMZ2 [up/up] fe80::a693:4cff:feaa:f787

BVI77 [up/up]
```

Verify that EIGRP is functional between ASA1, R2, and SW2:

```
ASA12# show eigrp neighbors DMZ2

EIGRP-IPv4 neighbors for process 200
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
2   140.1.71.2              Et0/0.73         12  00:24:07 1    200  0   6
1   140.1.71.10             Et0/0.73         14  00:25:44 4    200  0   11
```

https://t.me/learningnets

Verify the connection table on ASA4 for EIGRP traffic, based on the timing the command is issued; IPv6 session may be visible, initiated by **TEST-PC-B**, which confirms that ASA does not drop IPv6 packets:

```
ASA4# show conn

10 in use, 21 most used EIGRP OUTSIDE 140.1.71.2 DMZ2 224.0.0.10, idle 0:00:03, bytes 13534
EIGRP DMZ2 224.0.0.10 INSIDE 140.1.71.10, idle 0:00:01, bytes 14638
EIGRP OUTSIDE 224.0.0.10 DMZ2 140.1.71.15, idle 0:00:00, bytes 13680
EIGRP OUTSIDE 224.0.0.10 INSIDE 140.1.71.10, idle 0:00:01, bytes 14638
UDP OUTSIDE ff02::1:2:547 DMZ1 fe80::642f:86ea:6ae8:931f:546, idle 0:00:54, bytes 623, flags -

EIGRP OUTSIDE 140.1.71.2 INSIDE 224.0.0.10, idle 0:00:03, bytes 13534
EIGRP DMZ2 140.1.71.15 INSIDE 224.0.0.10, idle 0:00:00, bytes 13680
EIGRP OUTSIDE 140.1.71.2 DMZ1 224.0.0.10, idle 0:00:03, bytes 13534
EIGRP DMZ1 224.0.0.10 DMZ2 140.1.71.15, idle 0:00:00, bytes 13680
EIGRP DMZ1 224.0.0.10 INSIDE 140.1.71.10, idle 0:00:01, bytes 14638
```

Task 1.5 Solution

```
R3:

ip inspect name CBAC_VLAN93 tcp
ip inspect name CBAC_VLAN93 udp
ip inspect name CBAC_VLAN93 icmp
!
ip access-list extended VLAN93_INBOUND
 permit eigrp any any
!
interface FastEthernet0/0.93
 ip inspect CBAC_VLAN93 out
 ip access-group VLAN93_INBOUND in
```

Task 1.5 Verification

Verify CBAC configuration and that it is being applied in the requested direction:

```
R3#show ip inspect interfaces

Interface Configuration Interface FastEthernet0/0.93
  Inbound inspection rule is not set Outgoing inspection rule is CBAC_VLAN93
```

https://t.me/learningnets

```
tcp alert is on audit-trail is off timeout 3600
 udp alert is on audit-trail is off timeout 30
 icmp alert is on audit-trail is off timeout 10
 Inbound access list is VLAN93_INBOUND

  Outgoing access list is not set
```

Verify that all interfaces grouped in the bridge-group are in STP forwarding state:

```
R3#show bridge 39 group


Bridge Group 39 is running the IEEE compatible Spanning Tree protocol

   Port 6 (FastEthernet0/0.3 DOT1Q) of bridge group 39 is forwarding
   Port 7 (FastEthernet0/0.39 DOT1Q) of bridge group 39 is forwarding
   Port 8 (FastEthernet0/0.93 DOT1Q) of bridge group 39 is forwarding
```

Generate traffic through the firewall and verify the session table:

```
SW1#ping 172.16.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.6.1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
!
!R3#show ip inspect sessions detail

Established Sessions Session 4A00A110 (172.16.6.9:8)=>(172.16.6.1:0) icmp SIS_OPEN
  Created 00:00:03, Last heard 00:00:03
   ECHO request
  Bytes sent (initiator:responder) [360:360]
In  SID 172.16.6.1[0:0]=>172.16.6.9[0:0] on ACL VLAN93_INBOUND  (5 matches)

  In  SID 0.0.0.0[0:0]=>172.16.6.9[3:3] on ACL VLAN93_INBOUND
  In  SID 0.0.0.0[0:0]=>172.16.6.9[11:11] on ACL VLAN93_INBOUND
```

Verify that inbound traffic received on the untrusted interface is dropped:

```
ASA3# ping 172.16.6.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.6.9, timeout is 2 seconds:?????
```

https://t.me/learningnets

```
Success rate is 0 percent (0/5)
```

Task 1.6 Solution

```
R3:

ip inspect name CBAC_BVI38 tcp router-traffic
ip inspect name CBAC_BVI38 udp router-traffic
ip inspect name CBAC_BVI38 icmp audit-trail on router-traffic timeout 30
!
ip access-list extended BVI83_INBOUND
 permit ospf any any
 permit eigrp any any
 deny ip host 150.1.1.1 any
 deny ip 140.1.12.0 0.0.0.255 any
 deny ip host 140.1.38.1 any
 permit ip any any
!
interface BVI38
 ip inspect CBAC_BVI38 out
 ip access-group BVI83_INBOUND in
```

Task 1.6 Verification

Verify CBAC configuration and that it is being applied in the outbound direction to also match on router-originated traffic:

```
R3#show ip inspect interfaces

Interface Configuration
 Interface FastEthernet0/0.93
  Inbound inspection rule is not set
  Outgoing inspection rule is CBAC_VLAN93
    tcp alert is on audit-trail is off timeout 3600
    udp alert is on audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
  Inbound access list is VLAN93_INBOUND
  Outgoing access list is not set Interface BVI38
  Inbound inspection rule is not set Outgoing inspection rule is CBAC_BVI38
    tcp alert is on audit-trail is off timeout 3600
 inspection of router local traffic is enabled
    udp alert is on audit-trail is off timeout 30
 inspection of router local traffic is enabled
```

https://t.me/learningnets

```
icmp alert is on audit-trail is on timeout 30
 inspection of router local traffic is enabled
  Inbound access list is BVI83_INBOUND

  Outgoing access list is not set
```

Verify that all interfaces grouped in the bridge-group are in STP forwarding state:

```
R3#show spanning-tree summary

Root bridge for: none.
PortFast BPDU Guard is disabled
UplinkFast is disabled
BackboneFast is disabled

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
Bridge group 38      0        0         0        3          3

Bridge group 39      0        0         0        3          3
-------------------- -------- --------- -------- ---------- ----------
     2 Bridge Groups 0        0         0        6          6
```

Generate both transit and router-originated traffic, and verify the session table:

```
ASA3# ping 150.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
!
!R3#ping 150.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!R3#show ip inspect sessions

Established Sessions Session 4A091370 (140.1.38.3:8)=>(150.1.1.1:0) icmp SIS_OPEN
Half-open Sessions Session 4A0919D0 (140.1.38.17:8)=>(150.1.1.1:0) icmp SIS_OPENING
```

The following log messages should appear on the R3 console for start/stop of the

https://t.me/learningnets

ICMP sessions:

```
%FW-6-SESS_AUDIT_TRAIL_START: Start icmp session: initiator (140.1.38.17:8) -- responder (150.1.1.1:0)
%FW-6-SESS_AUDIT_TRAIL_START: Start icmp session: initiator (140.1.38.3:8) -- responder (150.1.1.1:0)
!
!
%FW-6-SESS_AUDIT_TRAIL: Stop icmp session: initiator (140.1.38.17:8) sent 360 bytes -- responder (150.1.1.1:0) sent
%FW-6-SESS_AUDIT_TRAIL: Stop icmp session: initiator (140.1.38.3:8) sent 360 bytes -- responder (150.1.1.1:0) sent 3
```

Verify that inbound traffic received on untrusted interfaces is dropped:

```
R1#ping 150.1.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.4.4, timeout is 2 seconds:U.U.U
Success rate is 0 percent (0/5)
!
!R1#ping 150.1.4.4 source loopback0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.4.4, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1 U.U.U
Success rate is 0 percent (0/5)
!
!R1#ping 150.1.4.4 source gigabitEthernet0/0.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.4.4, timeout is 2 seconds:
Packet sent with a source address of 140.1.12.1 U.U.U

Success rate is 0 percent (0/5)
```

Task 1.7 Solution

```
R3:
ip access-list extended VLAN93_INBOUND
 permit icmp host 140.1.38.3 any time-exceeded
 permit icmp host 172.16.6.1 any time-exceeded
 permit icmp host 140.1.38.1 any port-unreachable
!
ip access-list extended BVI83_INBOUND
 41 permit icmp host 140.1.38.1 any port-unreachable

ASA3:
```

https://t.me/learningnets

```
access-list OUTSIDE_IN extended permit icmp host 140.1.38.3 any time-exceeded
access-list OUTSIDE_IN extended permit icmp host 140.1.38.1 any unreachable
!
access-group OUTSIDE_IN in interface OUTSIDE
!
!
access-list DECREMENT_TTL extended permit udp host 172.16.6.9 host 150.1.1.1
!
class-map DECREMENT_TTL
 match access-list DECREMENT_TTL
!
policy-map global_policy
 class DECREMENT_TTL
  set connection decrement-ttl
```

Task 1.7 Verification

Verify that both traceroutes are functional and requested output is being matched:

```
ASA12# traceroute 150.1.1.1

Type escape sequence to abort.
Tracing the route to 150.1.1.1

 1  140.1.91.9 0 msec 0 msec 0 msec
 2  140.1.38.3 10 msec 0 msec 0 msec
 3  140.1.38.1 10 msec *  0 msec
!
!SW1#traceroute 150.1.1.1


Type escape sequence to abort.
Tracing the route to 150.1.1.1

  1 172.16.6.1 8 msec *  0 msec
  2 140.1.38.3 0 msec 9 msec 0 msec
  3 140.1.38.1 8 msec *  0 msec
```

Verify the TTL decrement configuration on the ASA:

```
ASA3# show service-policy set connection


Global policy:
```

https://t.me/learningnets

```
  Service-policy: global_policy
    Class-map: DECREMENT_TTL
      Set connection policy:         drop 0 Set connection decrement-ttl
```

Verify that only traffic from SW1 matches on the class-map with TTL decrement configuration:

```
ASA3# show service-policy flow udp host 172.16.6.9 host 150.1.1.1

Global policy:
  Service-policy: global_policy Class-map: DECREMENT_TTL
 Match: access-list DECREMENT_TTL
 Access rule: permit udp host 172.16.6.9 host 150.1.1.1
      Action: Input flow:  set connection decrement-ttl
    Class-map: class-default
      Match: any
      Action:
       Output flow:
!
!ASA3# show service-policy flow udp host 140.1.91.15 host 150.1.1.1


Global policy:
  Service-policy: global_policy
    Class-map: class-default
      Match: any
      Action:
        Output flow:
```

Task 1.8 Solution

```
ASA3:
object network R4_L0_REAL
 host 150.1.4.4
object network R4_L0_MAPPED
 host 172.16.6.4
!
!
nat (OUTSIDE,INSIDE) source static R4_L0_REAL R4_L0_MAPPED unidirectional
!
object network R1_L0_REAL
 host 150.1.1.1
```

https://t.me/learningnets

```
 nat (OUTSIDE,INSIDE) dynamic interface
!
!
access-list OUTSIDE_IN permit tcp host 150.1.4.4 host 150.1.9.9
access-list OUTSIDE_IN permit icmp host 150.1.4.4 host 150.1.9.9 echo
access-list OUTSIDE_IN permit tcp host 150.1.1.1 host 150.1.9.9
access-list OUTSIDE_IN permit icmp host 150.1.1.1 host 150.1.9.9 echo
!
!
policy-map global_policy
 class inspection_default
 inspect icmp
```

R3:

```
ip access-list extended VLAN93_INBOUND
 permit tcp host 172.16.6.4 host 150.1.9.9 eq 23
 permit icmp host 172.16.6.4 host 150.1.9.9 echo
 permit tcp host 172.16.6.1 host 150.1.9.9 eq 23
 permit icmp host 172.16.6.1 host 150.1.9.9 echo
!
!
ip access-list extended BVI83_INBOUND
 21 permit tcp host 150.1.1.1 host 150.1.9.9 eq 23
 22 permit icmp host 150.1.1.1 host 150.1.9.9 echo
```

Task 1.8 Verification

Verify that telnet and ping is functional from R1's Loopback0 to SW1's Loopback0:

```
R1#ping 150.1.9.9 source loopback0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.9.9, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1 !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
!
!R1#telnet 150.1.9.9 /source-interface loopback0
Trying 150.1.9.9 ... Open
SW1>
!
!ASA3# show xlate

2 in use, 3 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
TCP PAT from OUTSIDE:150.1.1.1/56853 to INSIDE:172.16.6.1/3842 flags ri idle 0:00:33 timeout 0:00:30
```

https://t.me/learningnets

```
!
!
ASA3# show conn long
5 in use, 37 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service moduleTCP OUTSIDE:150.1.1.1/56853 (172.16.6.1/3842)
 INSIDE:150.1.9.9/23 (150.1.9.9/23), flags UIOB, idle 46s, uptime 47s, timeout 1h0m, bytes 51
```

Verify that telnet and ping are functional from R4's Loopback0 to SW1's Loopback0:

https://t.me/learningnets

```
R4#ping 150.1.9.9 source loopback0


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.9.9, timeout is 2 seconds:
Packet sent with a source address of 150.1.4.4 !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!
!R4#telnet 150.1.9.9 /source-interface loopback0

Trying 150.1.9.9 ... Open
SW1>

!
!ASA3# show conn long

5 in use, 37 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service moduleTCP OUTSIDE:150.1.4.4/32834 (172.16.6.4/32834)
 INSIDE:150.1.9.9/23 (150.1.9.9/23), flags UIOB, idle 16s, uptime 16s, timeout 1h0m, bytes 60
```

Verify NAT configuration and that, because of static unidirectional configuration, sessions cannot be initiated from **INSIDE** to 172.16.6.4:

```
ASA3# show nat detail

Manual NAT Policies (Section 1)1 (OUTSIDE) to (INSIDE) source static R4_L0_REAL R4_L0_MAPPED
unidirectional
    translate_hits = 29, untranslate_hits = 0Source - Origin: 150.1.4.4/32, Translated: 172.16.6.4/32

Auto NAT Policies (Section 2)
1 (OUTSIDE) to (INSIDE) source dynamic R1_L0_REAL interface
    translate_hits = 4, untranslate_hits = 2
```

https://t.me/learningnets

```
Source - Origin: 150.1.1.1/32, Translated: 172.16.6.1/24


!
!SW1#ping 172.16.6.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.6.4, timeout is 2 seconds:.....

Success rate is 0 percent (0/5)
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 1

CCIE SCv4 Lab 1 Solutions Section 2

1. Task 2.1 Solution
2. Task 2.2 Solution
3. Task 2.3 Solution
4. Task 2.4 Solution
5. Task 2.5 Solution
6. Task 2.6 Solution

Task 2.1 Solution

SW3:

```
interface GigabitEthernet1/0/10
 switchport mode access
 switchport access vlan 57
 no shutdown
```

IPS:

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# host-name IPS
sensor(config-hos-net)# host-ip 140.1.57.100/24,140.1.57.9
sensor(config-hos-net)# telnet-option enabled
sensor(config-hos-net)# login-banner-text This is IPS from CCIE Lab Exam
sensor(config-hos-net)# access-list 140.1.71.0/24
sensor(config-hos-net)# access-list 140.1.57.9/32
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes?[yes]:
```

```
ASA4:
access-list GLOBAL_ACL extended permit tcp 140.1.71.0 255.255.255.0 host 140.1.57.100 eq 23
```

https://t.me/learningnets

```
access-list GLOBAL_ACL extended permit tcp 140.1.71.0 255.255.255.0 host 140.1.57.100 eq 80
```

Task 2.1 Verification

Verify IPS settings:

https://t.me/learningnets

```
sensor(config-hos-net)# show settings

    network-settings
    ------------------------------------------------
 host-ip: 140.1.57.100/24,140.1.57.9 default: 192.168.1.2/24,192.168.1.1
 host-name: IPS default: sensor
 telnet-option: enabled default: disabled

        access-list (min: 0, max: 512, current: 2)
        ------------------------------------------------ network-address: 140.1.57.9/32

            ------------------------------------------------ network-address: 140.1.71.0/24

            ------------------------------------------------
        ------------------------------------------------
        ftp-timeout: 300 seconds <defaulted> login-banner-text: This is IPS from CCIE Lab Exam default:

        dns-primary-server
        ------------------------------------------------
            disabled
            ------------------------------------------------
            ------------------------------------------------
        ------------------------------------------------
        dns-secondary-server
        ------------------------------------------------
            disabled
            ------------------------------------------------
            ------------------------------------------------
        ------------------------------------------------
        dns-tertiary-server
        ------------------------------------------------
            disabled
            ------------------------------------------------
            ------------------------------------------------
        ------------------------------------------------
        http-proxy
        ------------------------------------------------
            no-proxy
            ------------------------------------------------
            ------------------------------------------------
        ------------------------------------------------
    ------------------------------------------------
```

https://t.me/learningnets

Verify that ping and telnet from default gateway are allowed:

```
SW1#ping 140.1.57.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 140.1.57.100, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
!
!SW1#telnet 140.1.57.100
Trying 140.1.57.100 ... Open
This is IPS from CCIE Lab Exam
login: cisco
Password:
Last login: Wed Mar 26 04:45:10 on ttyS0
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on this IPS platform.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.IPS#
```

Task 2.2 Solution

```
SW3:
interface GigabitEthernet1/0/8
 switchport mode access
 switchport access vlan 45
```

https://t.me/learningnets

```
 no shutdown
```

SW4:

```
interface GigabitEthernet1/0/9
 switchport mode access
 switchport access vlan 43
 no shutdown
```

IPS:

```
sensor(config)# service interface
sensor(config-int)# physical-interfaces gigabitEthernet0/0
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# exit
sensor(config-int)# physical-interfaces gigabitEthernet0/2
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# exit
sensor(config-int)# inline-interfaces VLAN43-VLAN45
sensor(config-int-inl)# interface1 gigabitEthernet0/0
sensor(config-int-inl)# interface2 gigabitEthernet0/2
sensor(config-int-inl)# exit
sensor(config-int)# exit
Apply Changes?[yes]:
!
!
sensor(config)# service analysis-engine
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)# logical-interface VLAN43-VLAN45
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
Apply Changes?[yes]:
```

Task 2.2 Verification

Verify the physical and logical state of interfaces on the IPS:

```
sensor# show interfaces brief

CC   Interface            Sensing State   Link   Inline Mode                              Pair Status
GigabitEthernet0/0   Enabled         Up     Paired with interface GigabitEthernet0/2   Up

*    Management0/0        Disabled        Up
     GigabitEthernet0/1   Disabled        Down   Unpaired                                 N/A
GigabitEthernet0/2   Enabled         Up     Paired with interface GigabitEthernet0/0   Up
```

https://t.me/learningnets

```
     GigabitEthernet0/3   Disabled        Down   Unpaired                                  N/A
!
!sensor(config-int-inl)# show settings
 name: VLAN43-VLAN45
   -----------------------------------------------
      description:  <defaulted> interface1: GigabitEthernet0/0
interface2: GigabitEthernet0/2

      subinterface-type
      ------------------------------------------------
         none
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
```

Verify that SW3 and ASA1 are now EIGRP neighbors:

```
SW3#show ip eigrp neighbors vlan 45
EIGRP-IPv4 Neighbors for AS(200)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   140.1.45.15             Vl45                     14 00:11:20   32   192  0  129
!
!SW3#ping 140.1.45.15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 140.1.45.15, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
```

Verify that traffic flows through the IPS; note the EIGRP hello packets:

```
sensor# packet display gigabitEthernet0/0
Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_0, link-type EN10MB (Ethernet), capture size 65535 bytes
05:55:11.355000 CDPv2, ttl: 180s, Device-ID 'SW3', length 444
05:55:11.488000 STP 802.1d, Config, Flags [none], bridge-id 802b.70:81:05:39:fe:80.8009, length 43
05:55:12.460000
05:55:13.491000 STP 802.1d, Config, Flags [none], bridge-id 802b.70:81:05:39:fe:80.8009, length 43
05:55:14.567000 IP 140.1.45.15 > 224.0.0.10: EIGRP Hello, length: 40
05:55:14.996000 IP 140.1.45.11 > 224.0.0.10: EIGRP Hello, length: 40

05:55:15.497000 STP 802.1d, Config, Flags [none], bridge-id 802b.70:81:05:39:fe:80.8009, length 43
```

https://t.me/learningnets

```
05:55:17.502000 STP 802.1d, Config, Flags [none], bridge-id 802b.70:81:05:39:fe:80.8009, length 43
```

Verify that the analysis-engine inspects packets between these VLANs:

```
sensor# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 175719
   Processing Load Percentage
         Thread    5 sec   1 min   5 min
         0         1       1       1
         Average   1       1       1

   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 0
   Receiver Statistics Total number of packets processed since reset = 811
Total number of IP packets processed since reset = 317

   Transmitter Statistics
      Total number of packets transmitted = 1348
      Total number of packets denied = 0
      Total number of packets reset = 0
```

Task 2.3 Solution

IPS:

```
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 60001 0
sensor(config-sig-sig)# engine atomic-ip
sensor(config-sig-sig-ato)# specify-l4-protocol yes
sensor(config-sig-sig-ato-yes)# l4-protocol other-protocol
sensor(config-sig-sig-ato-yes-oth)# other-ip-protocol-id 88
sensor(config-sig-sig-ato-yes-oth)# exit
sensor(config-sig-sig-ato-yes)# exit
sensor(config-sig-sig-ato)# event-action produce-verbose-alert
sensor(config-sig-sig-ato)# exit
sensor(config-sig-sig)# alert-severity medium
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# enabled true
sensor(config-sig-sig-sta)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
```

https://t.me/learningnets

```
Apply Changes?[yes]:
```

Task 2.3 Verification

Verify that EIGRP packets trigger an event with produce-verbose-alert and a severity of medium:

```
sensor# show events

 evIdsAlert: eventId=1395295337431000801 severity=medium
  vendor=Cisco alarmTraits=32768
   originator:
     hostId: IPS
     appName: sensorApp
     appInstanceId: 1202
   time: 2014/03/26 06:17:36 2014/03/26 06:17:36 UTC signature: description=My Sig id=60001
  created=20000101 type=other version=custom
     subsigId: 0
     sigDetails: My Sig Info
   interfaceGroup: vs0
   vlan: 0
   participants:
     attacker:  addr: locality=OUT 140.1.45.11
     target:  addr: locality=OUT 224.0.0.10
       os: idSource=unknown relevance=relevant type=unknown
   triggerPacket:
000000  01 00 5E 00 00 0A 44 D3  CA 63 99 C1 08 00 45 C0  ..^...D..c....E.
000010  00 3C 00 00 00 00 02 58  1E 94 8C 01 2D 0B E0 00  .<.....X....-...
000020  00 0A 02 05 F1 0A 00 00  00 00 00 00 00 00 00 00  ................
000030  00 00 00 00 00 C8 00 01  00 0C 01 00 01 00 00 00  ................
000040  00 0F 00 04 00 08 07 00  03 00                    ..........
   riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 66
   threatRatingValue: 66
   interface: ge0_0 protocol: IP protocol 88
```

Task 2.4 Solution

```
SW6:
interface FastEthernet1/0/10
 switchport mode access
 switchport access vlan 3
```

https://t.me/learningnets

```
 no shutdown

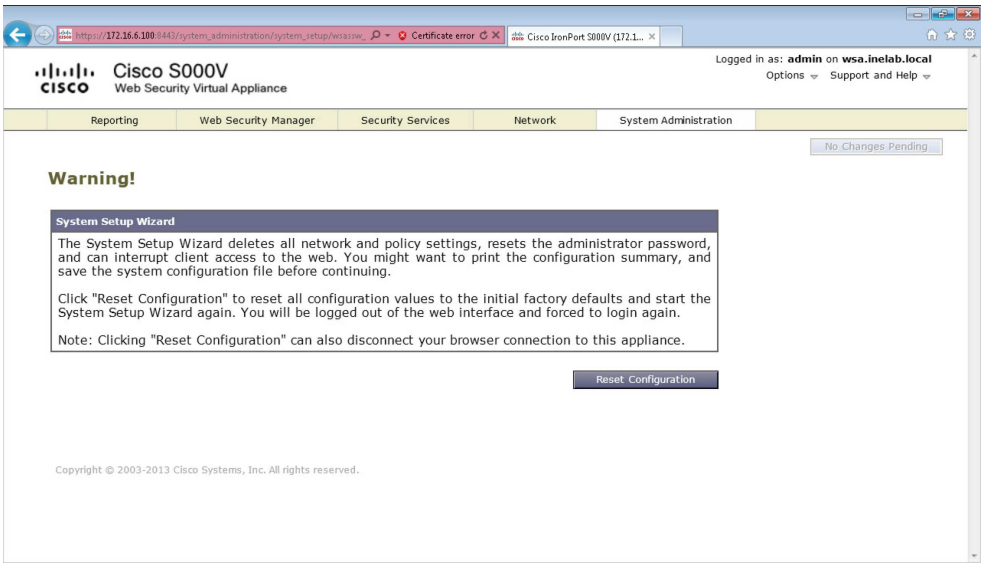
R3:
ip access-list extended VLAN93_INBOUND
 permit tcp host 172.16.6.100 eq 8443 host 140.1.71.100

ASA4:
access-list GLOBAL_ACL extended permit tcp host 140.1.71.100 host 172.16.6.100 eq 8443

ASA3:

same-security-traffic permit intra-interface
!
access-list WSA_MANAGEMENT extended permit tcp host 172.16.6.100 eq 8443 host 140.1.71.100
!
class-map WSA_MANAGEMENT
 match access-list WSA_MANAGEMENT
!
policy-map global_policy
 class WSA_MANAGEMENT
  set connection advanced-options tcp-state-bypass
```

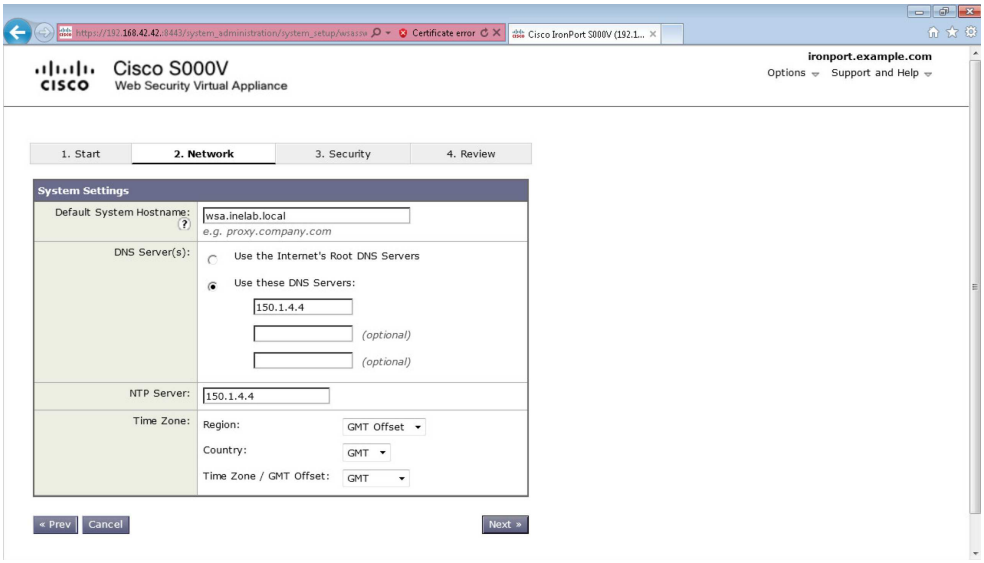
Using Internet Explorer from **TEST-PC-B**, navigate to **https://172.16.6.100:8443 **, authenticate and browse to **System Administration -> System Setup Wizard**, and click **Reset Configuration**:



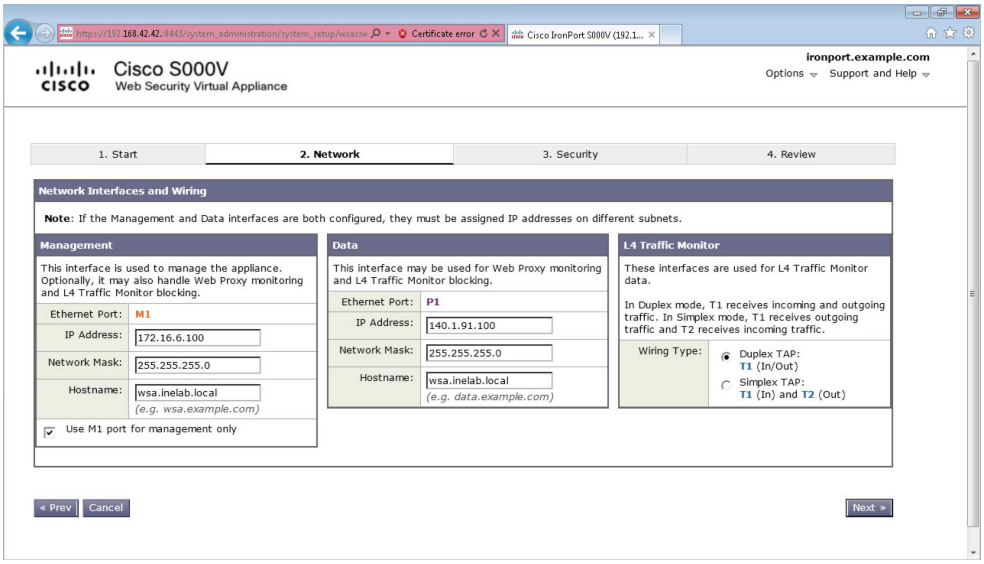
Configure **TEST-PC-B** with IPv4 address from subnet 192.168.42.0/24 , allocate its switchport in the same VLAN as WSA, and using Internet Explorer navigate to **https://192.168.42.42:8443**. Authenticate with the default credentials of **admin/ironport**

https://t.me/learningnets

and browse to **System Administration -> System Setup Wizard**. Configure hostname, DNS, and NTP server:

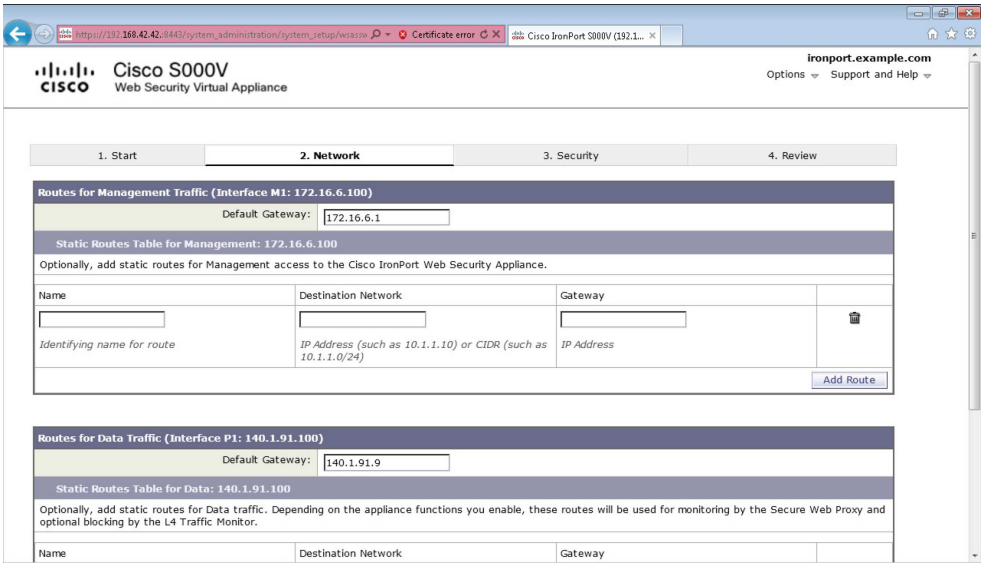


Configure M1 for management traffic only, and the P1 port for proxy (based on the following task information):

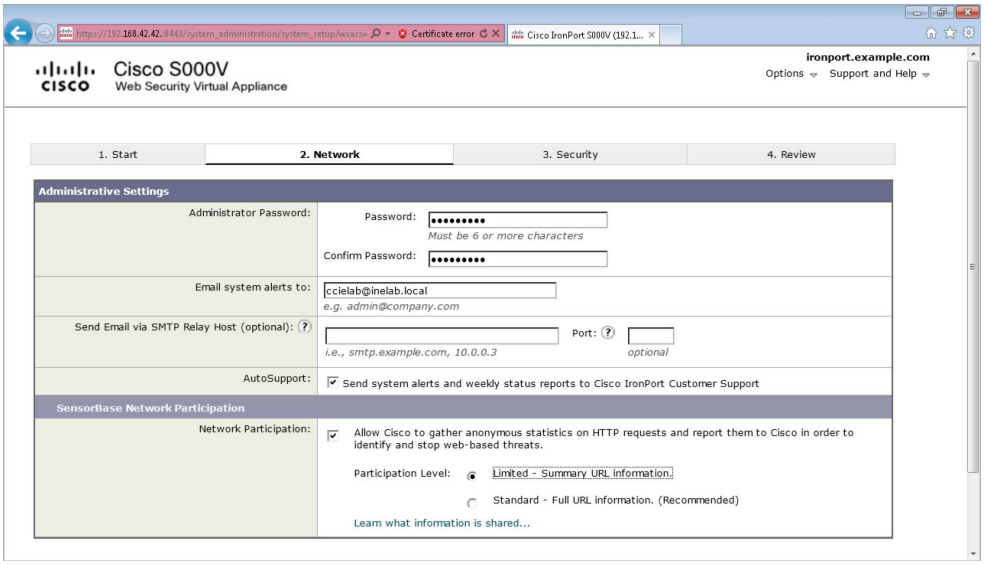


Configure default gateways for both M1 and P1 ports:

https://t.me/learningnets



Configure the administrator password, e-mail address, and SensorBase participation:



All other settings are left at their default values, so screens are missing from the complete **System Setup Wizard**. Install the configuration and put **TEST-PC-B** back in VLAN 71.

Task 2.4 Verification

Use Internet Explorer to manage the WSA. When the sessions is successful, note on the ASA that the session is in **TCP state-bypass** because of the **b** flag:

```
ASA3# show conn long address 172.16.6.100

38 in use, 87 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
```

https://t.me/learningnets

```
        B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
        D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
        G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
        i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
        k - Skinny media, M - SMTP data, m - SIP media, n - GUP
        O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
        q - SQL*Net data, R - outside acknowledged FIN,
        R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
        s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
        V - VPN orphan, W - WAAS,
        X - inspected by service module
TCP INSIDE:140.1.71.100/1347 (140.1.71.100/1347) INSIDE:172.16.6.100/8443 (172.16.6.100/8443),flags b
, idle 8m9s, uptime 8m9s, timeout 1h0m, bytes 1772
```

Task 2.5 Solution

SW1:

```
sdm prefer routing
!
reload
```

SW1:

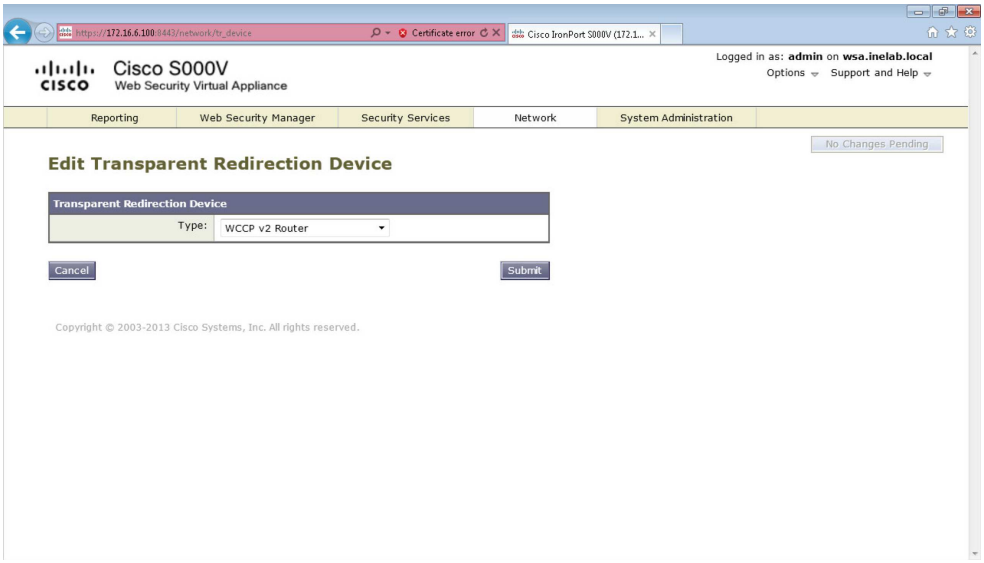
```
ip access-list extended REDIRECTED_TRAFFIC
 deny tcp host 140.1.91.100 any eq www
 deny tcp any host 140.1.91.100 eq www
 permit tcp any any eq 80
!
ip wccp 91 redirect-list REDIRECTED_TRAFFIC password wsapass
!
interface Vlan91
 ip wccp 91 redirect in
```

SW6:

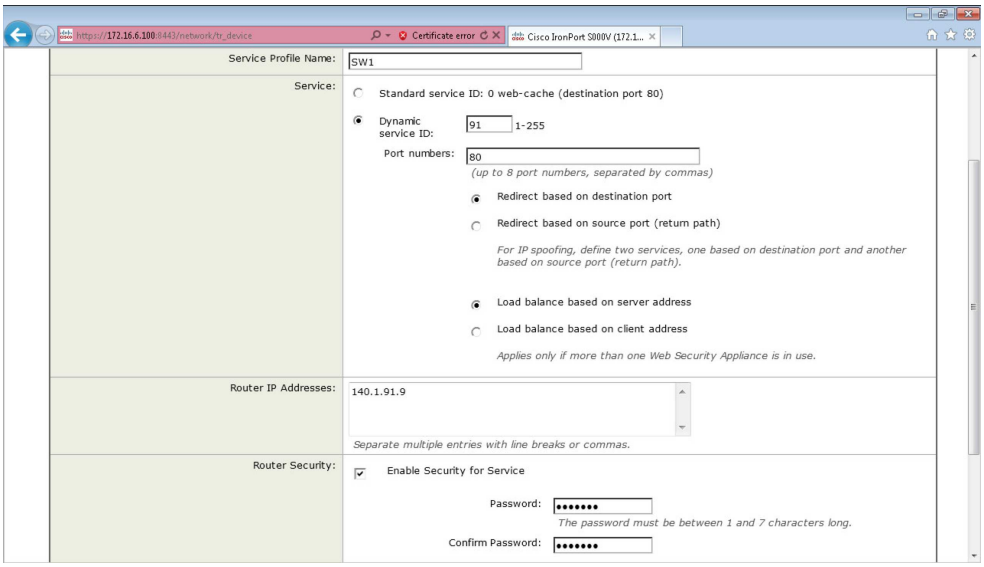
```
interface FastEthernet1/0/11
 switchport mode access
 switchport access vlan 91
 no shutdown
```

https://t.me/learningnets

Using Internet Explorer from **TEST-PC-B**, navigate to **https://172.16.6.100:8443**, authenticate and browse to **Network -> Transparent Redirection**, and select **WCCP v2 Router**:



Click **Add Service**, configure the same service-id as on the switch, enable it only for HTTP traffic, and specify the same password as on the switch (authentication string was randomly selected):



Commit changes on WSA; the following message should be logged on SW1, confirming that the WCCP client (WSA) registered with the WCCP server (SW1):

```
%WCCP-5-SERVICEFOUND: Service 91 acquired on WCCP Client 140.1.91.100
```

https://t.me/learningnets

Task 2.5 Verification

Verify that TCAM memory is allocated for WCCP, based on the configured SDM template:

```
SW1#show sdm prefer

 The current template is "desktop routing" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  3K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    11K
    number of directly-connected IPv4 hosts:        3K
    number of indirect IPv4 routes:                 8K
number of IPv4 policy based routing aces:          0.5K

  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
```

Verify WCCP configuration and that it is functional as the WCCP server selected the router identifier:

```
SW1#show ip wccp

Global WCCP information:
    Router information: Router Identifier:                   150.1.9.9
 Protocol Version:                    2.0

    Service Identifier: 91 Number of Service Group Clients:     1
 Number of Service Group Routers:     1
        Total Packets s/w Redirected:        0
          Process:                           0
          CEF:                               0 Redirect access-list:                 REDIRECTED_TRAFFIC
        Total Packets Denied Redirect:       0
        Total Packets Unassigned:            0
        Group access-list:                   -none-
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
!
```

https://t.me/learningnets

```
!SW1#show ip wccp interfaces

WCCP interface configuration: Vlan91
        Output services: 0 Input services:  1

        Mcast services:  0
        Exclude In:      FALSE
```

Verify that the requested output is being matched:

```
SW1#show ip wccp 91 detail

WCCP Client information: WCCP Client ID:          140.1.91.100
        Protocol Version:        2.0 State:                  Usable
Redirection:              L2
Packet Return:            L2

        Packets Redirected:    0
        Connect Time:          00:05:46
        Assignment:            MASK
```

Task 2.6 Solution

Configure the WSA to cache as much content as possible; this is available only from CLI:

```
wsa.inelab.local> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters - CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters[]> CACHING

Enter values for the caching options:

The following predefined choices exist for configuring advanced caching
```

https://t.me/learningnets

```
options:
1. Safe Mode
2. Optimized Mode3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:[2]> 3

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]>
wsa.inelab.local> commit

Warning: In order to process these changes, the
proxy process will restart after Commit. This will cause
a brief interruption in service. Additionally, the
authentication cache will be cleared, which might require
some users to authenticate again.

Please enter some comments describing your changes:
[]>
Changes committed: Thu Mar 27 04:06:59 2014 GMT
```

Enable the **User Acknowledgement Page** and modify the default inactivity/idle timeout, and leave all other settings at defaults; this can be done from both GUI and CLI:

```
wsa.inelab.local> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
```

https://t.me/learningnets

```
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters[]> EUN

Enter values for the EUN options:

Currently using: Standard EUN pages

Choose:1. Refresh EUN pages
2. Use Custom EUN pages
3. Use Standard EUN pages[3]> 1

Would you like to turn on presentation of the User Acknowledgement page?[N]> Y

Enter the method to be used for tracking User Acknowledgements ("ip" or
"session").
[ip]>

Enter maximum time to remember User Acknowledgement (in seconds).
[86400]>

Enter maximum idle timeout for User Acknowledgement based on IP Address (in
seconds).[14400]> 7200

Would you like to enable decryption in order to display End User
Acknowledgement for HTTPS transaction:
[Y]>

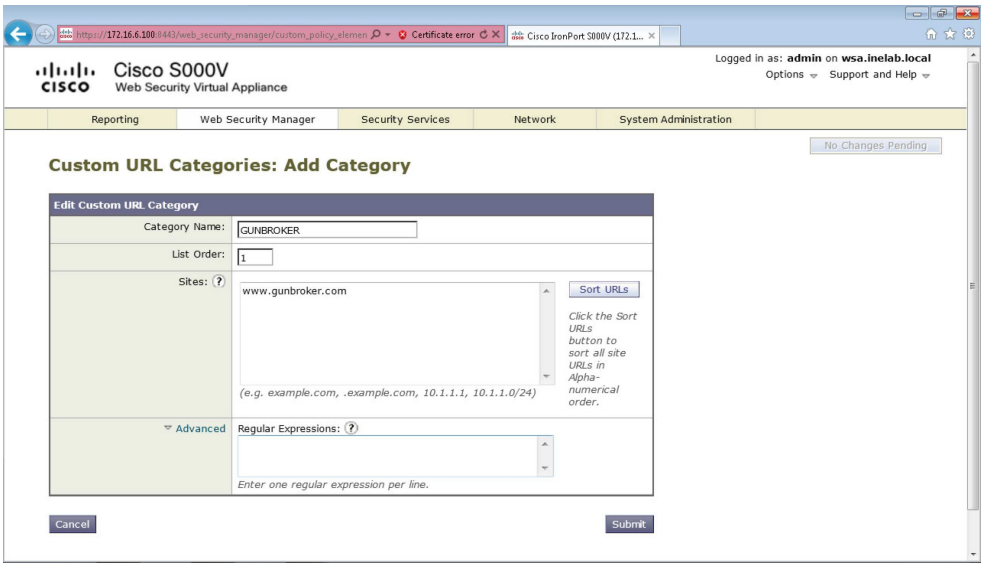
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]>
wsa.inelab.local> commit
```

https://t.me/learningnets

```
Warning: In order to process these changes, the
proxy process will restart after Commit. This will cause
a brief interruption in service. Additionally, the
authentication cache will be cleared, which might require
some users to authenticate again.

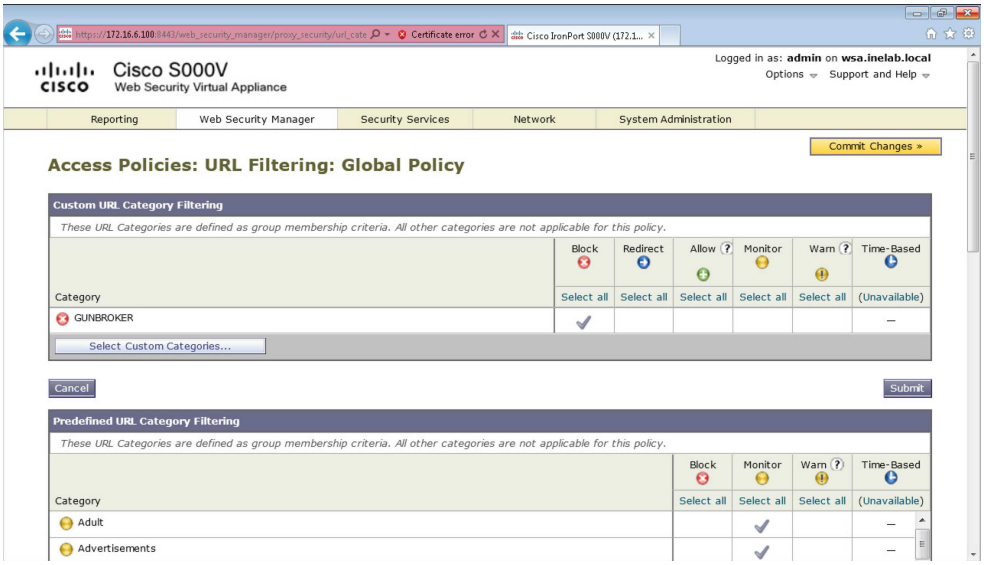
Please enter some comments describing your changes:
[]>
Changes committed: Thu Mar 27 04:08:51 2014 GMT
```

Configure a **Custom URL category** for **www.gunbroker.com**, navigate to **Web Security Manager -> Custom URL Categories**, and click **Add Custom Category**:



Attach the configured category to the **Global Policy**, navigate to **Web Security Manager -> Access Policies**, and edit the **URL Filtering** settings:

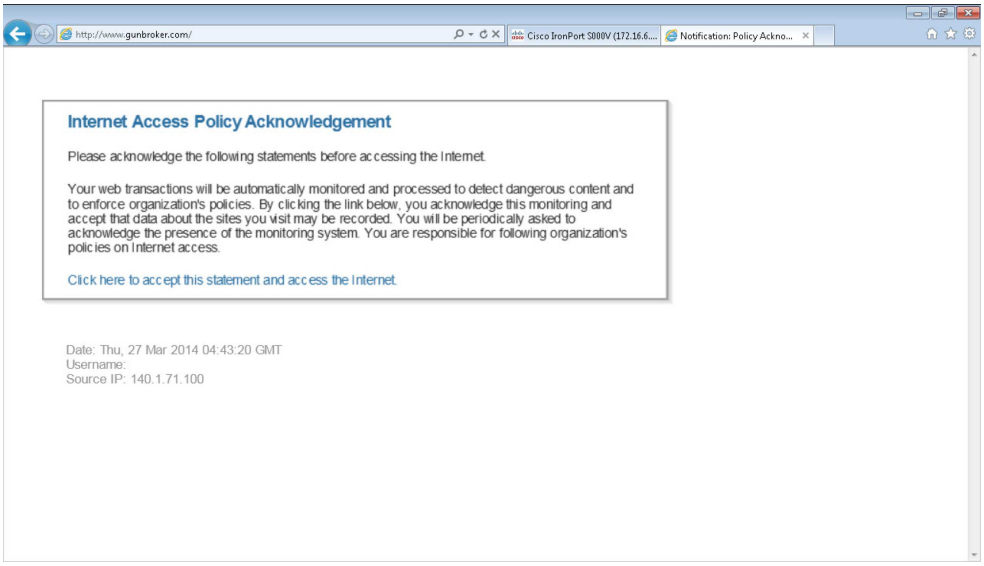
https://t.me/learningnets



Commit changes.

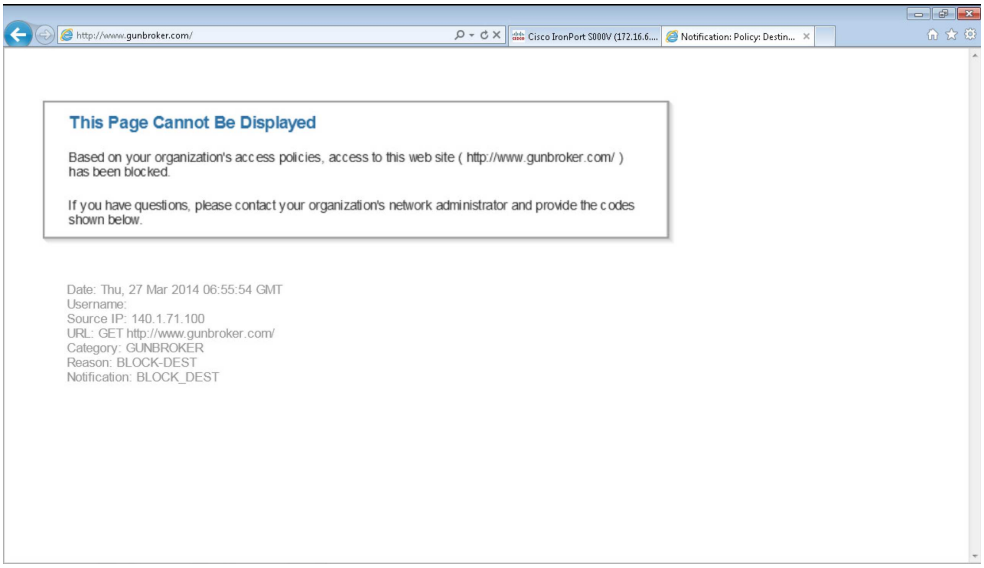
Task 2.6 Verification

To avoid doing any firewall changes and simulate client traffic for testing purposes, add **TEST-PC-B** in VLAN 73 and configure its DNS server to be R4's Loopback0. Initiate the session from the client to **www.gunbroker.com** and verify that you are first presented with the EUN ackonwledgement page:

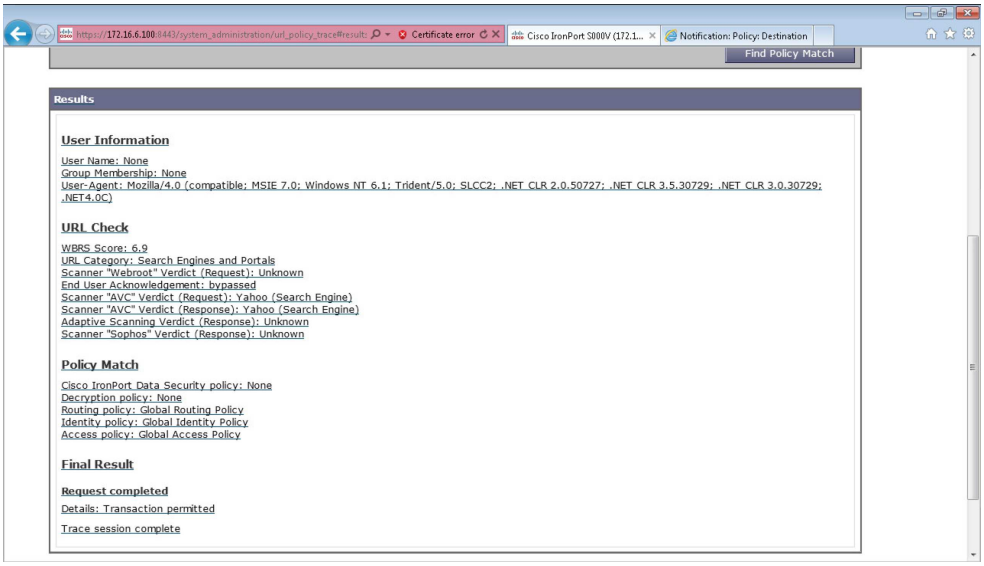


After accepting the policy, WSA will reject the user request and display the reason:

https://t.me/learningnets



The same check can be performed using the **Policy Trace Tool** from the **System Administration** menu:



The following error message is displayed in the access logs of the WSA for the session, the reject reason being Custom URL Category configuration:

```
1395903354.566 0 140.1.71.100 TCP_DENIED/403 0 GET http://www.gunbroker.com/ - NONE/- - BLOCK_CUSTOMCAT
_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-NONE <C_GUNB,-,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,-,-,"-","-",
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 1

CCIE SCv4 Lab 1 Solutions Section 3

1. Task 3.1 Solution
2. Task 3.2 Solution
3. Task 3.3 Solution
4. Task 3.4 Solution
5. Task 3.5 Solution

Task 3.1 Solution

R1:

```
crypto ikev2 proposal default
 encryption 3des
!
!
crypto ikev2 keyring R1_ASA3_KEYRING
 peer ASA3
  address 140.1.38.17
  pre-shared-key local ikev2psk
  pre-shared-key remote ikev2psk
!
!
crypto ikev2 profile R1_ASA3_PROFILE
 match identity remote address 140.1.38.17
 authentication local pre-share
 authentication remote pre-share
 keyring local R1_ASA3_KEYRING
!
!
ip access-list extended R1_ASA3_ACL
 permit ip host 150.1.1.1 host 150.1.9.9
!
!
crypto ipsec transform-set default esp-3des esp-sha-hmac
!
crypto map VPN 100 ipsec-isakmp
```

https://t.me/learningnets

```
 set peer 140.1.38.17
 match address R1_ASA3_ACL
 set ikev2-profile R1_ASA3_PROFILE
!
interface GigabitEthernet0/0.83
 crypto map VPN
```

ASA3:

```
crypto ikev2 enable OUTSIDE
crypto ikev2 policy 200
!
access-list R1_ASA3_ACL permit ip host 150.1.9.9 host 150.1.1.1
!
crypto ipsec ikev2 ipsec-proposal R1_ASA3_PROPOSAL
!
tunnel-group 140.1.38.1 type ipsec-l2l
tunnel-group 140.1.38.1 ipsec-attributes
 ikev2 local-authentication pre-shared-key ikev2psk
 ikev2 remote-authentication pre-shared-key ikev2psk
!
crypto map VPN 100 set peer 140.1.38.1
crypto map VPN 100 match address R1_ASA3_ACL
crypto map VPN 100 set ikev2 ipsec-proposal R1_ASA3_PROPOSAL
crypto map VPN interface OUTSIDE
!
!
object network SW1_L0_REAL
 host 150.1.9.9
!
nat (OUTSIDE,INSIDE) source static R1_L0_REAL R1_L0_REAL destination static SW1_L0_REAL SW1_L0_REAL
```

R3:

```
ip access-list extended VLAN93_INBOUND
 91 permit ip host 150.1.1.1 host 150.1.9.9
!
ip access-list resequence VLAN93_INBOUND 10 10
```

Task 3.1 Verification

Generate interesting traffic and verify that it can be initiated both ways:

```
R1#ping 150.1.9.9 source loopback0
```

https://t.me/learningnets

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.9.9, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1 .!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/4 ms
!
!SW1#ping 150.1.1.1 source loopback0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.9.9 !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
```

Verify IKEv2 and IPsec tunnel states:

```
R1#show crypto ikev2 session detailed

 IPv4 Crypto IKEv2 Session
Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         140.1.38.1/500        140.1.38.17/500       none/none            READY
Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/159 sec
      CE id: 1023, Session-id: 3
      Status Description: Negotiation done
      Local spi: BF080591C12D114F       Remote spi: 28A4C183CD2C928E
      Local id: 140.1.38.1
      Remote id: 140.1.38.17
      Local req msg id:  2              Remote req msg id:  10
      Local next msg id: 2              Remote next msg id: 10
      Local req queued:  2              Remote req queued:  10
      Local window:      5              Remote window:      1
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : YesChild sa: local selector  150.1.1.1/0 - 150.1.1.1/65535
remote selector 150.1.9.9/0 - 150.1.9.9/65535
          ESP spi in/out: 0xC54D7C69/0x2B300918
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: 3DES, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

 IPv6 Crypto IKEv2 Session
```

https://t.me/learningnets

```
!
!ASA3# show crypto ikev2 sa detail


IKEv2 SAs:
 Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                 Remote     Status         Role
 26625947       140.1.38.17/500        140.1.38.1/500      READY    RESPONDER
 Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
       Life/Active Time: 86400/211 sec
       Session-id: 3
       Status Description: Negotiation done
       Local spi: 28A4C183CD2C928E       Remote spi: BF080591C12D114F
       Local id: 140.1.38.17
       Remote id: 140.1.38.1
       Local req mess id: 15             Remote req mess id: 2
       Local next mess id: 15            Remote next mess id: 2
       Local req queued: 15              Remote req queued: 2
       Local window: 1                   Remote window: 5
       DPD configured for 10 seconds, retry 2
       NAT-T is not detected  Child sa: local selector  150.1.9.9/0 - 150.1.9.9/65535
 remote selector 150.1.1.1/0 - 150.1.1.1/65535

           ESP spi in/out: 0x2b300918/0xc54d7c69
           AH spi in/out: 0x0/0x0
           CPI in/out: 0x0/0x0
           Encr: 3DES, esp_hmac: SHA96
           ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Verify that packets are encrypted and decrypted over the IPsec tunnel:

```
R1#show crypto ipsec sa


interface: GigabitEthernet0/0.83
    Crypto map tag: VPN, local addr 140.1.38.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (150.1.1.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (150.1.9.9/255.255.255.255/0/0)
   current_peer 140.1.38.17 port 500
     PERMIT, flags={origin_is_acl,} #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
 #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
```

https://t.me/learningnets

```
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 140.1.38.1, remote crypto endpt.: 140.1.38.17
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0.83
     current outbound spi: 0x2B300918(724568344)
     PFS (Y/N): N, DH group: none
inbound esp sas:
      spi: 0xC54D7C69(3310189673)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: Onboard VPN:6, sibling_flags 80000040, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4181391/3227)
        IV size: 8 bytes
        replay detection support: Y Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:
outbound esp sas:
      spi: 0x2B300918(724568344)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: Onboard VPN:5, sibling_flags 80000040, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4181391/3227)
        IV size: 8 bytes
        replay detection support: Y Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
!
!ASA3# show vpn-sessiondb detail l2l


Session Type: LAN-to-LAN Detailed

Connection   : 140.1.38.1
Index        : 23                    IP Addr      : 140.1.38.1
Protocol     : IKEv2 IPsec
Encryption   : 3DES                  Hashing      : SHA1
Bytes Tx     : 900                   Bytes Rx     : 900
Login Time   : 11:18:29 UTC Thu Mar 27 2014
Duration     : 0h:05m:23s
```

https://t.me/learningnets

```
IKEv2 Tunnels: 1 IPsec Tunnels: 1


IKEv2:
  Tunnel ID    : 23.1
  UDP Src Port : 500                    UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : 3DES                   Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86077 Seconds
  PRF          : SHA1                   D/H Group    : 2
  Filter Name  :
  IPv6 Filter  :
IPsec:
  Tunnel ID    : 23.2
  Local Addr   : 150.1.9.9/255.255.255.255/0/0
  Remote Addr  : 150.1.1.1/255.255.255.255/0/0
  Encryption   : 3DES                   Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28477 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 25 Minutes
  Bytes Tx     : 900                    Bytes Rx     : 900
Pkts Tx      : 9                      Pkts Rx      : 9


NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 325 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

Task 3.2 Solution

ASA3:

```
crypto ikev1 enable INSIDE
crypto ikev1 policy 100
 authentication pre-share
 encryption 3des
 hash md5
 group 2
!
vpn-addr-assign local
ip local pool TEST_PC_B 140.1.50.1-140.1.50.254
```

https://t.me/learningnets

```
!
access-list SPLIT_TUNNEL standard permit host 150.1.1.1
access-list VPN_FILTER permit icmp any host 150.1.1.1
!
username testpcb password testpcb
!
group-policy testpcb internal
group-policy testpcb attributes
 address-pools value TEST_PC_B
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT_TUNNEL
 vpn-filter value VPN_FILTER
!
tunnel-group TEST_PC_B type remote-access
tunnel-group TEST_PC_B general-attributes
  authentication-server-group LOCAL
  default-group-policy testpcb
!
tunnel-group TEST_PC_B ipsec-attributes
  ikev1 pre-shared-key testpcb
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
crypto dynamic-map DYNAMIC 100 set transform-set 3DES_MD5
crypto dynamic-map DYNAMIC 100 set reverse-route
crypto map VPN 100 ipsec-isakmp dynamic DYNAMIC
crypto map VPN interface INSIDE
!
router eigrp 200
 redistribute static metric 100000 100 255 1 1500
!
crypto ikev1 ipsec-over-tcp port 80
!
!
object network VPN_RA_POOL
 subnet 140.1.50.0 255.255.255.0
!
nat (OUTSIDE,INSIDE) source static R1_L0_REAL R1_L0_REAL destination static VPN_RA_POOL VPN_RA_POOL
```

ASA4:

```
access-list GLOBAL_ACL extended permit tcp 140.1.71.0 255.255.255.0 host 172.16.6.1 eq 80
```

SW1:

```
ip access-list extended REDIRECTED_TRAFFIC
```

https://t.me/learningnets

```
11 deny tcp 140.1.71.0 0.0.0.255 host 172.16.6.1
```

Task 3.2 Verification

Configure the VPN Client on **TEST-PC-B** for IPsec-over-TCP in port 80 and initiate the session; authenticate with configured username and password. Verify that output is being matched:

```
ASA3# show vpn-sessiondb detail ra-ikev1-ipsec


Session Type: IKEv1 IPsec Detailed
Username     : testpcb
               Index        : 28
Assigned IP  : 140.1.50.1            Public IP    : 140.1.71.100Protocol     : IKEv1 IPsecOverTCP
License      : Other VPN
Encryption   : 3DES                  Hashing      : MD5
Bytes Tx     : 0                     Bytes Rx     : 0
Pkts Tx      : 0                     Pkts Rx      : 0
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : testpcb               Tunnel Group : TEST_PC_B
Login Time   : 13:49:39 UTC Thu Mar 27 2014
Duration     : 0h:09m:15s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none

IKEv1 Tunnels: 1
IPsecOverTCP Tunnels: 1

IKEv1:
  Tunnel ID    : 28.1
  UDP Src Port : 5211                  UDP Dst Port : 500
  IKE Neg Mode : Aggressive            Auth Mode    : preSharedKeys
Encryption   : 3DES                  Hashing      : MD5
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 85848 SecondsD/H Group    : 2
Filter Name  : VPN_FILTER
  Client OS    : WinNT                 Client OS Ver: 5.0.07.0410

IPsecOverTCP:
  Tunnel ID    : 28.2
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 140.1.50.1/255.255.255.255/0/0Encryption   : 3DES                  Hashing      : MD5
```

https://t.me/learningnets

```
  Encapsulation: Tunnel                TCP Src Port : 5211                TCP Dst Port : 80

  Rekey Int (T): 28800 Seconds         Rekey Left(T): 28245 Seconds
  Idle Time Out: 30 Minutes            Idle TO Left : 20 Minutes
  Bytes Tx     : 0                     Bytes Rx     : 0
  Pkts Tx      : 0                     Pkts Rx      : 0

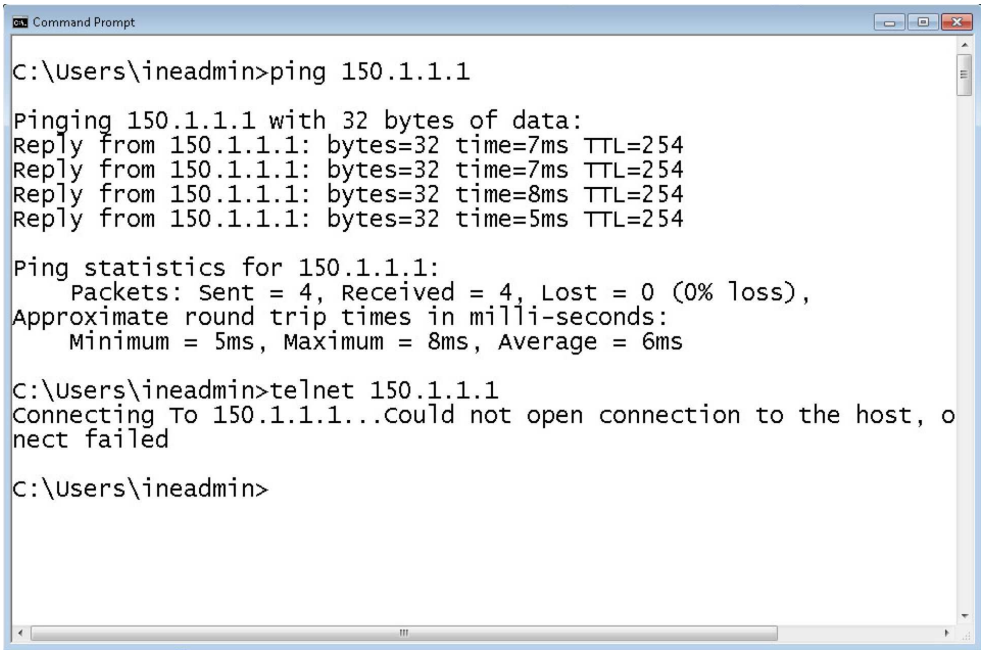
NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 555 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

Verify that the RRI routes have been redistributed:

```
R1#show ip route 140.1.50.1

Routing entry for 140.1.50.1/32
  Known via "ospf 200", distance 110, metric 20, type extern 2, forward metric 1
  Last update from 140.1.38.3 on GigabitEthernet0/0.83, 00:11:15 ago
  Routing Descriptor Blocks:
  * 140.1.38.3, from 150.1.3.3, 00:11:15 ago, via GigabitEthernet0/0.83
      Route metric is 20, traffic share count is 1
```

Verify that ICMP traffic is allowed through the tunnel, but TCP is not:



https://t.me/learningnets

Task 3.3 Solution

R2:

```
interface Tunnel256
 vrf forwarding DMVPN
 ipv6 address 2001:256:256::22/64
 ipv6 nhrp nhs 2001:256:256::66 nbma 150.1.6.6 multicast
```

R5:

```
interface Tunnel256
 vrf forwarding DMVPN
 ipv6 address 2001:256:256::55/64
 ipv6 nhrp nhs 2001:256:256::66 nbma 150.1.6.6 multicast
```

R6:

```
interface Tunnel256
 vrf forwarding DMVPN
 ipv6 address 2001:256:256::66/64
 ipv6 nhrp authentication CISCO
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
```

ASA4:

```
access-list GLOBAL_ACL permit udp host 150.1.2.2 host 150.1.6.6 eq 500
access-list GLOBAL_ACL permit udp host 150.1.5.5 host 150.1.6.6 eq 500
access-list GLOBAL_ACL permit udp host 150.1.6.6 host 150.1.2.2 eq 500
access-list GLOBAL_ACL permit udp host 150.1.6.6 host 150.1.5.5 eq 500
access-list GLOBAL_ACL permit esp host 150.1.2.2 host 150.1.6.6
access-list GLOBAL_ACL permit esp host 150.1.5.5 host 150.1.6.6
access-list GLOBAL_ACL permit esp host 150.1.6.6 host 150.1.2.2
access-list GLOBAL_ACL permit esp host 150.1.6.6 host 150.1.5.5
```

ASA1:

```
access-list DMZ2_IN permit udp host 150.1.2.2 host 150.1.6.6 eq 500
access-list DMZ2_IN permit udp host 150.1.5.5 host 150.1.6.6 eq 500
access-list DMZ2_IN permit esp host 150.1.2.2 host 150.1.6.6
access-list DMZ2_IN permit esp host 150.1.5.5 host 150.1.6.6
access-list DMZ2_IN extended permit tcp host 140.1.71.100 host 172.16.6.100 eq 8443
access-list DMZ2_IN extended permit tcp 140.1.71.0 255.255.255.0 any eq 80
access-list DMZ2_IN extended permit tcp 140.1.71.0 255.255.255.0 host 140.1.57.100 eq 23
access-list DMZ2_IN extended permit tcp 140.1.71.0 255.255.255.0 host 140.1.57.100 eq 443
!
```

https://t.me/learningnets

```
!
access-group DMZ2_IN in interface DMZ2
```

Task 3.3 Verification

Verify that the output is being matched, which means the DMVPN setup is functional:

```
R2#ping vrf DMVPN 2001::55 source loopback256
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::55, timeout is 2 seconds:
Packet sent with a source address of 2001::22%DMVPN!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
!
!R2#ping vrf DMVPN 2001::66 source loopback256
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::66, timeout is 2 seconds:
Packet sent with a source address of 2001::22%DMVPN!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

Verify the IPv6 EIGRP adjacencies in VRF **DMVPN** and the routing table entries:

https://t.me/learningnets

```
R6#show eigrp address-family ipv6 vrf DMVPN neighbors

EIGRP-IPv6 VR(DMVPN) Address-Family Neighbors for AS(256)
           VRF()
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   Link-local address:     Tu256             14 00:07:49    9  1416  0  3

    FE80::217:E0FF:FE4A:9678 0   Link-local address:     Tu256             11 00:07:55   15  1416  0  4

    FE80::DA67:D9FF:FEE0:BBC0
!
!R6#show ipv6 route vrf  DMVPN eigrp

IPv6 Routing Table - DMVPN - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, NM - NEMO, ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 D   2001::22/128 [90/26880256]

     via FE80::DA67:D9FF:FEE0:BBC0, Tunnel256 D   2001::55/128 [90/27008000]

 via FE80::217:E0FF:FE4A:9678, Tunnel256
```

Verify the IKE session status, NHRP mappings, and IPsec tunnel status:

```
R6#show crypto session

Crypto session current status

Interface: Tunnel256 Session status: UP-ACTIVE
     Peer: 150.1.2.2 port 500
  IKEv1 SA: local 150.1.6.6/500 remote 150.1.2.2/500 Active
  IPSEC FLOW: permit 47 host 150.1.6.6 host 150.1.2.2
        Active SAs: 2, origin: crypto map

Interface: Tunnel256 Session status: UP-ACTIVE
     Peer: 150.1.5.5 port 500
  IKEv1 SA: local 150.1.6.6/500 remote 150.1.5.5/500 Active
  IPSEC FLOW: permit 47 host 150.1.6.6 host 150.1.5.5
        Active SAs: 2, origin: crypto map
!
```

https://t.me/learningnets

```
!R6#show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface Tunnel256 is up/up, Addr. is 0.0.0.0, VRF ""
   Tunnel Src./Dest. addr: 150.1.6.6/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN"
   Interface State Control: Disabled
Type:Hub, Total NBMA Peers (v4/v6): 2 1.Peer NBMA Address: 150.1.2.2
        Tunnel IPv6 Address: 2001:256:256::22
        IPv6 Target Network: 2001:256:256::22/128
# Ent: 2, Status: UP, UpDn Time: 00:13:58, Cache Attrib: D
 2.Peer NBMA Address: 150.1.2.2
        Tunnel IPv6 Address: 2001:256:256::22
        IPv6 Target Network: FE80::DA67:D9FF:FEE0:BBC0/128
# Ent: 0, Status: UP, UpDn Time: 00:13:58, Cache Attrib: D
 3.Peer NBMA Address: 150.1.5.5
        Tunnel IPv6 Address: 2001:256:256::55
        IPv6 Target Network: 2001:256:256::55/128
# Ent: 2, Status: UP, UpDn Time: 00:00:54, Cache Attrib: D
 4.Peer NBMA Address: 150.1.5.5
        Tunnel IPv6 Address: 2001:256:256::55
        IPv6 Target Network: FE80::217:E0FF:FE4A:9678/128
# Ent: 0, Status: UP, UpDn Time: 00:00:54, Cache Attrib: D

Pending DMVPN Sessions:

Interface: Tunnel256
  IKEv1 SA: local 150.1.6.6/500 remote 150.1.2.2/500 Active
          Capabilities:(none) connid:1027 lifetime:23:45:51
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 150.1.2.2 IPSEC FLOW: permit 47 host 150.1.6.6 host 150.1.2.2
 Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 238 drop 0 life (KB/Sec) 4407359/2751
        Outbound: #pkts enc'ed 216 drop 0 life (KB/Sec) 4407361/2751
   Outbound SPI : 0xCBFDDB84, transform : esp-3des esp-md5-hmac
    Socket State: Open


Interface: Tunnel256
  IKEv1 SA: local 150.1.6.6/500 remote 150.1.5.5/500 Active
```

https://t.me/learningnets

```
          Capabilities:(none) connid:1028 lifetime:23:59:05
  IKEv1 SA: local 150.1.6.6/500 remote 150.1.5.5/500 Inactive
          Capabilities:(none) connid:1026 lifetime:0
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 150.1.5.5 IPSEC FLOW: permit 47 host 150.1.6.6 host 150.1.5.5
 Active SAs: 2, origin: crypto map

        Inbound:  #pkts dec'ed 37 drop 0 life (KB/Sec) 4501807/3545
        Outbound: #pkts enc'ed 24 drop 0 life (KB/Sec) 4501808/3545
   Outbound SPI : 0xD41E0884, transform : esp-3des esp-md5-hmac
    Socket State: Open
```

Task 3.4 Solution

R1:

```
crypto gdoi group GETVPN_GROUP_GM
 client registration interface Tunnel16
```

R4:

```
crypto gdoi group GETVPN_GROUP_GM
 client registration interface Tunnel46
```

R6:

```
access-list 100 permit ip 150.1.4.4 0.0.0.0 150.1.1.1 0.0.0.0
```

R3:

```
ip access-list extended VLAN93_INBOUND
 permit gre host 140.1.38.1 host 140.1.63.6
 permit gre host 140.1.38.4 host 140.1.63.6
!
ip access-list extended BVI83_INBOUND
 41 permit esp host 150.1.1.1 host 150.1.4.4
 71 permit gre host 140.1.38.4 host 140.1.63.6
 72 permit gre host 140.1.38.1 host 140.1.63.6
!
ip access-list resequence BVI83_INBOUND 10 10
```

ASA3:

```
access-list OUTSIDE_IN  permit gre host 140.1.38.1 host 140.1.63.6
access-list OUTSIDE_IN  permit gre host 140.1.38.4 host 140.1.63.6
```

ASA1:

```
access-list OUTSIDE_IN  permit gre host 140.1.38.1 host 140.1.63.6
```

https://t.me/learningnets

```
access-list OUTSIDE_IN  permit gre host 140.1.38.4 host 140.1.63.6
!
!
access-group OUTSIDE_IN in interface OUTSIDE
```

Task 3.4 Verification

Verify that the output is being matched, so GMs used the Tunnel interface IPv4 address to register:

```
R6#show crypto gdoi ks members | i ID

Group Member ID    : 16.16.16.1
 Group ID          : 146
 Key Server ID     : 6.6.6.6
Group Member ID    : 46.46.46.4
 Group ID          : 146
 Key Server ID     : 6.6.6.6
```

Verify that traffic between R1 and R4 Loopback0 prefixes is functional and protected:

```
R1#ping 150.1.4.4 source loopback0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.4.4, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1 !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!R4#ping 150.1.1.1 source loopback0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.4.4 !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!R1#show crypto ipsec sa peer 0.0.0.0 | i pkts
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
```

https://t.me/learningnets

```
    #pkts not decompressed: 0, #pkts decompress failed: 0
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
```

Verify the group policy and IPsec SAs:

```
R1#show crypto gdoi gm acl

Group Name: GETVPN_GROUP_GM
 ACL Downloaded From KS 6.6.6.6:
   access-list  permit ip host 150.1.1.1 host 150.1.4.4
   access-list  permit ip host 150.1.4.4 host 150.1.1.1
 ACL Configured Locally:
!
!R1#show crypto gdoi ipsec sa


SA created for group GETVPN_GROUP_GM:
  GigabitEthernet0/0.83:
    protocol = ip
      local ident  = 150.1.1.1, port = 0
      remote ident = 150.1.4.4, port = 0
      direction: Both, replay(method/window): Counter/64
    protocol = ip
      local ident  = 150.1.4.4, port = 0
      remote ident = 150.1.1.1, port = 0
      direction: Both, replay(method/window): Counter/64
```

Task 3.5 Solution

```
R3:
ip access-list extended BVI83_INBOUND
 61 permit udp 140.1.12.0 0.0.0.255 host 172.16.5.100 eq 5246
 61 permit udp 140.1.12.0 0.0.0.255 host 172.16.5.100 eq 5247
```

https://t.me/learningnets

```
!
ip access-list resequence BVI83_INBOUND 10 10
```

ASA1:

```
access-list DMZ2_IN permit tcp 140.1.71.0 255.255.255.0 host 172.16.5.100 eq 443
```

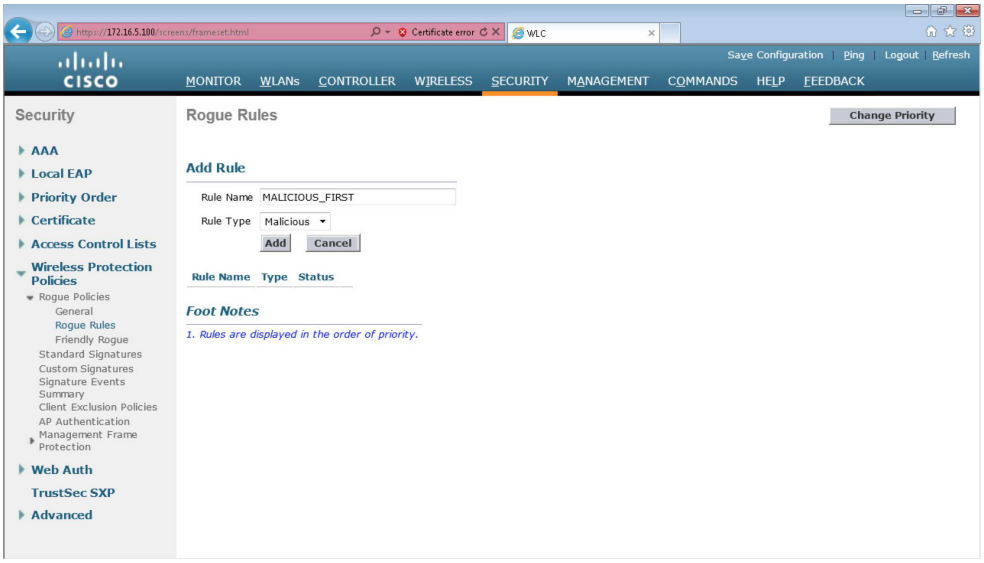
ASA3:

```
access-list OUTSIDE_IN permit udp 140.1.12.0 255.255.255.0 host 172.16.5.100 eq 5246
access-list OUTSIDE_IN permit udp 140.1.12.0 255.255.255.0 host 172.16.5.100 eq 5247
```

ASA4:

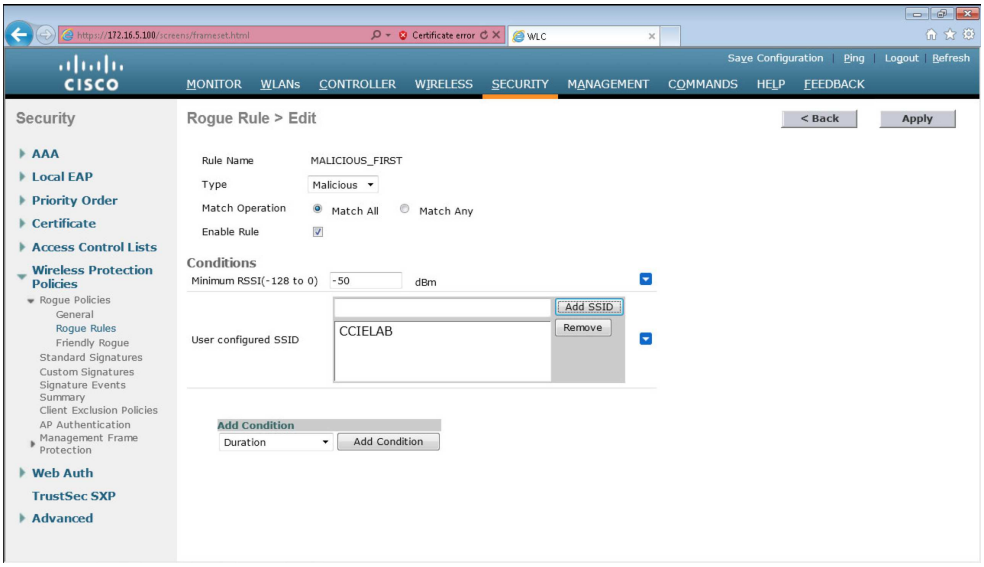
```
access-list GLOBAL_ACL permit tcp 140.1.71.0 255.255.255.0 host 172.16.5.100 eq 443
```

From **TEST-PC-B**, using Internet Explorer navigate through WLC GUI to add Rogue Rules. Go to **Security -> Wireless Protection Policies -> Rogue Policies -> Rogue Rules**, click **Add Rule**, specify type of **Malicious**, and assign the required name:



Modify the default operation to **Match all**, enable the rule, and add the two conditions:

https://t.me/learningnets



Task 3.5 Verification

Verify that the AP joined the WLC, so CAPWAP traffic is allowed through the transit devices:

```
(Cisco Controller) >show ap summary


Number of APs.................................... 1

Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model              Ethernet MAC       Location          Port  Country  Priority
------------------  -----  --------------------  -----------------  ----------------  ----  -------  --------
RACK1-AP             2     AIR-LAP1262N-A-K9     00:06:f6:3b:9a:da  default location  1        US       1
```

Verify the configured rogue rule parameters:

```
(Cisco Controller) >show rogue rule detailed MALICIOUS_FIRST

Priority.......................................... 1
Rule Name......................................... MALICIOUS_FIRST
State............................................. Enabled
Type.............................................. Malicious
Match Operation................................... All
Hit Count......................................... 0
Total Conditions.................................. 2
Condition 1
```

https://t.me/learningnets

```
    type..................................... Rssi
value (dBm)............................... -50
Condition 2
    type..................................... Ssid
    SSID Count............................... 1
SSID 1.................................... CCIELAB
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 1

CCIE SCv4 Lab 1 Solutions Section 4

1. Task 4.1 Solution
2. Task 4.2 Solution
3. Task 4.3 Solution

Task 4.1 Solution

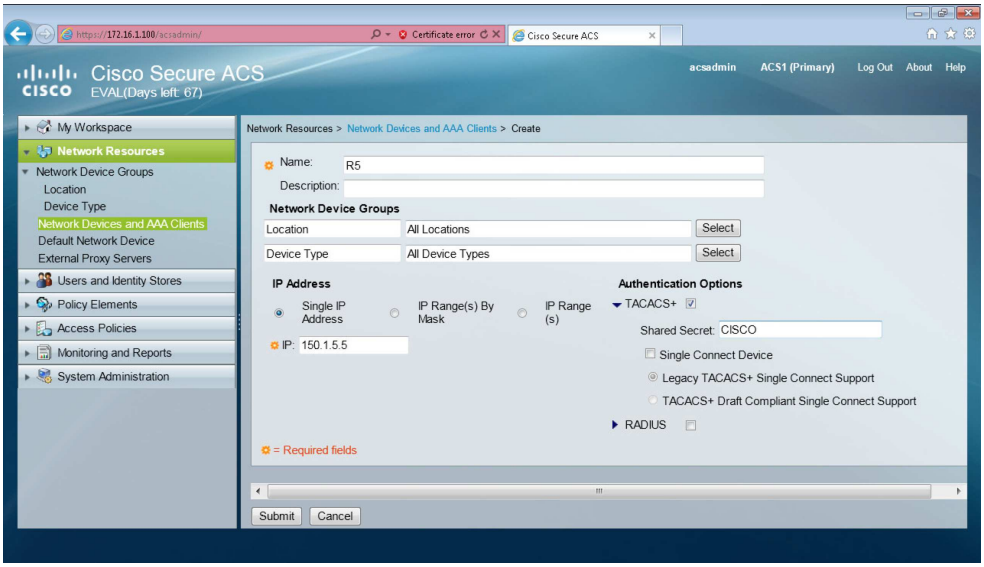
```
R5:
aaa new-model
aaa authentication login HTTP group tacacs+
aaa authorization exec HTTP group tacacs+
!
!
ip tacacs source-interface Loopback0
tacacs-server host 172.16.1.100 key CISCO
!
!
ip http server
ip http port 8080
ip http authentication aaa login-authentication HTTP
ip http authentication aaa exec-authorization HTTP

ASA4:

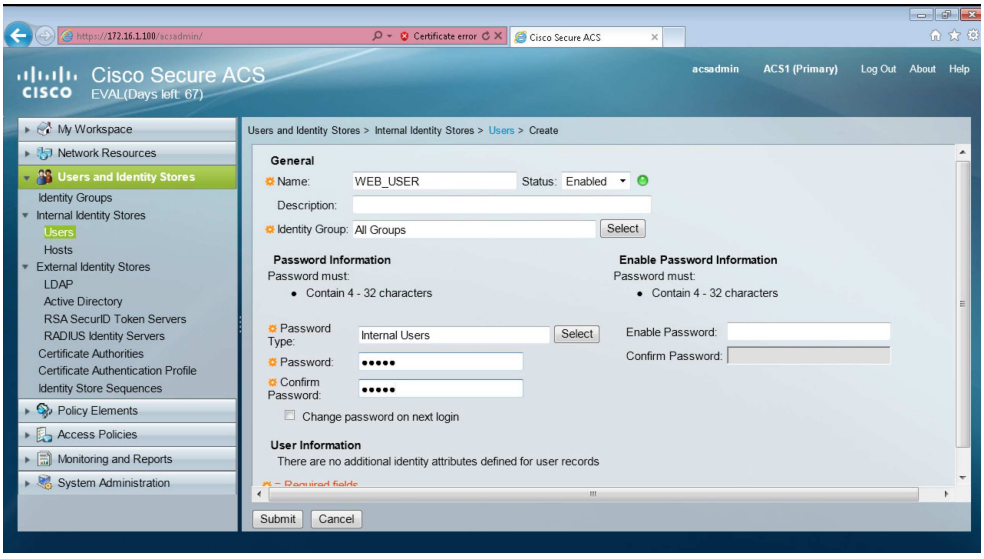
access-list GLOBAL_ACL permit tcp host 150.1.5.5 host 172.16.1.100 eq 49
```

Move **TEST-PC-B** into VLAN 2 to configure the ACS server. From **TEST-PC-B**, using Internet Explorer navigate to ACS, **Network Resources -> Network Device Groups -> Network Devices and AAA Client** and click **Create** to add R5 as a NAD client:

https://t.me/learningnets

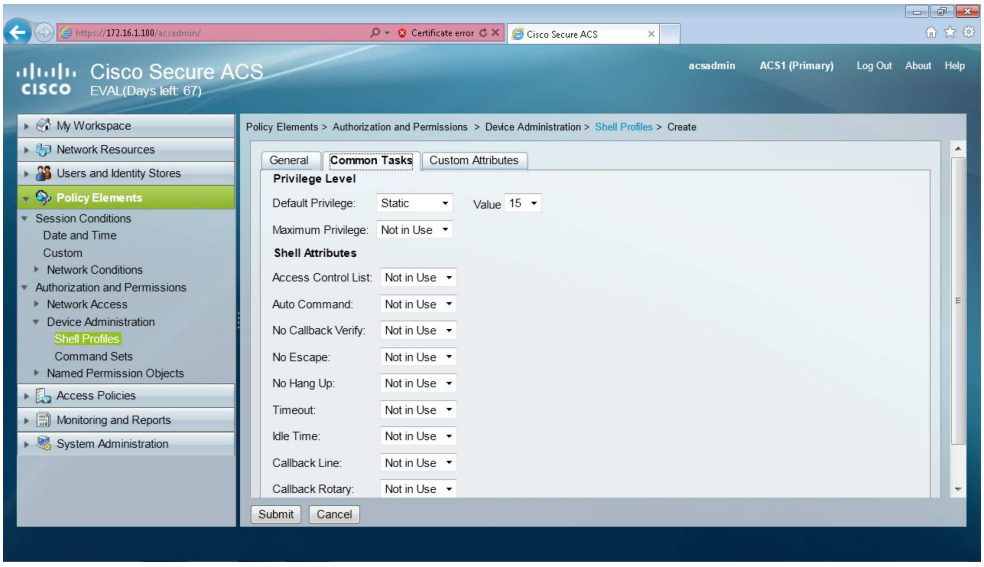


Navigate to **Users and Identity Stores -> Internal Identity Stores -> Users** and click **Create** to configure the username:

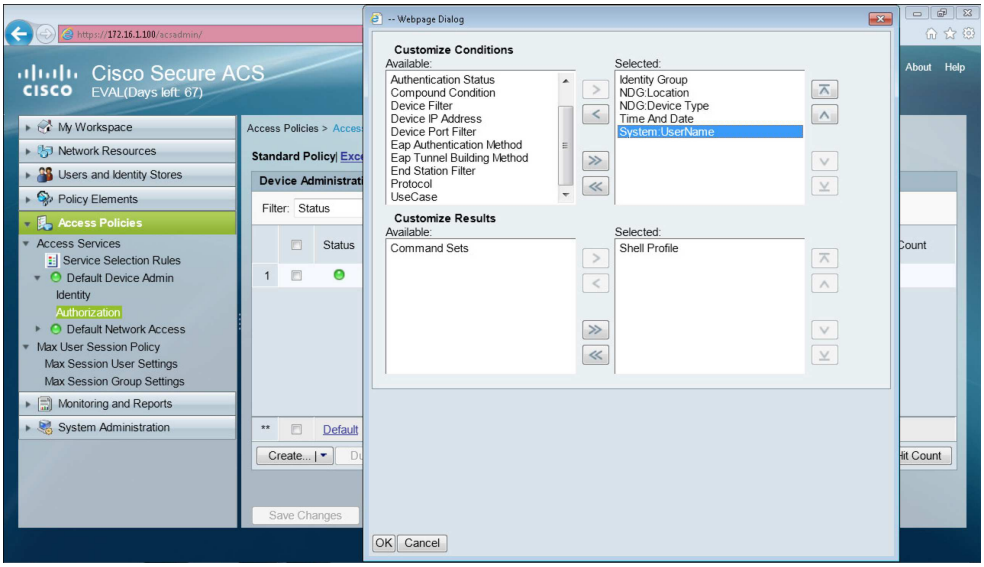


Navigate to **Policy Elements -> Authorization and Permissions -> Device Administration -> Shell Profiles** and click **Create** to configure a profile and assign privilege level 15:

https://t.me/learningnets

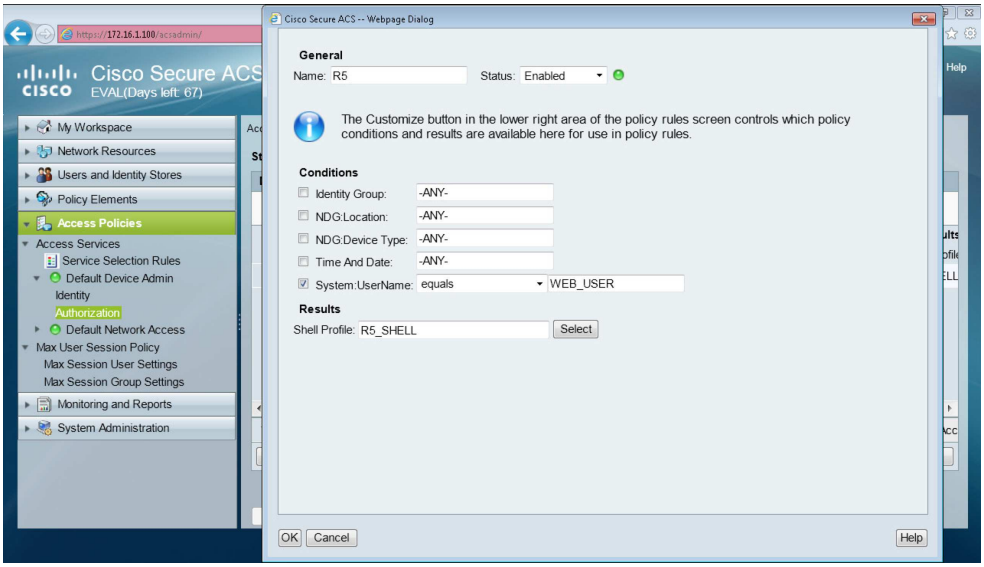


Navigate to **Access Policies -> Access Services -> Default Device Admin -> Authorization**, click **Customize**, and add the username as a condition:



Navigate to **Access Policies -> Access Services -> Default Device Admin -> Authorization** and click **Create** to configure the authorization rule:

https://t.me/learningnets



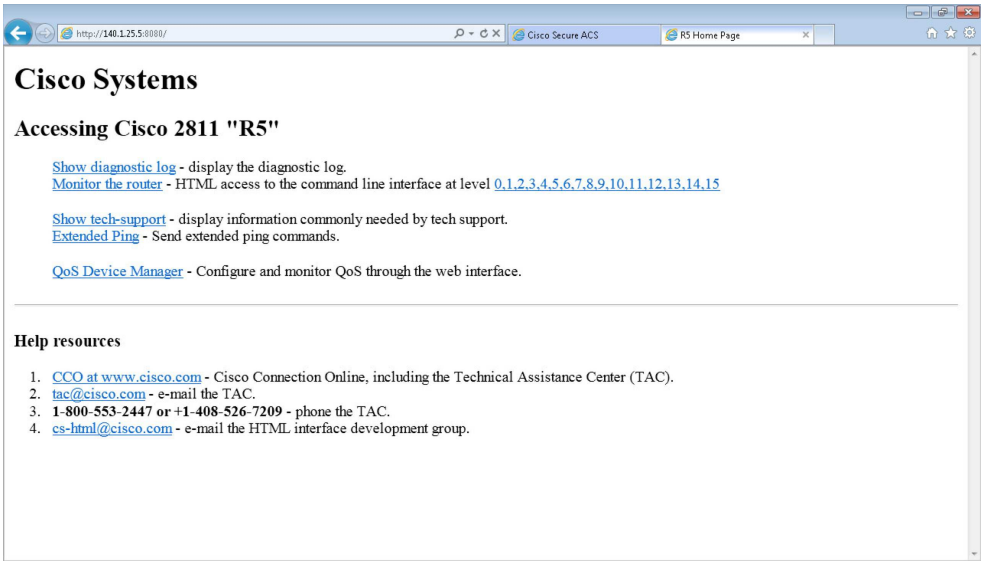
Task 4.1 Verification

Verify that authentication is successful:

```
R5#test aaa group tacacs+ WEB_USER CISCO legacy

Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

Move **TEST-PC-B** in VLAN 23 and access R5 via HTTP on port 8080; authenticate with the configured username/password pair:



Verify the HTTP server history:

https://t.me/learningnets

```
R5#show ip http server history


HTTP server history:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes  end-time
140.1.25.5:8080       140.1.25.50:5427  442          1986        17:52:36 03/30
140.1.25.5:8080       140.1.25.50:5428  0            0           17:53:36 03/30
```

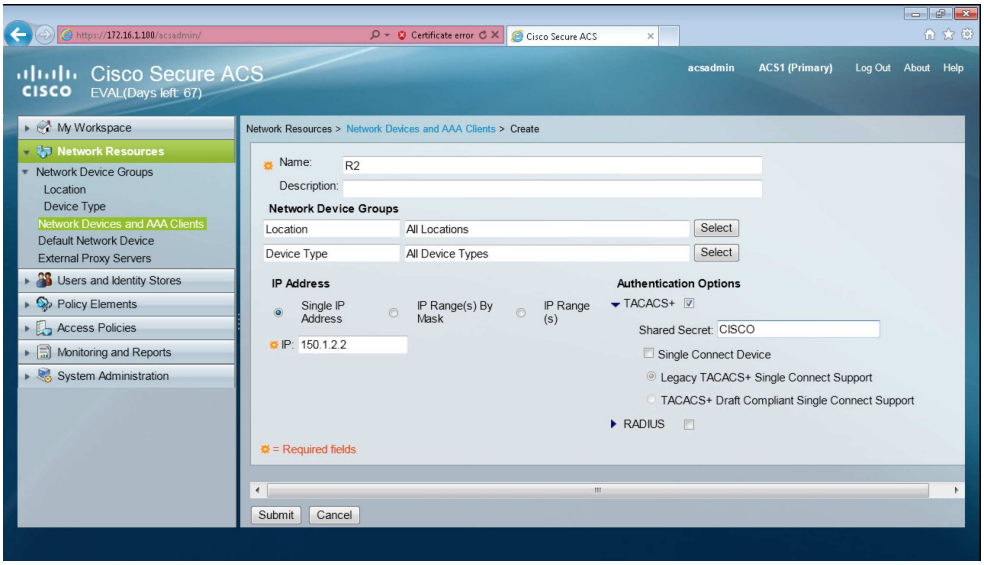
Task 4.2 Solution

```
R2:

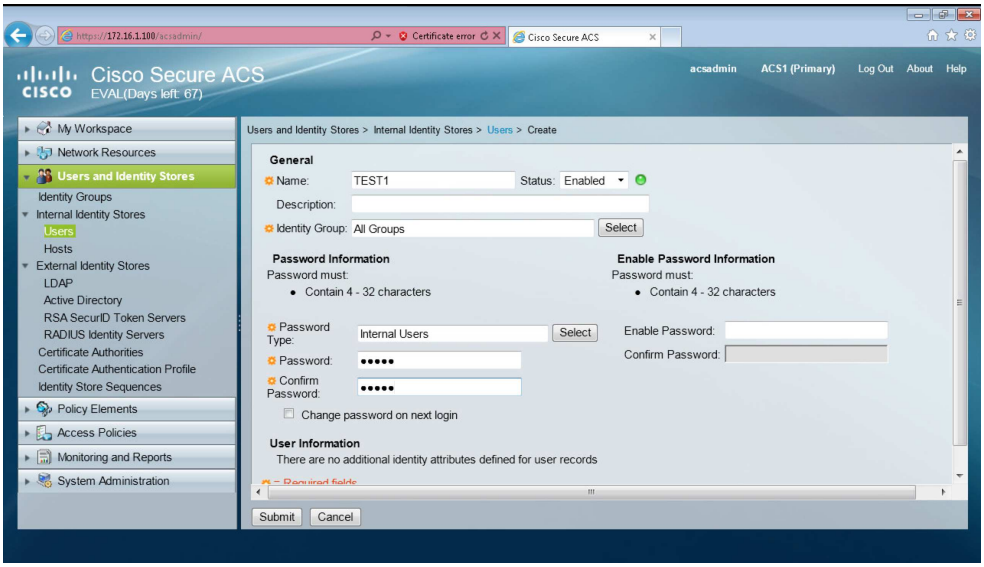
aaa new-model
aaa group server tacacs+ ACS
 server-private 172.16.1.100 key CISCO
 ip tacacs source-interface Loopback0
!
aaa authentication login TELNET group ACS
aaa authorization exec TELNET group ACS
aaa authorization commands 0 TELNET group ACS
aaa authorization commands 1 TELNET group ACS
aaa authorization commands 15 TELNET group ACS
!
!
ip tacacs source-interface Loopback0
tacacs-server host 172.16.1.100 key CISCO
!
!
line vty 0 15
 ?login authentication TELNET
 authorization commands 0 TELNET
 authorization commands 1 TELNET
 authorization commands 15 TELNET
 authorization exec TELNET
```

Move **TEST-PC-B** into VLAN 2 to configure the ACS server. From **TEST-PC-B**, using Internet Explorer navigate to ACS, **Network Resources -> Network Device Groups -> Network Devices and AAA Client** and click **Create**:

https://t.me/learningnets

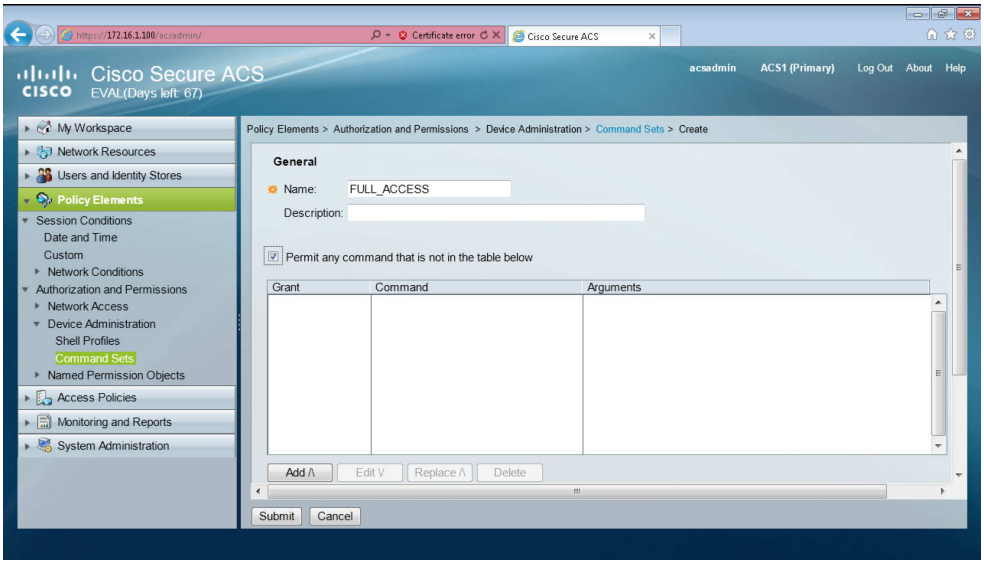


Navigate to **Users and Identity Stores -> Internal Identity Stores -> Users**, click **Create**, and add both users:

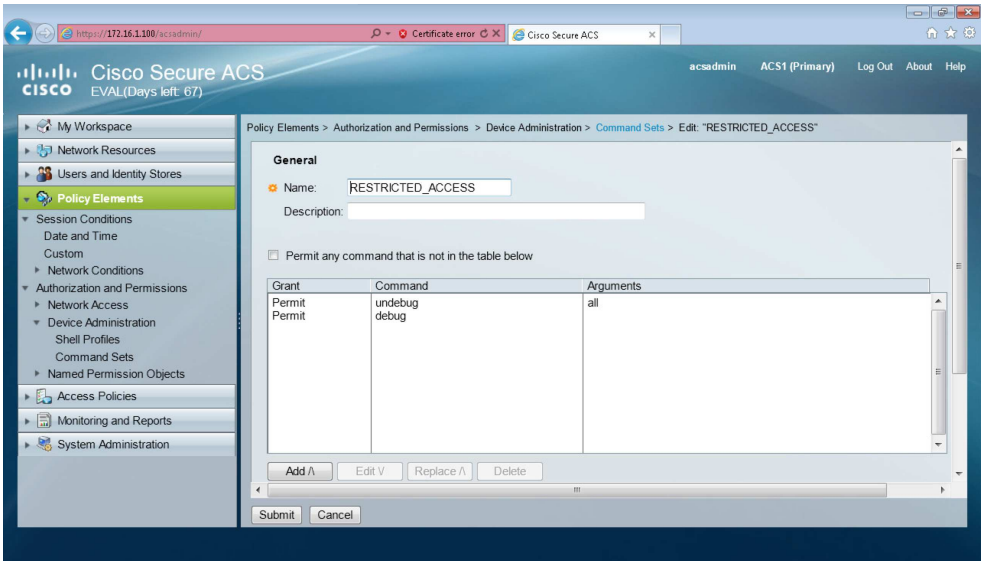


Navigate to **Policy Elements -> Authorization and Permissions -> Device Administration -> Command Sets** and click **Create** to configure the command set for full access:

https://t.me/learningnets

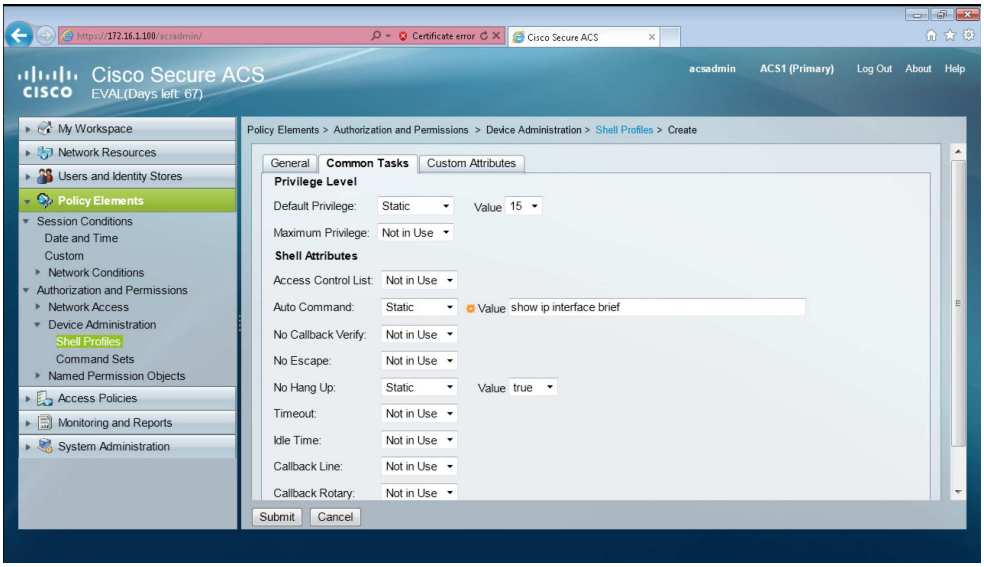


Navigate to **Policy Elements -> Authorization and Permissions -> Device Administration -> Command Sets** and click **Create** to configure the command set for debug and undebug command access:

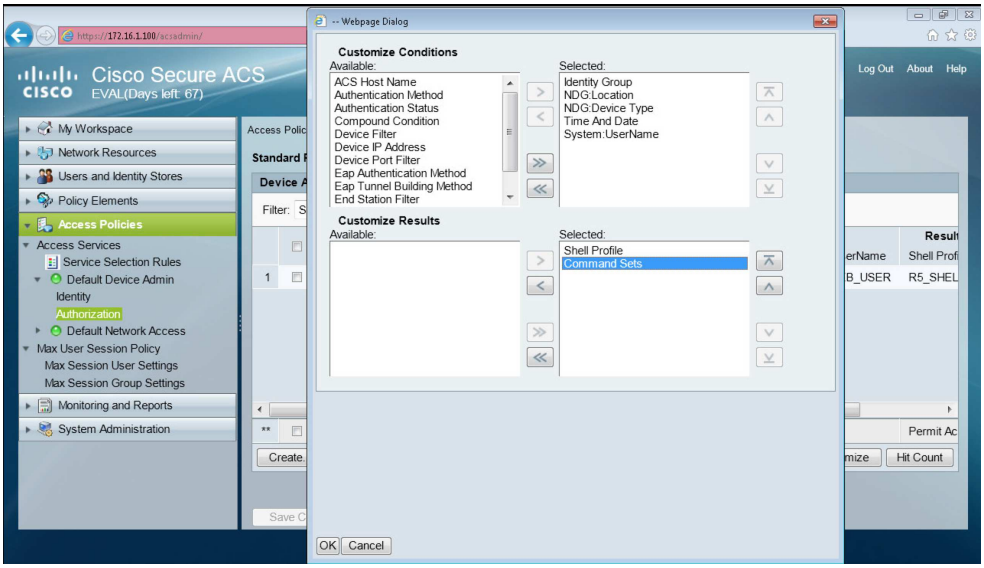


Navigate to **Policy Elements -> Authorization and Permissions -> Device Administration -> Shell Profiles** and click **Create** to configure a profile to automatically run the command **show ip interface brief**:

https://t.me/learningnets

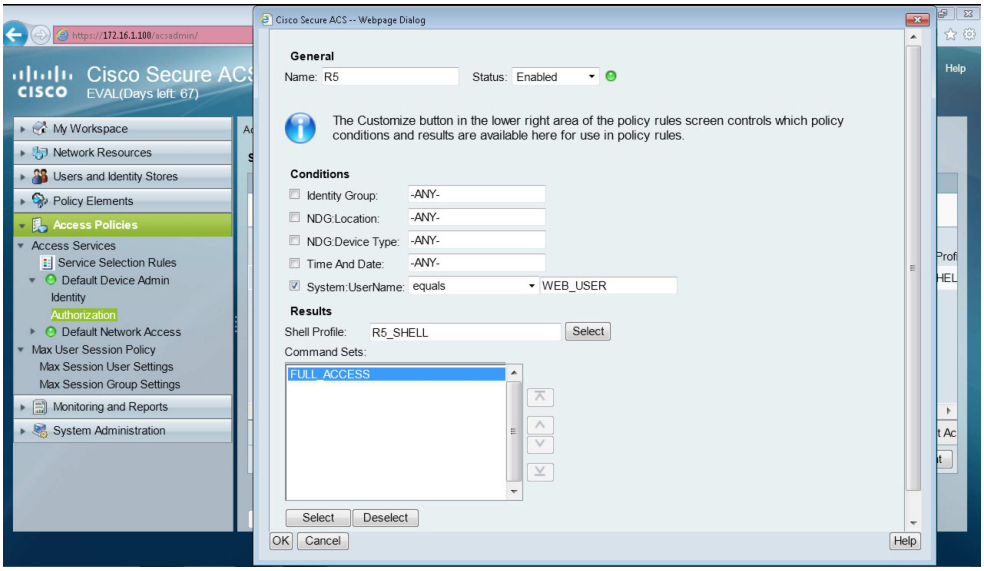


Navigate to **Access Policies -> Access Services -> Default Device Admin -> Authorization**, click **Customize**, and add the command set as a result:

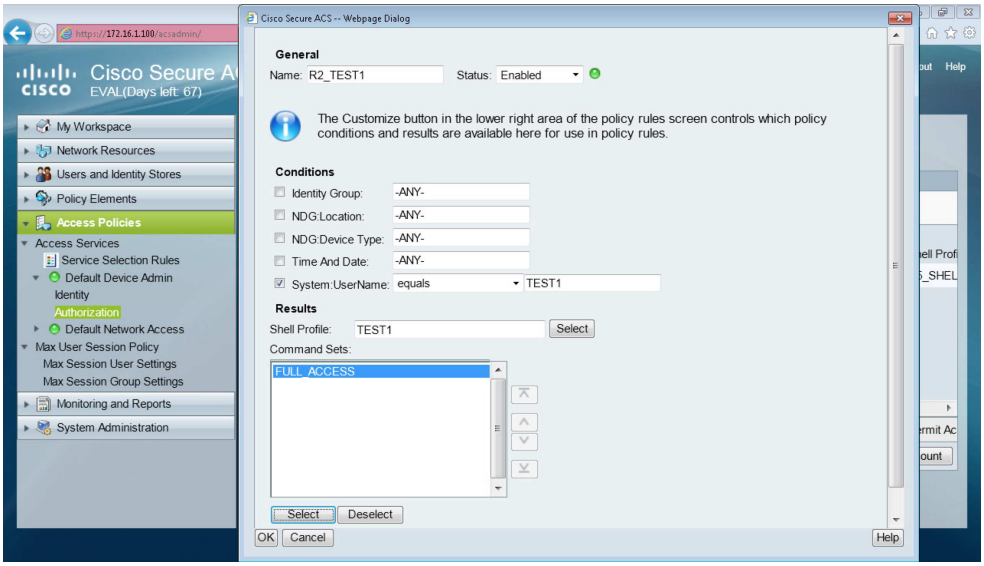


Navigate to **Access Policies -> Access Services -> Default Device Admin -> Authorization**, edit the rule from previous task, and assign the command set with full access to all commands:

https://t.me/learningnets

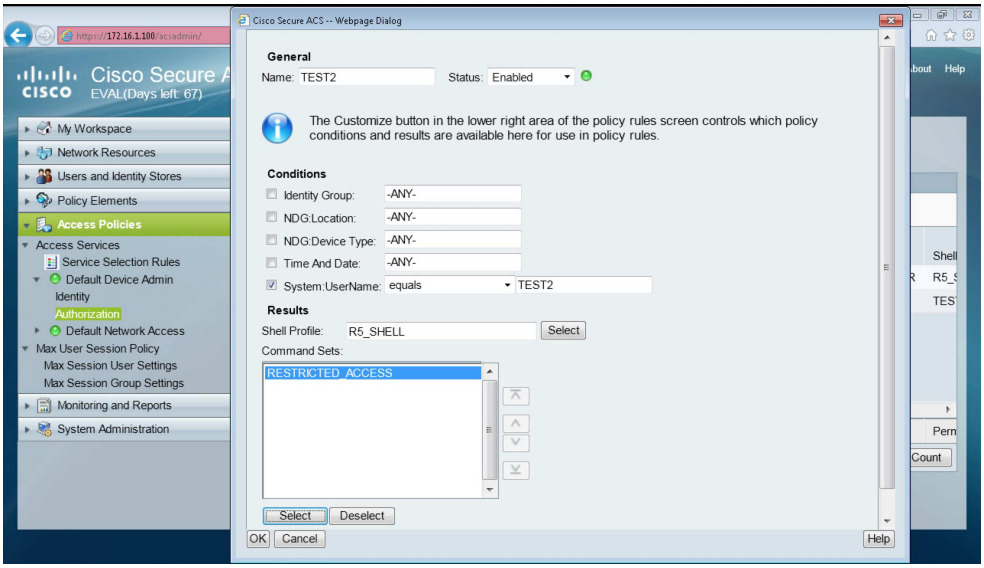


Navigate to **Access Policies -> Access Services -> Default Device Admin -> Authorization** and add a rule for user **TEST1**:



Navigate to **Access Policies -> Access Services -> Default Device Admin -> Authorization** and add a rule for user **TEST2**:

https://t.me/learningnets



Task 4.2 Verification

Verify that when authenticated with user **TEST1**, the session is not disconnected and the **show ip interfae brief** command is automatically issued:

```
R2#telnet 150.1.2.2
Trying 150.1.2.2 ... Open
username: TEST1
password:

Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  up                    up
GigabitEthernet0/0.2       172.16.1.1      YES NVRAM  up                    up
GigabitEthernet0/0.72      140.1.71.2      YES NVRAM  up                    up
GigabitEthernet0/1         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/2         unassigned      YES NVRAM  administratively down down
Loopback0                  150.1.2.2       YES NVRAM  up                    up
Loopback256                unassigned      YES unset  up                    up
Tunnel256                  unassigned      YES unset  up                    up      username:
```

Authenticate using **TEST2**, and verify that access to all debug and **undebug all** commands is granted:

```
R2#telnet 150.1.2.2
Trying 150.1.2.2 ... Open
username: TEST2
```

https://t.me/learningnets

```
password:
R2#configure terminal
Command authorization failed.
R2#R2#debug tacacs authentication

TACACS+ authentication debugging is on
R2#R2#undebug all

All possible debugging has been turned off
```

Task 4.3 Solution

SW3:

```
aaa new-model
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
!
ip access-list extended REDIRECT_ACL
 deny udp any eq bootpc any eq bootps
 deny udp any host 150.1.4.4 eq domain
 deny tcp any host 140.1.45.100 eq 8443
 permit tcp any any eq www
 permit tcp any any eq 443
!
ip http server
ip http secure-server
!
interface GigabitEthernet1/0/5
 authentication port-control auto
 mab
!
aaa group server radius ISE
 server-private 140.1.45.100 key CISCO
 ip radius source-interface Loopback0
!
aaa server radius dynamic-author
 client 140.1.45.100 server-key CISCO
```

ASA1:

```
static (INSIDE,DMZ1) 140.1.45.100 172.16.3.100 netmask 255.255.255.255
static (INSIDE,DMZ2) 140.1.45.100 172.16.3.100 netmask 255.255.255.255
!
access-list DMZ1_IN permit udp host 150.1.11.11 host 140.1.45.100 eq 1645
access-list DMZ1_IN permit udp host 150.1.11.11 host 140.1.45.100 eq 1812
```

https://t.me/learningnets

```
access-list DMZ1_IN permit tcp host 150.1.6.6 eq 80 140.1.71.0 255.255.255.0
access-list DMZ1_IN permit udp host 150.1.6.6 host 150.1.2.2 eq 500
access-list DMZ1_IN permit udp host 150.1.6.6 host 150.1.5.5 eq 500
access-list DMZ1_IN permit esp host 150.1.6.6 host 150.1.2.2
access-list DMZ1_IN permit esp host 150.1.6.6 host 150.1.5.5
access-list DMZ1_IN permit gre host 140.1.63.6 host 140.1.38.1
access-list DMZ1_IN permit gre host 140.1.63.6 host 140.1.38.4
!
access-group DMZ1_IN in interface DMZ1
!
!
access-list DMZ2_IN permit tcp 140.1.71.0 255.255.255.0 host 140.1.45.100 eq 8443
access-list DMZ2_IN permit udp 140.1.71.0 255.255.255.0 host 150.1.4.4 eq 53
!
access-list CWA_REDIRECT permit tcp host 150.1.6.6 eq 80 140.1.71.0 255.255.255.0
!
class-map CWA_REDIRECT
 match access-list CWA_REDIRECT
!
policy-map global_policy
 class CWA_REDIRECT
  set connection advanced-options tcp-state-bypass
```

ASA4:

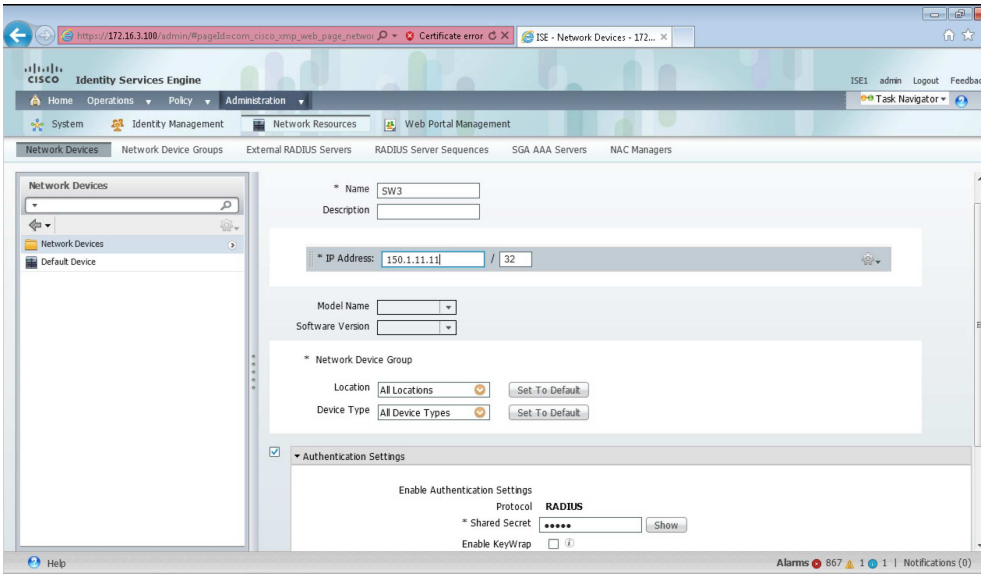
```
access-list GLOBAL_ACL permit udp 140.1.71.0 255.255.255.0 host 150.1.4.4 eq 53
access-list GLOBAL_ACL permit tcp 140.1.71.0 255.255.255.0 host 140.1.45.100 eq 8443
access-list GLOBAL_ACL permit tcp host 150.1.6.6 eq 80 140.1.71.0 255.255.255.0
!
access-list CWA_REDIRECT permit tcp host 150.1.6.6 eq 80 140.1.71.0 255.255.255.0
!
class-map CWA_REDIRECT
 match access-list CWA_REDIRECT
!
policy-map global_policy
 class CWA_REDIRECT
  set connection advanced-options tcp-state-bypass
```

R4:

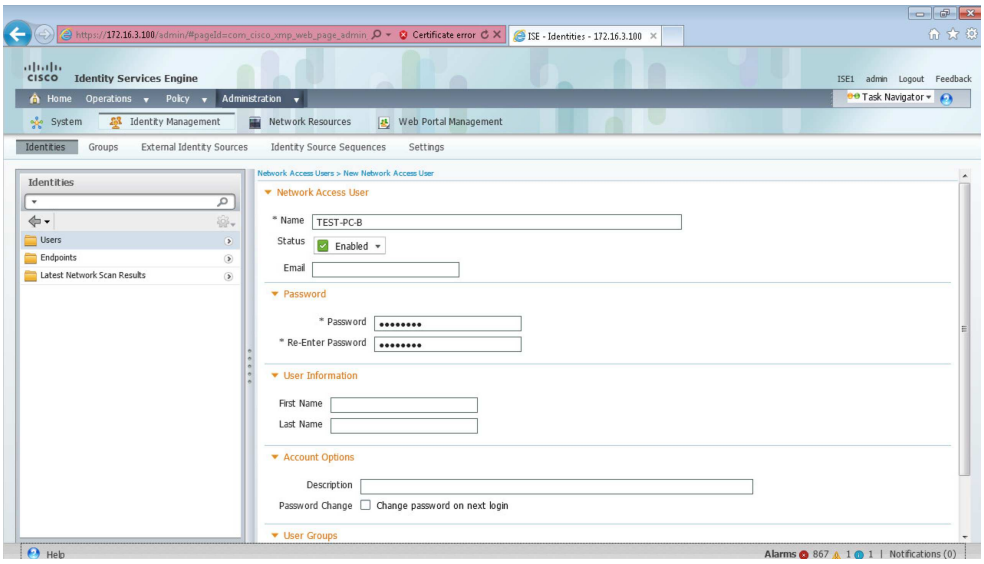
```
ip host ise1.inelab.local 140.1.45.100
```

https://t.me/learningnets

Move **TEST-PC-B** into VLAN 40 to configure the ISE server. From **TEST-PC-B**, using Internet Explorer navigate to ISE, **Administration -> Network Resources -> Network Devices** and click **Add** to add SW3 as a NAD client:

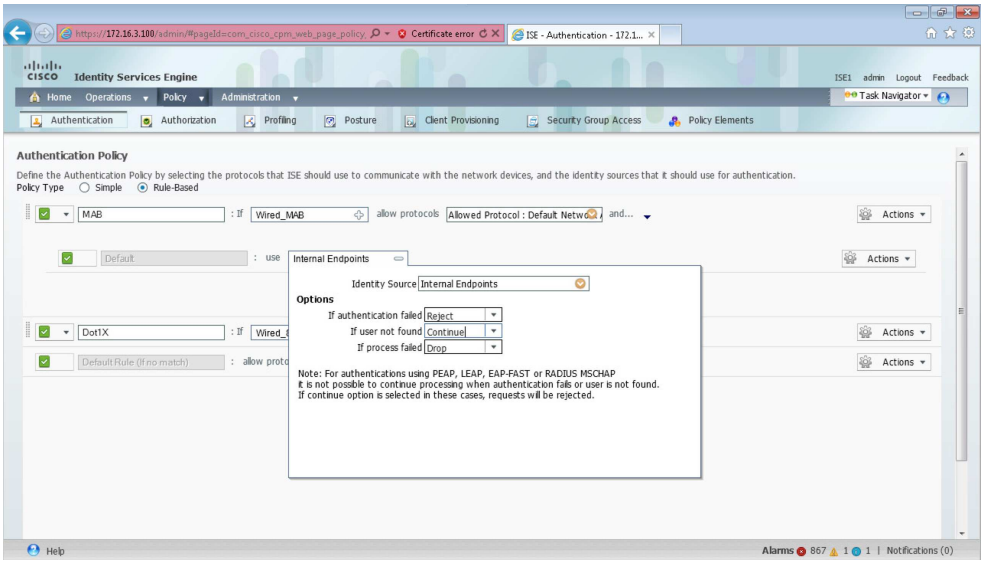


Navigate to **Administration -> Identity Management -> Identities -> Users** and click **Add** to add the username/password used for web authentication:

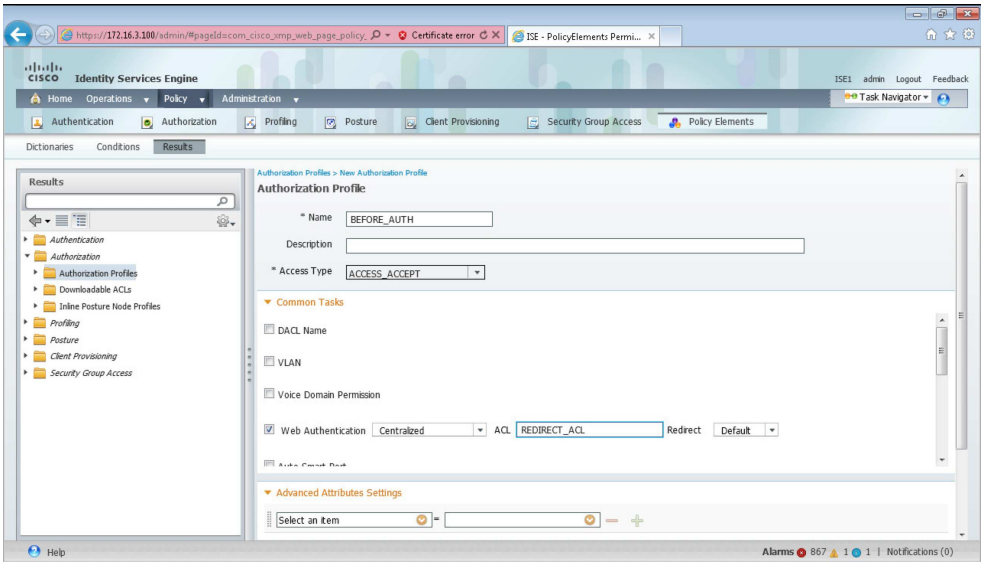


Modify the default **MAB** authentication policy so that if the user is not found (MAC address of the client), the action is set to **Continue**. Navigate to **Policy -> Authentication**:

https://t.me/learningnets

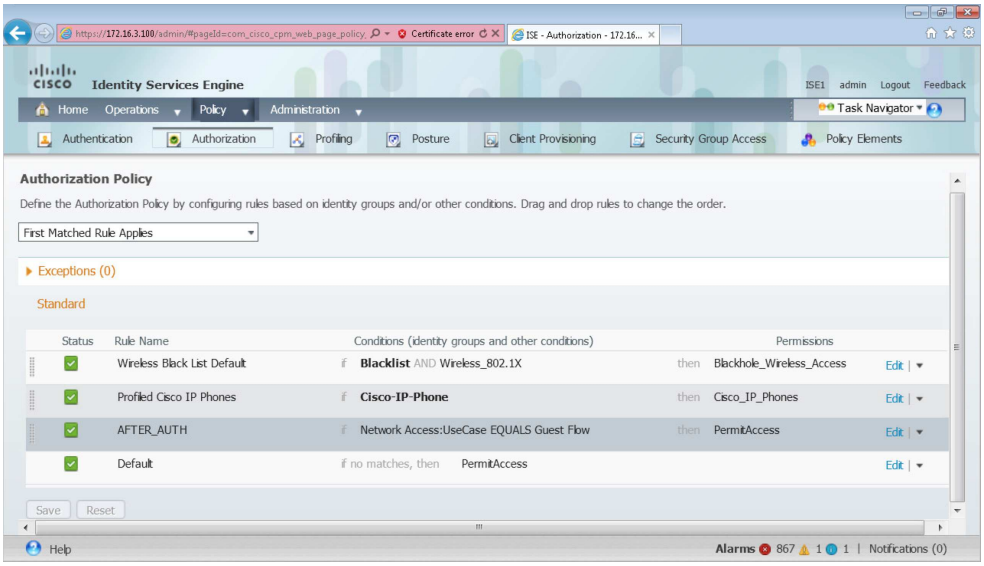


Navigate to **Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles** and click **Add** to create the initial authorization profile for central web authentication:

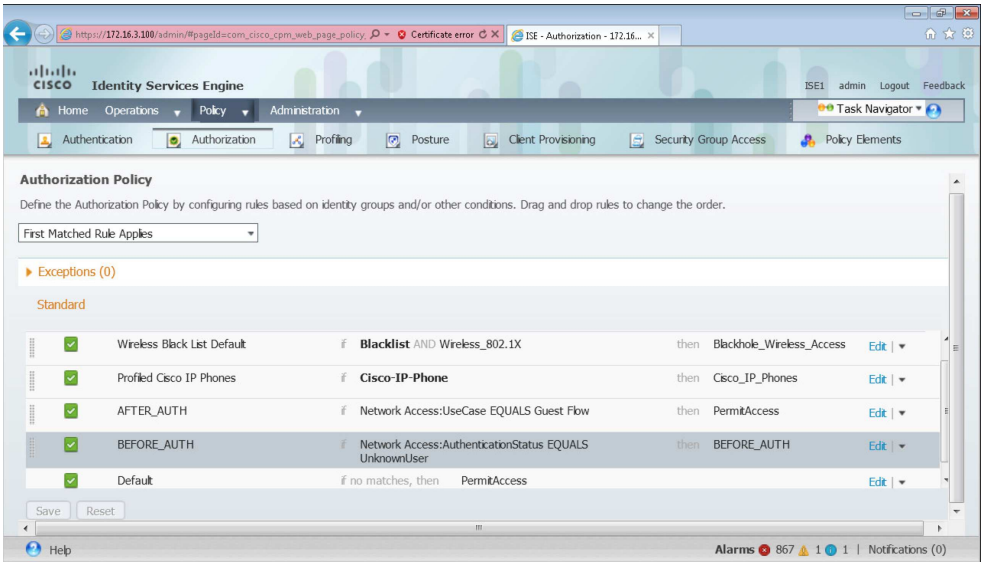


Navigate to **Policy -> Authorization** and configure the second authorization policy, matched after the user is authenticated in the guest portal:

https://t.me/learningnets

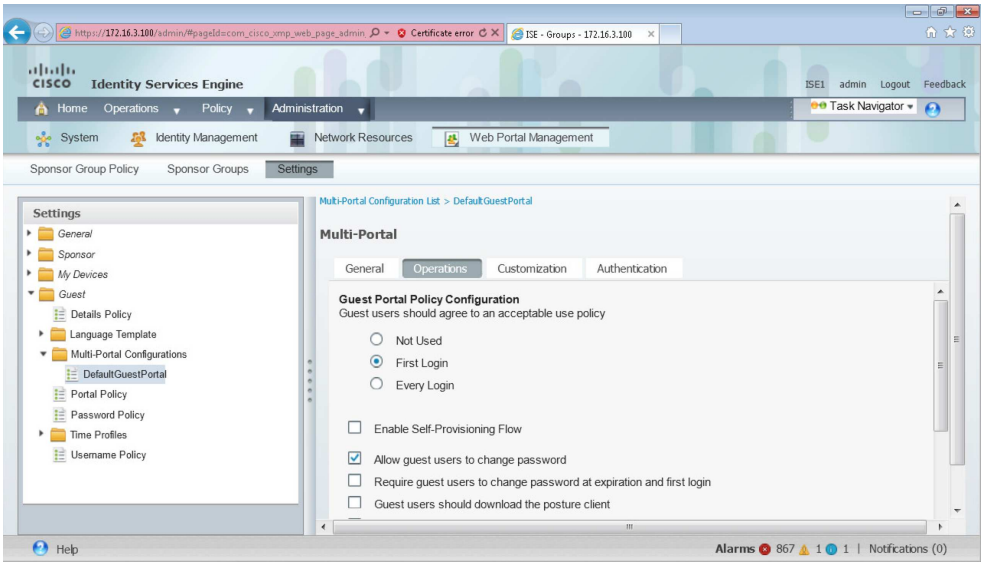


Navigate to **Policy -> Authorization** and configure the first authorization policy, matched before the user is authenticated in the guest portal:



Navigate to **Administration -> Web Portal Management -> Settings -> Guest -> Multi-Portal Configurations -> DefaultGuestPortal** and disable access to the self-provisioning functionality:

https://t.me/learningnets



Task 4.3 Verification

Verify the initial authorization, before the user is authenticated in the ISE portal:

```
SW3#show authentication sessions

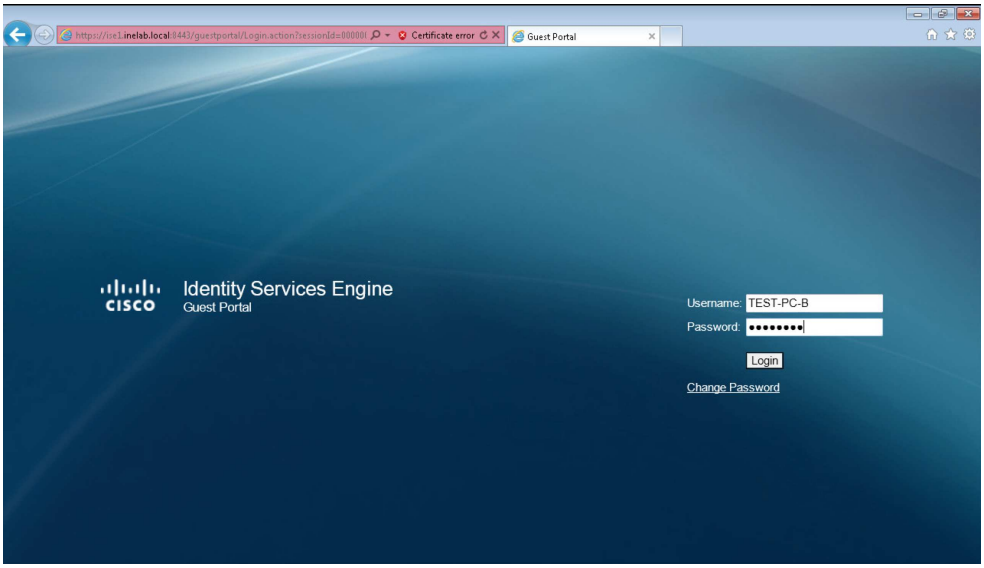

Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/0/5    48f8.b32e.2532  mab      DATA     Authz Success  0000000000264E5144AF861
!
!SW3#show authentication sessions interface gigabitEthernet1/0/5
            Interface:  GigabitEthernet1/0/5
          MAC Address:  48f8.b32e.2532
           IP Address:  172.16.3.50
            User-Name:  48-F8-B3-2E-25-32 Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A URL Redirect ACL:  REDIRECT_ACL

URL Redirect:  https://ISE1.inelab.local:8443/guestportal/gateway?sessionId=0000000000264E5144AF861&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0000000000264E5144AF861
      Acct Session ID:  0x000006C6
               Handle:  0xCA0007ED
```

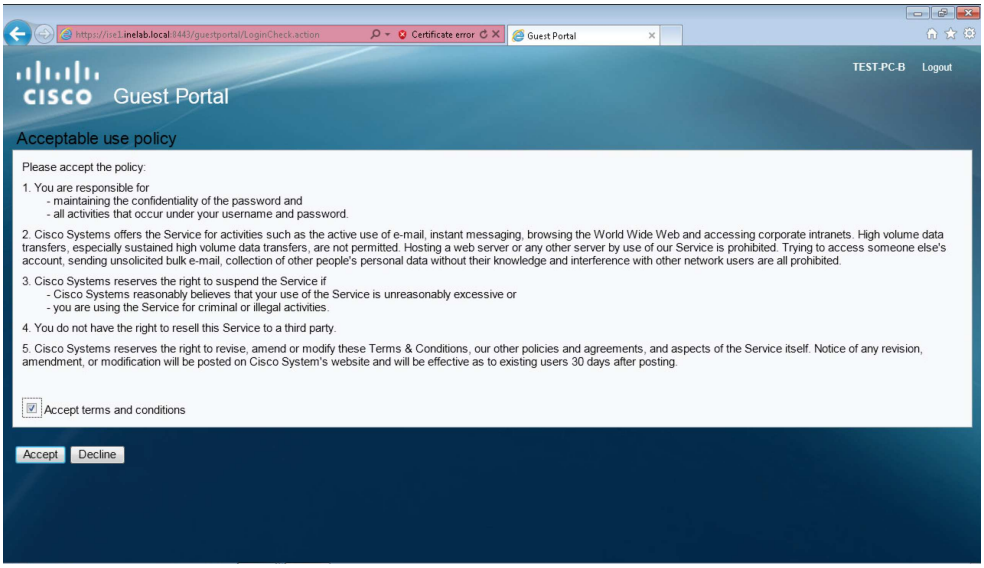
https://t.me/learningnets

```
Runnable methods list:
       Method   State
mab        Authc Success
```

Configure **TEST-PC-B** in VLAN 71 with the required settings and navigate to **http://150.1.6.6**. If the configuration is correct, you should be redirected to ISE portal; authenticate with the configured username/password:



Click **Accept** in the presented page after being successfully authenticated:



Verify the final authorization, after the user is authenticated in the ISE portal:

```
SW3#show authentication sessions


Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/0/5    48f8.b32e.2532  mab      DATA     Authz Success  0A0B0C0D00026B7C14744D33
```

https://t.me/learningnets

```
!
!SW3#show authentication sessions interface gigabitEthernet1/0/5
            Interface:  GigabitEthernet1/0/5
          MAC Address:  48f8.b32e.2532
           IP Address:  140.1.71.100 User-Name:  TEST-PC-B
Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0000000000026B7C14744D33
      Acct Session ID:  0x00000D5D
               Handle:  0x83000EC6

Runnable methods list:
       Method   State mab        Authc Success
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 1

CCIE SCv4 Lab 1 Solutions Section 5

1. Task 5.1 Solution
2. Task 5.2 Solution
3. Task 5.3 Solution
4. Task 5.4 Solution
5. Task 5.5 Solution

Task 5.1 Solution

R6:

```
class-map type port-filter match-all CLOSED_PORTS
 match closed-ports
 match not port udp 848
 match not port tcp 3001
 match not port tcp 5001
!
ip access-list extended ROUTING_TRAFFIC
 permit tcp any any eq bgp
 permit tcp any eq bgp any
 permit eigrp any any
!
class-map match-all ROUTING_TRAFFIC
 match access-group name ROUTING_TRAFFIC
!
policy-map COPP
 class ROUTING_TRAFFIC
 class class-default
  police rate 20000 pps
!
policy-map type port-filter PORT_FILTER
 class CLOSED_PORTS
  drop
!
control-plane host
```

https://t.me/learningnets

```
 service-policy type port-filter input PORT_FILTER
!
control-plane
 service-policy input COPP
```

Task 5.1 Verification

Verify control-plane implemented features:

```
R6#show control-plane features

Total 2 features configured

Control plane aggregate path features :

-------------------------------------------------------
Control-plane Policing activated Mar 30 2014 22:5

-------------------------------------------------------

Control plane host path features :

-------------------------------------------------------TCP/UDP Portfilter activated Mar 30 2014 22:5



-------------------------------------------------------
```

Verify counters and opened ports; note that, for example, GDOI UDP port of 848 is not listed:

```
R6#show control-plane host open-ports

Active internet connections (servers and established)
Prot               Local Address            Foreign Address                 Service    State
 tcp                        *:22                       *:0              SSH-Server   LISTEN
 tcp                        *:23                       *:0                  Telnet   LISTEN
 udp                     *:4500                        *:0                 ISAKMP   LISTEN
 udp                     *:1975                        *:0                    IPC   LISTEN
 udp                      *:500                        *:0                 ISAKMP   LISTEN
!
!R6#show control-plane counters

Feature Path             Packets processed/dropped/errors
Aggregate                   64661/0/0
```

https://t.me/learningnets

```
Host                        42677/0/0
Transit                       115/0/0
Cef-exception               21874/0/0
```

Verify the aggregate control-plane configuration:

```
R6#show policy-map control-plane

 Control Plane

  Service-policy input: COPP
 Class-map: ROUTING_TRAFFIC (match-all)
129 packets, 9546 bytes
      5 minute offered rate 0 bps
      Match: access-group name ROUTING_TRAFFIC
 Class-map: class-default (match-any)
293 packets, 28858 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  police:
rate 20000 pps, burst 4882 packets

        conformed 293 packets; actions:
          transmit
        exceeded 0 packets; actions:
          drop
        conformed 0 pps, exceed 0 pps
```

Task 5.2 Solution

https://t.me/learningnets

```
R2:

snmp-server engineID remote 172.16.10.100 12345CCCEEE
snmp-server group TRAP_GROUP v3 priv
snmp-server user TRAP_USER TRAP_GROUP remote 172.16.10.100 v3 auth sha CISCO priv 3des CISCO
!
snmp-server host 172.16.10.100 informs version 3 priv TRAP_USER
snmp-server source-interface informs loopback0
snmp-server enable traps envmon temperature

ASA4:

access-list GLOBAL_ACL permit udp host 150.1.2.2 host 172.16.10.100 eq 162
```

Task 5.2 Verification

Verify the remote SNMP engineID, required when SNMPv3 informs are configured:

```
R2#show  snmp engineID

Local SNMP engineID: 8000000903000000000000000
Remote Engine ID          IP-addr    Port12345CCCEE0E             remote  172.16.10.100   162
```

Verify the user and group settings:

https://t.me/learningnets

```
R2#show  snmp group | b TRAP_GROUP
groupname: TRAP_GROUP                       security model:v3 priv

contextname: <no context specified>         storage-type: nonvolatile
readview : v1default                        writeview: <no writeview specified>
notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
row status: active
!
!R2#show snmp user

User name: TRAP_USER

Engine ID: 12345CCCEE0E
storage-type: nonvolatile        active Authentication Protocol: SHA
Privacy Protocol: 3DES
Group-name: TRAP_GROUP
```

Verify that SNMP informs are configured for **TEST-SRV-A**:

```
R2#show snmp host
 Notification host: 172.16.10.100         udp-port: 162   type: inform
user: TRAP_USER security model: v3 priv
!
!R2#show  snmp | b SNMP informs
SNMP informs: enabled
    Informs in flight 0/25 (current/max) Logging to 172.16.10.100.162

        0 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped
```

Task 5.3 Solution

```
R6:

ip domain name inelab.local
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
!
login on-failure log every 1
login on-success log every 1
!
username ssh privilege 15 password cisco
```

https://t.me/learningnets

```
!
access-list 101 permit tcp 150.1.0.0 0.0.255.255 any eq 22
access-list 101 permit tcp any any eq telnet
!
!
line vty 0 15
 login local
 access-class 101 in
```

Task 5.3 Verification

Verify that telnet traffic is allowed from non-Loopback0 sources:

```
SW3#telnet 150.1.6.6
Trying 150.1.6.6 ... Open


User Access Verification
Username: ssh
Password:R6#show users

    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:16
*514 vty 0     ssh        idle                 00:00:00 140.1.63.11


  Interface    User               Mode         Idle     Peer Address
```

Verify that SSH is allowed only from Loopback0 sources:

https://t.me/learningnets

```
SW3#ssh -l ssh 150.1.6.6
% Connection refused by remote host

!
!R6#ssh -l ssh 150.1.6.6


Password:
R6#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 150.1.6.6            00:00:00
*514 vty 0     ssh        idle                 00:00:00 150.1.6.6


  Interface    User               Mode         Idle     Peer Address
```

Messages similar to the following are logged on each failed or successful session:

```
%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ssh] [Source: 140.1.63.11] [localport: 23] at 23:51:24 UTC Sun Mar
%SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ssh] [Source: 150.1.6.6] [localport: 22] [Reason: Login Authenticatio
```

Verify the login settings:

```
R6#show login

     No login delay has been applied.
     No Quiet-Mode access list has been configured. All successful login is logged.
 All failed login is logged.


     Router NOT enabled to watch for login Attacks
```

Task 5.4 Solution

```
R6:
router bgp 66
 neighbor 150.1.9.9 ebgp-multihop 2

SW1:
```

https://t.me/learningnets

```
router bgp 99
 neighbor 150.1.6.6 ebgp-multihop 2

ASA1:
access-list DMZ1_IN permit tcp host 150.1.6.6 host 150.1.9.9 eq 179
access-list OUTSIDE_IN permit tcp host 150.1.9.9 host 150.1.6.6 eq 179
!
!
access-list BGP extended permit tcp host 150.1.6.6 eq 179 host 150.1.9.9
access-list BGP extended permit tcp host 150.1.9.9 eq 179 host 150.1.6.6
access-list BGP extended permit tcp host 150.1.6.6 host 150.1.9.9 eq 179
access-list BGP extended permit tcp host 150.1.9.9 host 150.1.6.6 eq 179
!
tcp-map MD5_AUTH
 tcp-options range 19 19 allow
!
class-map BGP
 match access-list BGP
!
policy-map global_policy
 class BGP
  set connection random-sequence-number disable
  set connection advanced-options MD5_AUTH

IPS:

IPS(config)# service signature-definition sig0
IPS(config-sig)# signatures 1306 0
IPS(config-sig-sig)# status
IPS(config-sig-sig-sta)# enabled false
IPS(config-sig-sig-sta)# exit
IPS(config-sig-sig)# exit
IPS(config-sig)# exit
Apply Changes?[yes]:
```

Task 5.4 Verification

Verify that eBGP session is established:

```
R6#show ip bgp summary

BGP router identifier 150.1.6.6, local AS number 66
BGP table version is 1, main routing table version 1
```

https://t.me/learningnets

```
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
150.1.9.9       4           99       3       5        1    0    0 00:00:49        0

!
!R6#show ip bgp neighbors | i Option|TTL
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 2
Option Flags: nagle, path mtu capable, md5
```

Task 5.5 Solution

```
R2:

interface GigabitEthernet0/0.2
 no ip proxy-arp
!
ip icmp rate-limit unreachable 1000
no service dhcp
no ip bootp server
!
banner login $ Unathorized access to this device is prohibited $
```

Task 5.5 Verification

Verify that proxy-ARP is disabled:

```
R2#show ip interface gigabitEthernet 0/0.2 | i ARP
 Proxy ARP is disabled

  Local Proxy ARP is disabled
```

Verify the ICMP rate-limiting:

```
R2#show ip icmp rate-limit


                         DF bit unreachables       All other unreachables
Interval (millisecond)   1000                      1000


Interface                # DF bit unreachables     # All other unreachables
---------                ---------------------     ------------------------
```

https://t.me/learningnets

```
GigabitEthernet0/0.2       0                        1
GigabitEthernet0/0.72      0                        0
Loopback0                  0                        0

Greatest number of unreachables on GigabitEthernet0/0.2
```

Verify the banner login message:

```
R2#telnet 150.1.2.2
Trying 150.1.2.2 ... Open Unathorized access to this device is prohibited
username: TEST2
password:
R2#
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 1

CCIE SCv4 Lab 1 Solutions Section 6

1. Task 6.1 Solution
2. Task 6.2 Solution
3. Task 6.3 Solution
4. Task 6.4 Solution

Task 6.1 Solution

```
R5:

access-list 100 permit icmp any any echo
!
!
interface FastEthernet0/0.5
 rate-limit input access-group 100 64000 2000 2000 conform-action transmit exceed-action drop
```

Task 6.1 Verification

Verify the configured values:

```
R5#show interfaces fastEthernet0/0.5 rate-limit

FastEthernet0/0.5
  Input
    matches: access-group 100 params:  64000 bps, 2000 limit, 2000 extended limit
conformed 0 packets, 0 bytes; action: transmit
exceeded 0 packets, 0 bytes; action: drop

      last packet: 225098352ms ago, current burst: 0 bytes
      last cleared 00:00:23 ago, conformed 0 bps, exceeded 0 bps
```

https://t.me/learningnets

Task 6.2 Solution

Identify the MAC address of **TEST-SRV-A**; this will be different based on the rack being assigned:

```
SW1#show mac address-table interface fastEthernet1/0/4
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
5    0018.199f.161d    STATIC      Fa1/0/4
Total Mac Addresses for this criterion: 1

SW1:

interface FastEthernet1/0/4
 switchport port-security violation protect
 switchport port-security mac-address 0018.199f.161d
 switchport port-security aging static
 switchport port-security aging type inactivity
 switchport port-security aging time 10
 switchport port-security
```

Task 6.2 Verification

Verify the configured port-security settings:

```
SW1#show port-security interface fastEthernet1/0/4
Port Security              : Enabled
Port Status                : Secure-upViolation Mode             : Protect
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Enabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0Last Source Address:Vlan   : 0018.199f.161d:5
Security Violation Count   : 0
!
!SW1#show port-security address

          Secure Mac Address Table
```

https://t.me/learningnets

```
-----------------------------------------------------------------------
Vlan    Mac Address       Type                        Ports   Remaining Age
                                                                 (mins)
----    -----------       ----                        -----   -------------
5    0018.199f.161d    SecureConfigured           Fa1/0/4     10 (I)

-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 3072
```

Task 6.3 Solution

ASA1:

```
access-list ISE_TCP permit tcp any host 140.1.45.100
!
class-map ISE_TCP
 match access-list ISE_TCP
!
tcp-map ISE_MAP
 checksum-verification
 reserved-bits clear
 syn-data drop
 tcp-options range 6 7 allow
!
policy-map DMZ1
 class ISE_TCP
 set connection conn-max 5000 embryonic-conn-max 1000
 set connection advanced-options ISE_MAP
!
service-policy DMZ1 interface DMZ1
```

Task 6.3 Verification

Verify the configured settings:

```
ASA12# show service-policy interface DMZ1 set connection


Interface DMZ1:
  Service-policy: DMZ1
    Class-map: ISE_TCP Set connection policy: conn-max 1000 embryonic-conn-max 100
```

https://t.me/learningnets

```
        current embryonic conns 0, current conns -1, drop 0
      Set connection advanced-options: ISE_MAP
        Retransmission drops: 0                  TCP checksum drops : 0
        Exceeded MSS drops  : 0                  SYN with data drops: 0
        Invalid ACK drops   : 0                  SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0           OoO no buffer drops: 0
        OoO buffer timeout drops : 0             SEQ past window drops: 0
        Reserved bit cleared: 0                  Reserved bit drops : 0
        IP TTL modified     : 0                  Urgent flag cleared: 0
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0               Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

For testing purposes, allow TCP traffic on the inbound configured ACL and use packet-tracer to verify that configured settings are applied:

```
ASA1:
access-list DMZ1_IN permit tcp any host 140.1.45.100
!
!ASA12#packet-tracer input DMZ1 tcp 150.1.6.6 2000 140.1.45.100 80 detailed


Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xaba8c3e8, priority=1, domain=permit, deny=false
        hits=136466, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0100.0000.0000

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (INSIDE,DMZ1) 140.1.45.100 172.16.3.100 netmask 255.255.255.255
  match ip INSIDE host 172.16.3.100 DMZ1 any
```

https://t.me/learningnets

```
    static translation to 140.1.45.100
    translate_hits = 2, untranslate_hits = 31
Additional Information:
NAT divert to egress interface INSIDE
Untranslate 140.1.45.100/0 to 172.16.3.100/0 using netmask 255.255.255.255

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group DMZ1_IN in interface DMZ1
access-list DMZ1_IN extended permit tcp any host 140.1.45.100
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xabd66b20, priority=12, domain=permit, deny=false
        hits=13, user_data=0xa8b13900, cs_id=0x0, flags=0x0, protocol=6
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=140.1.45.100, mask=255.255.255.255, port=0, dscp=0x0
Phase: 4
Type: CONN-SETTINGS
Subtype: Result: ALLOW

Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xabc95d70, priority=8, domain=conn-set, deny=false
        hits=0, user_data=0xabd64d20, cs_id=0x0, flags=0x0, protocol=6
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=140.1.45.100, mask=255.255.255.255, port=0, dscp=0x0
```

Task 6.4 Solution

R5:

```
ip cef
ip nbar port-map http tcp 80 8080
!
class-map match-all WORM_ATTACK
 match protocol http url "*root.exe*"
!
policy-map WORM_ATTACK
 class WORM_ATTACK
  drop
```

https://t.me/learningnets

```
!
interface FastEthernet0/0.5
 ip nbar protocol-discovery
 service-policy input WORM_ATTACK
```

Task 6.4 Verification

Verify the configured policy:

```
R5#show policy-map interface fastEthernet0/0.5
 FastEthernet0/0.5

  Service-policy input: WORM_ATTACK
 Class-map: WORM_ATTACK (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps Match: protocol http url "*root.exe*"
drop


    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Verify NBAR identified protocols:

```
R5#ping 172.16.10.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.100, timeout is 2 seconds:.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
!
!R5#show ip nbar protocol-discovery interface fastEthernet0/0.5

 FastEthernet0/0.5

 Last clearing of "show ip nbar protocol-discovery" counters 00:04:51


                            Input                  Output
                            -----                  ------
   Protocol                 Packet Count           Packet Count
                            Byte Count             Byte Count
                            5min Bit Rate (bps)    5min Bit Rate (bps)
```

https://t.me/learningnets

```
                          5min Max Bit Rate (bps)  5min Max Bit Rate (bps)
   ----------------------- ----------------------- -----------------------
icmp                      4                         10

                          472                       1180
                          0                         0
                          0                         0
   Total                  4                         10
                          472                       1180
                          0                         0
                          0                         0
```

Verify that traffic on both TCP port 80 and TCP port 8080 is identified by NBAR as HTTP traffic:

```
R5#show ip nbar port-map http
 port-map http                         tcp 80 8080

```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 2

CCIE SCv4 Lab 2 Introduction

Lab Guidelines

The following scenarios are practice labs designed to test your readiness for the Cisco Systems CCIE Security Lab Exam. However, remember that in addition to being designed as a simulation of the actual CCIE lab exam, these practice labs should be used as a learning tool. Instead of rushing through the labs to complete all the configuration steps, take the time to research the networking technology and gain a deeper understanding of the principles behind its operation. For each lab of the CCIE Security Practice Labs Workbook, follow these guidelines:

- Read the entire lab exam before starting the configuration, and correlate tasks within a section to get a complete overview of the lab objectives.
- There are dependencies between tasks of the same section and between tasks from different sections. Carefully read throughout the lab to identify and make notes of it
- The lab consists of six sections that don't necessarily need to be completed in the presented order. However some tasks must be completed before others (such as initialization of ASA firewalls).
- All sections total 100 points, and you must earn a minimum of 80 points to receive a passing grade. To earn the points assigned to each task, you must fulfill all requirements and conform to all restrictions.
- No partial credit is awarded. You will earn all points or zero points for each task; if multiple solutions are available for a task, choose the one that technically best meets the requirements.
- Some tasks present a set of requirements for implementing a technology, and some tasks present outputs to be matched.
- Labs include both configuration and troubleshooting tasks; the number of faults relevant to each troubleshooting task may or not be specified.
- Before starting the exam, verify that all equipment is functional, powered up and that you can access it at the console.
- Routers and switches are preconfigured, do not change it unless specifically allowed

https://t.me/learningnets

by the task. On troubleshooting tickets, you may change any of the initial configurations.

- IPv4/IPv6 static and default routes are allowed to complete any task, but only if this is the only available option, and unless otherwise stated in any task.
- Make sure you do not to lock yourself out of any device, because password recovery or device reset is not available in the lab.
- At the end of the exam, ensure that all devices are accessible at the console by using preconfigured credentials or the ones from specific task requirements.
- For IPv4/IPv6 addressing configuration, the following variables will be used as a reference:
  - **X** is the rack number; the value for **Rack1** will be **1**.
  - **Y** is the device number, with routers ranging from one (1) to seven (7), switches from nine (9) to fourteen (14), and ASA firewalls from fifteen (15) to eighteen (18); the value for **Router1** will be **1**, **Switch1** will be **9**, and **ASA1** will be **15**.

All routers and switches are accessible at the console without requiring any authentication; do not change this. To access other devices within the lab, use the following tables as a reference:

Device	Username	Password
TESTPC-A	ineadmin	ciscoccie
TESTSRV-A	Administrator	Cisco1234
TESTPC-B	ineadmin	ciscoccie
TESTSRV-B	Administrator	Cisco1234
TESTPC-WIFI	ineadmin	ciscoccie

Device	Username	Password
WSA CLI&GUI	admin	default1A

https://t.me/learningnets

Device	Username	Password
ACS1 CLI	admin	default1A
ACS1 GUI	acsadmin	default1A
ACS2 CLI	admin	default1A
ACS2 GUI	acsadmin	default1A
ISE1 CLI&GUI	admin	default1A
ISE2 CLI&GUI	admin	default1A
WLC CLI&GUI	admin	default1A
LAP CLI	cisco	Cisco
IPS CLI&GUI	cisco	ciscoips4240

Lab Instructions

Before you begin, make sure that the initial configuration scripts for each lab have been applied. If you have any questions related to the scenario solutions, visit our CCIE support forum at http://IEOC.com. Refer to the attached physical and logical diagrams on each lab for interface and protocol assignments; you may access these by clicking the **Resources** button in the upper-right corner. Upon lab completion, end-to-end IPv4/IPv6 connectivity is not a requirement unless specifically asked for, but you are required to meet task requirements and restrictions.

Lab Restrictions

Each lab scenario contains explicit general restrictions that you must conform to while configuring the lab. These restrictions are defined in the introductory section for each scenario. Examples of such restrictions include, but are not limited to, not adding additional IP addressing, not changing the default authentication methods,

https://t.me/learningnets

etc. There may also be certain restrictions for particular tasks within a lab scenario. Examples of these restrictions include, but are not limited to, not issuing a particular configuration command, not using the legacy configuration for a technology, etc.

TIP

You may do whatever is necessary to complete a task unless the general requirements for the lab scenario or the specific requirements for the task explicitly prohibit you from doing so. This may include using static routing, NAT statements, ACL exceptions, IPsec/GRE tunneling, etc.

Difficulty Rating

Each lab scenario has been assigned a difficulty rating. Ratings are on a scale of one (1) to ten (10), with 10 being the most difficult. Labs are designed to be more technically challenging than the actual CCIE Security Lab Exam. Do not be discouraged if you score low or do not understand a particular set of technologies. If you are having trouble with a certain area, do not hesitate to read the explanation contained within the solutions guide and study the respective technology using the Technologies Workbook or the Advanced Technologies video course. Remember that these labs are designed to teach you required skills for implementing and troubleshooting a complex network with several technologies mixed together, just as much as they are intended to test your current technical knowledge.

Point Values

As in the actual CCIE Lab exam, each task within a lab is assigned a specific point value. Points are awarded only if the presented solution meets all the given requirements and does not violate any restrictions. No partial credit is awarded for any task. A minimum score of 80 points is required to pass a particular scenario. Some tasks have multiple solutions; as long as the presented solution meets the given requirements, points will be awarded for that task. However, certain solutions may negatively affect previous or future tasks. Make sure that you carefully read all presented requirements and try your best to come up with a technically appropriate solution.

TIP

https://t.me/learningnets

Points will never be awarded for a task in which you have violated the requirements. However, remember the relative point value of the task in question as compared to future tasks. If you cannot find an appropriate solution for a particular task, it is advisable to solve the task by whatever means necessary to complete the future tasks that depend on it.

Loading Initial Config

Each lab contains a set of initial configuration scripts for routers and switches. These configuration scripts include basic Layer 2 and Layer 3 routing connectivity (as well as possible more advanced functionalities for troubleshooting tickets), and must be loaded on your rack before beginning the configuration of the scenario. These are available to be loaded from the Rack Rental Control Panel, or if you are using your own rack, they are attached to each individual lab and available for download. Initial configurations and physical and logical diagrams of each lab are attached to this Introduction; you may access these by clicking the **Resources** button in the upper-right corner.

Rack Rentals

INE has designed the CCIE Security Practice Labs Workbook based around the publicly stated hardware specification used in the actual CCIE Lab exam. To eliminate the cost of buying all the equipment used in the workbook, INE offers cost-effective equipment rentals specifically designed to be used with this and other self-paced training product lines. For more information on rack rentals. visit http://INE.com.

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 2

CCIE SCv4 Lab 2 Tasks

1. Perimeter Security and Services
2. Intrusion Prevention and Content Security
3. Confidentiality and Secure Access
4. Identity Management
5. System Hardening and Availability
6. Threat Identification and Mitigation

Difficulty Rating (10 highest): 8

Point Values

The point values for each section are as follows:

Section	Point Value
Perimeter Security and Services	23
Intrusion Prevention and Content Security	18
Confidentiality and Secure Access	18
Identity Management	14
System Hardening and Availability	15

https://t.me/learningnets

Section	Point Value
Threat Identification and Mitigation	12

GOOD LUCK!

TIP

In the CCIE lab exam, you will be provided with a few sheets of scratch paper for notes and diagrams. You should create two diagrams at a minimum: one for the logical layer 2 topology and one for the logical layer 3 topology. Note that the physical diagram and the logical layer 2 diagram are not the same.

Although you are provided with the logical Layer 3 diagram in the lab, it will be in electronic format, which means that you cannot add notes to it and may need to switch between windows to see it on the computer. By having your own diagram, you will be able to take notes on it and quickly reference it as you work through the configuration section. Finally, drawing the Layer 2 and Layer 3 topologies will help you become familiar with a complex network toplogy at first sight.

---

1. Perimeter Security and Services

1.1 ASA Routed Mode (3 points)

- Configure ASA1 in routed single mode with a hostname of **ASA1**, using the information from the table:

Interface	Nameif	Security Level	IPv4 Address
E0/0	OUTSIDE	0	130.1.55.Y/24
E0/1.15	ISE	50	172.16.3.1/24

https://t.me/learningnets

Interface	Nameif	Security Level	IPv4 Address
E0/1.19	PHONE	100	130.1.19.Y/24
E0/1.91	TESTPC	100	130.1.91.Y/24
E0/1.54	INSIDE	50	130.1.54.Y/24

- Enable RIP on ASA1, do not advertise VLAN 15 prefix.
- ASA1 should send RIP updates only on its **OUTSIDE** and **INSIDE** interfaces.
- Additionally ASA1 should advertise a default route only to R4.

1.2 ASA Routed Mode (3 points)

- Configure ASA2 in routed single mode with a hostname of **ASA2**, using the information from the table:

Interface	Nameif	Security Level	IPv4 Address
E0/0	OUTSIDE	10	130.1.18.Y/24
E0/1	INSIDE	80	130.1.81.Y/24

- Enable EIGRP in AS 202 on ASA2, do not advertise VLAN 81 prefix.
- Configure ASA2 so that it is not queried in case of EIGRP re-convergence.

1.3 ASA Multiple Context Transparent (4 points)

- Configure ASA3 in transparent multiple mode with a hostname of **ASA34**, using the information from the table:

https://t.me/learningnets

Interface	Nameif	Security Level	Bridge-Group	BVI IPv4 Adress	Context Name	Context File
Gi0/0.31	OUTSIDE	20	13	130.1.13.Y/24	VLAN13	VLAN13.c
Gi0/0.61	OUTSIDE	20	16	130.1.16.Y/24	VLAN16	VLAN16.c
Gi0/1.13	INSIDE	70	13	130.1.13.Y/24	VLAN13	VLAN13.c
Gi0/1.16	INSIDE	70	16	130.1.16.Y/24	VLAN16	VLAN16.c

- Use a dedicated admin context.
- Configure trunk interfaces of SW1 and SW2 with VLAN 13 and VLAN 31 as native.
- Configure firewall rules as appropriate to ensure OSPF is functional between SW1, R3 and R6, considering it was preconfigured for unicast.

1.4 ASA Active-Active Failover (3 points)

- Configure ASA3 and ASA4 for secure stateful failover so that ASA3 is forwarding for context **VLAN13** and ASA4 for context **VLAN16**.
- Match the following output from ASA3:

```
ASA34/act# show failover interface

        interface FAILOVER GigabitEthernet0/2
                System IP Address: 130.1.100.17 255.255.255.0
                My IP Address    : 130.1.100.17
                Other IP Address : 130.1.100.18
```

- Match the following output from ASA3:

```
ASA34/VLAN13/act# show failover

Failover On
Last Failover at: 09:38:48 UTC Apr 1 2014
        This context: Active
```

https://t.me/learningnets

```
                Active time: 1234 (sec)
                  Interface OUTSIDE (130.1.13.17): Normal (Monitored)
                  Interface INSIDE (130.1.13.17): Normal (Monitored)
        Peer context: Standby Ready
                Active time: 0 (sec)
                  Interface OUTSIDE (130.1.13.18): Normal (Monitored)
                  Interface INSIDE (130.1.13.18): Normal (Monitored)
```

- Match the following output from ASA4:

```
ASA34/VLAN16/act# show failover

Failover On
Last Failover at: 09:42:17 UTC Apr 1 2014
        This context: Active
                Active time: 1081 (sec)
                  Interface OUTSIDE (130.1.16.17): Normal (Monitored)
                  Interface INSIDE (130.1.16.17): Normal (Monitored)
        Peer context: Standby Ready
                Active time: 208 (sec)
                  Interface OUTSIDE (130.1.16.18): Normal (Monitored)
                  Interface INSIDE (130.1.16.18): Normal (Monitored)
```

1.5 ASA Transparent Security (3 points)

- Configure the ASA failover pair to secure ARP traffic between SW1 and R3.
- Drop all ARP traffic for unknown mappings.

1.6 ASA NAT (2 points)

- Configure ASA2 so that no traffic is allowed to pass through unless being NAT'ed.
- VLAN 81 traffic should be dynamically translated into pool 130.X.8.1-130.X.8.31.
- When all IPv4 addresses from pool have been exhausted, ASA2 should NAT traffic into its **OUTSIDE** interface.
- For testing purposes, telnet traffic from VLAN 81 to SW1 should work.

1.7 ZBPF Transparent Mode (3 points)

https://t.me/learningnets

- Configure R7 for ZBPF, using two zones named **VLAN17** and **VLAN76**.
- For TCP, UDP and ICMP traffic initiated from **VLAN76**, R7 should create sessions in the firewall state table.
- For the above firewall policy, police ICMP traffic to 64Kbps with a burst value of 16Kbps.
- For traffic destined to R7 from **VLAN17**, allow only ICMP Echo and Echo-Reply.

1.8 ZBPF Tuning (3 points)

- Modify the default settings on R7 so that for the configured firewall policy:
  - it allows DHCP traffic to pass through without being inspected.
  - it allows a maximum of 100 embryonic sessions before it starts clamping and stops when session number reaches 80.
  - it denies access to a host for 10 minutes if the number of embryonic sessions for that host exceeds 10.
  - it closes TCP sessions after 120 seconds of no traffic and UDP sessions after 10 seconds.

2. Intrusion Prevention and Content Security

2.1 IPS Initialization (3 points)

- Initialize the IPS using the information from the table:

Variables	Values
Hostname	IPS
IPv4 Address	130.1.9.100/24
Default Gateway	130.1.9.10
Telnet	Enabled
Login Banner	This is IPS from CCIE Lab Exam

https://t.me/learningnets

Variables	Values
Management Access	130.1.9.0/24
Management Access	130.1.91.0/24
Management Type	HTTP Port 8080

- To protect the IPS web service against possible attacks, configure it to diplay a value of **Unknown** instead of the default web server version.

2.2 IPS Inline Vlan-Pair (2 points)

- Configure the IPS inline between R2 and R3 using the information from the diagram.
- Ensure traffic between these VLANs is inspected by the IPS.

2.3 IPS Custom Signature (4 points)

- Configure a signature on IPS to detect password changes in telnet sessions and block the attacker for 15 minutes.
  - the signature should not be case-sensitive and match on string **password**.
- Additionally, generate an alarm of maximum fidelity and severity.
  - for telnet sessions to R2's Loopback0, only the alarm should be triggered.
- Do not modify the event action override settings.

2.4 WSA Initialization (3 points)

- Initialize the WSA using the information from the table:

Variables	Values
Hostname	wsa.inelab.local

https://t.me/learningnets

Variables	Values
DNS Server	150.1.4.4
NTP Server	150.1.4.4
Proxy Ports	M1 and P1
M1 IPv4 Address	172.16.6.100/24
M1 Default Gateway	172.16.6.1
Admin Password	default1A
Email Address	ccielab@inelab.local
Senderbase Participation	Minimum

- Assign **TEST-PC-A** the IPv4 address of 130.1.91.100/24 for this scope with a default gateway of ASA1.
- WSA should allow management sessions from VLAN 91 only.
- Ensure VLAN 91 administrators can manage the WSA over HTTPS.

2.5 WSA WCCP Integration (3 points)

- Configure R1 to redirect HTTP traffic from VLAN 91, received inbound on its VLAN 51 interface to the WSA.
- Enabling P1 port in VLAN 76, match the output:

```
R1#show ip wccp 91 clients

WCCP Client information:
        WCCP Client ID:          130.1.76.100
        Protocol Version:        2.00
        State:                   Usable
        Redirection:             L2
```

https://t.me/learningnets

```
        Packet Return:          L2
        Assignment:             MASK
        Connect Time:           00:08:28
        Redirected Packets:
          Process:              0
          CEF:                  0
        GRE Bypassed Packets:
          Process:              0
          CEF:                  0
        Mask Allotment:         32 of 32 (100.00%)
```

- Configure R1 to allow only WSA as the WCCP client.

2.6 WSA Traffic Policies (3 points)

- Configure WSA to block access to URLs from **Computers and Internet** category.
  - ensure the policy applies only to VLAN 91 users.
  - create identity and access policy named **VLAN91** for this.

- Configure **TEST-PC-A** with IPv4 address from VLAN 91 and a DNS server of 150.1.4.4.
  - test that access to **www.cisco.com** is blocked.
  - test that access to **www.yahoo.com** is allowed.

- Both of te above are resolved to SW1's Loopback0 address.
- Without using proxy-bypass lists, match the following output when accessing **www.yahoo.com**, assuming that **TEST-PC-A** was assigned an IPv4 address of 130.1.91.100:

```
SW1#show ip http server history


HTTP server history:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes  end-time
      150.1.9.9:80       130.1.91.100:47264 472        192        03:18:07 03/02
      150.1.9.9:80       130.1.91.100:45593 472        192        03:18:50 03/02
```

https://t.me/learningnets

3. **Confidentiality and Secure Access**

3.1 ASA IPsec Routing (3 points)

- Configure a IKEv1 IPsec tunnel between ASA1 and ASA2, using 3DES, MD5 and DH group 5 as algorithms and PSK authentication.
- Enable OSPF routing over the tunnel to protect and advertise VLAN 15 and VLAN 81 prefixes.
- Both ASA's should be able to initiate the negotiation.
- Match the following output:

```
ASA1# show vpn-sessiondb l2l


Session Type: LAN-to-LAN

Connection   : ASA2.inelab.local
Index        : 6                     IP Addr      : 130.1.18.16
Protocol     : IKE IPsec
Encryption   : 3DES                  Hashing      : MD5
Bytes Tx     : 1012                  Bytes Rx     : 1064
Login Time   : 08:42:08 UTC Wed Apr 2 2014
Duration     : 0h:02m:01s
```

```
ASA2# show vpn-sessiondb l2l


    Session Type: LAN-to-LAN

    Connection   : ASA1.inelab.local
    Index        : 6                     IP Addr      : 130.1.55.15
    Protocol     : IKE IPsec
    Encryption   : 3DES                  Hashing      : MD5
    Bytes Tx     : 1540                  Bytes Rx     : 1420
    Login Time   : 08:42:06 UTC Wed Apr 2 2014
    Duration     : 0h:03m:03s
```

https://t.me/learningnets

- Once the tunnel is up, test using the following:

```
ISE1/admin# ping 130.1.81.16

ping 130.1.81.16
PING 130.1.81.16 (130.1.81.16) 56(84) bytes of data.
64 bytes from 130.1.81.16: icmp_seq=2 ttl=255 time=2.17 ms
64 bytes from 130.1.81.16: icmp_seq=3 ttl=255 time=1.56 ms
64 bytes from 130.1.81.16: icmp_seq=4 ttl=255 time=1.64 ms

--- 130.1.81.16 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3001ms
rtt min/avg/max/mdev = 1.565/1.793/2.175/0.273 ms
```

3.2 ASA AnyConnect SSL (3 points)

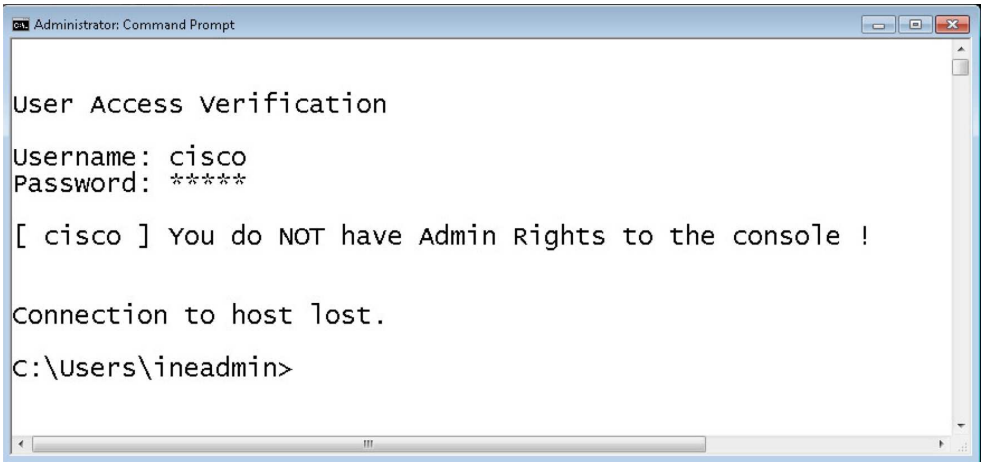
- Configure ASA2 for AnyConnect SSL session on its **OUTSIDE** interface.
- Authenticate sessions against the local database using **cisco/cisco** as username/password pair.
- Allocate IPv4 addresses from 130.200.0.0/24 subnnet and allow only traffic for VLAN 81 to be sent through the tunnel.
- Allow only client-based SSL VPN sessions and negotiate the use of UDP for traffic sent through the tunnel.
- Match the following output without allowing users to select or cache the connection-profile settings:

```
ASA2# show vpn-sessiondb svc | i CCIELAB

Group Policy : CCIELAB                Tunnel Group : CCIELAB
```

- Test from **TEST-PC-A** , by connecting to **130.1.18.16/CCIELAB**.
- Match the following output if users try to telnet on the **INSIDE** interface of the ASA and authenticate with the VPN user:

https://t.me/learningnets



3.3 EzVPN Remote Troubleshooting (3 points)

- R4 is configured as EzVPN server and R6 as EzVPN Remote to protect traffic between VLAN 44 and VLAN 69 subnets.
- R6 should authenticate using the username/password of **ezvpn/ezvpn**.
- Fix the configuration in order to match the output:

```
R6#show crypto ipsec client ezvpn

Easy VPN Remote Phase: 8

Tunnel name : EZVPN_CLIENT
Inside interface list: FastEthernet0/0.69
Outside interface: FastEthernet0/1
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Save Password: Disallowed
Split Tunnel List: 1
       Address    : 130.1.44.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Current EzVPN Peer: 150.1.4.4
```

- If firewall rules are required, use the minimum possible ACE entries.

https://t.me/learningnets

3.4 IPv4 VRF Aware DMVPN Troubleshooting (3 points)

- VRF named **DMVPN** has been configured on R1, R2 and R4.
- IPv4 VRF aware DMVPN has been configured on all three routers, with R4 being the hub.
- EIGRP AS 124 is the routing protocol used to advertise Loopback1 prefixes.
- Fix the configuration errors so that you match the following outputs:

```
R1#ping vrf DMVPN 150.1.22.22 source loopback1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.22.22, timeout is 2 seconds:
Packet sent with a source address of 150.1.11.11
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!
!R1#show ip route vrf DMVPN nhrp


Routing Table: DMVPN
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      150.1.0.0/16 is variably subnetted, 3 subnets, 2 masks
H        150.1.22.22/32 [250/1] via 130.1.220.2, 00:00:21, Tunnel0
```

- If firewall rules are required, use the minimum possible ACE entries.

3.5 IKEv2 FlexVPN Server-Client (3 points)

- Configure a IKEv2 IPsec tunnel between R1 an R2, with R1 being the FlexVPN client

https://t.me/learningnets

and R2 being the FlexVPN server.

- Tunnel should protect traffic between Loopback2 interfaces with IPv4 addresses in the format of **150.1.11X.Y/32**.
- Using the smart defaults, symmetric PSK authentication and IKEv2 routing, match the output:

```
R1#show crypto ikev2 client flexvpn


  Profile : R1_R2_CLIENT
  Current state:ACTIVE
  Peer : 130.1.32.2
  Source : GigabitEthernet0/0.11
  ivrf : IP DEFAULT
  fvrf : IP DEFAULT
  Backup group: Default
  Tunnel interface : Tunnel12
```

3.6 WLC PSK Authentication (3 points)

- Configure a WLAN on the WLC with the following parameters:

Variables	Values
Profile	CCIELAB
SSID	CCIELAB-RACK-X
VLAN	3
Authentication	WPA2 PSK
Encryption	AES and TKIP
PSK	thisisthewifikey

https://t.me/learningnets

Variables	Values
Interface	Management
WLC DHCP Server	No
IPv4 Subnet	172.16.5.0/24
Default Gateway	172.16.5.1

- WLC should filter all inbound traffic from the clients and allow only DNS and HTTP/HTTPS.
- Traffic between WiFi clients should be restricted.
- R3 has been preconfigured as DHCP server, ensure WiFi clients are assigned IPv4 addresses.
- Test that **WIFI-PC** is sucessfully authenticated.

4. Identity Management

4.1 IOS Authentication Proxy (4 points)

- Configure R6 to restrict all inbound traffic on its VLAN 6 interface and require users to authenticate.
- Once users are authenticated through the RADIUS server from ACS, all traffic should be allowed.
- Authentication should be triggered only by telnet traffic to SW2's Loopback0 address.
- Ensure to match the following settings:

Variables	Values
RADIUS Key	cisco
RADIUS Client Address	Loopback0

https://t.me/learningnets

Variables	Values
RADIUS Authorization	dACL
Auth-Proxy Username	AUTH-PROXY
Auth-Proxy Password	cisco
Auth-Proxy Inactivity Timeout	10 minutes

4.2 MAB Authentication and Authorization (6 points)

- Configure SW1 to authenticate both **TEST-PC-A** and **IP Phone** on its Fa1/0/5 interface using the ISE server.
- Source RADIUS packets from SW1's Loopback0 interface, use a PSK of **cisco** and a RADIU Service-Type of **Framed**.
- No static routes or NAT is allowed for this task.
- Match the following output for the device on the voice domain:

```
SW1#show authentication sessions mac 0003.6b3c.35f0

            Interface:  FastEthernet1/0/5
          MAC Address:  0003.6b3c.35f0
           IP Address:  130.1.19.16
            User-Name:  00036b3c35f0
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0000000000000005600173B64
      Acct Session ID:  0x00000057
               Handle:  0xF1000056
```

https://t.me/learningnets

```
Runnable methods list:
       Method   State
       mab      Authc Success
```

- Match the following output for the device in the data domain:

```
SW1#show authentication sessions mac 48f8.b32e.2423

            Interface:  FastEthernet1/0/5
          MAC Address:  48f8.b32e.2423
           IP Address:  130.1.91.100
            User-Name:  48f8b32e2423
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  91
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
      Session timeout:  3600s (server), Remaining: 3523s
       Timeout action:  Reauthenticate
         Idle timeout:  1800s (server), Remaining: 1723s
    Common Session ID:  00000000000000057001769EC
      Acct Session ID:  0x00000058
               Handle:  0x56000057

Runnable methods list:
       Method   State
       mab      Authc Success
```

- Enable critical VLAN for both data and voice domains.
- As the **IP Phone** does not support **CDP Enhancements for Second Port Disconnect** , configure SW1 to support MAC address change in the data VLAN.

4.3 IOS Local Authentication (2 points)

- Authenticate users logging into R6 using local case-sensitive database.

https://t.me/learningnets

- Configure users **RESTRICTED** and **UNRESTRICTED**, both with a password of **cisco**.
- Assign **RESTRCITED** user privilege-level of 0 and allow access to privilege-level 1 by using the password of **level1pass**.
- Assign **UNRESTRICTED** user a privilege-level of 15.

4.4 ASA Local Authorization (2 points)

- Configure ASA2 to allow SSH version 2 and ASDM sessions on port 4443 from Anyconnect VPN sessions on its **INSIDE** interface.
- Configure user **sshuser** with a password of **cisco** which is not allowed configuration access from ASDM.
- Configure user **unrestricted** with a password of **cisco**, which is allowed configuration access from both SSH and ASDM.
- Access to privilege-level 15 should be granted by the password of **cisco**.

5. System Hardening and Availability

5.1 Remotely Triggered Blackhole (3 points)

- An attack has been detected in the network, targeting a server in VLAN 66 with the IP address of 172.16.6.99.
- Consider R2 as being the trigger router using BGP in AS 126 to instruct edge routers of R1 and R6 to silently drop malicious traffic.
- Configure BGP peering based on Loopback0 IPv4 addresses.
- Ensure BGP sessions can be intiated by all routers.

5.2 ASA System Logging (3 points)

- Configure ASA2 for logging as follows:
  - emergency level messages to the console.
  - error level messages to SSH sessions.
  - debug level messages at the syslog server 172.16.3.99.
  - ensure debug messages don't appear to a monitor session.
  - timestamp all syslog messages.

5.3 Telnet DoS Prevention (3 points)

https://t.me/learningnets

- To mitigate a known telnet vulnerability, configure R5 to drop transit telnet sessions exiting its VLAN 51 interface.
- Do not use **match protocol** commands or any type of ACL filtering for this.
- Telnet traffic on non-standard ports should not be affected.

5.4 Traffic Suppression (2 points)

- Configure SW1 to provide traffic suppression if broadcasts traffic exceeds 5% of the maximum bandwidth on its Fa1/0/1 and Fa1/0/2 ports.
- Disable the ports if policy is violated and automatically recover it after 10 minutes.

5.5 IOS Time Synchronization (3 points)

- Configure R3 as the NTP server.
- R2 should synchronize its time via unicast from R3 and authenticate it with a password of **ntpkeyunicast**.
- SW1 should synchronize its time via broadcast from R3 and authenticate it with a password of **ntpkeybroadcast**.
- Ensure R3 ignores all NTP packets received on its VLAN 3 interface.

6. **Threat Identification and Mitigation**

6.1 Preventing DHCP Attacks (3 points)

- Configure ASA1 as DHCP server for both VLAN 19 and VLAN 91, allocate IPv4 addresses starting with **.16** in the last octet.
- Each leased IPv4 address is valid for 4 hours unless renegotiated.
- Configure SW1 to protect VLAN 3, VLAN 19 and VLAN 91 from spoofed DHCP servers allocating rogue IPv4 addresses.

6.2 IPv6 First-Hop Security (3 points)

- R4 has been precomfigured for IPv6 routing and with IPv6 addresses on its Fa0/1 interface.
- Configure SW4 to drop all IPv6 RA messages in VLAN 44 unless coming from R4.
- Additionally R4 should perform following checks on IPv6 RA messages received from R4:

https://t.me/learningnets

- allow it only if sourced from its configured **FE80::4** IPv6 link-local address.
- allow it only for its configured IPv6 prefix of **2004:44::/64**.

6.3 Preventing STP Attacks (2 points)

- To avoid any accidental changes in the STP domain, configure SW1 to:
  - disable all portfast enabled ports if a BPDU is received.
  - move its trunk ports to SW5 and SW6 into **inconsistent** state if a superior BPDU is received.

- SW1 has been preconfigured with the lowest STP priority among all switches.

6.4 IPS Traffic Optimization (2 points)

- SW3 constantly floods the IPS with traffic causing the following log messages on the IPS:

```
IPS# packet display gigabitEthernet0/1

Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
05:41:18.583000 01:00:0c:cc:cc:cd (oui Unknown) > 44:d3:ca:63:99:89 (oui Unknown) SNAP Unnumbered, ui, Flags [Co
05:41:18.583000 01:00:0c:cc:cc:cd (oui Unknown) > 44:d3:ca:63:99:89 (oui Unknown) SNAP Unnumbered, ui, Flags [Co
```

- Configure SW3 so that such messages dissapear.

6.5 Mitigating IPv4 Address Spoofing (2 points)

- Configure R1 to prevent IPv4 address spoofing inbound on its VLAN 17 interface.
- All packets without a strict verifiable source IPv4 address should be dropped.
- Match the follwoign output:

https://t.me/learningnets

```
R1#ping 130.1.76.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 130.1.76.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 2

CCIE SCv4 Lab 2 Solutions Section 1

1. Task 1.1 Solution
2. Task 1.2 Solution
3. Task 1.3 Solution
4. Task 1.4 Solution
5. Task 1.5 Solution
6. Task 1.6 Solution
7. Task 1.7 Solution
8. Task 1.8 Solution

Task 1.1 Solution

SW1:

```
interface FastEthernet1/0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 15,19,91,54
 no shutdown
```

SW2:

```
interface FastEthernet1/0/12
 switchport mode access
 switchport access vlan 55
 no shutdown
```

ASA1:

```
hostname ASA1
!
interface Ethernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 130.1.55.15 255.255.255.0
 rip authentication mode md5
```

https://t.me/learningnets

```
 rip authentication key cisco key_id 1
 no shutdown
!
interface Ethernet0/1
 no shutdown
!
interface Ethernet0/1.15
 vlan 15
 ip address 172.16.3.1 255.255.255.0
 nameif ISE
 security-level 50
!
interface Ethernet0/1.19
 vlan 19
 ip address 130.1.19.15 255.255.255.0
 nameif PHONE
 security-level 100
!
interface Ethernet0/1.91
 vlan 91
 ip address 130.1.91.15 255.255.255.0
 nameif TESTPC
 security-level 100
!
interface Ethernet0/1.54
 vlan 54
 ip address 130.1.54.15 255.255.255.0
 nameif INSIDE
 security-level 50
!
access-list RIP_DEFAULT standard deny host 0.0.0.0
access-list RIP_DEFAULT standard permit any
!
router rip
 version 2
 no auto-summary
 network 130.1.0.0
 passive-interface default
 no passive-interface OUTSIDE
 no passive-interface INSIDE
 default-information originate
 distribute-list RIP_DEFAULT out interface OUTSIDE
```

https://t.me/learningnets

Task 1.1 Verification

To identify the clear-text password string used for RIP authentication, issue the **show key chain** command:

```
R5#show key chain
Key-chain RIP: key 1 -- text "cisco"

        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
```

Verify the switch-level port configuration:

```
SW1#show interfaces fastEthernet1/0/13 trunk


Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/13    on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa1/0/13    15,19,54,91

Port        Vlans allowed and active in management domain
Fa1/0/13    15,19,54,91

Port        Vlans in spanning tree forwarding state and not pruned Fa1/0/13    15,19,54,91
!
!SW2#show interfaces fastEthernet1/0/12 switchport

Name: Fa1/0/12
Switchport: Enabled
Administrative Mode: static access Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off Access Mode VLAN: 55 (VLAN0055)

Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
```

https://t.me/learningnets

```
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Verify security-level, nameif, and IPv4 addressing:

```
ASA1# show nameif
Interface                Name                    Security
Ethernet0/0              OUTSIDE                   0
Ethernet0/1.15           ISE                      50
Ethernet0/1.19           PHONE                   100
Ethernet0/1.54           INSIDE                   50
Ethernet0/1.91           TESTPC                  100
!
!ASA1# show ip address

System IP Addresses:
Interface                Name                    IP address      Subnet mask     Method
Ethernet0/0              OUTSIDE                 130.1.55.15     255.255.255.0   manual
Ethernet0/1.15           ISE                     172.16.3.1      255.255.255.0   manual
Ethernet0/1.19           PHONE                   130.1.19.15     255.255.255.0   manual
Ethernet0/1.54           INSIDE                  130.1.54.15     255.255.255.0   manual
Ethernet0/1.91           TESTPC                  130.1.91.15     255.255.255.0   manual
Current IP Addresses:
Interface                Name                    IP address      Subnet mask     Method
Ethernet0/0              OUTSIDE                 130.1.55.15     255.255.255.0   manual
Ethernet0/1.15           ISE                     172.16.3.1      255.255.255.0   manual
Ethernet0/1.19           PHONE                   130.1.19.15     255.255.255.0   manual
Ethernet0/1.54           INSIDE                  130.1.54.15     255.255.255.0   manual
Ethernet0/1.91           TESTPC                  130.1.91.15     255.255.255.0   manual
```

https://t.me/learningnets

Verify that RIP routes are being learned from both 4 and R5:

```
ASA1# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    172.16.3.0 255.255.255.0 is directly connected, ISE
R    130.1.11.0 255.255.255.0 [120/2] via 130.1.55.5, 0:00:26, OUTSIDE
R    130.1.13.0 255.255.255.0 [120/2] via 130.1.55.5, 0:00:26, OUTSIDE
C    130.1.19.0 255.255.255.0 is directly connected, PHONE
R    130.1.18.0 255.255.255.0 [120/2] via 130.1.55.5, 0:00:26, OUTSIDE
R    130.1.16.0 255.255.255.0 [120/2] via 130.1.55.5, 0:00:26, OUTSIDE
R    130.1.44.0 255.255.255.0 [120/1] via 130.1.54.4, 0:00:26, INSIDE
R    130.1.51.0 255.255.255.0 [120/1] via 130.1.55.5, 0:00:26, OUTSIDE
C    130.1.55.0 255.255.255.0 is directly connected, OUTSIDE
C    130.1.54.0 255.255.255.0 is directly connected, INSIDE
R    130.1.76.0 255.255.255.0 [120/2] via 130.1.55.5, 0:00:26, OUTSIDE
C    130.1.91.0 255.255.255.0 is directly connected, TESTPC
R    150.1.9.9 255.255.255.255 [120/2] via 130.1.55.5, 0:00:26, OUTSIDE
R    150.1.5.5 255.255.255.255 [120/2] via 130.1.55.5, 0:00:26, OUTSIDE
R    150.1.1.1 255.255.255.255 [120/2] via 130.1.55.5, 0:00:00, OUTSIDE
R    150.1.4.4 255.255.255.255 [120/1] via 130.1.54.4, 0:00:00, INSIDE
```

Verify that ASA1 sends RIP updates only on its **OUTSIDE** and **INSIDE** interface and that RIP packets are authenticated through MD5:

```
ASA1# debug rip events
 RIP event debugging is on
ASA1# RIP: received packet with MD5 authentication
RIP: received v2 update from 130.1.55.5 on OUTSIDE
     130.1.11.0255.255.255.0 via 0.0.0.0 in 2 hops
     130.1.13.0255.255.255.0 via 0.0.0.0 in 2 hops
     130.1.16.0255.255.255.0 via 0.0.0.0 in 2 hops
     130.1.18.0255.255.255.0 via 0.0.0.0 in 2 hops
     130.1.51.0255.255.255.0 via 0.0.0.0 in 1 hops
     130.1.76.0255.255.255.0 via 0.0.0.0 in 2 hops
```

https://t.me/learningnets

```
     150.1.1.1255.255.255.255 via 0.0.0.0 in 2 hops
     150.1.5.5255.255.255.255 via 0.0.0.0 in 2 hops
     150.1.9.9255.255.255.255 via 0.0.0.0 in 2 hops
RIP: Update contains 9 routesRIP: sending v2 update to 224.0.0.9 via OUTSIDE (130.1.55.15)
RIP: build update entries
        130.1.19.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        130.1.44.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        130.1.54.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        130.1.91.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        150.1.4.4 255.255.255.255 via 0.0.0.0, metric 2, tag 0
RIP: Update contains 5 routes
RIP: Update queuedRIP: sending v2 update to 224.0.0.9 via INSIDE (130.1.54.15)
RIP: build update entries
        0.0.0.0 0.0.0.0 via 0.0.0.0, metric 1, tag 0
        130.1.11.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        130.1.13.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        130.1.16.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        130.1.18.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        130.1.19.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        130.1.51.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        130.1.55.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        130.1.76.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        130.1.91.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        150.1.1.1 255.255.255.255 via 0.0.0.0, metric 3, tag 0
        150.1.5.5 255.255.255.255 via 0.0.0.0, metric 3, tag 0
        150.1.9.9 255.255.255.255 via 0.0.0.0, metric 3, tag 0
RIP: Update contains 13 routes
RIP: Update queuedRIP: Update sent via OUTSIDE rip-len:152
RIP: Update sent via INSIDE rip-len:272
```

Verify that R4 receives the RIP default route from ASA1, and R5 does not:

```
R4#show ip rip database 0.0.0.0 0.0.0.0
0.0.0.0/0 [1] via 130.1.54.15, 00:00:00, FastEthernet0/0
!
!R4#show ip route rip

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
```

https://t.me/learningnets

```
       + - replicated route, % - next hop override

Gateway of last resort is 130.1.54.15 to network 0.0.0.0
R*    0.0.0.0/0 [120/1] via 130.1.54.15, 00:00:11, FastEthernet0/0
      130.1.0.0/16 is variably subnetted, 13 subnets, 2 masks
R        130.1.11.0/24 [120/3] via 130.1.54.15, 00:00:11, FastEthernet0/0
R        130.1.13.0/24 [120/3] via 130.1.54.15, 00:00:11, FastEthernet0/0
R        130.1.16.0/24 [120/3] via 130.1.54.15, 00:00:11, FastEthernet0/0
R        130.1.18.0/24 [120/3] via 130.1.54.15, 00:00:11, FastEthernet0/0
R        130.1.19.0/24 [120/1] via 130.1.54.15, 00:00:11, FastEthernet0/0
R        130.1.51.0/24 [120/2] via 130.1.54.15, 00:00:11, FastEthernet0/0
R        130.1.55.0/24 [120/1] via 130.1.54.15, 00:00:11, FastEthernet0/0
R        130.1.76.0/24 [120/3] via 130.1.54.15, 00:00:11, FastEthernet0/0
R        130.1.91.0/24 [120/1] via 130.1.54.15, 00:00:11, FastEthernet0/0
      150.1.0.0/32 is subnetted, 4 subnets
R        150.1.1.1 [120/3] via 130.1.54.15, 00:00:11, FastEthernet0/0
R        150.1.5.5 [120/3] via 130.1.54.15, 00:00:11, FastEthernet0/0
R        150.1.9.9 [120/3] via 130.1.54.15, 00:00:11, FastEthernet0/0
!
!R5#show ip rip database 0.0.0.0 0.0.0.0
%Route not in database
!
!R5#show ip route rip

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      130.1.0.0/16 is variably subnetted, 13 subnets, 2 masks
R        130.1.19.0/24 [120/1] via 130.1.55.15, 00:00:11, FastEthernet0/0
R        130.1.44.0/24 [120/2] via 130.1.55.15, 00:00:11, FastEthernet0/0
R        130.1.54.0/24 [120/1] via 130.1.55.15, 00:00:11, FastEthernet0/0
R        130.1.91.0/24 [120/1] via 130.1.55.15, 00:00:11, FastEthernet0/0
      150.1.0.0/32 is subnetted, 4 subnets
R        150.1.4.4 [120/2] via 130.1.55.15, 00:00:11, FastEthernet0/0
```

https://t.me/learningnets

Task 1.2 Solution

```
SW1:
interface FastEthernet1/0/15
 switchport mode access
 switchport access vlan 81
 no shutdown

SW2:
interface FastEthernet1/0/14
 switchport mode access
 switchport access vlan 18
 no shutdown

ASA1:

hostname ASA2
!
interface Ethernet0/0
 nameif OUTSIDE
 security-level 10
 ip address 130.1.18.16 255.255.255.0
 no shutdown
!
interface Ethernet0/1
 nameif INSIDE
 security-level 80
 ip address 130.1.81.16 255.255.255.0
 no shutdown
!
router eigrp 202
 no auto-summary
 network 130.1.18.0 255.255.255.0
 eigrp stub connected
```

Task 1.2 Verification

Verify that switch ports are active in the correct VLANs:

```
SW1#show spanning-tree interface fastEthernet1/0/15

Vlan                Role Sts Cost      Prio.Nbr Type
```

https://t.me/learningnets

```
------------------- ---- --- --------- -------- --------------------------------
VLAN0081            Desg FWD 19        128.17   P2p

!
!SW2#show spanning-tree interface fastEthernet1/0/14

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
VLAN0018            Desg FWD 19        128.16   P2p
```

Verify that EIGRP is functional and ASA2 learns prefixes:

```
ASA2# show eigrp neighbors

EIGRP-IPv4 neighbors for process 202
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   130.1.18.1              Et0/0            11  00:03:05 1    200   0   23
!
!ASA2# show route OUTSIDE


Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
D    130.1.11.0 255.255.255.0 [90/28416] via 130.1.18.1, 0:03:37, OUTSIDE

D EX 130.1.13.0 255.255.255.0 [170/54016] via 130.1.18.1, 0:03:37, OUTSIDE
D EX 130.1.19.0 255.255.255.0 [170/54016] via 130.1.18.1, 0:03:37, OUTSIDE
C    130.1.18.0 255.255.255.0 is directly connected, OUTSIDE
D EX 130.1.16.0 255.255.255.0 [170/54016] via 130.1.18.1, 0:03:37, OUTSIDE
D EX 130.1.44.0 255.255.255.0 [170/54016] via 130.1.18.1, 0:03:37, OUTSIDE
D    130.1.51.0 255.255.255.0 [90/28416] via 130.1.18.1, 0:03:37, OUTSIDE
D EX 130.1.55.0 255.255.255.0 [170/54016] via 130.1.18.1, 0:03:37, OUTSIDE
D EX 130.1.54.0 255.255.255.0 [170/54016] via 130.1.18.1, 0:03:37, OUTSIDE
D    130.1.76.0 255.255.255.0 [90/28416] via 130.1.18.1, 0:03:37, OUTSIDE
D EX 130.1.91.0 255.255.255.0 [170/54016] via 130.1.18.1, 0:03:37, OUTSIDE
D EX 150.1.4.4 255.255.255.255 [170/54016] via 130.1.18.1, 0:03:37, OUTSIDE
```

https://t.me/learningnets

```
D    150.1.5.5 255.255.255.255 [90/156416] via 130.1.18.1, 0:03:37, OUTSIDE
D    150.1.9.9 255.255.255.255 [90/156416] via 130.1.18.1, 0:03:37, OUTSIDE
D    150.1.1.1 255.255.255.255 [90/130816] via 130.1.18.1, 0:03:38, OUTSIDE
```

Verify that ASA2 does not advertise its VLAN 81 prefix into EIGRP, and that it is configured as stub:

```
R1#show ip eigrp topology 130.1.81.0 255.255.255.0
EIGRP-IPv4 Topology Entry for AS(202)/ID(150.1.1.1)%Entry 130.1.81.0/24 not in topology table
!
!R1#show ip eigrp neighbors detail gigabitEthernet0/0.18
EIGRP-IPv4 Neighbors for AS(202)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
2   130.1.18.16             Gi0/0.18                 14 00:05:03    1   150  0  7
   Version 8.4/3.0, Retrans: 1, Retries: 0
   Topology-ids from peer - 0 Stub Peer Advertising (CONNECTED ) Routes
Suppressing queries


BFD sessions
 NeighAddr         Interface
```

Task 1.3 Solution

```
SW1:
interface FastEthernet1/0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 13,16
 switchport trunk native vlan 13
 no shutdown
!
vlan dot1q tag native

SW2:

interface FastEthernet1/0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 31,61
 switchport trunk native vlan 31
 no shutdown
```

https://t.me/learningnets

```
!
vlan dot1q tag native
```

First, convert ASA3 into multiple-context mode:

```
ciscoasa(config)# mode multiple
 WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]

ASA3 System Context:
firewall transparent
hostname ASA34
!
interface GigabitEthernet0/0
 no shutdown
!
interface GigabitEthernet0/0.31
 vlan 31
!
interface GigabitEthernet0/0.61
 vlan 61
!
interface GigabitEthernet0/1
 no shutdown
!
interface GigabitEthernet0/1.13
 vlan 13
!
interface GigabitEthernet0/1.16
 vlan 16
!
!
delete /noconfirm disk0:/*.cfg
!
!
context VLAN13
 allocate-interface GigabitEthernet0/0.31
 allocate-interface GigabitEthernet0/1.13
 config-url disk0:/VLAN13.cfg
!
context VLAN16
 allocate-interface GigabitEthernet0/0.61
 allocate-interface GigabitEthernet0/1.16
```

https://t.me/learningnets

```
 config-url disk0:/VLAN16.cfg
!
admin-context admin
context admin
 config-url disk0:/admin.cfg

ASA3 VLAN13 Context:
interface GigabitEthernet0/0.31
 nameif OUTSIDE
 security-level 20
 bridge-group 13
!
interface GigabitEthernet0/1.13
 nameif INSIDE
 security-level 70
 bridge-group 13
!
interface Bvi13
 ip address 130.1.13.17 255.255.255.0
!
access-list OUTSIDE_IN extended permit ospf host 130.1.13.3 host 130.1.13.9
access-group OUTSIDE_IN in interface OUTSIDE

ASA3 VLAN16 Context:

interface GigabitEthernet0/0.61
 nameif OUTSIDE
 security-level 20
 bridge-group 16
!
interface GigabitEthernet0/1.16
 nameif INSIDE
 security-level 70
 bridge-group 16
!
interface Bvi16
 ip address 130.1.16.17 255.255.255.0
!
access-list OUTSIDE_IN extended permit ospf host 130.1.16.6 host 130.1.16.9
access-group OUTSIDE_IN in interface OUTSIDE
```

Task 1.3 Verification

https://t.me/learningnets

Verify switch-level port states and that native VLAN tagging is enabled:

```
SW1#show interfaces fastEthernet1/0/17 trunk


Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/17    on               802.1q         trunking      13

Port        Vlans allowed on trunk
Fa1/0/17    13,16

Port        Vlans allowed and active in management domain
Fa1/0/17    13,16

Port        Vlans in spanning tree forwarding state and not pruned Fa1/0/17    13,16
!
!SW1#show vlan dot1q tag native
 dot1q native vlan tagging is enabled
!
!SW2#show interfaces fastEthernet1/0/16 trunk


Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/16    on               802.1q         trunking      31

Port        Vlans allowed on trunk
Fa1/0/16    31,61

Port        Vlans allowed and active in management domain
Fa1/0/16    31,61

Port        Vlans in spanning tree forwarding state and not pruned Fa1/0/16    31,61
!
!SW2#show vlan dot1q tag native
               dot1q native vlan tagging is enabled
```

Verify the allocated interfaces for each context, nameif, security-levels:

```
ASA34# show context

Context Name      Class      Interfaces           URL
*admin            default                         disk0:/admin.cfg
 VLAN13           default    GigabitEthernet0/0.31, disk0:/VLAN13.cfg
                             GigabitEthernet0/1.13
```

https://t.me/learningnets

```
 VLAN16           default    GigabitEthernet0/0.61, disk0:/VLAN16.cfg
                             GigabitEthernet0/1.16

Total active Security Contexts: 3
!
!ASA34/VLAN13# show nameif
Interface                Name                    Security
GigabitEthernet0/0.31    OUTSIDE                  20
GigabitEthernet0/1.13    INSIDE                   70
!
!ASA34/VLAN16# show nameif

Interface                Name                    Security
GigabitEthernet0/0.61    OUTSIDE                  20
GigabitEthernet0/1.16    INSIDE                   70
```

Verify the bridge-groups and allocated IPv4 addresses:

```
ASA34/VLAN13# show bridge-group

 Static mac-address entries:  0 (in use), 65535 (max)
 Dynamic mac-address entries: 4 (in use), 65535 (max)
  Bridge Group: 13
 Interfaces:
 GigabitEthernet0/0.31
 GigabitEthernet0/1.13

  Management System IP Address:  130.1.13.17 255.255.255.0
 Management Current IP Address: 130.1.13.17 255.255.255.0
  Management IPv6 Global Unicast Address(es):
     N/A
  Static mac-address entries:  0
  Dynamic mac-address entries: 4
 !
 !ASA34/VLAN16# show bridge-group

 Static mac-address entries:  0 (in use), 65535 (max)
 Dynamic mac-address entries: 2 (in use), 65535 (max)
  Bridge Group: 16
 Interfaces:
 GigabitEthernet0/0.61
 GigabitEthernet0/1.16

  Management System IP Address:  130.1.16.17 255.255.255.0
 Management Current IP Address: 130.1.16.17 255.255.255.0
```

https://t.me/learningnets

```
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 2
```

Verify that OSPF is functional between R3, R6, and SW1:

```
SW1#show ip ospf neighbor


 Neighbor ID     Pri   State           Dead Time   Address         Interface
 150.1.6.6         1   FULL/BDR        00:01:31    130.1.16.6      Vlan16
 150.1.3.3         1   FULL/BDR        00:01:32    130.1.13.3      Vlan13
 !
 !
 SW1#show ip route ospf
      172.16.0.0/24 is subnetted, 2 subnets O       172.16.5.0 [110/2] via 130.1.13.3, 00:11:16, Vlan13
 O       172.16.1.0 [110/3] via 130.1.16.6, 00:11:16, Vlan16
      130.1.0.0/24 is subnetted, 15 subnets
 O       130.1.6.0 [110/2] via 130.1.16.6, 00:11:16, Vlan16
 O       130.1.9.0 [110/3] via 130.1.16.6, 00:11:16, Vlan16
 O       130.1.32.0 [110/2] via 130.1.13.3, 00:11:16, Vlan13
 O       130.1.69.0 [110/2] via 130.1.16.6, 00:11:16, Vlan16
      150.1.0.0/32 is subnetted, 7 subnets
 O       150.1.10.10 [110/3] via 130.1.16.6, 00:11:17, Vlan16
 O       150.1.6.6 [110/2] via 130.1.16.6, 00:11:17, Vlan16
 O       150.1.3.3 [110/2] via 130.1.13.3, 00:11:17, Vlan13
 !
 !ASA34/VLAN13# show conn

 2 in use, 4 most used
 OSPF OUTSIDE 130.1.13.3 INSIDE 130.1.13.9, idle 0:00:13, bytes 2756
 OSPF OUTSIDE 130.1.13.3 INSIDE 130.1.13.9, idle 0:00:15, bytes 3104
 !
 !ASA34/VLAN16# show conn

 2 in use, 2 most used
 OSPF OUTSIDE 130.1.16.6 INSIDE 130.1.16.9, idle 0:00:04, bytes 1916
 OSPF OUTSIDE 130.1.16.6 INSIDE 130.1.16.9, idle 0:00:16, bytes 2532
```

Task 1.4 Solution

```
SW1:
```

https://t.me/learningnets

```
interface FastEthernet1/0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 13,16
 switchport trunk native vlan 13
 no shutdown
```

SW2:

```
interface FastEthernet1/0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 31,61
 switchport trunk native vlan 31
 no shutdown
!
interface range FastEthernet1/0/17 , FastEthernet1/0/19
 switchport mode access
 no shutdown
```

ASA3 System Context:

```
prompt hostname context state
!
failover group 1
 primary
 preempt
!
failover group 2
 secondary
 preempt
!
context VLAN13
 join-failover-group 1
!
context VLAN16
 join-failover-group 2
!
interface GigabitEthernet0/2
 no shutdown
!
failover lan unit primary
failover lan interface FAILOVER GigabitEthernet0/2
failover link failover GigabitEthernet0/2
failover interface ip FAILOVER 130.1.100.17 255.255.255.0 standby 130.1.100.18
failover key secretpassword
failover
```

https://t.me/learningnets

```
ASA3 VLAN13 Context:

interface Bvi13
 ip address 130.1.13.17 255.255.255.0 standby 130.1.13.18
!
monitor-interface OUTSIDE
monitor-interface INSIDE

ASA3 VLAN16 Context:

interface Bvi16
 ip address 130.1.16.17 255.255.255.0 standby 130.1.16.18
!
!
monitor-interface OUTSIDE
monitor-interface INSIDE
```

First, convert ASA4 into multiple-context mode:

```
ciscoasa(config)# mode multiple
 WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]

ASA4 System Context:

delete /noconfirm disk0:/*.cfg
!
interface GigabitEthernet0/2
 no shutdown
!
failover lan unit secondary
failover lan interface FAILOVER GigabitEthernet0/2
failover link failover GigabitEthernet0/2
failover interface ip FAILOVER 130.1.100.17 255.255.255.0 standby 130.1.100.18
failover key secretpassword
failover
```

Task 1.4 Verification

Verify that the failover interface and IP addressing output is matched on ASA3:

https://t.me/learningnets

```
ASA34/act# show failover interface

        interface FAILOVER GigabitEthernet0/2
                System IP Address: 130.1.100.17 255.255.255.0
                My IP Address    : 130.1.100.17
                Other IP Address : 130.1.100.18
```

Verify that the failover output is matched on ASA3 and ASA4; also note the system prompt:

```
ASA34/VLAN13/act# show failover

Failover On
Last Failover at: 09:38:48 UTC Apr 1 2014
        This context: Active
                Active time: 1854 (sec)
                  Interface OUTSIDE (130.1.13.17): Normal (Monitored)
                  Interface INSIDE (130.1.13.17): Normal (Monitored)
        Peer context: Standby Ready
                Active time: 0 (sec)
                  Interface OUTSIDE (130.1.13.18): Normal (Monitored)
                  Interface INSIDE (130.1.13.18): Normal (Monitored)
!
!ASA34/VLAN16/act# show failover

Failover On
Last Failover at: 09:42:17 UTC Apr 1 2014
        This context: Active
                Active time: 1666 (sec)
                  Interface OUTSIDE (130.1.16.17): Normal (Monitored)
                  Interface INSIDE (130.1.16.17): Normal (Monitored)
        Peer context: Standby Ready
                Active time: 208 (sec)
                  Interface OUTSIDE (130.1.16.18): Normal (Monitored)
                  Interface INSIDE (130.1.16.18): Normal (Monitored
```

Task 1.5 Solution

First, identify the MAC addresses of SW1 and R3; this may differ based on the rack being assigned:

```
ASA34/VLAN13/act# show arp
```

https://t.me/learningnets

```
        OUTSIDE 130.1.13.3 001e.f779.4771 4
        INSIDE 130.1.13.9 001b.d58b.21c2 7

ASA3 VLAN13 Context:

arp INSIDE 130.1.13.9 001b.d58b.21c2
arp OUTSIDE 130.1.13.3 001e.f779.4771
!
!
arp-inspection OUTSIDE enable no-flood
arp-inspection INSIDE enable no-flood
```

Task 1.5 Verification

Verify that ARP inspection is enabled:

```
ASA34/VLAN13/act# show arp-inspection

interface                arp-inspection         miss
-----------------------------------------------------
OUTSIDE                  enabled                no-flood
INSIDE                   enabled                no-flood
```

Task 1.6 Solution

```
ASA2:
nat-control
nat (INSIDE) 10 130.1.81.0 255.255.255.0
!
global (OUTSIDE) 10 130.1.8.1-130.1.8.31
global (OUTSIDE) 10 interface

R1:

ip route 130.1.8.0 255.255.255.224 130.1.18.16
!
router eigrp 202
 redistribute static
```

https://t.me/learningnets

Task 1.6 Verification

Use packet-tracer on ASA2 to simulate traffic and verify that it matches the NAT configuration:

```
ASA2# packet-tracer input iNSIDE tcp 130.1.81.100 2000 150.1.1.1 23

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   150.1.1.1       255.255.255.255 OUTSIDE

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:nat (INSIDE) 10 130.1.81.0 255.255.255.0
nat-control
  match ip INSIDE 130.1.81.0 255.255.255.0 OUTSIDE any
    dynamic translation to pool 10 (130.1.18.16 [Interface PAT])
    translate_hits = 2, untranslate_hits = 0
Additional Information:Dynamic translate 130.1.81.100/0 to 130.1.8.27/0 using netmask 255.255.255.255

Phase: 5
Type: NAT
Subtype: host-limits
```

https://t.me/learningnets

```
Result: ALLOW
Config:
nat (INSIDE) 10 130.1.81.0 255.255.255.0
nat-control
  match ip INSIDE 130.1.81.0 255.255.255.0 OUTSIDE any
    dynamic translation to pool 10 (130.1.18.16 [Interface PAT])
    translate_hits = 2, untranslate_hits = 0
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 8, packet dispatched to next module

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: upAction: allow
!
!ASA2# show xlate detail

1 in use, 1 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
       r - portmap, s - staticNAT from INSIDE:130.1.81.100 to OUTSIDE:130.1.8.27 flags i
```

Verify that R1 redistributes the static route:

```
SW1#show ip route 130.1.8.0
Routing entry for 130.1.8.0/27
  Known via "eigrp 202", distance 170, metric 28416, type external
  Redistributing via eigrp 202, ospf 202
```

https://t.me/learningnets

```
  Advertised by ospf 202 subnets
  Last update from 130.1.11.1 on Vlan11, 00:09:50 ago
  Routing Descriptor Blocks: * 130.1.11.1, from 130.1.11.1, 00:09:50 ago, via Vlan11

      Route metric is 28416, traffic share count is 1
      Total delay is 110 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Task 1.7 Solution

R7:

```
zone security VLAN17
zone security VLAN76
!
class-map type inspect match-any TCP_UDP
 match protocol tcp
 match protocol udp
!
class-map type inspect match-any ICMP
 match protocol icmp
!
!
policy-map type inspect VLAN76_TO_VLAN17
 class TCP_UDP
  inspect
 class ICMP
  inspect
  police rate 64000 burst 2000
!
!
zone-pair security VLAN76_TO_VLAN17 source VLAN76 destination VLAN17
 service-policy type inspect VLAN76_TO_VLAN17
!
!
ip access-list extended ACL_ICMP
 permit icmp any any echo
 permit icmp any any echo-reply
!
!
class-map type inspect match-all SELF_ICMP
 match access-group name ACL_ICMP
 match protocol icmp
```

https://t.me/learningnets

```
!
policy-map type inspect ALL_TO_SELF
 class SELF_ICMP
  pass
!
zone-pair security VLAN17_TO_SELF source VLAN17 destination self
 service-policy type inspect ALL_TO_SELF
!
!
interface FastEthernet0/0.17
 zone-member security VLAN17
!
interface FastEthernet0/0.76
 zone-member security VLAN76
!
interface Bvi17
 zone-member security VLAN17
```

Task 1.7 Verification

Verify that ICMP traffic from VLAN76 to VLAN17 is inspected and policed:

```
SW6#ping 150.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
!
!R7#show policy-firewall session
 Established Sessions = 1
Session 49E3C240 (130.1.76.14:8)=>(150.1.1.1:0) icmp SIS_OPEN
          Created 00:00:01, Last heard 00:00:01
          ECHO request
          Bytes sent (initiator:responder) [360:360]
!
!R7#show policy-firewall stats zone-pair VLAN76_TO_VLAN17


policy exists on zp VLAN76_TO_VLAN17
 Zone-pair: VLAN76_TO_VLAN17

  Service-policy inspect : VLAN76_TO_VLAN17

    Class-map: TCP_UDP (match-any)
      Match: protocol tcp
```

https://t.me/learningnets

```
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol udp
        0 packets, 0 bytes
        30 second rate 0 bps

   Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0
        TCP reassembly statistics
        received 0 packets out-of-order; dropped 0
        peak memory usage 0 KB; current usage: 0 KB
        peak queue length 0

 Class-map: ICMP (match-any)
      Match: protocol icmp
        1 packets, 80 bytes
        30 second rate 0 bps

   Inspect
        Packet inspection statistics [process switch:fast switch] icmp packets: [0:10]

        Session creations since subsystem startup or last reset 1
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:0]
        Last session created 00:01:43
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 1
        Last half-open session total 0
        TCP reassembly statistics
        received 0 packets out-of-order; dropped 0
        peak memory usage 0 KB; current usage: 0 KB
        peak queue length 0
 Police
 rate 64000 bps,2000 limit
 conformed 10 packets, 1140 bytes; actions: transmit

        exceeded 0 packets, 0 bytes; actions: drop
        conformed 0 bps, exceed 0 bps
```

https://t.me/learningnets

```
    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

Verify that packets in the reverse direction are dropped because no firewall policy is configured:

```
R1#ping 150.1.14.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.14.14, timeout is 2 seconds:.....
Success rate is 0 percent (0/5)
!
!R7#show policy-firewall stats drop-counters
 policy match failure                                    5
```

Verify that PING traffic to and from the self-zone is functional:

```
R7#ping 150.1.1.1



Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!R7#ping 150.1.14.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.14.14, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!R1#ping 130.1.76.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 130.1.76.7, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!SW6#ping 130.1.76.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 130.1.76.7, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
!
!R7#show policy-firewall stats zone-pair VLAN17_TO_SELF
```

https://t.me/learningnets

```
policy exists on zp VLAN17_TO_SELF
 Zone-pair: VLAN17_TO_SELF

  Service-policy inspect : ALL_TO_SELF
 Class-map: SELF_ICMP (match-all)
      Match: access-group name ACL_ICMP
      Match: protocol icmp Pass
 20 packets, 1600 bytes


    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

Verify that other traffic to and from the self-zone is dropped because it matches the default class-map:

https://t.me/learningnets

```
R1#telnet 130.1.76.7

Trying 130.1.76.7 ... % Connection timed out; remote host not responding

!
!R7#telnet 150.1.14.14

Trying 150.1.14.14 ... % Connection timed out; remote host not responding

!
!R7#show policy-firewall stats zone-pair VLAN17_TO_SELF


policy exists on zp VLAN17_TO_SELF
 Zone-pair: VLAN17_TO_SELF

  Service-policy inspect : ALL_TO_SELF

    Class-map: SELF_ICMP (match-all)
      Match: access-group name ACL_ICMP
      Match: protocol icmp
      Pass
        20 packets, 1600 bytes
 Class-map: class-default (match-any)

      Match: any  Drop
 11 packets, 252 bytes

!
!R7#show policy-firewall stats drop-counters
 DROP action found in policy-map                              11
```

Task 1.8 Solution

```
R7:
parameter-map type inspect default
 max-incomplete low 80
 max-incomplete high 100
 udp idle-time 10
 tcp idle-time 120
 tcp max-incomplete host 10 block-time 10
```

https://t.me/learningnets

```
!
parameter-map type inspect global
 l2-transparent dhcp-passthrough enable
```

Task 1.8 Verification

Verify the parameter-map settings:

```
R7#show parameter-map type inspect default

  audit-trail off
  alert on max-incomplete low 80
 max-incomplete high 100

  one-minute low 2147483647
  one-minute high 2147483647 udp idle-time 10
  icmp idle-time 10
  dns-timeout 5 tcp idle-time 120
  tcp finwait-time 5
  tcp synwait-time 30 tcp max-incomplete host 10 block-time 10
  sessions maximum 2147483647
!
!R7#show parameter-map type inspect global

  alert on
  sessions maximum 2147483647
  waas disabled l2-transparent dhcp-passthrough enabled

  log dropped-packets disabled
  log summary disabled
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  tcp reset-PSH disabled
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 2

CCIE SCv4 Lab 2 Solutions Section 2

1. Task 2.1 Solution
2. Task 2.2 Solution
3. Task 2.3 Solution
4. Task 2.4 Solution
5. Task 2.5 Solution
6. Task 2.6 Solution

Task 2.1 Solution

SW3:

```
interface GigabitEthernet1/0/10
 switchport mode access
 switchport access vlan 9
 no shutdown
```

IPS:

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# host-name IPS
sensor(config-hos-net)# host-ip 130.1.9.100/24,130.1.9.10
sensor(config-hos-net)# telnet-option enabled
sensor(config-hos-net)# access-list 130.1.9.0/24
sensor(config-hos-net)# access-list 130.1.91.0/24
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes?[yes]:
!
!
sensor(config)# service web-server
sensor(config-web)# enable-tls false
sensor(config-web)# port 8080
```

https://t.me/learningnets

```
sensor(config-web)# server-id Unknown
sensor(config-web)# exit
Apply Changes?[yes]:
```

Task 2.1 Verification

Verify the default HTTP server-id being displayed before making the changes:

```
R5#telnet 130.1.9.100 8080
Trying 130.1.9.100, 8080 ... Open

^]
 400 Bad Request
Connection: Close
Date: Tue, 01 Apr 2014 06:31:42 UTCServer: HTTP/1.1 compliant

Content-Length: 123
Content-Type: text/html

<html><head><title>Bad Request</title></head><body><h2>Bad Request</h2><p>Parser found an invalid method.</p></body>
[Connection to 130.1.9.100 closed by foreign host]
```

Verify the HTTP server-id being displayed after making the changes:

```
R5#telnet 130.1.9.100 8080
Trying 130.1.9.100, 8080 ... Open
]
 400 Bad Request
Connection: Close
Date: Tue, 01 Apr 2014 06:41:28 UTCServer: Unknown

Content-Length: 123
Content-Type: text/html

<html><head><title>Bad Request</title></head><body><h2>Bad Request</h2><p>Parser found an invalid method.</p></body>
[Connection to 130.1.9.100 closed by foreign host]
```

Verify the configured IPS settings:

```
sensor(config)# service web-server
 sensor(config-web)# show settings
```

https://t.me/learningnets

```
enable-tls: false default: true
 port: 8080 default: 443
server-id: Unknown default: HTTP/1.1 compliant
   configurable-service (min: 0, max: 99, current: 0)
   ---------------------------------------------
   ---------------------------------------------
!
!sensor(config)# service host
 sensor(config-hos)# network-settings
 sensor(config-hos-net)# show settings
   network-settings
   ---------------------------------------------
host-ip: 130.1.9.100/24,130.1.9.10 default: 192.168.1.2/24,192.168.1.1
 host-name: IPS default: sensor
 telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 2)
      --------------------------------------------- network-address: 130.1.9.0/24
         --------------------------------------------- network-address: 130.1.91.0/24


         ---------------------------------------------
```

Task 2.2 Solution

```
SW3:
interface GigabitEthernet1/0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 23,32
 no shutdown

IPS:


sensor(config)# service interface
sensor(config-int)# physical-interfaces gigabitEthernet0/1
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# subinterface-type inline-vlan-pair
sensor(config-int-phy-inl)# subinterface 1
sensor(config-int-phy-inl-sub)# vlan1 23
sensor(config-int-phy-inl-sub)# vlan2 32
sensor(config-int-phy-inl-sub)# exit
sensor(config-int-phy-inl)# exit
sensor(config-int-phy)# exit
sensor(config-int)# exit
Apply Changes?[yes]:
```

https://t.me/learningnets

```
!
!
sensor(config)# service analysis-engine
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)# physical-interface gigabitEthernet0/1 subinterface-number 1
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
Apply Changes?[yes]:
```

Task 2.2 Verification

Verify the physical and logical state of interfaces on the IPS:

```
sensor# show interfaces brief

CC   Interface            Sensing State   Link   Inline Mode        Pair Status
     GigabitEthernet0/0   Disabled        Down   Unpaired           N/A
*    Management0/0        Disabled        Up
GigabitEthernet0/1   Enabled         Up     Inline-vlan-pair   N/A

     GigabitEthernet0/2   Disabled        Down   Unpaired           N/A
     GigabitEthernet0/3   Disabled        Down   Unpaired           N/A
!
!sensor(config-int-phy-inl)# show settings

   inline-vlan-pair
   ------------------------------------------------
      subinterface (min: 1, max: 255, current: 1)
      ------------------------------------------------ subinterface-number: 1
         ------------------------------------------------
            description:  <defaulted> vlan1: 23
 vlan2: 32

         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
```

To confirm that traffic flows through the IPS, verify whether R2 and R3 are OSPF neighbors:

```
R2#show ip ospf neighbor gigabitEthernet0/0

Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.3.3         1   FULL/DR         00:00:35    130.1.32.3      GigabitEthernet0/0
```

https://t.me/learningnets

```
!
!sensor# packet display gigabitEthernet0/1
Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
06:57:13.899000 IP 130.1.32.3 > 224.0.0.5: OSPFv2, Hello, length: 60
06:57:13.900000 IP 130.1.32.3 > 224.0.0.5: OSPFv2, Hello, length: 60
06:57:15.404000 IP 130.1.32.2 > 224.0.0.5: OSPFv2, Hello, length: 60

06:57:15.404000 IP 130.1.32.2 > 224.0.0.5: OSPFv2, Hello, length: 60
```

Task 2.3 Solution

IPS:

```
IPS(config)# service signature-definition sig0
IPS(config-sig)# signatures 60005 0
IPS(config-sig-sig)# engine string-tcp
IPS(config-sig-sig-str)# service-ports 23
IPS(config-sig-sig-str)# direction to-service
IPS(config-sig-sig-str)# regex-string [Pp][Aa][Ss][Ss][Ww][Oo][Rr][Dd]
IPS(config-sig-sig-str)# event-action produce-alert|deny-attacker-inline
IPS(config-sig-sig-str)# exit
IPS(config-sig-sig)# alert-severity high
IPS(config-sig-sig)# sig-fidelity-rating 100
IPS(config-sig-sig)# exit
IPS(config-sig)# exit
Apply Changes?[yes]:
!
!
IPS(config)# service event-action-rules rules0
IPS(config-eve)# general
IPS(config-eve-gen)#  global-deny-timeout 900
IPS(config-eve-gen)# exit
IPS(config-eve)# filters edit alert-only
IPS(config-eve-fil)# actions-to-remove deny-attacker-inline|deny-packet-inline
IPS(config-eve-fil)# signature-id-range 60005
IPS(config-eve-fil)# victim-address-range 150.1.2.2-150.1.2.2
IPS(config-eve-fil)# exit
IPS(config-eve)# filters edit deny-attacker
IPS(config-eve-fil)# actions-to-remove deny-packet-inline
IPS(config-eve-fil)# signature-id-range 60005
IPS(config-eve-fil)# exit
```

https://t.me/learningnets

```
IPS(config-eve)# exit
Apply Changes?[yes]:
```

Task 2.3 Verification

Telnet to R2's Loopback0 and verify that only the alarm is triggered:

```
R3#telnet 150.1.2.2
Trying 150.1.2.2 ... Open


User Access Verification

Username: cisco
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z. R2(config)#username test PasswOrd test
!
!IPS# show events

evIdsAlert: eventId=1395308977431000518 severity=high vendor=Cisco alarmTraits=32768
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 1202
  time: 2014/04/01 08:34:47 2014/04/01 08:34:47 UTC
 signature: description=My Sig id=60005 created=20000101 type=other version=custom
    subsigId: 0
    sigDetails: My Sig Info
  interfaceGroup: vs0
  vlan: 32
  participants:
    attacker:
      addr: locality=OUT 130.1.32.3
      port: 12535 target:
 addr: locality=OUT 150.1.2.2
 port: 23

      os: idSource=unknown relevance=relevant type=unknown
  context:
    fromTarget:
000000  FF FB 01 FF FB 03 FF FD  18 FF FD 1F 0D 0A 0D 0A  ................
000010  55 73 65 72 20 41 63 63  65 73 73 20 56 65 72 69  User Access Veri
000020  66 69 63 61 74 69 6F 6E  0D 0A 0D 0A 55 73 65 72  fication....User
000030  6E 61 6D 65 3A 20 FF FE  20 FF FD 21 FF FA 21 00  name: .. ..!..!.
```

https://t.me/learningnets

```
000040  FF F0 FF FE 18 63 69 73  63 6F 0D 0A 50 61 73 73  .....cisco..Pass
000050  77 6F 72 64 3A 20 0D 0A  52 32 23 63 6F 6E 66 69  word: ..R2#confi
000060  67 75 72 65 20 65 74 72  08 20 08 08 20 08 08 20  gure etr. .. ..
000070  08 74 65 72 6D 6E 61 6C  08 20 08 08 20 08 08 20  .termnal. .. ..
000080  08 69 6E 61 6C 0D 0A 45  6E 74 65 72 20 63 6F 6E  .inal..Enter con
000090  66 69 67 75 72 61 74 69  6F 6E 20 63 6F 6D 6D 61  figuration comma
0000A0  6E 64 73 2C 20 6F 6E 65  20 70 65 72 20 6C 69 6E  nds, one per lin
0000B0  65 2E 20 20 45 6E 64 20  77 69 74 68 20 43 4E 54  e.  End with CNT
0000C0  4C 2F 5A 2E 0D 0A 52 32  28 63 6F 6E 66 69 67 29  L/Z...R2(config)
0000D0  23 75 73 65 72 6E 61 6D  65 20 74 65 73 74 20 50  #username test P
0000E0  61 73 73 77 4F 72                                 asswOr
    fromAttacker:
000000  FF FD 03 FF FB 20 FF FB  1F FF FB 21 FF FD 01 FF  ..... .....!....
000010  FC 18 FF FA 1F 00 50 00  18 FF F0 FF FC 20 63 69  ......P...... ci
000020  73 63 6F 0D 0A 63 69 73  63 6F 0D 0A 63 6F 6E 66  sco..cisco..conf
000030  69 67 75 72 65 20 65 74  72 08 08 08 74 65 72 6D  igure etr...term
000040  6E 61 6C 08 08 08 69 6E  61 6C 0D 0A 75 73 65 72  nal...inal..user
000050  6E 61 6D 65 20 74 65 73  74 20 50 61 73 73 77 4F  name test PasswO
000060  72 64                                            rd
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 100
  threatRatingValue: 100
  interface: ge0_1
  protocol: tcp
```

Disconnect and repeat the test, but telnet on R2's VLAN 23 IPv4 address; sessions should freeze because IPS denies the attacker:

```
R3#telnet 130.1.32.2
Trying 130.1.32.2 ... Open


User Access Verification


Username: cisco
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z. R2(config)#username test Passwor
!
!IPS# show events



evIdsAlert: eventId=1395308977431000529 severity=high vendor=Cisco alarmTraits=32768
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 1202
```

https://t.me/learningnets

```
  time: 2014/04/01 08:46:23 2014/04/01 08:46:23 UTC
  signature: description=My Sig id=60005 created=20000101 type=other version=custom
    subsigId: 0
    sigDetails: My Sig Info
  interfaceGroup: vs0
  vlan: 32
  participants:
    attacker:
      addr: locality=OUT 130.1.32.3
      port: 54807 target:
addr: locality=OUT 130.1.32.2
port: 23
      os: idSource=unknown relevance=relevant type=unknown actions:
deniedAttacker: true
  context:
    fromTarget:
000000  FF FB 01 FF FB 03 FF FD  18 FF FD 1F 0D 0A 0D 0A  ................
000010  55 73 65 72 20 41 63 63  65 73 73 20 56 65 72 69  User Access Veri
000020  66 69 63 61 74 69 6F 6E  0D 0A 0D 0A 55 73 65 72  fication....User
000030  6E 61 6D 65 3A 20 FF FE  20 FF FD 21 FF FA 21 00  name: .. ..!..!.
000040  FF F0 FF FE 18 63 69 73  63 6F 0D 0A 50 61 73 73  .....cisco..Pass
000050  77 6F 72 64 3A 20 0D 0A  52 32 23 63 6F 6E 66 69  word: ..R2#confi
000060  67 75 72 65 20 74 65 72  6D 69 6E 61 61 6C 08 20  gure terminaal.
000070  08 08 20 08 6C 0D 0A 45  6E 74 65 72 20 63 6F 6E  .. .l..Enter con
000080  66 69 67 75 72 61 74 69  6F 6E 20 63 6F 6D 6D 61  figuration comma
000090  6E 64 73 2C 20 6F 6E 65  20 70 65 72 20 6C 69 6E  nds, one per lin
0000A0  65 2E 20 20 45 6E 64 20  77 69 74 68 20 43 4E 54  e.  End with CNT
0000B0  4C 2F 5A 2E 0D 0A 52 32  28 63 6F 6E 66 69 67 29  L/Z...R2(config)
0000C0  23 75 73 65 72 07 0D 0A  52 32 28 63 6F 6E 66 69  #user...R2(confi
0000D0  67 29 23 75 73 65 72 6E  0D 0A 52 32 28 63 6F 6E  g)#usern..R2(con
0000E0  66 69 67 29 23 75 73 65  72 6E 61 6D 65 20 74 65  fig)#username te
0000F0  73 74 20 50 61 73 73 77  4F 72                    st PasswOr
    fromAttacker:
000000  FF FD 03 FF FB 20 FF FB  1F FF FB 21 FF FD 01 FF  ..... .....!....
000010  FC 18 FF FA 1F 00 50 00  18 FF F0 FF FC 20 63 69  ......P...... ci
000020  73 63 6F 0D 0A 63 69 73  63 6F 0D 0A 63 6F 6E 66  sco..cisco..conf
000030  69 67 75 72 65 20 74 65  72 6D 69 6E 61 61 6C 08  igure terminaal.
000040  08 6C 0D 0A 75 73 65 72  09 6E 09 74 65 73 74 20  .l..user.n.test
000050  50 61 73 73 77 4F 72 64                           PasswOrd
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 100
  threatRatingValue: 55
  interface: ge0_1
  protocol: tcp



evStatus: eventId=1395308977431000530 vendor=Cisco
```

https://t.me/learningnets

```
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 1202
  time: 2014/04/01 08:46:23 2014/04/01 08:46:23 UTC denyAttackerStarted:
description: denyAttackerStarted for address: 130.1.32.3

    address: 130.1.32.3
```

Verify the denied attackers list:

```
IPS# show statistics denied-attackers
Statistics for Virtual Sensor vs0
   Denied Attackers and hit count for each.
      130.1.32.3 = 29
   Denied Attackers with percent denied and hit count for each.
         Attacker Address    Victim Address    Port    Protocol    Requested Percentage    Actual Percentage    Hit Count

130.1.32.3                                                100                 100                 29                false
```

Task 2.4 Solution

SW6:

```
interface FastEthernet1/0/10
 switchport mode access
 switchport access vlan 66
 no shutdown
```

ASA1:

```
access-list OUTSIDE_IN permit udp host 172.16.6.100 host 150.1.4.4 eq 53
access-list OUTSIDE_IN permit udp host 172.16.6.100 host 150.1.4.4 eq 123
!
access-group OUTSIDE_IN in interface OUTSIDE
```

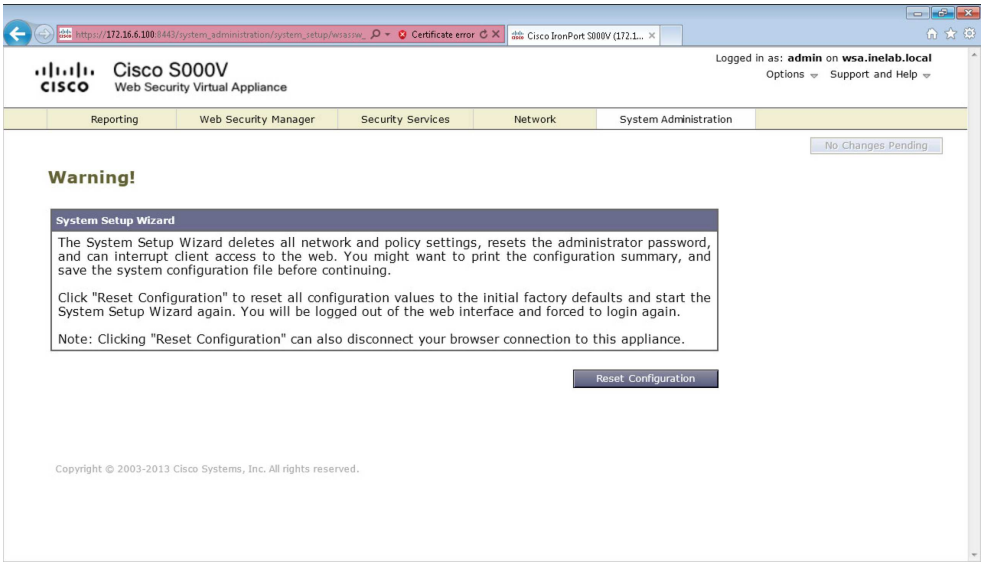
R7:

```
ip access-list extended HTTPS_WSA
 permit tcp 130.1.91.0 0.0.0.255 host 172.16.6.100 eq 8443
!
class-map type inspect match-all TCP
 match access-group name HTTPS_WSA
 match protocol tcp
```

https://t.me/learningnets

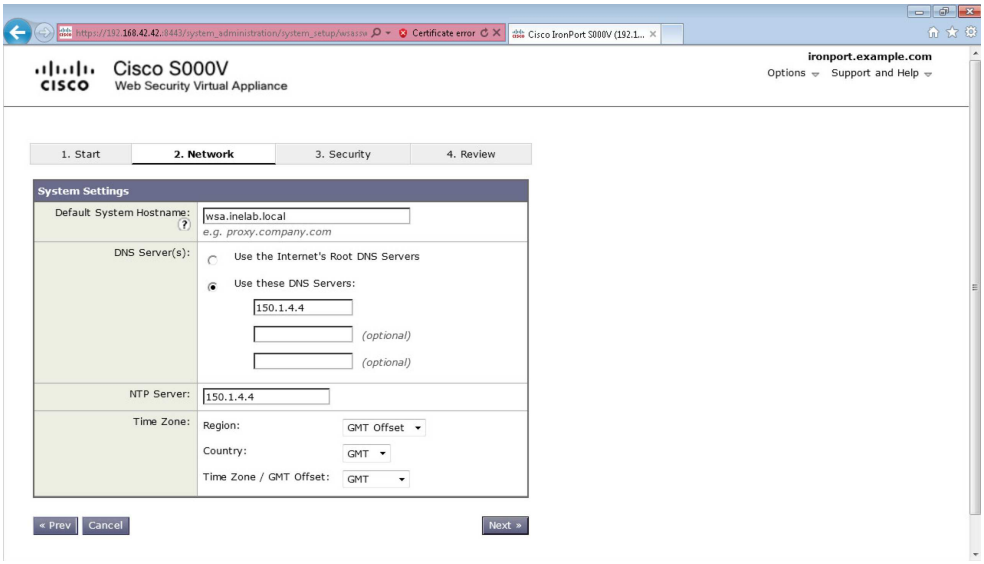
```
!
policy-map type inspect VLAN17_TO_VLAN76
 class TCP
  inspect
!
zone-pair security VLAN17_TO_VLAN76 source VLAN17 destination VLAN76
 service-policy type inspect VLAN17_TO_VLAN76
```

Using Internet Explorer from **TEST-PC-A**, navigate to **https://172.16.6.100:8443**, authenticate and browse to **System Administration -> System Setup Wizard**, and click **Reset Configuration**:

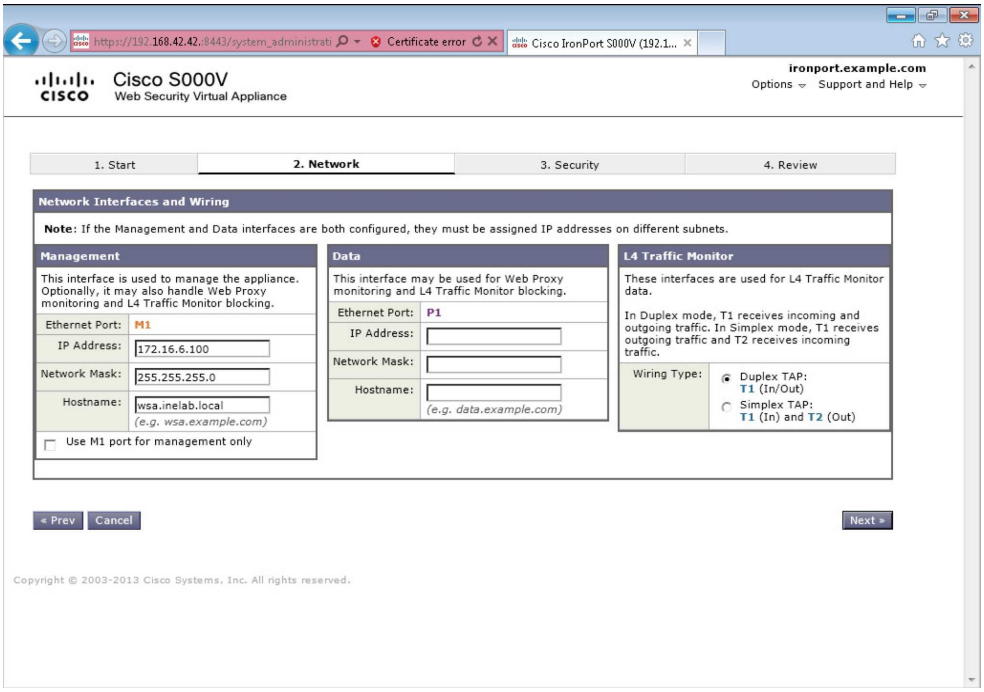


Configure **TEST-PC-A** with the IPv4 address from subnet 192.168.42.0/24, allocate its switchport in the same VLAN as WSA, and using Internet Explorer navigate to **https://192.168.42.42:8443**. Authenticate with the default credentials of **admin/ironport** and browse to **System Administration -> System Setup Wizard**. Configure hostname, DNS, and NTP server:

https://t.me/learningnets

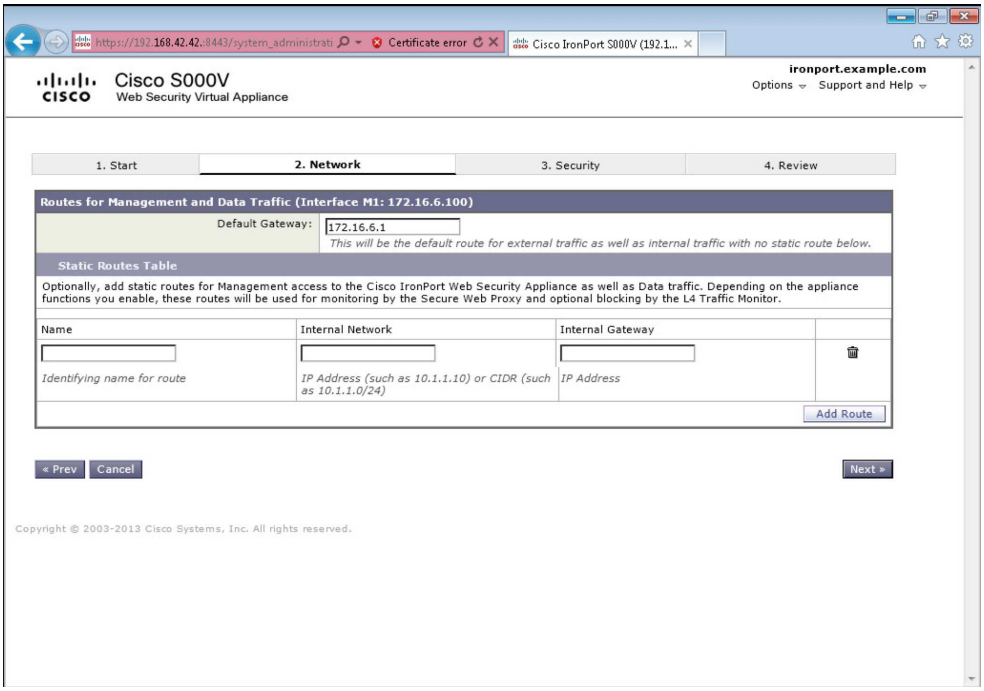


Configure the M1 interface for both proxy and management:

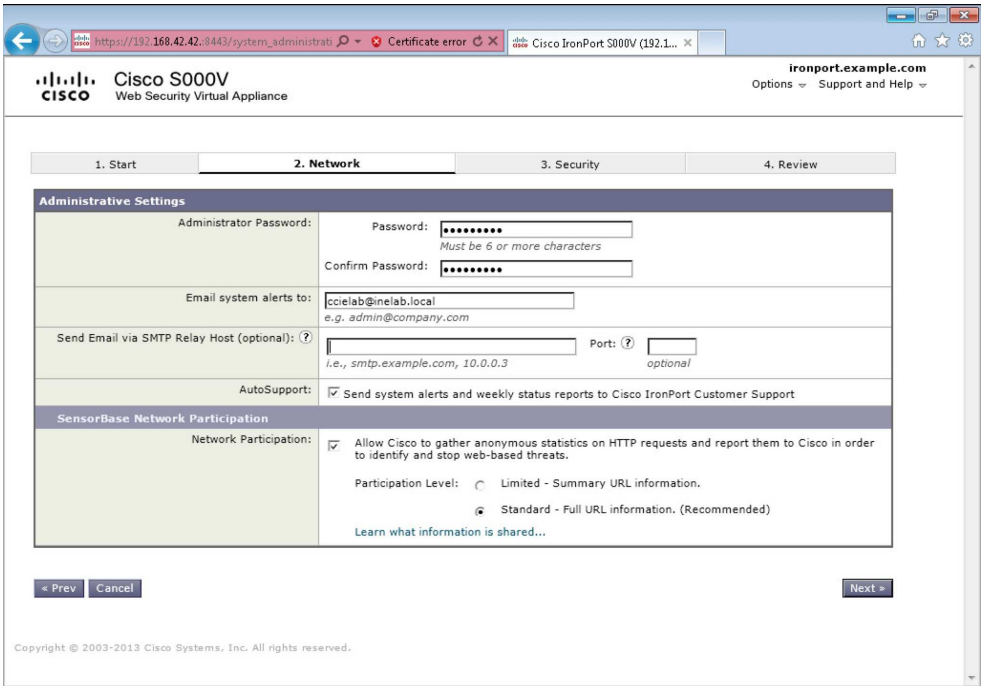


Configure the default gateway for M1 port:

https://t.me/learningnets

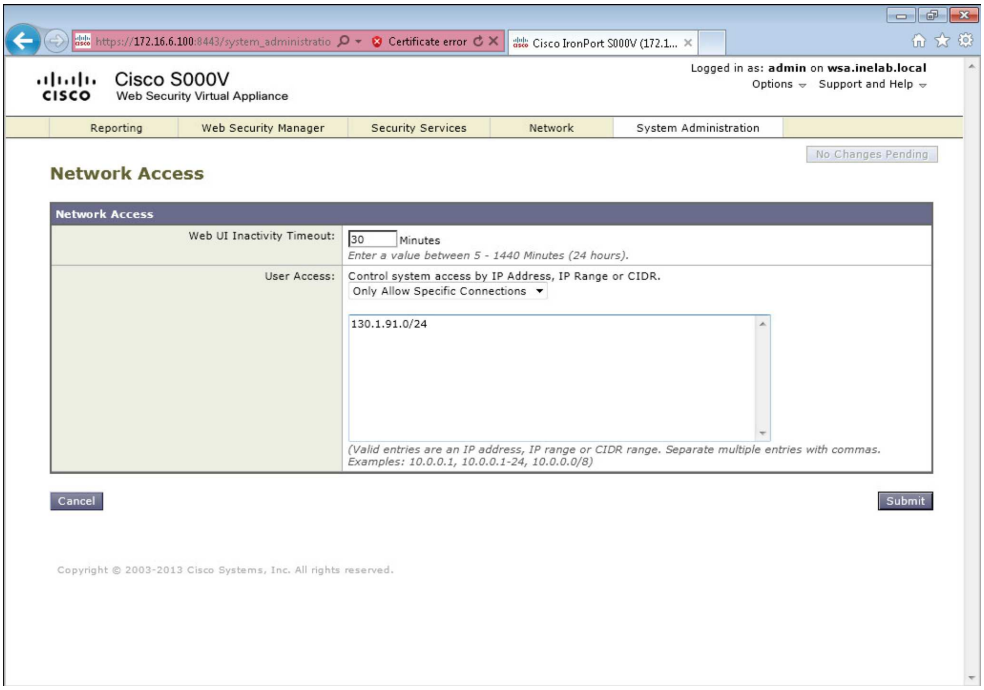


Configure the administrator password and email address:



All other settings are left at their default values, so screens are missing from the complete **System Setup Wizard**. Install the configuration and put **TEST-PC-A** back in VLAN 91. Using Internet Explorer from **TEST-PC-A**, navigate to **https://172.16.6.100:8443**, authenticate and browse to **System Administration -> Network Access**, and click **Edit Settings**. Configure WSA to allow management sessions only from VLAN 91.

https://t.me/learningnets



Task 2.4 Verification

Use Internet Explorer to manage the WSA. When the sessions is successful, check the connection table for both ASA1 and R7:

```
R7#show policy-firewall session

      Established Sessions = 1
        Session 4A137E00 (130.1.91.100:18476)=>(172.16.6.100:8443) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:03, Last heard 00:00:03
          Bytes sent (initiator:responder) [0:0]
!
!ASA1# show conn protocol tcp address 172.16.6.100

22 in use, 41 most used
TCP OUTSIDE 172.16.6.100:443 TESTPC 130.1.91.100:18478, idle 0:00:23, bytes 0, flags saA
```

Task 2.5 Solution

```
R1:
ip access-list extended REDIRECTED_TRAFFIC
 permit tcp 130.1.91.0 0.0.0.255 any eq 80
!
ip access-list standard GROUP_LIST
 permit host 130.1.76.100
```

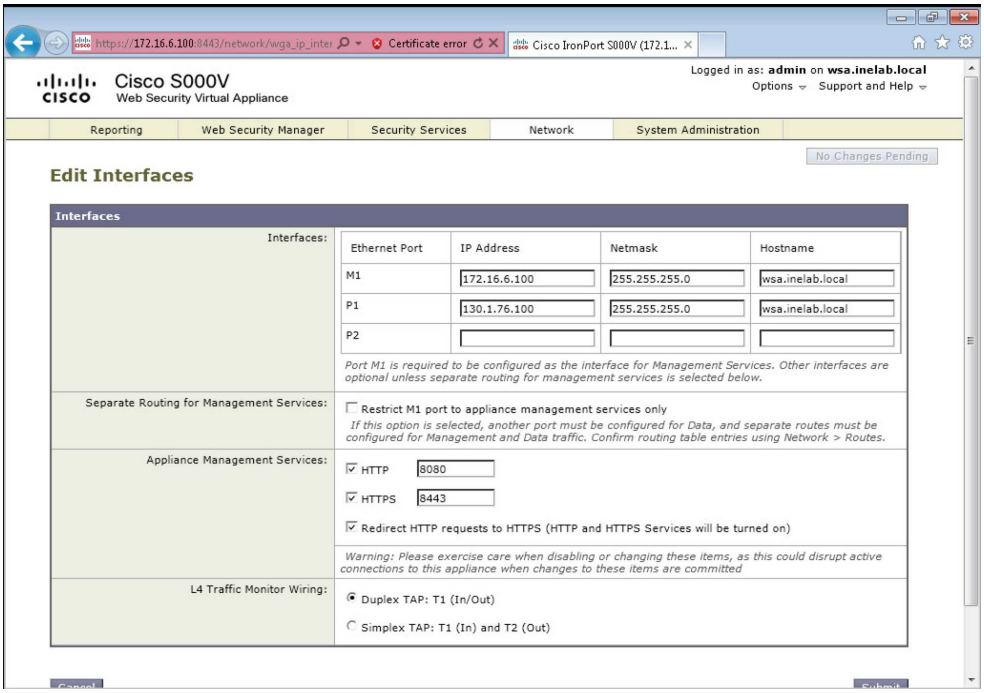
https://t.me/learningnets

```
!
ip wccp 91 redirect-list REDIRECTED_TRAFFIC group-list GROUP_LIST
!
interface GigabitEthernet0/1
 ip wccp 91 redirect in

SW6:

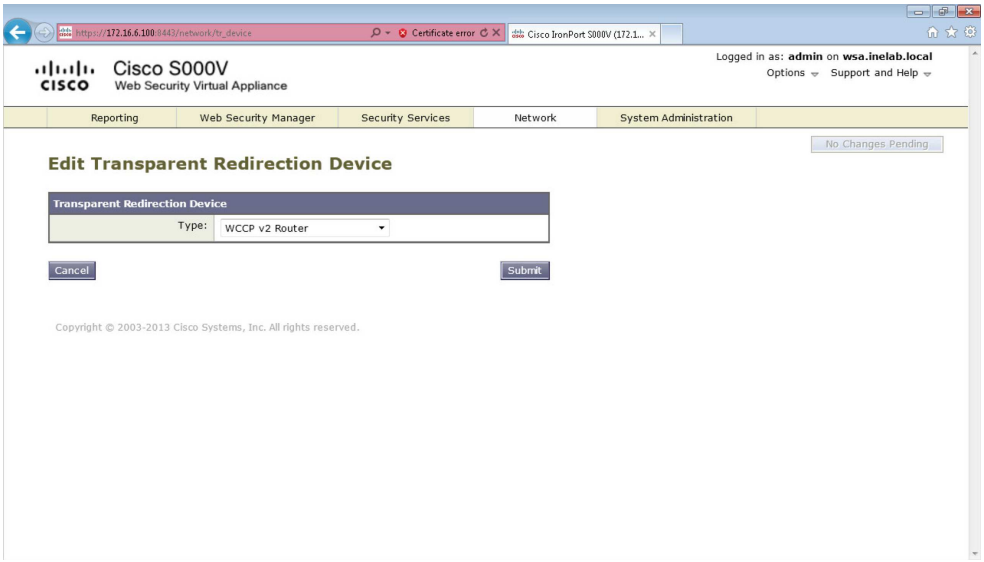
interface FastEthernet1/0/11
 switchport mode access
 switchport access vlan 76
 no shutdown
```

Using Internet Explorer from **TEST-PC-A**, navigate to **https://172.16.6.100:8443**, authenticate and browse to **Network -> Interfaces**, and click **Edit Settings** to configure the P1 port:

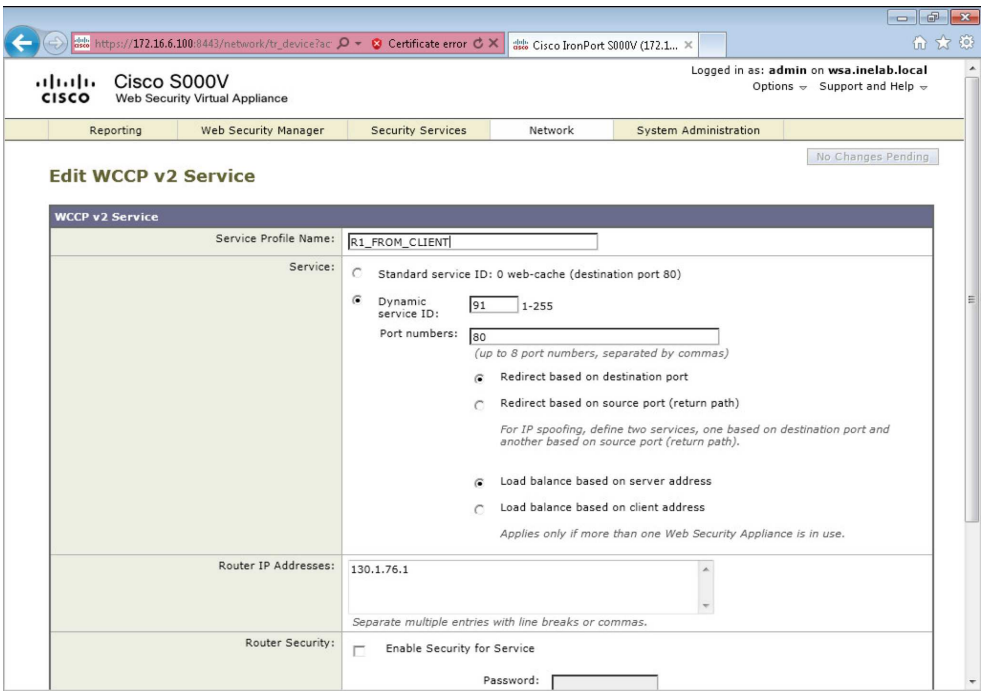


Browse to **Network -> Transparent Redirection** and select **WCCP v2 Router**:

https://t.me/learningnets



Click **Add Service**, configure the same service-id as on the router, and enable it only for HTTP traffic:



Task 2.5 Verification

Verify WCCP configuration and that it is functional because the WCCP server selected the router identifier:

```
R1#show ip wccp 91
Global WCCP information:
    Router information: Router Identifier:                   150.1.1.1


    Service Identifier: 91
        Protocol Version:                   2.00
```

https://t.me/learningnets

```
        Number of Service Group Clients:     1
        Number of Service Group Routers:     1
        Total Packets Redirected:            0
          Process:                           0
          CEF:                               0
        Service mode:                        Open
        Service Access-list:                 -none-
        Total Packets Dropped Closed:        0 Redirect access-list:                 REDIRECTED_TRAFFIC
        Total Packets Denied Redirect:       0
        Total Packets Unassigned:            0 Group access-list:                    GROUP_LIST

        Total Messages Denied to Group:      5
        Total Authentication failures:       0
        Total GRE Bypassed Packets Received: 0
          Process:                           0
          CEF:                               0
```

Verify that requested output is matched; WCCP is deployed in L2 mode:

```
R1#show ip wccp 91 clients

WCCP Client information:
        WCCP Client ID:          130.1.76.100
        Protocol Version:        2.00
        State:                   Usable
        Redirection:             L2
        Packet Return:           L2
        Assignment:              MASK
        Connect Time:            00:17:33
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Mask Allotment:          32 of 32 (100.00%)
```

Task 2.6 Solution

R7:

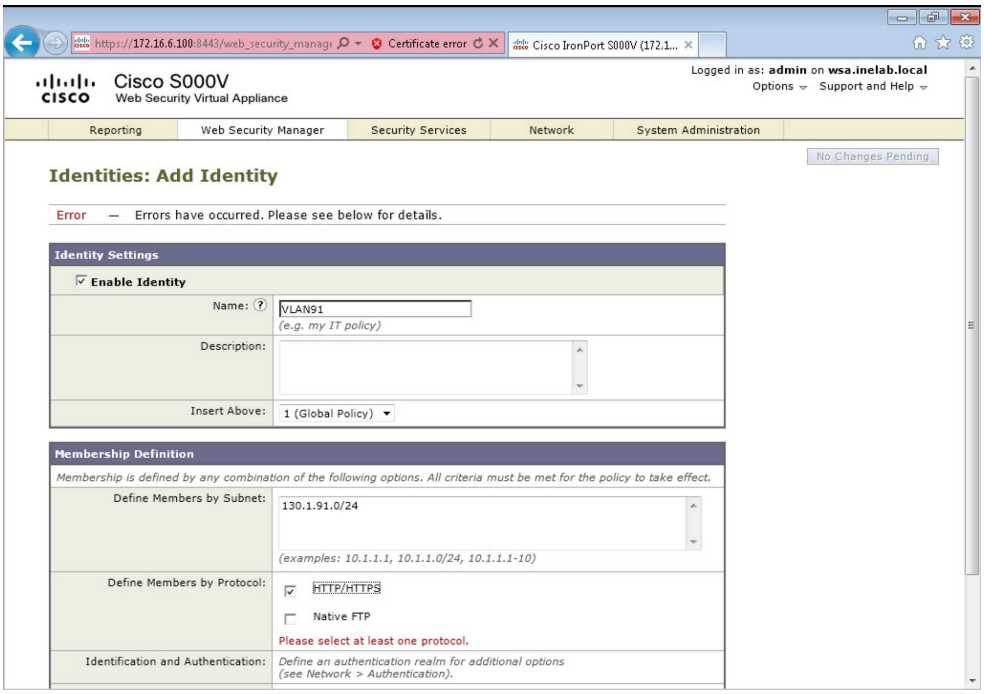
```
ip access-list extended HTTPS_WSA
 permit tcp 130.1.91.0 0.0.0.255 any eq 80
```

R1:

https://t.me/learningnets

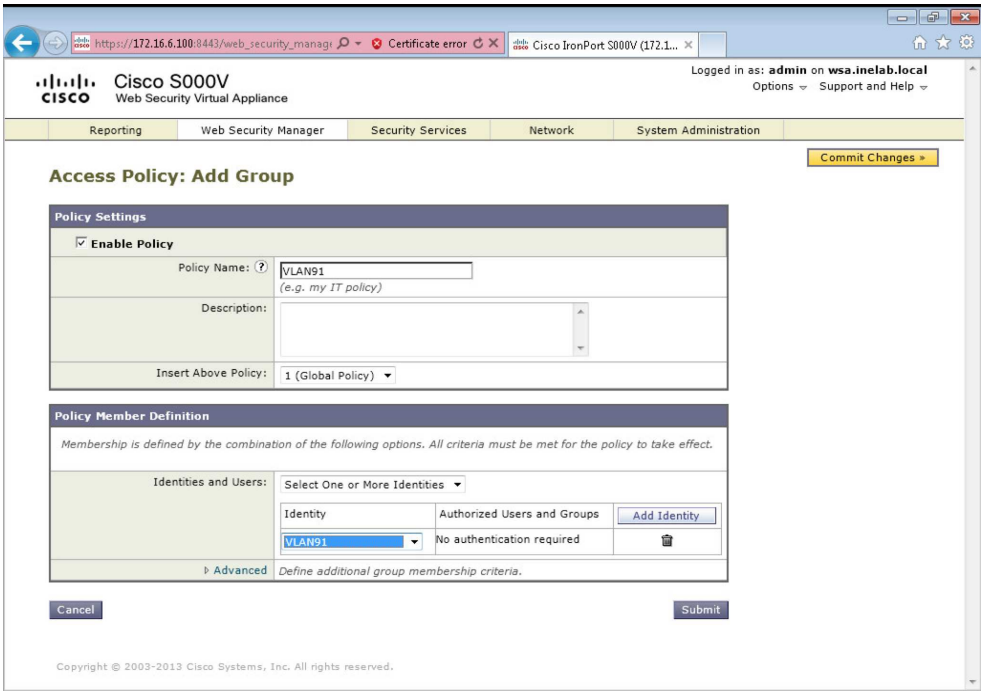
```
ip access-list extended RETURN_TRAFFIC
 permit tcp any eq 80 130.1.91.0 0.0.0.255
!
ip wccp 92 redirect-list RETURN_TRAFFIC group-list GROUP_LIST
!
interface GigabitEthernet0/0.11
 ip wccp 92 redirect in
```

Using Internet Explorer from **TEST-PC-A**, navigate to **https://172.16.6.100:8443**, authenticate and browse to **Web Security Manager -> Identities**, and click **Add Identity**:

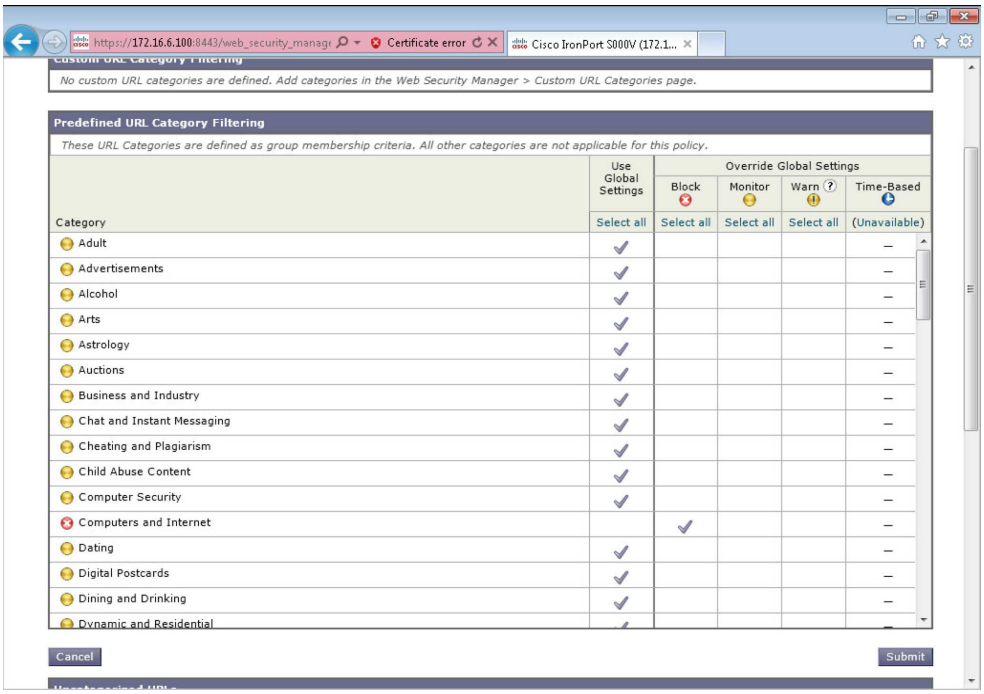


Navigate to **Web Security Manager -> Access Policies** and click **Add Policy**:

https://t.me/learningnets

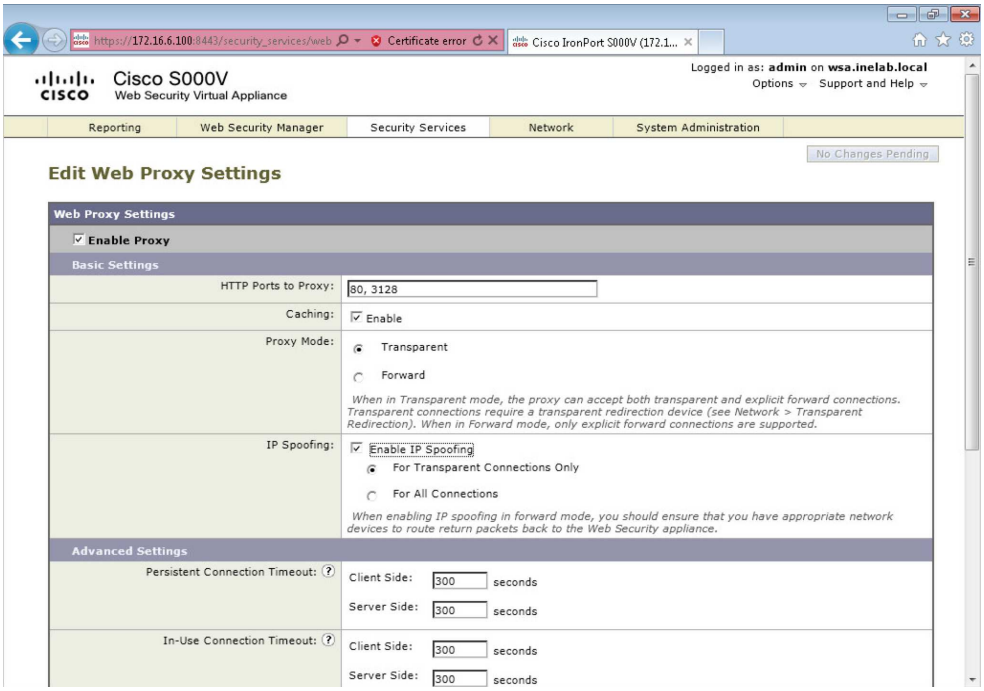


Edit the URL Filtering settings for the configured policy and set the **Block** action for the required category:

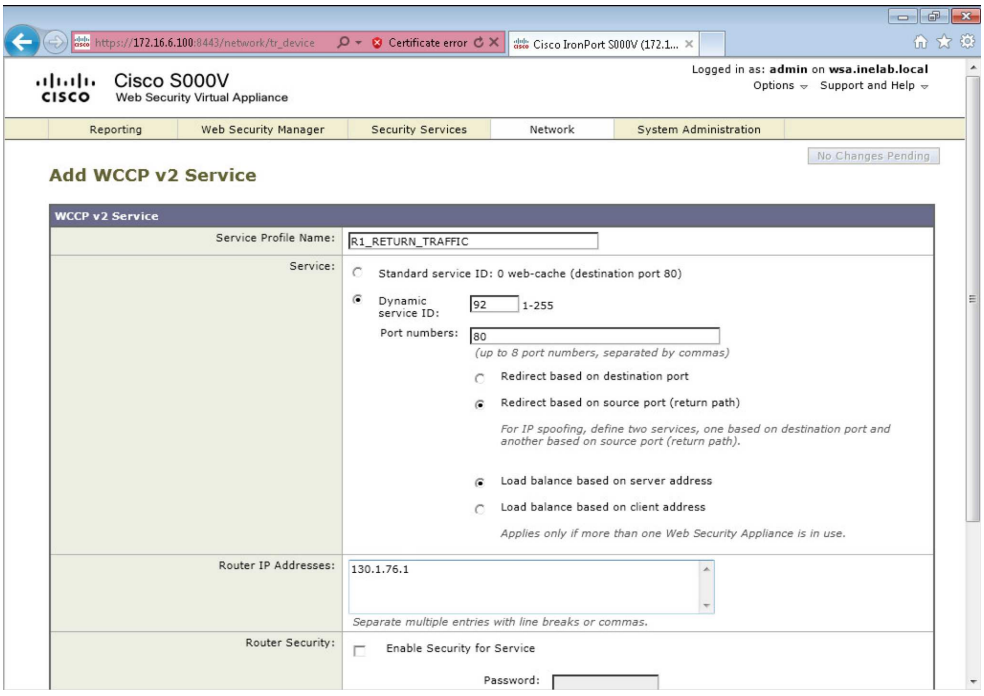


Navigate to **Security Services -> Web Proxy**, click **Edit Settings**, and enable **IP Spoofing**:

https://t.me/learningnets



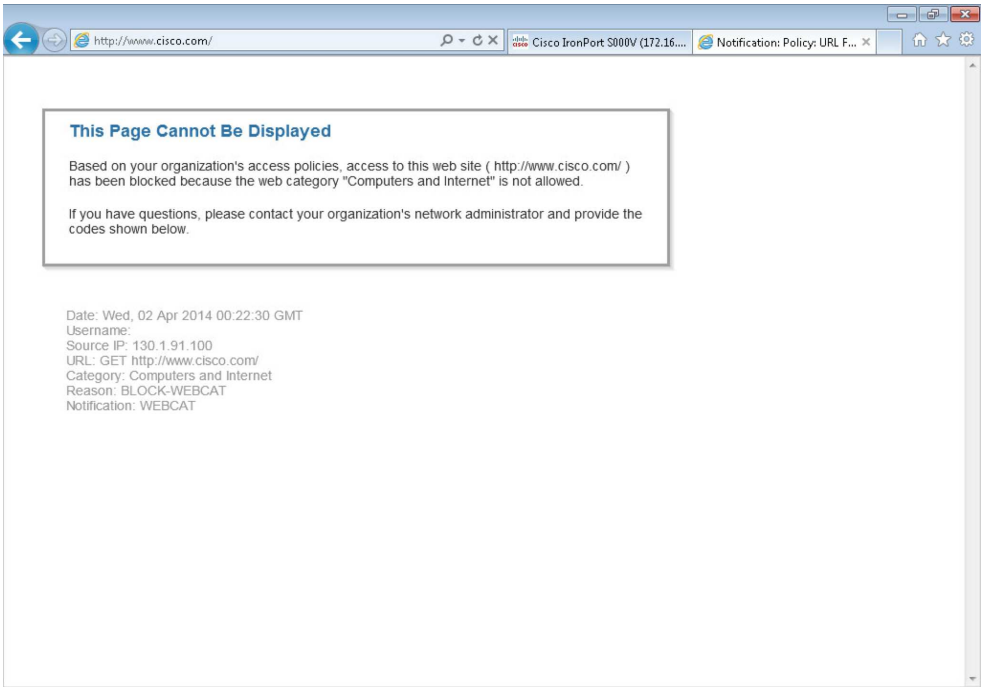
Navigate to **Network -> Transparent Redirection** and click **Add Service**; enable redirection based on source port and use the same service-id as configured on the router:



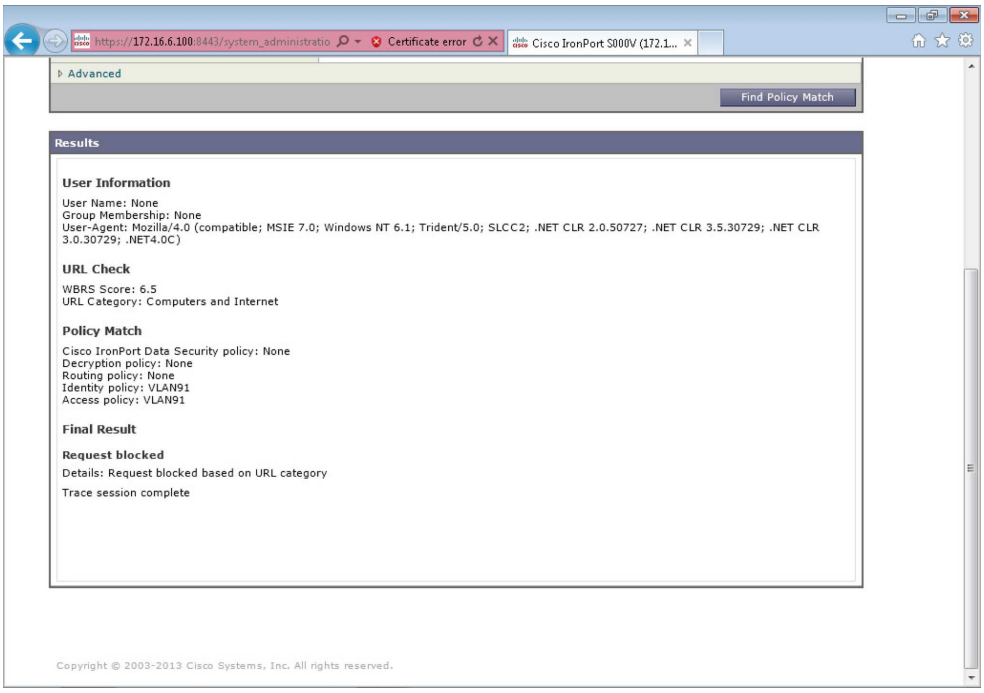
Task 2.6 Verification

From **TEST-PC-A**, browse to **www.cisco.com** and verify that access is restricted based on configured policy:

https://t.me/learningnets



Use the WSA Policy Trace tool to verify the same and also that configured identity/access-policy is being matched:

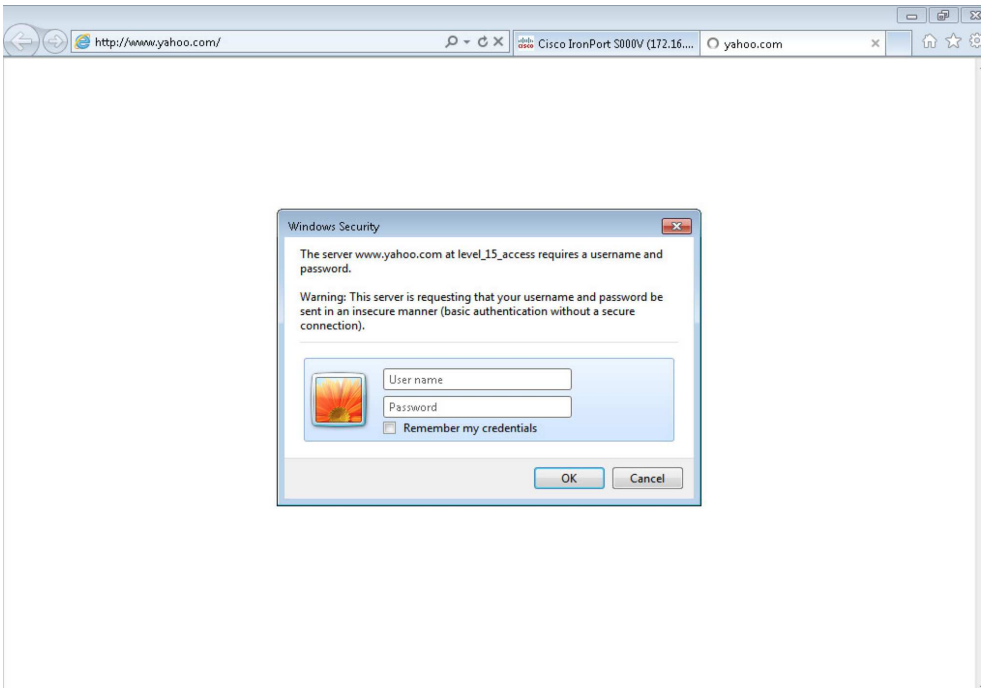


Looking in the WSA logs, the following message is displayed:

```
1396398150.192 10 130.1.91.100
TCP_DENIED/403 0 GET http://www.cisco.com/ - NONE/- - BLOCK_WEBCAT_12-VLAN91-VLAN91
-NONE-NONE-NONE-NONE <IW_comp,6.5,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown",
```

https://t.me/learningnets

Verify that access to **www.yahoo.com** is functional:



Verify that the requested output is matched and the WSA performs IP address spoofing:

```
SW1#show ip http server history


HTTP server history:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes  end-time
      150.1.9.9:80       130.1.91.100:47264 472        192        03:18:07 03/02
      150.1.9.9:80       130.1.91.100:45593 472        192        03:18:50 03/02
      150.1.9.9:80       130.1.91.100:16740 476        192        03:40:52 03/02
```

Verify that access to **www.yahoo.com** is visible in R7's firewall session table:

https://t.me/learningnets

```
R7#show policy-firewall session zone-pair VLAN17_TO_VLAN76

 Zone-pair: VLAN17_TO_VLAN76
  Service-policy inspect : VLAN17_TO_VLAN76
    Class-map : TCP(match-all)
      Established Sessions =  1
Session 4A13F500 (130.1.91.100:20644)=>(150.1.9.9:80) tcp SIS_OPEN/TCP_CLOSEWAIT

          Created 00:02:02, Last heard 00:01:29
          Bytes sent (initiator:responder) [397:253]
    Class-map : class-default(match-any)
```

Verify that the newly created WCCP service is functional:

```
R1#show ip wccp 92
Global WCCP information:
    Router information: Router Identifier:                   150.1.1.1

    Service Identifier: 92
        Protocol Version:                   2.00
        Number of Service Group Clients:    1
        Number of Service Group Routers:    1
        Total Packets Redirected:           30
          Process:                          0
          CEF:                              30
        Service mode:                       Open
        Service Access-list:                -none-
        Total Packets Dropped Closed:       0 Redirect access-list:               RETURN_TRAFFIC
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           1 Group access-list:                  GROUP_LIST

        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total GRE Bypassed Packets Received: 0
          Process:                          0
          CEF:                              0
!
!
R1#show ip wccp summary
WCCP version 2 enabled, 2 services

Service     Clients   Routers   Assign      Redirect   Bypass
-------     -------   -------   ------      --------   ------
Default routing table (Router Id: 150.1.1.1):
```

https://t.me/learningnets

91	1	1	MASK	L2	L2
92	1	1	MASK	L2	L2

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 2

CCIE SCv4 Lab 2 Solutions Section 3

1. Task 3.1 Solution
2. Task 3.2 Solution
3. Task 3.3 Solution
4. Task 3.4 Solution
5. Task 3.5 Solution
6. Task 3.6 Solution

Task 3.1 Solution

ASA1:

```
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 5
!
crypto isakmp enable OUTSIDE
crypto isakmp identity hostname
domain-name inelab.local
!
tunnel-group ASA2.inelab.local type ipsec-l2l
tunnel-group ASA2.inelab.local ipsec-attributes
 pre-shared-key ciscopsk
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
access-list VLAN15_VLAN81 permit ip 172.16.3.0 255.255.255.0 130.1.81.0 255.255.255.0
access-list VLAN15_VLAN81 permit ospf interface OUTSIDE host 130.1.18.16
!
router ospf 202
 network 172.16.3.0 255.255.255.0 area 12
 network 130.1.55.0 255.255.255.0 area 12
 neighbor 130.1.18.16 interface OUTSIDE
```

https://t.me/learningnets

```
!
interface Ethernet0/0
 ospf network point-to-point non-broadcast
!
crypto map VPN 10 match address VLAN15_VLAN81
crypto map VPN 10 set transform-set 3DES_MD5
crypto map VPN 10 set peer 130.1.18.16
crypto map VPN 10 set phase1-mode aggressive group5
!
crypto map VPN interface OUTSIDE
```

ASA2:

```
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 5
!
crypto isakmp enable OUTSIDE
crypto isakmp identity hostname
domain-name inelab.local
!
tunnel-group ASA1.inelab.local type ipsec-l2l
tunnel-group ASA1.inelab.local ipsec-attributes
 pre-shared-key ciscopsk
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
access-list VLAN15_VLAN81 permit ip 130.1.81.0 255.255.255.0 172.16.3.0 255.255.255.0
access-list VLAN15_VLAN81 permit ospf interface OUTSIDE host 130.1.55.15
!
router ospf 202
 network 130.1.18.0 255.255.255.0 area 12
 network 130.1.81.0 255.255.255.0 area 12
 neighbor 130.1.55.15 interface OUTSIDE
!
interface Ethernet0/0
 ospf network point-to-point non-broadcast
!
crypto map VPN 10 match address VLAN15_VLAN81
crypto map VPN 10 set transform-set 3DES_MD5
crypto map VPN 10 set peer 130.1.55.15
crypto map VPN 10 set phase1-mode aggressive group5
!
crypto map VPN interface OUTSIDE
```

https://t.me/learningnets

```
!
management-access INSIDE
!
access-list NAT0 extended permit ip 130.1.81.0 255.255.255.0 172.16.3.0 255.255.255.0
nat (INSIDE) 0 access-list NAT0
```

Task 3.1 Verification

Verify that the requested output is matched:

```
ASA1# show vpn-sessiondb l2l

Session Type: LAN-to-LAN

Connection   : ASA2.inelab.local
Index        : 6                     IP Addr      : 130.1.18.16
Protocol     : IKE IPsec
Encryption   : 3DES                  Hashing      : MD5
Bytes Tx     : 2964                  Bytes Rx     : 3084
Login Time   : 08:42:08 UTC Wed Apr 2 2014
Duration     : 0h:06m:14s
!
!ASA2# show vpn-sessiondb l2l


Session Type: LAN-to-LAN

Connection   : ASA1.inelab.local
Index        : 6                     IP Addr      : 130.1.55.15
Protocol     : IKE IPsec
Encryption   : 3DES                  Hashing      : MD5
Bytes Tx     : 3152                  Bytes Rx     : 3032
Login Time   : 08:42:06 UTC Wed Apr 2 2014
Duration     : 0h:06m:29s
```

Verify that ISE1 can ping ASA2's INSIDE interface through the IPsec tunnel:

```
ISE1/admin# ping 130.1.81.16
ping 130.1.81.16
PING 130.1.81.16 (130.1.81.16) 56(84) bytes of data.
64 bytes from 130.1.81.16: icmp_seq=1 ttl=255 time=2.04 ms
64 bytes from 130.1.81.16: icmp_seq=2 ttl=255 time=1.57 ms
64 bytes from 130.1.81.16: icmp_seq=3 ttl=255 time=1.54 ms
64 bytes from 130.1.81.16: icmp_seq=4 ttl=255 time=1.60 ms
```

https://t.me/learningnets

```
--- 130.1.81.16 ping statistics ---4 packets transmitted, 4 received, 0% packet loss, time 3002ms

rtt min/avg/max/mdev = 1.549/1.692/2.041/0.202 ms
```

Verify that ASA1 and ASA2 are OSPF neighbors and routes are learned:

```
ASA1# show ospf neighbor



Neighbor ID     Pri   State           Dead Time   Address         Interface
130.1.81.16       1   FULL/  -        0:00:34     130.1.18.16     OUTSIDE
!
!ASA1# show route OUTSIDE | i 130.1.18.16
O    130.1.18.0 255.255.255.0 [110/20] via 130.1.18.16, 0:08:43, OUTSIDE
O    130.1.81.0 255.255.255.0 [110/20] via 130.1.18.16, 0:08:43, OUTSIDE
!
!ASA2# show ospf neighbor



Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.3.1        1   FULL/  -        0:00:36     130.1.55.15     OUTSIDE
!
!ASA2# show route OUTSIDE | i 130.1.55.15
O    172.16.3.0 255.255.255.0 [110/20] via 130.1.55.15, 0:09:39, OUTSIDE

O    130.1.55.0 255.255.255.0 [110/20] via 130.1.55.15, 0:09:39, OUTSIDE
```

Verify the state of both IKEv1 and IPsec tunnels and the negotiated algorithms:

```
ASA2# show vpn-sessiondb detail l2l



Session Type: LAN-to-LAN Detailed

Connection    : ASA1.inelab.local
Index         : 6                     IP Addr      : 130.1.55.15
Protocol      : IKE IPsec
Encryption    : 3DES                  Hashing      : MD5
Bytes Tx      : 4984                  Bytes Rx     : 4864
Login Time    : 08:42:06 UTC Wed Apr 2 2014
Duration      : 0h:10m:05sIKE Tunnels: 1
IPsec Tunnels: 2
```

https://t.me/learningnets

```
IKE:

  Tunnel ID    : 6.1
  UDP Src Port : 500                    UDP Dst Port : 500
IKE Neg Mode : Aggressive               Auth Mode    : preSharedKeys
Encryption   : 3DES                     Hashing      : MD5
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 85794 Seconds D/H Group    : 5
  Filter Name  :
IPsec:
  Tunnel ID    : 6.2 Local Addr   : 130.1.18.16/255.255.255.255/89/0
Remote Addr  : 130.1.55.15/255.255.255.255/89/0
Encryption   : 3DES                     Hashing      : MD5

  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28194 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4607996 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 4396                   Bytes Rx     : 4276
  Pkts Tx      : 65                     Pkts Rx      : 63
IPsec:
  Tunnel ID    : 6.3 Local Addr   : 130.1.81.0/255.255.255.0/0/0
Remote Addr  : 172.16.3.0/255.255.255.0/0/0
Encryption   : 3DES                     Hashing      : MD5

  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28446 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 26 Minutes
  Bytes Tx     : 588                    Bytes Rx     : 588
  Pkts Tx      : 7                      Pkts Rx      : 7

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 607 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

Task 3.2 Solution

ASA2:

```
webvpn
 port 443
 enable OUTSIDE
```

https://t.me/learningnets

```
 svc image disk0:/anyconnect-win-3.0.11042-k9.pkg
 svc enable
!
access-list SPLIT_TUNNEL standard permit 130.1.81.0 255.255.255.0
!
group-policy CCIELAB internal
group-policy CCIELAB attributes
 vpn-tunnel-protocol svc
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT_TUNNEL
 webvpn
  svc dtls enable
!
ip local pool ANYCONNECT_POOL 130.200.0.1-130.200.0.254
!
tunnel-group CCIELAB type remote-access
tunnel-group CCIELAB general-attributes
 authentication-server-group LOCAL
 default-group-policy CCIELAB
 address-pool ANYCONNECT_POOL
!
tunnel-group CCIELAB webvpn-attributes
 group-url https://130.1.18.16/CCIELAB enable
 authentication aaa
!
username cisco password cisco
username cisco attributes
 service-type remote-access
!
management-access INSIDE
telnet 130.200.0.0 255.255.255.0 INSIDE
aaa authentication telnet console LOCAL
aaa authorization exec LOCAL
```

Task 3.2 Verification

From **TEST-PC-A**, start **AnyConnect**; in the connect window type **130.1.18.16/CCIELAB** and authenticate with **cisco/cisco** as username/password. Verify that DTLS was negotiated and most of the traffic is using the DTLS tunnel by packet counters:

```
ASA2# show vpn-sessiondb detail svc
```

https://t.me/learningnets

```
Session Type: SVC Detailed
Username     : cisco                  Index        : 13
Assigned IP  : 130.200.0.1            Public IP    : 130.1.91.100
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : SSL VPN
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 14574                  Bytes Rx     : 3926
Pkts Tx      : 53                     Pkts Rx      : 29
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : CCIELAB                Tunnel Group : CCIELAB
Login Time   : 09:56:57 UTC Wed Apr 2 2014
Duration     : 0h:09m:33s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

Clientless Tunnels: 1 SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

Clientless:
  Tunnel ID    : 13.1
  Public IP    : 130.1.91.100
  Encryption   : RC4                    Hashing      : SHA1
  Encapsulation: TLSv1.0                TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 20 Minutes
  Client Type  : Web Browser
  Client Ver   : AnyConnect Windows 3.0.11042
  Bytes Tx     : 12171                  Bytes Rx     : 2910
SSL-Tunnel:
  Tunnel ID    : 13.2
  Assigned IP  : 130.200.0.1            Public IP    : 130.1.91.100
  Encryption   : RC4                    Hashing      : SHA1
Encapsulation: TLSv1.0                TCP Src Port : 20722
                TCP Dst Port : 443                  Auth Mode    : userPassword

  Idle Time Out: 30 Minutes             Idle TO Left : 20 Minutes
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.0.11042
  Bytes Tx     : 721                    Bytes Rx     : 63
Pkts Tx      : 1                      Pkts Rx      : 1

  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
DTLS-Tunnel:
  Tunnel ID    : 13.3
  Assigned IP  : 130.200.0.1            Public IP    : 130.1.91.100
```

https://t.me/learningnets

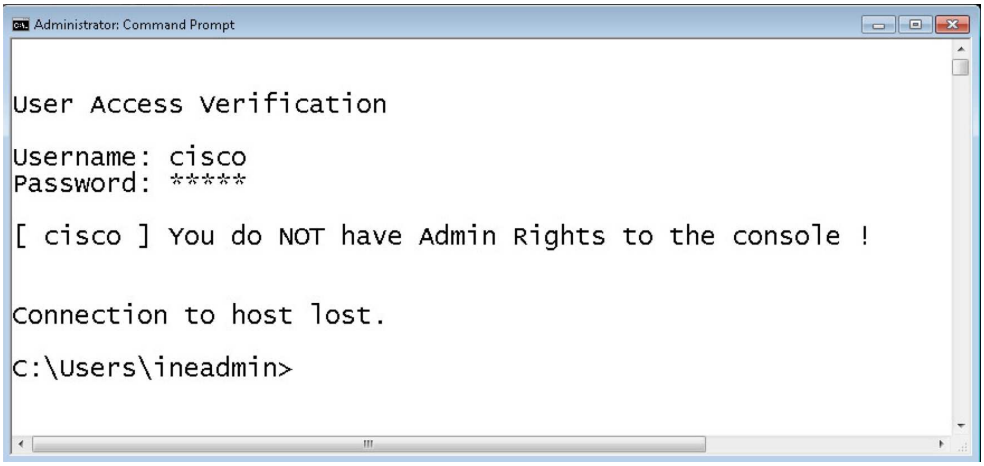
```
  Encryption    : AES128                  Hashing      : SHA1
Encapsulation: DTLSv1.0                 UDP Src Port : 50943
                UDP Dst Port : 443                    Auth Mode    : userPassword

  Idle Time Out: 30 Minutes             Idle TO Left : 21 Minutes
  Client Type  : DTLS VPN Client
  Client Ver   : AnyConnect Windows 3.0.11042
  Bytes Tx     : 1682                   Bytes Rx     : 953
Pkts Tx       : 38                      Pkts Rx      : 22

  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 578 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

When the AnyConnect session is successfully established, verify that requested output is matched; users are not allowed to authenticate with the VPN user on a telnet session:



Task 3.3 Solution

R4:

```
crypto map VPN client configuration address respond
crypto map VPN isakmp authorization list EZVPN
crypto map VPN local-address Loopback0
```

R6:

```
crypto ipsec client ezvpn EZVPN_CLIENT
 mode network-extension
```

https://t.me/learningnets

```
!
interface FastEthernet0/1
 no crypto ipsec client ezvpn EZVPN_CLIENT inside
 crypto ipsec client ezvpn EZVPN_CLIENT outside
!
interface FastEthernet0/0.69
 no crypto ipsec client ezvpn EZVPN_CLIENT outside
 crypto ipsec client ezvpn EZVPN_CLIENT inside

ASA4 VLAN16 Context:
object-group service VPN
 service-object esp
 service-object udp destination eq 500
!
access-list OUTSIDE_IN permit object-group VPN host 150.1.6.6 host 150.1.4.4

ASA1:

object-group service VPN
 service-object esp
 service-object udp eq 500
!
access-list OUTSIDE_IN permit object-group VPN host 150.1.6.6 host 150.1.4.4
```

Task 3.3 Verification

On R6, trigger XAUTH using the command **`crypto ipsec client ezvpn xauth`** :

```
R6#
EZVPN(EZVPN_CLIENT): Pending XAuth Request, Please enter the following command:
EZVPN: crypto ipsec client ezvpn xauth
R6#crypto ipsec client ezvpn xauth
Username: ezvpn
Password:
R6#
%CRYPTO-6-EZVPN_CONNECTION_UP: (Client)  User=  Group=EZVPN  Client_public_addr=130.1.16.6  Server_public_addr=150.1
```

Verify that requested output is matched:

```
R6#show crypto ipsec client ezvpn

Easy VPN Remote Phase: 8
```

https://t.me/learningnets

```
Tunnel name : EZVPN_CLIENT
Inside interface list: FastEthernet0/0.69
Outside interface: FastEthernet0/1
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Save Password: Disallowed
Split Tunnel List: 1
       Address    : 130.1.44.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Current EzVPN Peer: 150.1.4.4
```

Generate traffic through the tunnel and verify IKEv1/IPsec tunnel state and packet counters:

https://t.me/learningnets

```
R6#ping 130.1.44.4 source fastEthernet0/0.69


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 130.1.44.4, timeout is 2 seconds:
Packet sent with a source address of 130.1.69.6 !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!
!R6#show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: FastEthernet0/1
Uptime: 00:03:55
Session status: UP-ACTIVE
Peer: 150.1.4.4 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 150.1.4.4
      Desc: (none) IKEv1 SA: local 150.1.6.6/500 remote 150.1.4.4/500 Active

          Capabilities:CX connid:1138 lifetime:23:55:00
 IPSEC FLOW: permit ip 130.1.69.0/255.255.255.0 130.1.44.0/255.255.255.0

        Active SAs: 2, origin: crypto map Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) 4461576/3354
 Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) 4461576/3354
```

Verify the connection table on both ASA1 and ASA4:

```
ASA34/VLAN16/act# show conn address 150.1.6.6
9 in use, 16 most used
ESP OUTSIDE 150.1.6.6 INSIDE 150.1.4.4, idle 0:00:11, bytes 620
UDP OUTSIDE 150.1.6.6:500 INSIDE 150.1.4.4:500, idle 0:00:18, bytes 4737, flags -
ESP OUTSIDE 150.1.6.6 INSIDE 150.1.4.4, idle 0:00:11, bytes 620
!
!ASA1# show conn address 150.1.6.6

12 in use, 18 most used
ESP OUTSIDE 150.1.6.6 INSIDE 150.1.4.4, idle 0:00:02, bytes 620
UDP OUTSIDE 150.1.6.6:500 INSIDE 150.1.4.4:500, idle 0:00:51, bytes 4737, flags -
```

https://t.me/learningnets

```
ESP OUTSIDE 150.1.6.6 INSIDE 150.1.4.4, idle 0:00:02, bytes 620
```

Task 3.4 Solution

R4:

```
no crypto map VPN client authentication list EZVPN
no crypto map VPN isakmp authorization list EZVPN
no crypto map VPN client configuration address respond
!
crypto isakmp profile EZVPN
 match identity group EZVPN
 client authentication list EZVPN
 isakmp authorization list EZVPN
 client configuration address respond
!
crypto dynamic-map EZVPN_DYNAMIC 100
 set isakmp-profile EZVPN
!
interface tunnel 0
 ip summary-address eigrp 124 150.1.0.0 255.255.0.0
```

ASA3 VLAN13 Context:

```
object-group service VPN
 service-object esp
 service-object udp destination eq 500
!
object-group network DMVPN_DESTINATION
 network-object host 150.1.1.1
 network-object host 150.1.4.4
!
access-list OUTSIDE_IN permit object-group VPN host 150.1.2.2 object-group DMVPN_DESTINATION
```

ASA1:

```
object-group network DMVPN_SOURCE
 network-object host 150.1.1.1
 network-object host 150.1.2.2
!
access-list OUTSIDE_IN permit object-group VPN object-group DMVPN_SOURCE host 150.1.4.4
```

https://t.me/learningnets

Task 3.4 Verification

Verify that the requested output is being matched:

```
R1#ping vrf DMVPN 150.1.22.22 source loopback1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.22.22, timeout is 2 seconds:
Packet sent with a source address of 150.1.11.11 !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!R1#show ip route  vrf DMVPN nhrp


Routing Table: DMVPN
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      150.1.0.0/16 is variably subnetted, 3 subnets, 2 masks
H        150.1.22.22/32 [250/1] via 130.1.220.2, 00:00:07, Tunnel0
```

Verify the VRF EIGRP adjacencies and routing table:

```
R4#show ip eigrp vrf DMVPN neighbors

EIGRP-IPv4 Neighbors for AS(124) VRF(DMVPN)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   130.1.220.1             Tu0               11 00:11:23   12  1458  0  3
0   130.1.220.2             Tu0               10 00:14:31    6  3280  0  3
!
!R4#show ip route vrf DMVPN eigrp


Routing Table: DMVPN
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

https://t.me/learningnets

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      150.1.0.0/16 is variably subnetted, 4 subnets, 2 masks
D        150.1.0.0/16 is a summary, 01:37:36, Null0
D        150.1.11.11/32 [90/27008000] via 130.1.220.1, 00:11:45, Tunnel0
D        150.1.22.22/32 [90/27008000] via 130.1.220.2, 00:14:52, Tunnel0
```

Verify the NHRP mappings and IKE/IPsec tunnel states on the hub:

```
R4#show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface Tunnel0 is up/up, Addr. is 130.1.220.4, VRF "DMVPN"
   Tunnel Src./Dest. addr: 150.1.4.4/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN"
   Interface State Control: Disabled
Type:Hub, Total NBMA Peers (v4/v6): 2

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
1      150.1.1.1     130.1.220.1    UP 00:12:43    D     130.1.220.1/32
 1      150.1.2.2     130.1.220.2    UP 00:15:50    D     130.1.220.2/32



Crypto Session Details:
--------------------------------------------------------------------------------

Interface: Tunnel0
Session: [0x4B0C56CC]
```

https://t.me/learningnets

```
IKEv1 SA: local 150.1.4.4/500 remote 150.1.1.1/500 Active

          Capabilities:(none) connid:4104 lifetime:23:47:15
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 150.1.1.1 IPSEC FLOW: permit 47 host 150.1.4.4 host 150.1.1.1

        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 180 drop 0 life (KB/Sec) 4483802/2835
        Outbound: #pkts enc'ed 179 drop 0 life (KB/Sec) 4483802/2835
   Outbound SPI : 0x75CEFDE3, transform : esp-3des esp-md5-hmac
    Socket State: Open

Interface: Tunnel0
Session: [0x4B0C57BC] IKEv1 SA: local 150.1.4.4/500 remote 150.1.2.2/500 Active
          Capabilities:(none) connid:4099 lifetime:23:44:09
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 150.1.2.2 IPSEC FLOW: permit 47 host 150.1.4.4 host 150.1.2.2

        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 217 drop 0 life (KB/Sec) 4501381/2649
        Outbound: #pkts enc'ed 219 drop 1 life (KB/Sec) 4501381/2649
   Outbound SPI : 0x35B8A9DF, transform : esp-3des esp-md5-hmac
    Socket State: Open

Pending DMVPN Sessions:

Interface: FastEthernet0/0
```

Verify NHRP mappings and IKE/IPsec tunnel states on the spoke, and note the spoke-to-spoke tunnel:

```
R1#show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
============================================================================

Interface Tunnel0 is up/up, Addr. is 130.1.220.1, VRF "DMVPN"
   Tunnel Src./Dest. addr: 150.1.1.1/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN"
   Interface State Control: Disabled
   nhrp event-publisher : Disabled
```

https://t.me/learningnets

```
IPv4 NHS:
130.1.220.4  RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 3

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
2       150.1.2.2     130.1.220.2     UP 00:05:53     D     130.1.220.2/32
    0       150.1.2.2     130.1.220.2     UP 00:05:53  DT1     150.1.22.22/32
 1       150.1.4.4     130.1.220.4     UP 00:14:05     S     130.1.220.4/32

    1       150.1.1.1     130.1.220.1     UP 00:05:53  DLX     150.1.11.11/32



Crypto Session Details:
--------------------------------------------------------------------------------

Interface: Tunnel0
Session: [0x316E80C4] IKEv1 SA: local 150.1.1.1/500 remote 150.1.2.2/500 Active
          Capabilities:(none) connid:1010 lifetime:23:54:06
  IKEv1 SA: local 150.1.1.1/500 remote 150.1.2.2/500 Active
          Capabilities:(none) connid:1011 lifetime:23:54:06
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 150.1.2.2 IPSEC FLOW: permit 47 host 150.1.1.1 host 150.1.2.2
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 6 drop 0 life (KB/Sec) 4356462/3246
        Outbound: #pkts enc'ed 6 drop 0 life (KB/Sec) 4356462/3246
   Outbound SPI : 0x26785100, transform : esp-3des esp-md5-hmac
    Socket State: Open

Interface: Tunnel0
Session: [0x316E7FCC] IKEv1 SA: local 150.1.1.1/500 remote 150.1.4.4/500 Active
          Capabilities:(none) connid:1006 lifetime:23:45:54
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 150.1.4.4 IPSEC FLOW: permit 47 host 150.1.1.1 host 150.1.4.4

        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 197 drop 0 life (KB/Sec) 4157217/2754
        Outbound: #pkts enc'ed 197 drop 0 life (KB/Sec) 4157217/2754
   Outbound SPI : 0xEC56BA50, transform : esp-3des esp-md5-hmac
    Socket State: Open
```

https://t.me/learningnets

```
Pending DMVPN Sessions:
```

Task 3.5 Solution

R1:

```
aaa new-model
aaa authorization network IKE_LIST local
!
interface Tunnel12
 ip unnumbered Loopback2
 tunnel source GigabitEthernet0/0.11
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
!
interface Loopback2
 ip address 150.1.111.1 255.255.255.255
!
crypto ikev2 client flexvpn R1_R2_CLIENT
 peer 1 130.1.32.2
 connect auto
 client connect Tunnel12
!
ip access-list standard FLEXVPN
 permit host 150.1.111.1
!
crypto ikev2 authorization policy default
 route set access-list FLEXVPN
!
crypto ikev2 keyring R1_R2_KEYRING
 peer R2
  address 130.1.32.2
  pre-shared-key local ikev2key
  pre-shared-key remote ikev2key
!
crypto ikev2 profile R1_R2_PROFILE
 match identity remote address 130.1.32.2
 authentication local pre-share
 authentication remote pre-share
 keyring local R1_R2_KEYRING
 aaa authorization group psk list IKE_LIST default
!
crypto ipsec profile default
 set ikev2-profile R1_R2_PROFILE
```

https://t.me/learningnets

R2:

```
aaa new-model
aaa authorization network IKE_LIST local
!
interface Loopback2
 ip address 150.1.111.2 255.255.255.255
!
ip access-list standard FLEXVPN
 permit host 150.1.111.2
!
crypto ikev2 authorization policy default
 route set access-list FLEXVPN
!
crypto ikev2 keyring R1_R2_KEYRING
 peer R1
  address 130.1.11.1
  pre-shared-key local ikev2key
  pre-shared-key remote ikev2key
!
crypto ikev2 profile R1_R2_PROFILE
 match identity remote address 130.1.11.1
 authentication local pre-share
 authentication remote pre-share
 keyring local R1_R2_KEYRING
 aaa authorization group psk list IKE_LIST default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile R1_R2_PROFILE
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback2
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default


ASA3 VLAN13 Context:
access-list OUTSIDE_IN extended permit esp host 130.1.32.2 host 130.1.11.1
```

https://t.me/learningnets

Task 3.5 Verification

Verify that output is being matched:

```
R1#show crypto ikev2 client flexvpn


  Profile : R1_R2_CLIENT
  Current state:ACTIVE
  Peer : 130.1.32.2
  Source : GigabitEthernet0/0.11
  ivrf : IP DEFAULT
  fvrf : IP DEFAULT
  Backup group: Default
  Tunnel interface : Tunnel12
```

Verify the IKEv2/IPsec tunnel states:

```
R1#show crypto ikev2 session detailed

 IPv4 Crypto IKEv2 Session
Session-id:6, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         130.1.11.1/500        130.1.32.2/500        none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1456 sec
      CE id: 1009, Session-id: 6
      Status Description: Negotiation done
      Local spi: 7CFE95677EB0BD2B       Remote spi: 5EF0B6AB23CFBB05
      Local id: 130.1.11.1
      Remote id: 130.1.32.2
      Local req msg id:  3              Remote req msg id:  0
      Local next msg id: 3              Remote next msg id: 0
      Local req queued:  3              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes Remote subnets:
150.1.111.2 255.255.255.255

Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
```

https://t.me/learningnets

```
          ESP spi in/out: 0x4A39B7C7/0x54BAD197
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

 IPv6 Crypto IKEv2 Session
```

Verify that traffic between Loopback2 interfaces is sent through the tunnel:

```
R1#ping 150.1.111.2 source loopback2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.111.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.111.1 !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!R1#show crypto ipsec sa peer 130.1.32.2

interface: Tunnel12
    Crypto map tag: Tunnel12-head-0, local addr 130.1.11.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 130.1.32.2 port 500
     PERMIT, flags={origin_is_acl,} #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 130.1.11.1, remote crypto endpt.: 130.1.32.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0.11
     current outbound spi: 0x54BAD197(1421529495)
     PFS (Y/N): N, DH group: none
 inbound esp sas:
      spi: 0x4A39B7C7(1245296583)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2016, flow_id: Onboard VPN:16, sibling_flags 80000040, crypto map: Tunnel12-head-0
        sa timing: remaining key lifetime (k/sec): (4351895/2355)
        IV size: 16 bytes
        replay detection support: Y Status: ACTIVE(ACTIVE)
```

https://t.me/learningnets

```
     inbound ah sas:

     inbound pcp sas:
 outbound esp sas:
      spi: 0x54BAD197(1421529495)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2015, flow_id: Onboard VPN:15, sibling_flags 80000040, crypto map: Tunnel12-head-0
        sa timing: remaining key lifetime (k/sec): (4351895/2355)
        IV size: 16 bytes
        replay detection support: Y Status: ACTIVE(ACTIVE)


     outbound ah sas:

     outbound pcp sas:
```

Verify IKEv2 routing installing static routes:

```
R1#show ip route static

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      130.1.0.0/16 is variably subnetted, 22 subnets, 3 masks
S        130.1.8.0/27 [1/0] via 130.1.18.16
      150.1.0.0/16 is variably subnetted, 11 subnets, 2 masks
S        150.1.111.2/32 is directly connected, Tunnel12
!
!R2#show ip route static

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

https://t.me/learningnets

```
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

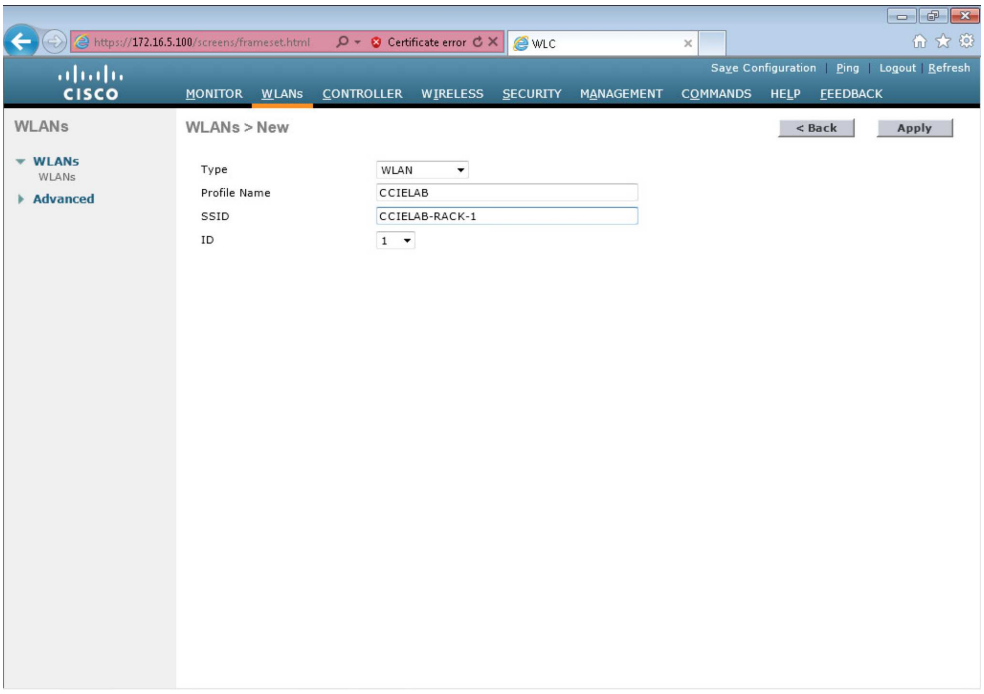
      150.1.0.0/16 is variably subnetted, 11 subnets, 2 masks
S        150.1.111.1/32 is directly connected, Virtual-Access1
```

Task 3.6 Solution

ASA3 VLAN16 Context:

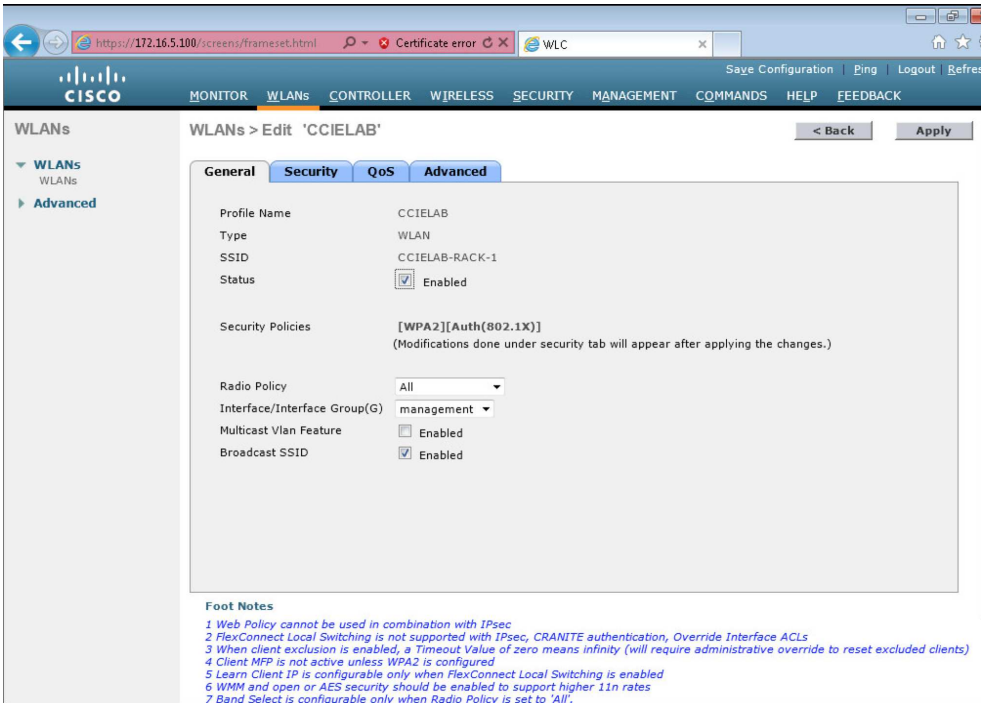
```
access-list OUTSIDE_IN permit udp 130.1.6.0 255.255.255.0 host 172.16.5.100 eq 5246
access-list OUTSIDE_IN permit udp 130.1.6.0 255.255.255.0 host 172.16.5.100 eq 5247
```

From **TEST-PC-A**, using Internet Explorer navigate through WLC GUI, and on the **WLANs** tab select **Create New** and click **Go**:

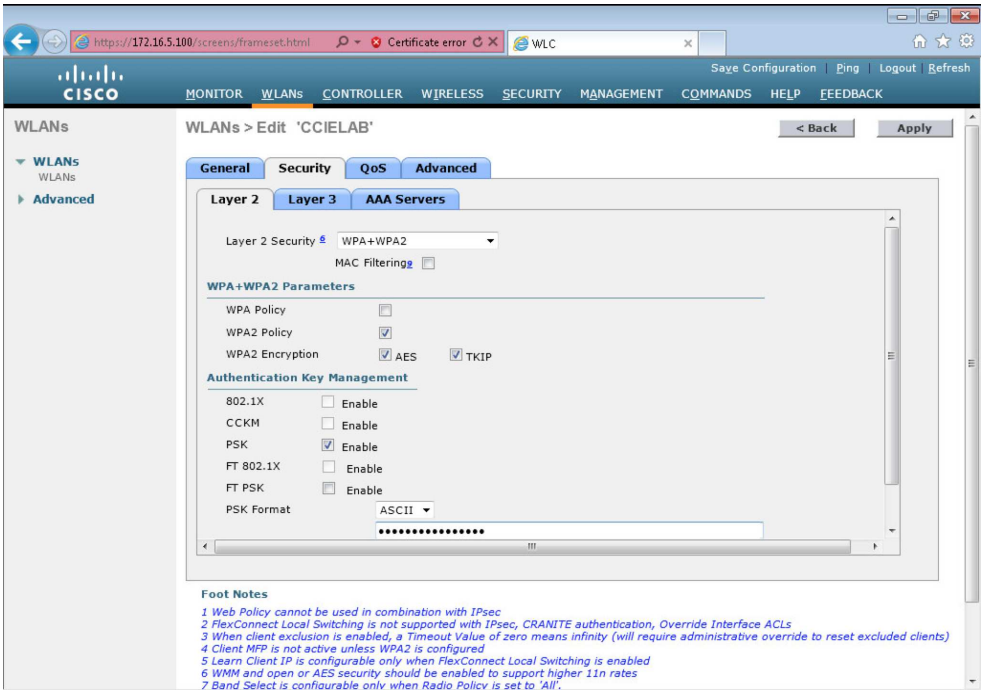


In the **General** section, enable the SSID:

https://t.me/learningnets

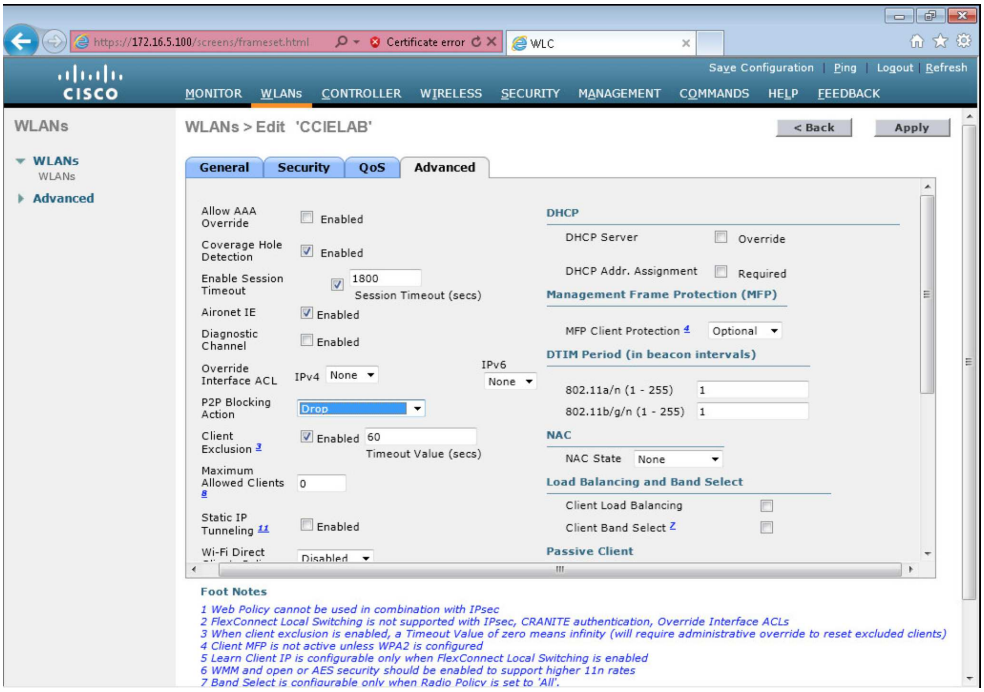


In **Security -> Layer2** select **WPA+WPA2** and enable PSK authentication with both AES and TKIP as encryption algorithms:

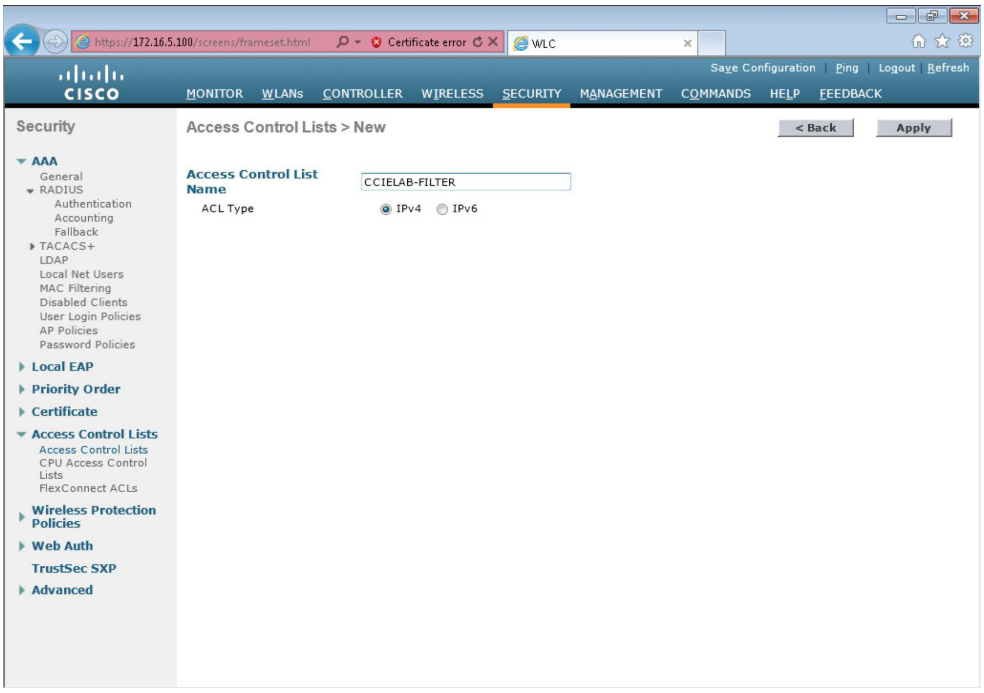


In the **Advanced** section, set the **P2P Blocking Action** to drop:

https://t.me/learningnets

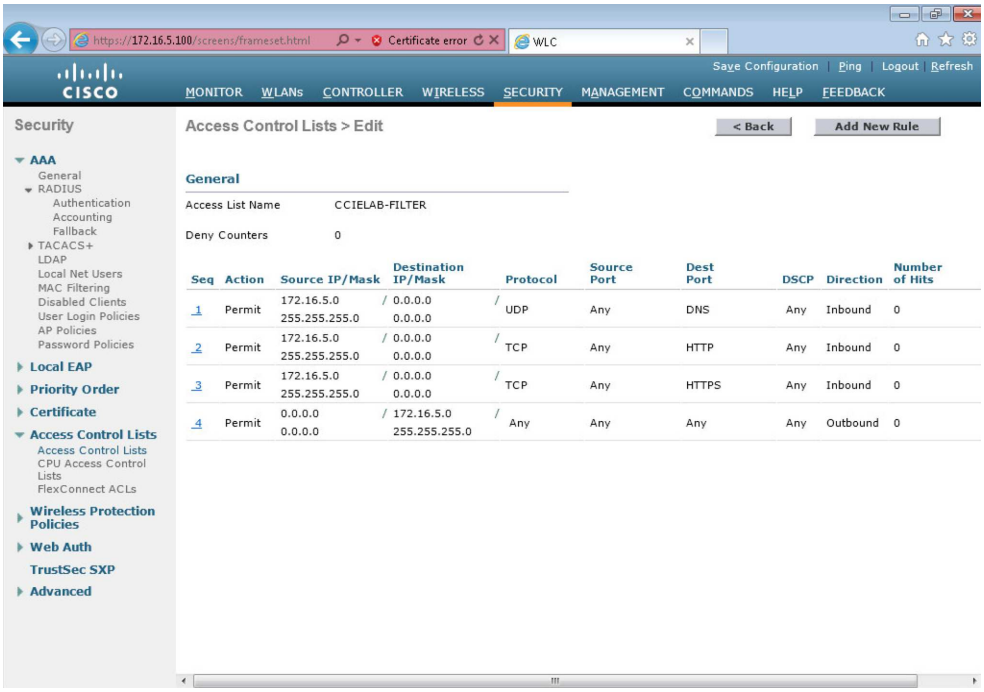


Navigate to **Security -> Access Control Lists -> Access Control Lists**, click **New**, give it a name, and click **Apply**:

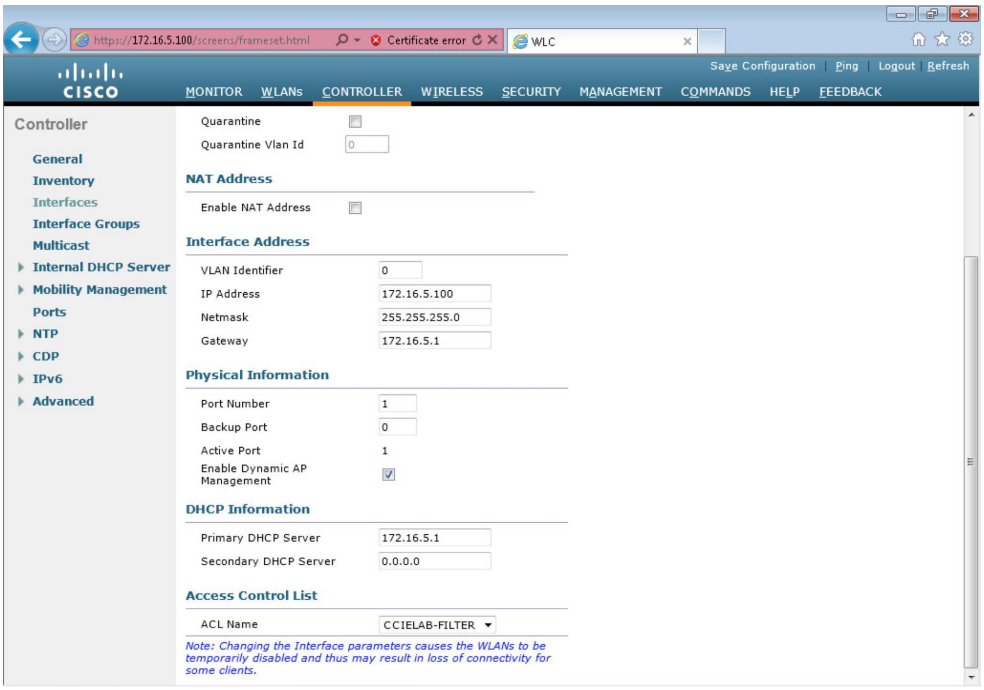


Configure the ACL to match the requirements:

https://t.me/learningnets



Navigate to **Controller -> Interfaces**, edit the **management** interface, and apply the configured ACL:



Task 3.6 Verification

Configure the **WIFI-PC** to join the configured SSID. Verify that LAP joined the WLC, that **WIFI-PC** is associated and authenticated, and that it has been assigned IPv4 address by R3:

```
(Cisco Controller) >show ap summary
```

https://t.me/learningnets

```
Number of APs.................................. 1

Global AP User Name............................ Not Configured
Global AP Dot1x User Name...................... Not Configured

AP Name             Slots  AP Model              Ethernet MAC       Location          Port  Country  Priority
------------------  -----  --------------------  -----------------  ----------------  ----  -------  --------
RACK1-AP             2     AIR-LAP1262N-A-K9     00:06:f6:3b:9a:da  default location  1        US       1
!
!(Cisco Controller) >show client summary


Number of Clients.............................. 1

MAC Address       AP Name           Status        WLAN/RLAN      Auth Protocol         Port Wired
----------------- ----------------- ------------- -------------- ---- ---------------- ---- -----
ac:f1:df:13:bd:8f RACK1-AP          Associated    1              Yes  802.11n(2.4 GHz) 1    N/A
!
!R3#show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
172.16.5.2          01ac.f1df.13bd.8f       Apr 03 2014 07:40 PM    Automatic
```

Verify the ACL configuration and that it is applied; note that counters have a value of zero as have not been activated:

```
(Cisco Controller) >show acl detailed CCIELAB-FILTER


                      Source                      Destination                Source Port  Dest Port
Index  Dir       IP Address/Netmask              IP Address/Netmask       Prot    Range       Range    DSCP  Action
------ --- ------------------------------ ------------------------------ ---- ----------- ----------- ----- ------
     1  In      172.16.5.0/255.255.255.0          0.0.0.0/0.0.0.0          17     0-65535    53-53     Any Permit
     2  In      172.16.5.0/255.255.255.0          0.0.0.0/0.0.0.0           6     0-65535    80-80     Any Permit
     3  In      172.16.5.0/255.255.255.0          0.0.0.0/0.0.0.0           6     0-65535   443-443    Any Permit
     4 Out         0.0.0.0/0.0.0.0             172.16.5.0/255.255.255.0    Any     0-65535     0-65535  Any Permit

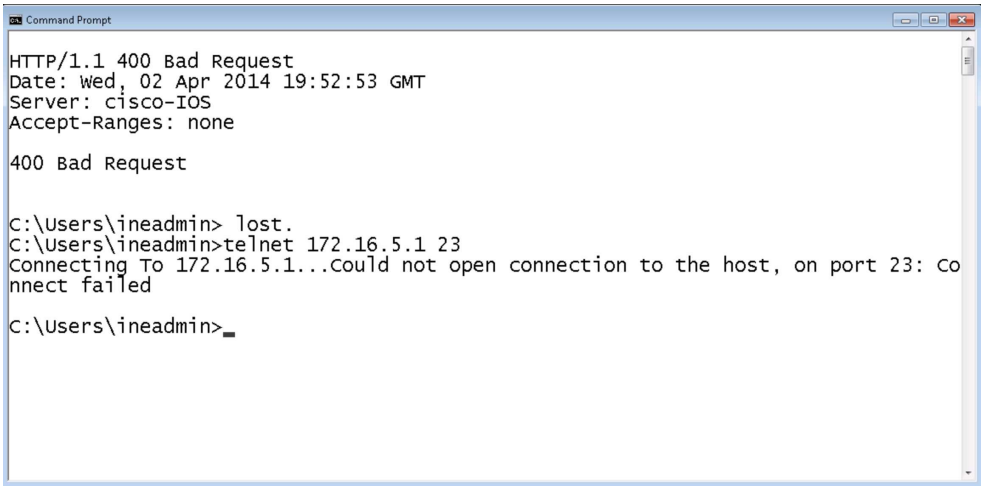
 DenyCounter : 0
!
!(Cisco Controller) >show interface detailed management
```

https://t.me/learningnets

```
Interface Name................................. management
MAC Address.................................... 68:86:a7:37:b2:c0
IP Address..................................... 172.16.5.100
IP Netmask..................................... 255.255.255.0
IP Gateway..................................... 172.16.5.1
External NAT IP State.......................... Disabled
External NAT IP Address........................ 0.0.0.0
VLAN........................................... untagged
Quarantine-vlan................................ 0
Active Physical Port........................... 1
Primary Physical Port.......................... 1
Backup Physical Port........................... Unconfigured
Primary DHCP Server............................ 172.16.5.1
Secondary DHCP Server.......................... Unconfigured
DHCP Option 82................................. Disabled
ACL............................................ CCIELAB-FILTER

AP Manager..................................... Yes
Guest Interface................................ No
L2 Multicast................................... Disabled
```

From **WIFI-PC**, verify that telnet traffic is restricted and HTTP traffic is allowed:



https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 2

CCIE SCv4 Lab 2 Solutions Section 4

1. Task 4.1 Solution
2. Task 4.2 Solution
3. Task 4.3 Solution
4. Task 4.4 Solution

Task 4.1 Solution

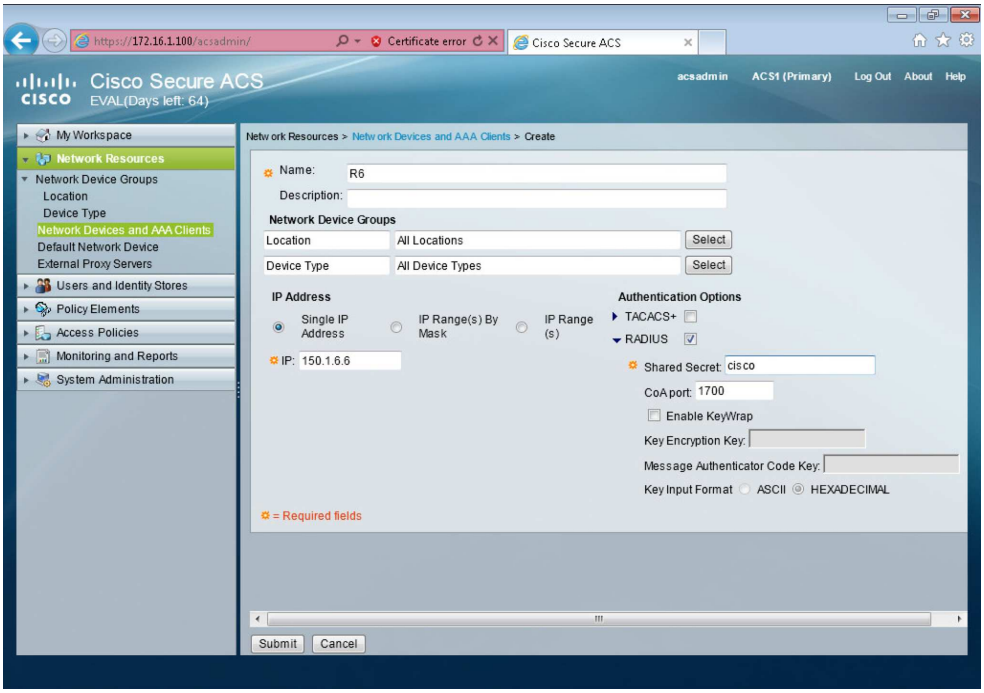
R6:

```
aaa new-model
aaa authentication login CONSOLE none
aaa authentication login default group ACS_RADIUS
aaa authorization auth-proxy default group ACS_RADIUS
aaa authorization network default group ACS_RADIUS
!
line console 0
 login authentication CONSOLE
!
aaa group server radius ACS_RADIUS
 server-private 172.16.1.100 key cisco
 ip radius source-interface Loopback0
!
radius-server vsa send authentication
!
ip auth-proxy name RADIUS_AUTH telnet inactivity-time 10 list AUTH_TRIGGER
!
ip access-list extended DEFAULT_ACL
 permit udp any eq bootpc any eq bootps
 permit udp 130.1.6.0 0.0.0.255 host 172.16.5.100 eq 5246
 permit udp 130.1.6.0 0.0.0.255 host 172.16.5.100 eq 5247
 deny ip any any
!
ip access-list extended AUTH_TRIGGER
 permit ip any host 150.1.10.10
```

https://t.me/learningnets

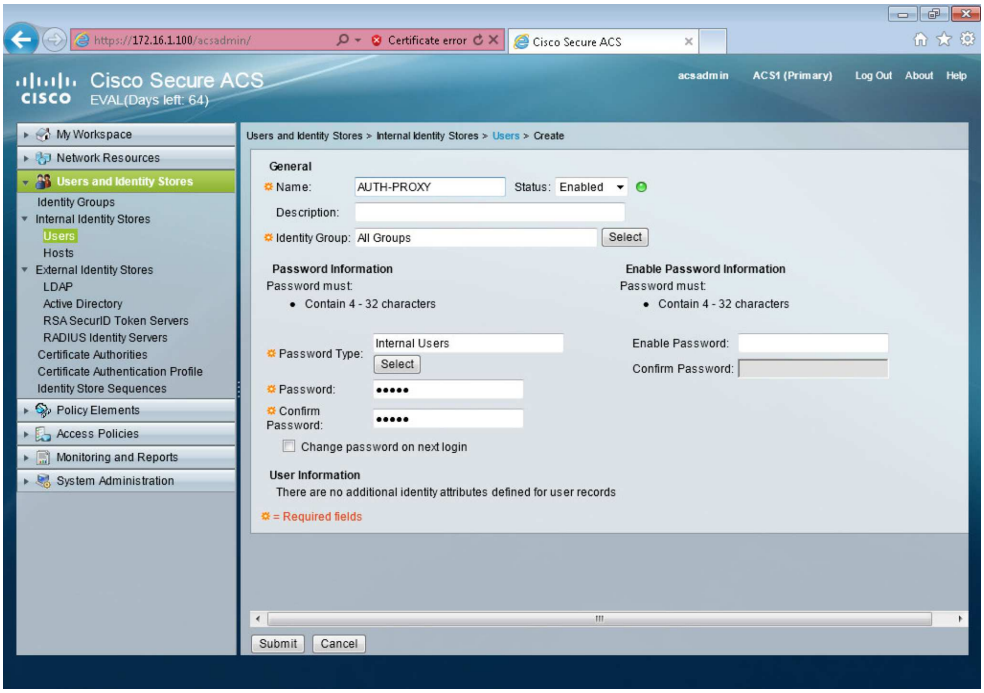
```
!
interface FastEthernet0/0.6
 ip access-group DEFAULT_ACL in
 ip auth-proxy RADIUS_AUTH
```

From **TEST-PC-A**, using Internet Explorer navigate to ACS, **Network Resources -> Network Device Groups -> Network Devices and AAA Client**, and click **Create** to add R6 as a NAD client:

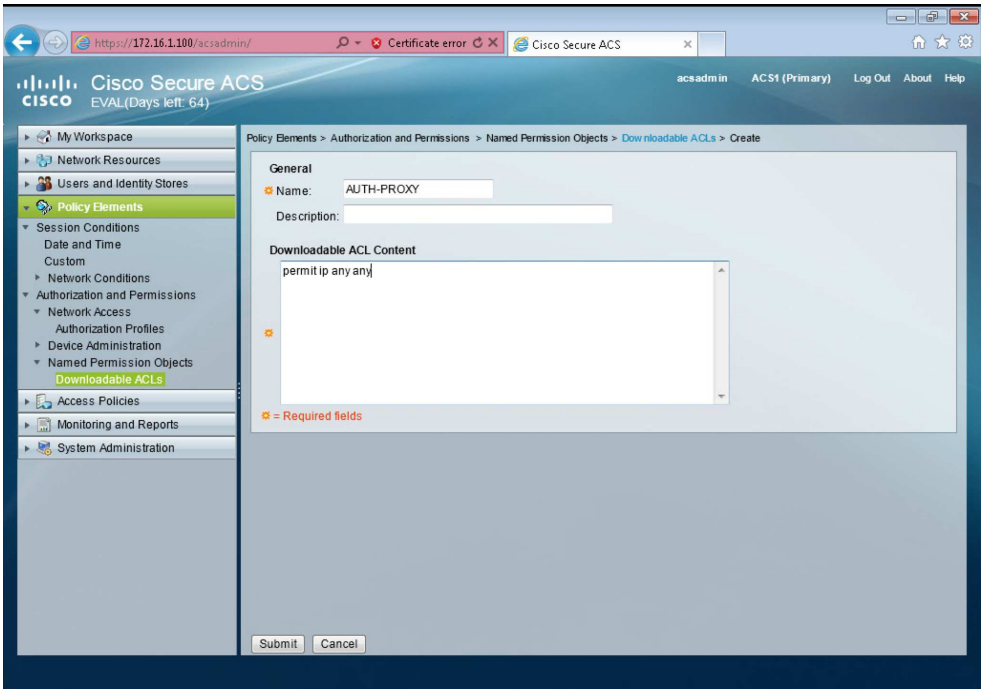


Navigate to **Users and Identity Stores -> Internal Identity Stores -> Users** and click **Create** to configure the username:

https://t.me/learningnets

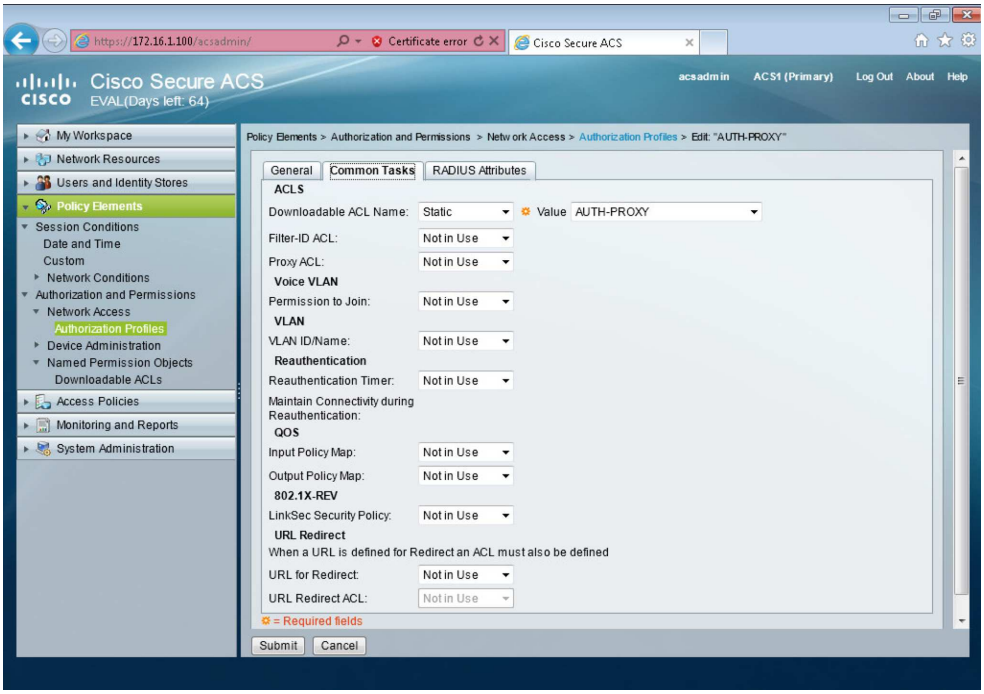


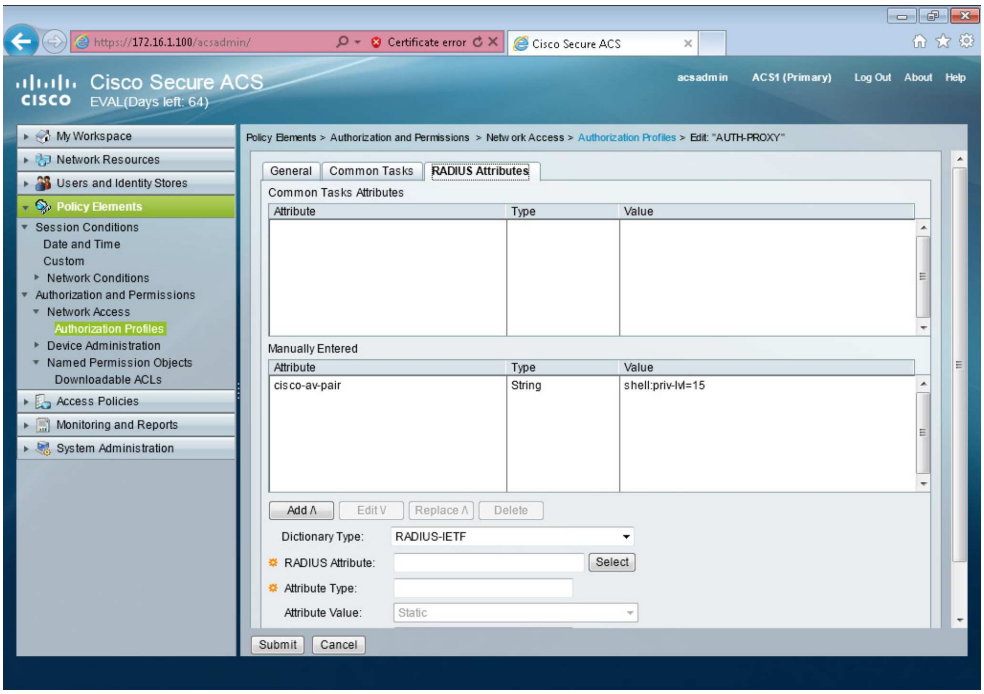
Navigate to **Policy Elements -> Authorization and Permissions -> Named Permission Objects -> Downloadable ACLs** and click **Create** to configure a dACL:



Navigate to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click **Create** to configure a profile; assign the dACL and privilege-level 15:

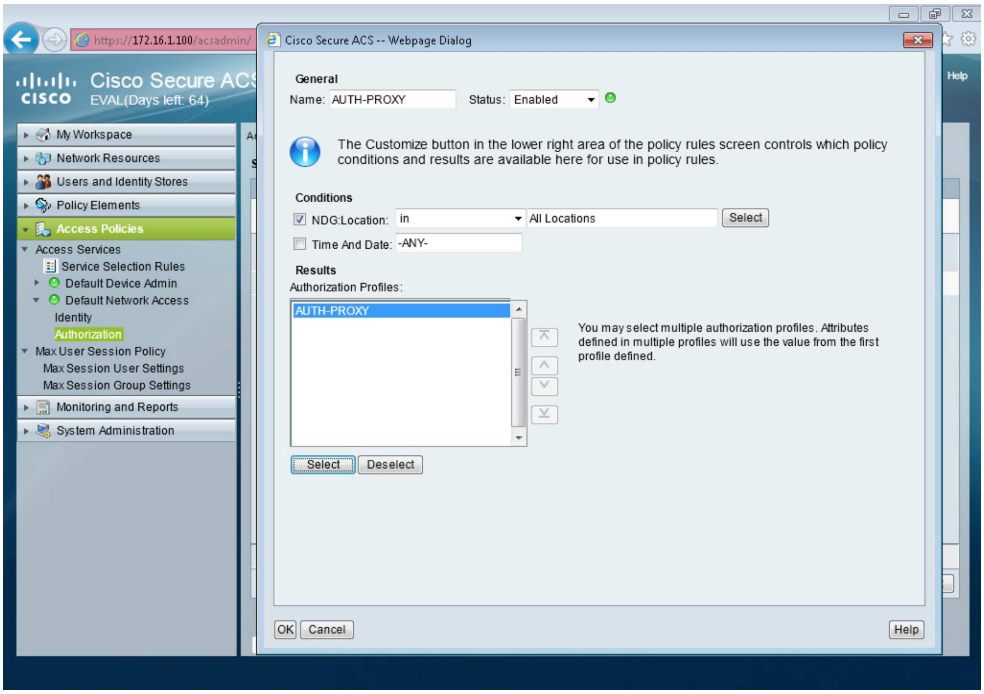
https://t.me/learningnets





Navigate to **Access Policies -> Access Services -> Default Network Access -> Authorization** and click **Create** to configure the authorization rule:

https://t.me/learningnets



Task 4.1 Verification

For testing, temporarily configure SW3 as a host in VLAN 6:

```
SW3:

interface Vlan6
 ip address 130.1.6.11 255.255.255.0
!
ip default-gateway 130.1.6.6
```

Verify that only telnet to SW2's Loopback0 triggers the authentication process:

```
SW3#telnet 130.1.69.10
Trying 130.1.69.10 ... % Destination unreachable; gateway or host down
!
!SW3#telnet 150.1.10.10
Trying 150.1.10.10 ... Open

Firewall authentication
Username:AUTH-PROXY
Password:Firewall authentication Success.
Connection will be closed if remote server does not respond
Connecting to remote server...

Password required, but none set
```

https://t.me/learningnets

```
[Connection to 150.1.10.10 closed by foreign host]
```

Verify that both authentication and authorization are successful:

```
R6#show ip auth-proxy cache username AUTH-PROXY
Authentication Proxy Cache
User Name                : AUTH-PROXY
Client IP                : 130.1.6.11
Client Port              : 18936          Timeout                 : 10

Time  Remaining          : 10             Connection state        : ESTAB

EPM information : Authproxy
Admission feature        : Authproxy
AAA Policies             :ACS ACL                 : xACSACLx-IP-AUTH-PROXY-533c7236

EOU information
--------------------------------------------------------------------------
Address         Interface              AuthType   Posture-Token Age(min)
--------------------------------------------------------------------------


EPM information : EOU


Existing Firewall Sessions Information:
!
!R6#show ip access-lists xACSACLx-IP-AUTH-PROXY-533c7236
Extended IP access list xACSACLx-IP-AUTH-PROXY-533c7236 (per-user) 10 permit ip any any
!
!R6#show epm session ip 130.1.6.11

Admission feature        : Authproxy
AAA Policies             :ACS ACL                 : xACSACLx-IP-AUTH-PROXY-533c7236
```

Task 4.2 Solution

First identity the MAC addresses of **TEST-PC-A** and IP Phone; this may differ based on the rack being assigned:

https://t.me/learningnets

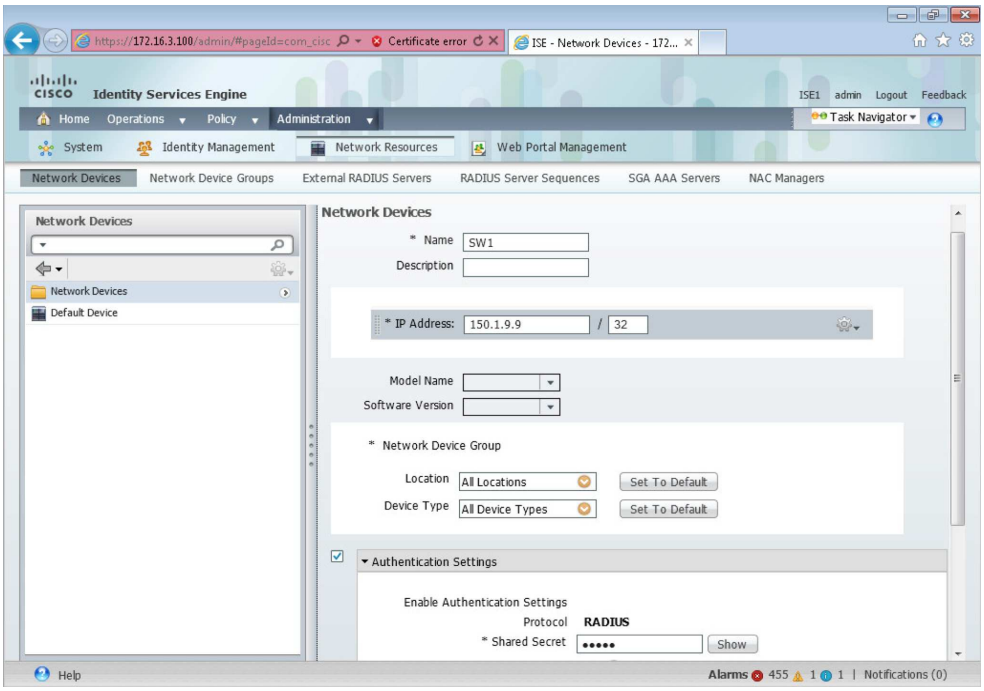
```
SW1#show mac address-table dynamic interface fastEthernet1/0/5


          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  91    0003.6b3c.35f0    DYNAMIC     Fa1/0/5

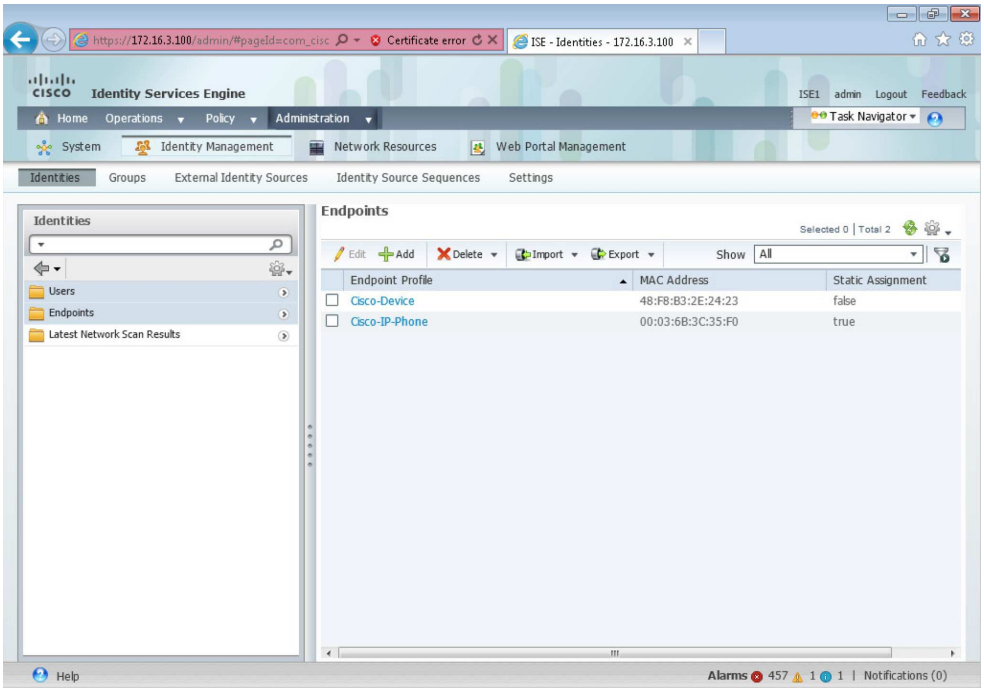
Total Mac Addresses for this criterion: 3
```

From **TEST-PC-A**, using Internet Explorer navigate to ISE, **Administration -> Network Resources -> Network Devices** and click **Add** to add SW1 as a NAD client:

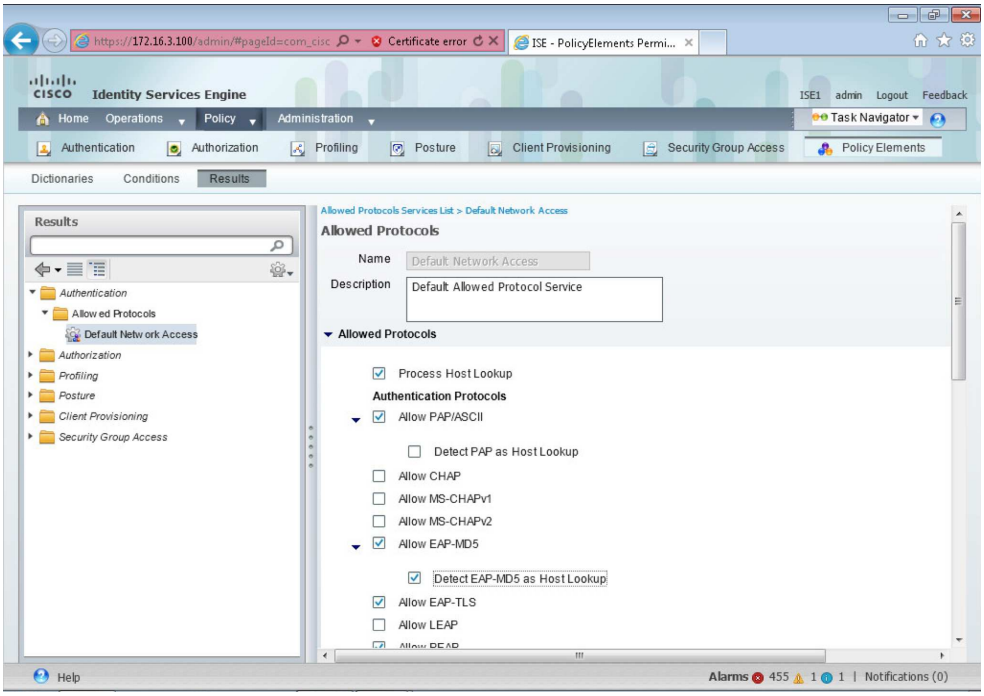


Navigate to **Administration -> Identity Management -> Identities -> Endpoints** and click **Add** to add the MAC addresses of both **TEST-PC-A** and IP Phone; associate the IP Phone with the **Cisco IP-Phone** Identity Group (**TEST-PC-A** has been automatically profiled based on the OUI of the MAC address):

https://t.me/learningnets

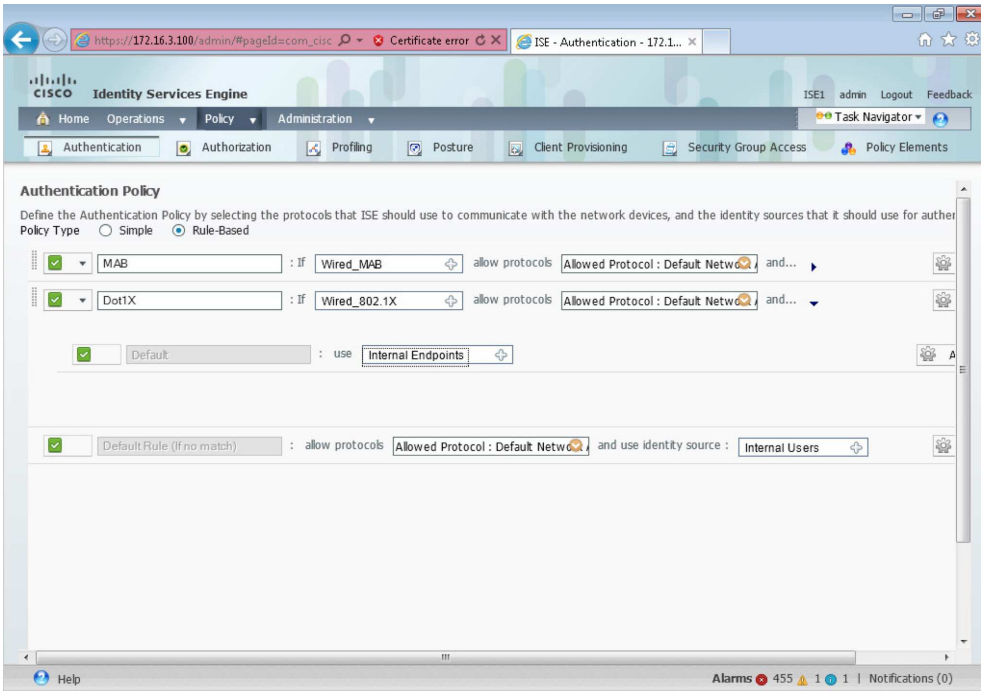


Navigate to **Policy -> Policy Elements -> Results -> Authentication -> Allowed Protocols -> Default Network Access** and enable **Process Host Lookup** for EAP-MD5 authentications (required for MAB-EAP).

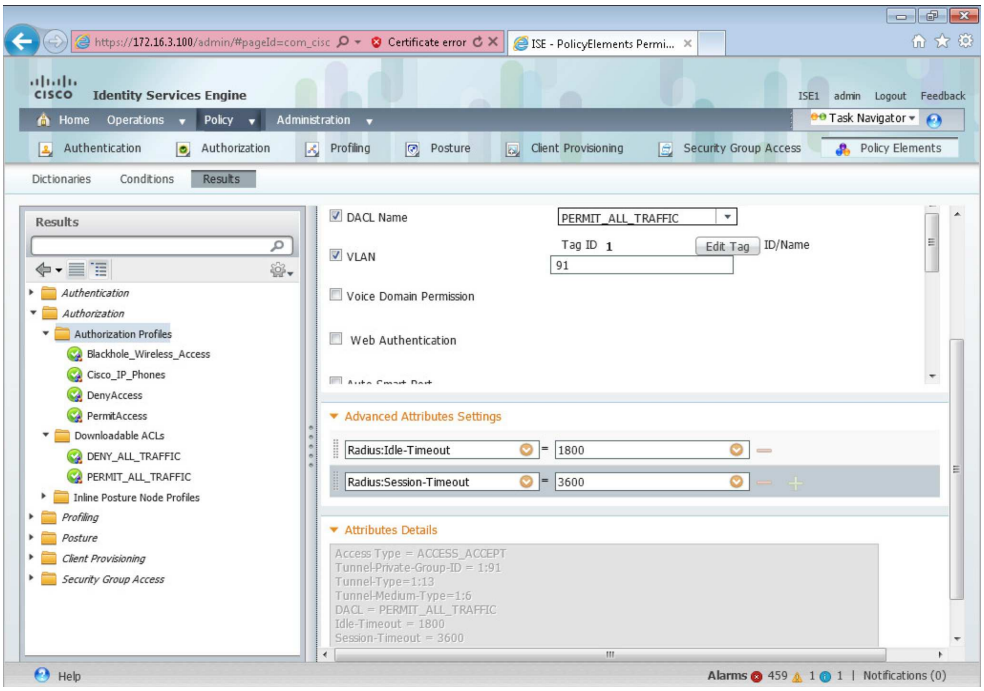


Navigate to **Policy -> Authentication** and edit the default **Dot1X** rule to authenticate against the **Internal Endpoints** store:

https://t.me/learningnets

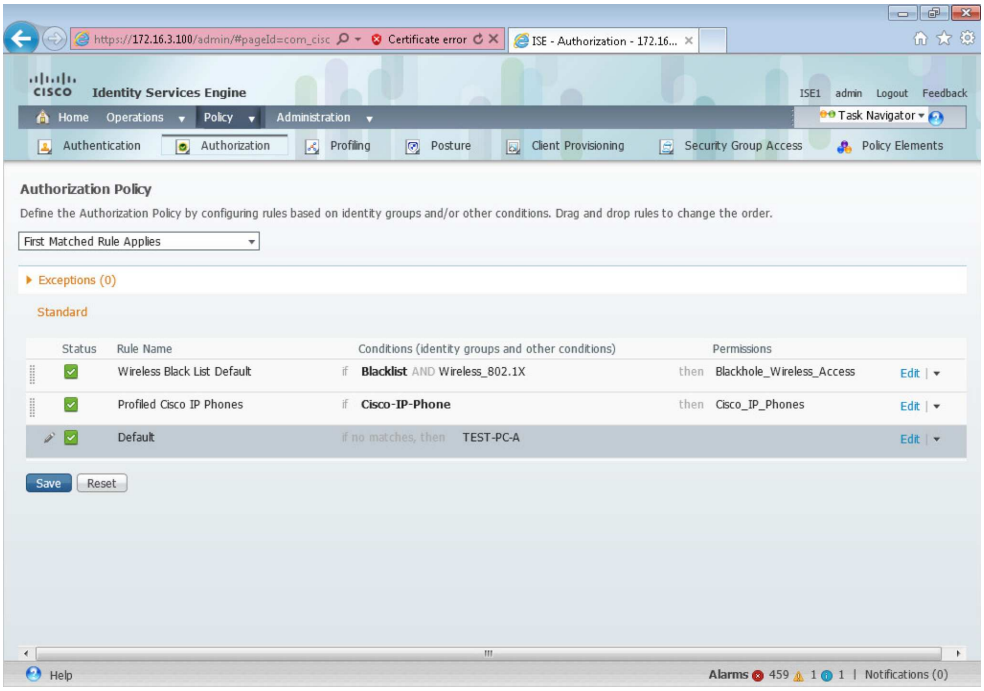


Navigate to **Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles** and configure one for **TEST-PC-A**, assign VLAN, dACL, inactivity, and reauthentication timers:



Navigate to **Policy -> Authorization** and modify the default rule by applying the configured authorization profile for **TEST-PC-A**:

https://t.me/learningnets



SW1:

```
aaa new-model
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
!
aaa group server radius ISE
 server-private 172.16.3.100 key cisco
 ip radius source-interface Loopback0
!
interface FastEthernet1/0/5
 authentication host-mode multi-domain
 authentication port-control auto
 authentication violation replace
 authentication periodic
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication event server dead action authorize voice
 authentication event server dead action authorize vlan 91
 mab eap
!
ip device tracking
radius-server vsa send authentication
```

ASA2:

```
access-list OSPF_TO_EIGRP permit 172.16.3.0 255.255.255.0
!
route-map OSPF_TO_EIGRP permit 10
```

https://t.me/learningnets

```
 match ip address OSPF_TO_EIGRP
!
router eigrp 202
 redistribute ospf 202 metric 100000 100 255 1 1500 route-map OSPF_TO_EIGRP
 eigrp stub connected redistributed
!
access-list OUTSIDE_IN permit udp host 150.1.9.9 host 172.16.3.100 eq 1645
access-list OUTSIDE_IN permit udp host 150.1.9.9 host 172.16.3.100 eq 1812
!
access-group OUTSIDE_IN in interface OUTSIDE
!
same-security-traffic permit intra-interface
!
access-list VLAN15_VLAN81 permit ip host 150.1.9.9 host 172.16.3.100
```

ASA1:

```
access-list VLAN15_VLAN81 extended permit ip host 172.16.3.100 host 150.1.9.9
```

Task 4.2 Verification

For both devices to be successfully authorized and dACL to be applied, the switch must learn the IP addresses of the IP Phone; so the DHCP task from the following sections must be completed first. Verify that both voice and data domains have been authenticated and authorized:

```
SW1#show authentication sessions


Interface  MAC Address     Method   Domain   Status         Session ID
Fa1/0/5    48f8.b32e.2423  mab      DATA     Authz Success  0000000000000057001769EC
Fa1/0/5    0003.6b3c.35f0  mab      VOICE    Authz Success  0000000000000005600173B64
```

Verify that the requested output is being matched for voice domain:

```
SW1#show authentication sessions mac 0003.6b3c.35f0


            Interface:  FastEthernet1/0/5
          MAC Address:  0003.6b3c.35f0
           IP Address:  130.1.19.16
            User-Name:  00036b3c35f0
               Status:  Authz Success
               Domain:  VOICE
```

https://t.me/learningnets

```
       Security Policy:  Should Secure
       Security Status:  Unsecure
        Oper host mode:  multi-domain
      Oper control dir:  both
         Authorized By:  Authentication Server
               ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
       Session timeout:  N/A
          Idle timeout:  N/A
     Common Session ID:  00000000000000005600173B64
       Acct Session ID:  0x00000057
                Handle:  0xF1000056

Runnable methods list:
        Method   State
        mab      Authc Success
```

Verify that the requested output is being matched for data domain:

https://t.me/learningnets

```
SW1#show authentication sessions mac 48f8.b32e.2423

            Interface:  FastEthernet1/0/5
          MAC Address:  48f8.b32e.2423
           IP Address:  130.1.91.100
            User-Name:  48f8b32e2423
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  91
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
      Session timeout:  3600s (server), Remaining: 593s
       Timeout action:  Reauthenticate
         Idle timeout:  1800s (server), Remaining: 590s
    Common Session ID:  0000000000000057001769EC
      Acct Session ID:  0x00000058
               Handle:  0x56000057

Runnable methods list:
       Method   State
       mab      Authc Success
```

Verify that dACL has been applied on the port, because device tracking is enabled and IP addresses have been learned by the switch:

```
SW1#show ip device tracking all

IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
---------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface               STATE
---------------------------------------------------------------------
130.1.19.16     0003.6b3c.35f0  19   FastEthernet1/0/5        ACTIVE
130.1.91.100    48f8.b32e.2423  91   FastEthernet1/0/5        ACTIVE

Total number interfaces enabled: 1
Enabled interfaces:
  Fa1/0/5
```

https://t.me/learningnets

```
!
!SW1#show ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2 (per-user) 10 permit ip any any
!
!SW1#show epm session ip 130.1.19.16
    Admission feature:  DOT1X ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
!
!SW1#show epm session ip 130.1.91.100
    Admission feature:  DOT1X ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
!
!SW1#show ip access-lists interface fastEthernet1/0/5

     permit ip host 130.1.91.100 any
     permit ip host 130.1.19.16 any
```

Verify that MAB EAP has been enabled on the port, so RADIUS **Service-Type** of **Framed** is used:

```
SW1#show mab all

MAB details for FastEthernet1/0/5
-------------------------------------Mac-Auth-Bypass            = Enabled (EAP)
```

Task 4.3 Solution

```
R6:

aaa authentication login VTY local-case
aaa authorization exec default local
!
username RESTRICTED privilege 0 password cisco
username UNRESTRICTED privilege 15 password cisco
enable secret level 1 level1pass
!
line vty 0 15
 login authentication VTY
```

Task 4.3 Verification

https://t.me/learningnets

Telnet to R6 and verify by authenticating with **RESTRICTED** user:

```
R6#telnet 150.1.6.6
Trying 150.1.6.6 ... Open


User Access Verification

Username: RESTRICTED
Password:
R6>show privilege
   ^% Invalid input detected at '^' marker.
R6>enable 1
Password: R6>show privilege
Current privilege level is 1
```

Telnet to R6 and verify by authenticating with **UNRESTRICTED** user:

```
R6#telnet 150.1.6.6
Trying 150.1.6.6 ... Open


User Access Verification

Username: UNRESTRICTED
Password:
R6#show privilege
Current privilege level is 15
R6#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.R6(config)#
```

Task 4.4 Solution

```
ASA2:

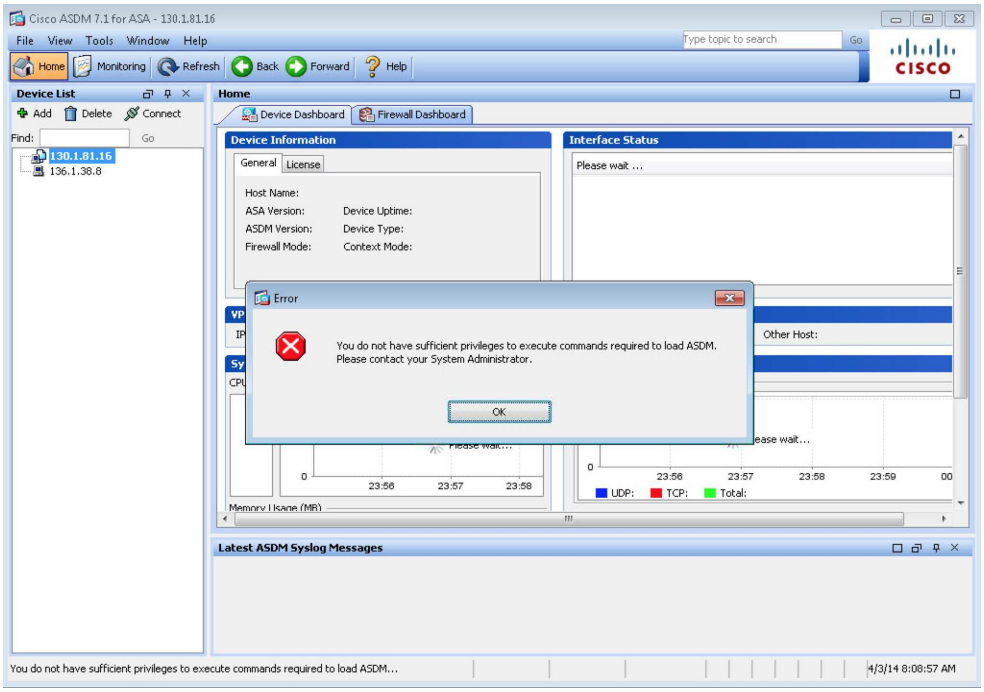
asdm image disk0:/asdm-712.bin
http server enable 4443
http 130.200.0.0 255.255.255.0 INSIDE
ssh 130.200.0.0 255.255.255.0 INSIDE
ssh version 2
```

https://t.me/learningnets

```
!
aaa authentication ssh console LOCAL
aaa authorization exec LOCAL
aaa authorization command LOCAL
enable password cisco
!
username unrestricted password cisco
!
username sshuser password cisco
username sshuser attributes
 service-type nas-prompt
```

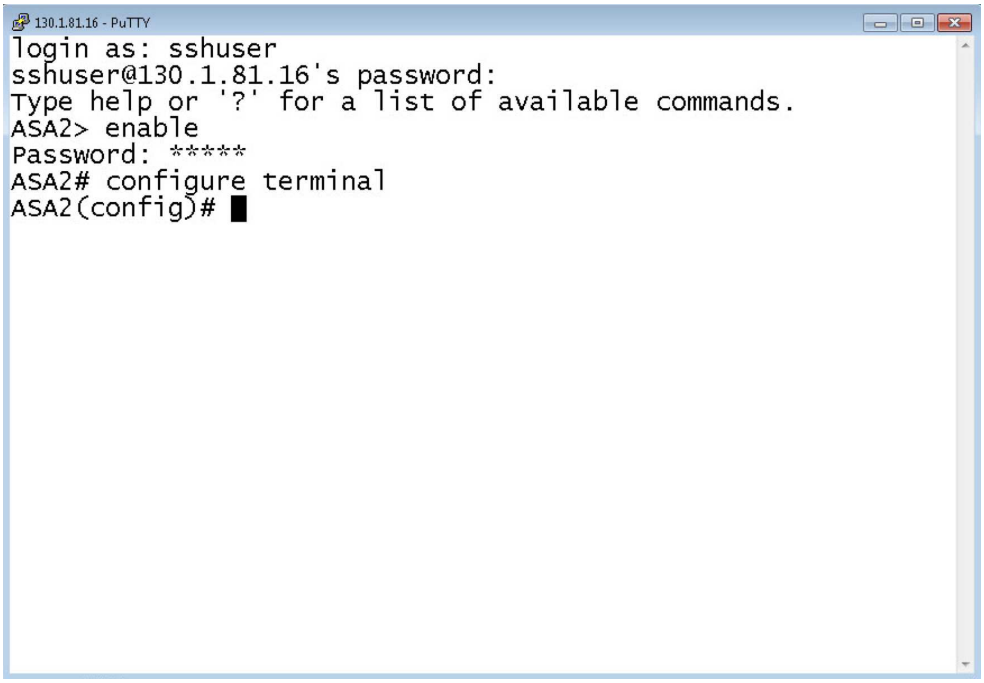
Task 4.4 Verification

Establish the AnyConnect SSL session from **TEST-PC-A**, and using ASDM authenticate to the ASA2 with the **sshuser** username; note the error message:



Establish the AnyConnect SSL session from **TEST-PC-A** and using Putty; initiate the SSH session and authenticate to the ASA2 with the **sshuser** username, and verify that configuration mode access is allowed:

https://t.me/learningnets



Verify that the ASA is listening on TCP ports 22 and 4443 on its **INSIDE** interface:

```
ASA2#show asp table socket



Protocol  Socket    Local Address               Foreign Address         State
SSL       0000c41f  130.1.18.16:443             0.0.0.0:*               LISTEN
DTLS      0001500f  130.1.18.16:443             0.0.0.0:*               LISTEN
TCP       0018e29f  130.1.81.16:23              0.0.0.0:*               LISTEN
TCP       002f8eef  130.1.81.16:22              0.0.0.0:*               LISTEN
SVC       0038a098  130.1.18.16:443             130.1.91.100:25341      ESTAB
SVC_UDP   00393288  130.1.18.16:443             130.1.91.100:57947      CONNECTED
SSL       0040059f  130.1.81.16:4443            0.0.0.0:*               LISTEN
```

Verify that only SSH version 2 sessions are allowed:

```
ASA2# show ssh

Timeout: 5 minutes Version allowed: 2

130.200.0.0 255.255.255.0 INSIDE
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 2

CCIE SCv4 Lab 2 Solutions Section 5

1. Task 5.1 Solution
2. Task 5.2 Solution
3. Task 5.3 Solution
4. Task 5.4 Solution
5. Task 5.5 Solution

Task 5.1 Solution

R2:

```
router bgp 126
 neighbor 150.1.1.1 remote-as 126
 neighbor 150.1.6.6 remote-as 126
 neighbor 150.1.1.1 update-source Loopback0
 neighbor 150.1.6.6 update-source Loopback0
 neighbor 150.1.1.1 send-community
 neighbor 150.1.6.6 send-community
 redistribute static route-map STATIC_TO_BGP
!
route-map STATIC_TO_BGP permit 10
 match tag 126
 set local-preference 200
 set origin igp
 set community no-export
 set ip next-hop 192.0.2.1
!
ip route 192.0.2.1 255.255.255.255 Null0
ip route 172.16.6.99 255.255.255.255 Null0 tag 126
```

R1:

```
router bgp 126
 neighbor 150.1.2.2 remote-as 126
 neighbor 150.1.2.2 update-source Loopback0
!
ip route 192.0.2.1 255.255.255.255 Null0
```

https://t.me/learningnets

```
!
interface Null0
 no ip unreachables

R6:
router bgp 126
 neighbor 150.1.2.2 remote-as 126
 neighbor 150.1.2.2 update-source Loopback0
!
ip route 192.0.2.1 255.255.255.255 Null0
!
interface Null0
 no ip unreachables

ASA3 VLAN13 Context:
access-list OUTSIDE_IN extended permit tcp host 150.1.2.2 host 150.1.1.1 eq 179
access-list OUTSIDE_IN extended permit tcp host 150.1.2.2 host 150.1.6.6 eq 179

ASA3 VLAN16 Context:

access-list OUTSIDE_IN extended permit tcp host 150.1.6.6 host 150.1.2.2 eq 179
```

Task 5.1 Verification

Verify that BGP sessions are established:

https://t.me/learningnets

```
R2#show ip bgp summary

BGP router identifier 150.1.111.2, local AS number 126
BGP table version is 2, main routing table version 2
1 network entries using 148 bytes of memory
1 path entries using 64 bytes of memory
1/1 BGP path/bestpath attribute entries using 136 bytes of memory
1 BGP community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 372 total bytes of memory
BGP activity 1/0 prefixes, 1/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
150.1.1.1       4          126       7       8        2    0    0 00:04:04        0
150.1.6.6       4          126       4       5        2    0    0 00:01:39        0
```

Verify that R1 and R6 receive the BGP update from R2:

```
R1#show ip bgp 172.16.6.99
BGP routing table entry for 172.16.6.99/32, version 2
Paths: (1 available, best #1, table default, not advertised to EBGP peer)
  Not advertised to any peer
  Refresh Epoch 1
  Local 192.0.2.1 from 150.1.2.2 (150.1.111.2)
 Origin IGP, metric 0, localpref 200, valid, internal, best
 Community: no-export
!
!R6#show ip bgp 172.16.6.99
BGP routing table entry for 172.16.6.99/32, version 2
Paths: (1 available, best #1, table default, not advertised to EBGP peer)
  Not advertised to any peer
  Local 192.0.2.1 from 150.1.2.2 (150.1.111.2)
 Origin IGP, metric 0, localpref 200, valid, internal, best
 Community: no-export
```

Verify that traffic is silently dropped because there are no ICMP unreachables generated by the routers:

```
R5#ping 172.16.6.99
```

https://t.me/learningnets

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.6.99, timeout is 2 seconds:.....
Success rate is 0 percent (0/5)
!
!R1#show ip route 172.16.6.99
Routing entry for 172.16.6.99/32
  Known via "bgp 126", distance 200, metric 0, type internal
  Last update from 192.0.2.1 00:07:11 ago
  Routing Descriptor Blocks: * 192.0.2.1, from 150.1.2.2, 00:07:11 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: none
!
!R1#show ip cef 172.16.6.99
172.16.6.99/32 nexthop 192.0.2.1 Null0
```

Task 5.2 Solution

```
ASA2:
logging timestamp
logging console emergencies
logging monitor errors
logging trap debugging
!
logging host OUTSIDE 172.16.3.99
logging debug-trace
logging enable
!
access-list VLAN15_VLAN81 permit ip interface OUTSIDE host 172.16.3.99

ASA1:

access-list VLAN15_VLAN81 permit ip host 172.16.3.99 host 130.1.18.16
```

Task 5.2 Verification

Verify the logging settings on ASA2:

```
ASA2# show logging

Syslog logging: enabled
```

https://t.me/learningnets

```
    Facility: 20 Timestamp logging: enabled
    Standby logging: disabled Debug-trace logging: enabled
Console logging: level emergencies, 3440 messages logged
Monitor logging: level errors, 0 messages logged
    Buffer logging: disabled Trap logging: level debugging, facility 20, 593 messages logged
Logging to OUTSIDE 172.16.3.99

    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

Verify that ASA1 and ASA2 have negotiated IPsec SA for the syslog traffic:

```
ASA2# show crypto ipsec sa peer 130.1.55.15

peer address: 130.1.55.15
    Crypto map tag: VPN, seq num: 10, local addr: 130.1.18.16

      access-list VLAN15_VLAN81 extended permit ip interface OUTSIDE host 172.16.3.99
local ident (addr/mask/prot/port): (130.1.18.16/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.16.3.99/255.255.255.255/0/0)
      current_peer: 130.1.55.15
#pkts encaps: 105, #pkts encrypt: 105, #pkts digest: 105
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 105, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 217, #recv errors: 0

      local crypto endpt.: 130.1.18.16, remote crypto endpt.: 130.1.55.15

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 60C1C6FA
      current inbound spi : A6BBFC0B
inbound esp sas:
      spi: 0xA6BBFC0B (2797337611)
         transform: esp-3des esp-md5-hmac no compression
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 69632, crypto-map: VPN
         sa timing: remaining key lifetime (kB/sec): (3915000/28613)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
```

https://t.me/learningnets

```
          0x00000000 0x00000001 outbound esp sas:

      spi: 0x60C1C6FA (1623312122)
         transform: esp-3des esp-md5-hmac no compression
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 69632, crypto-map: VPN
         sa timing: remaining key lifetime (kB/sec): (3914987/28613)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Task 5.3 Solution

```
R5:

load protocol system:/fpm/phdf/ip.phdf
load protocol system:/fpm/phdf/tcp.phdf
!
class-map type access-control match-any TELNET_TRAFFIC
 match field TCP dest-port eq 23
 match field TCP source-port eq 23
!
class-map type stack match-all TCP_TRAFFIC
 match field IP protocol eq 0x6 next TCP
!
policy-map type access-control DROP_TELNET
 class TELNET_TRAFFIC
  drop
!
policy-map type access-control INTERFACE_POLICY
 class TCP_TRAFFIC
  service-policy DROP_TELNET
!
interface FastEthernet0/1
 service-policy type access-control output INTERFACE_POLICY
```

Task 5.3 Verification

Verify that telnet traffic transiting R1 is dropped if exiting its VLAN 51 interface but allowed if terminated locally:

https://t.me/learningnets

```
R4#telnet 150.1.5.5

Trying 150.1.5.5 ... Open

Password required, but none set

[Connection to 150.1.5.5 closed by foreign host]
!
!R4#telnet 150.1.1.1
Trying 150.1.1.1 ... % Connection timed out; remote host not responding
```

Verify that packets have matched the configured policy:

```
R5#show policy-map type access-control interface fastEthernet0/1
 FastEthernet0/1

  Service-policy access-control output: INTERFACE_POLICY

    Class-map: TCP_TRAFFIC (match-all)
      11 packets, 666 bytes
      5 minute offered rate 0 bps
      Match: field IP protocol eq 0x6 next TCP

      Service-policy access-control : DROP_TELNET
 Class-map: TELNET_TRAFFIC (match-any)
4 packets, 232 bytes
          5 minute offered rate 0 bps Match: field TCP dest-port eq 23
Match: field TCP source-port eq 23
drop



        Class-map: class-default (match-any)
          7 packets, 434 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

    Class-map: class-default (match-any)
      22 packets, 3014 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

https://t.me/learningnets

Task 5.4 Solution

```
SW1:

errdisable recovery cause storm-control
errdisable recovery interval 600
!
!
interface range FastEthernet1/0/1 - 2
 storm-control broadcast level 5.00
 storm-control action shutdown
```

Task 5.4 Verification

Verify the configured settings:

```
SW1#show errdisable recovery | i Enabled|interval
storm-control                Enabled
Timer interval: 600 seconds
!
!SW1#show storm-control broadcast

Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  ----------
Fa1/0/1    Forwarding         5.00%        5.00%         0.00%
Fa1/0/2    Forwarding         5.00%        5.00%         0.00%
```

Task 5.5 Solution

```
R3:
ntp master
ntp authentication-key 1 md5 ntpkeyunicast
ntp authentication-key 2 md5 ntpkeybroadcast
ntp trusted-key 1
ntp trusted-key 2
!
interface FastEthernet0/1
 ntp broadcast key 2
!
```

https://t.me/learningnets

```
interface FastEthernet0/0.3
 ntp disable

R2:
ntp authenticate
ntp authentication-key 1 md5 ntpkeyunicast
ntp trusted-key 1
ntp server 150.1.3.3 key 1

SW1:
ntp authenticate
ntp authentication-key 2 md5 ntpkeybroadcast
ntp trusted-key 2
!
interface Vlan13
 ntp broadcast client

ASA3 VLAN13 Context:

access-list OUTSIDE_IN permit udp host 130.1.13.3 host 255.255.255.255 eq 123
```

Task 5.5 Verification

Verify that both SW1 and R2 have synchronized time with R3:

https://t.me/learningnets

```
R2#show ntp status
 Clock is synchronized, stratum 9, reference is 150.1.3.3

nominal freq is 250.0000 Hz, actual freq is 249.9998 Hz, precision is 2**21
reference time is D6E7CB43.B92FBF86 (11:57:55.723 UTC Thu Apr 3 2014)
clock offset is 0.6979 msec, root delay is 1.82 msec
root dispersion is 6.62 msec, peer dispersion is 4.24 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000639 s/s
system poll interval is 64, last update was 159 sec ago.
!
!SW1#show ntp status
 Clock is synchronized, stratum 9, reference is 130.1.13.3

nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**18
reference time is D6E7CBCC.7A7D1E4B (12:00:12.478 UTC Thu Apr 3 2014)
clock offset is 7.4015 msec, root delay is 3.65 msec
root dispersion is 397.40 msec, peer dispersion is 389.76 msec
```

Verify that NTP is authenticated, and note the synchronization method: unicast and broadcast:

```
R2#show ntp associations detail
 150.1.3.3 configured, authenticated, our_master, sane, valid, stratum 8
ref ID 127.127.1.1    , time D6E7CBFE.7C4CE829 (12:01:02.485 UTC Thu Apr 3 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.41, reach 177, sync dist 7.28
delay 1.88 msec, offset 0.9538 msec, dispersion 4.49
precision 2**24, version 4
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time D6E7CC09.B99E20B5 (12:01:13.725 UTC Thu Apr 3 2014)
xmt time D6E7CC09.B99E20B5 (12:01:13.725 UTC Thu Apr 3 2014)
filtdelay =     2.02    1.99    1.96    2.00    2.09    1.88    2.00    1.89
filtoffset =    2.45    2.13    1.82    1.60    1.21    0.95    0.73    0.68
filterror =     0.00    0.99    1.98    2.97    3.99    5.01    5.89    5.92
minpoll = 6, maxpoll = 10
!
!SW1#show ntp associations detail
 130.1.13.3 dynamic, authenticated, our_master, sane, valid, stratum 8
ref ID 127.127.1.1, time D6E7CBFE.7C4CE829 (12:01:02.485 UTC Thu Apr 3 2014)
our mode bdcast client, peer mode bdcast, our poll intvl 64, peer poll intvl 64

root delay 0.00 msec, root disp 0.46, reach 377, sync dist 136.505
delay 3.65 msec, offset 4.7495 msec, dispersion 134.23
precision 2**24, version 4
```

https://t.me/learningnets

```
org time D6E7CC0C.7C524536 (12:01:16.485 UTC Thu Apr 3 2014)
rcv time D6E7CC0C.7B2A0252 (12:01:16.481 UTC Thu Apr 3 2014)
xmt time D6E7CA54.8EE9186F (11:53:56.558 UTC Thu Apr 3 2014)
filtdelay =     3.65    3.65    3.65    3.65    3.65    3.65    3.65    0.00
filtoffset =    4.75    7.40   17.77  -21.60    1.20    2.72   -0.58    0.00
filterror =     0.99    1.98    2.96    3.95    4.96    5.95    6.73 16000.0
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 2

CCIE SCv4 Lab 2 Solutions Section 6

1. Task 6.1 Solution
2. Task 6.2 Solution
3. Task 6.3 Solution
4. Task 6.4 Solution
5. Task 6.5 Solution

Task 6.1 Solution

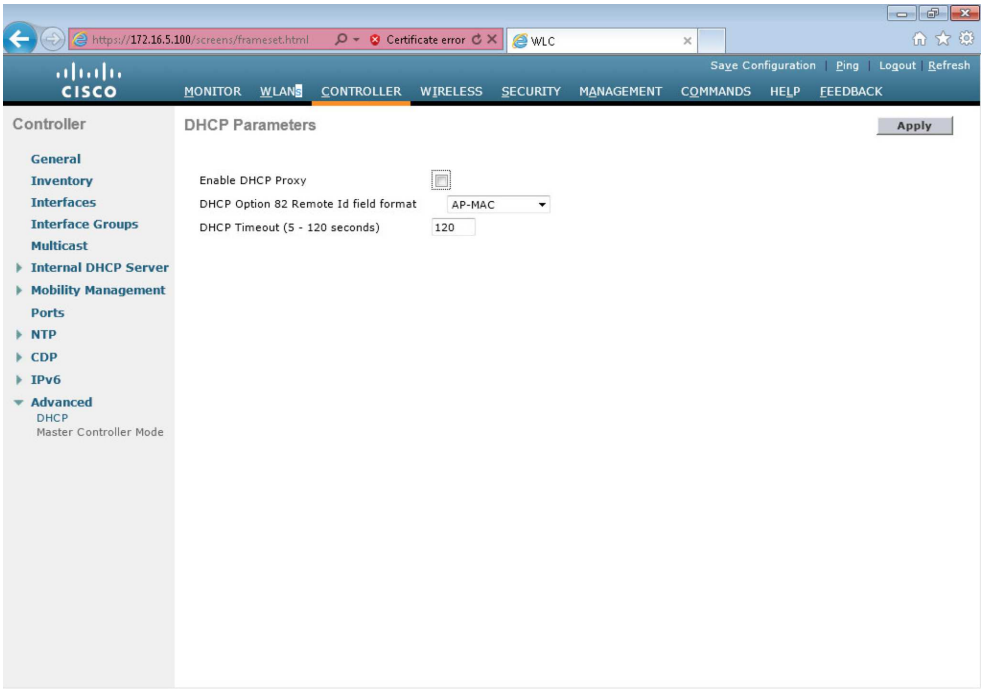
```
ASA1:
dhcpd address 130.1.19.16-130.1.19.254 PHONE
dhcpd lease 14400 interface PHONE
dhcpd enable PHONE
!
dhcpd address 130.1.91.16-130.1.91.254 TESTPC
dhcpd lease 14400 interface TESTPC
dhcpd enable TESTPC

SW1:

ip dhcp snooping
ip dhcp snooping vlan 3,19,91
no ip dhcp snooping information option
!
interface range FastEthernet1/0/3 , FastEthernet1/0/13
 ip dhcp snooping trust
```

Configure WLC to disable option 82 insertion into DHCP packets. Navigate to **Controller -> Advanced -> DHCP** and disable DHCP proxy:

https://t.me/learningnets



Task 6.1 Verification

Verify the DHCP snooping configuration:

```
SW1#show ip dhcp snooping
 Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
3,19,91
DHCP snooping is operational on following VLANs:
3,19,91
DHCP snooping is configured on the following L3 Interfaces:
 Insertion of option 82 is disabled
   circuit-id default format: vlan-mod-port
   remote-id: 001b.d58b.2180 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet1/0/3          yes        yes             unlimited
  Custom circuit-ids:FastEthernet1/0/13         yes        yes             unlimited

  Custom circuit-ids:
```

https://t.me/learningnets

Flap the IP Phone port and the WiFi client, and verify that IPv4 addresses are still assigned by ASA1 and R3:

```
R3#show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
172.16.5.2          01ac.f1df.13bd.8f       Apr 04 2014 12:41 PM    Automatic
!
!ASA1# show dhcpd binding


IP address       Client Identifier        Lease expiration        Type
 130.1.19.17     0100.036b.3c35.f0          14380 seconds     Automatic
!
!SW1# show ip dhcp snooping binding

MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:03:6B:3C:35:F0   130.1.19.17      14363       dhcp-snooping   19    FastEthernet1/0/5
AC:F1:DF:13:BD:8F   172.16.5.2       85302       dhcp-snooping   3     FastEthernet1/0/23

Total number of bindings: 2
```

Task 6.2 Solution

```
SW4:

ipv6 prefix-list RA_PREFIX permit 2004:44::/64
!
ipv6 access-list RA_SOURCE
 permit ipv6 host FE80::4 any
!
ipv6 nd raguard policy HOST_INSPECT
 device-role host
!
ipv6 nd raguard policy ROUTER
 device-role router
 match ra prefix-list RA_PREFIX
 match ipv6 access-list RA_SOURCE
!
```

https://t.me/learningnets

```
vlan configuration 44
 ipv6 nd raguard attach-policy HOST_INSPECT
!
interface GigabitEthernet1/0/1
 ipv6 nd raguard attach-policy ROUTER
```

Task 6.2 Verification

Verify that R4 sends IPV6 RA out on its Fa0/1 interface:

https://t.me/learningnets

```
R4#show ipv6 interface fastEthernet0/1

FastEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4
  No Virtual link-local address(es):
  Global unicast address(es):
    2004:44::4, subnet is 2004:44::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:4
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
 ND router advertisements are sent every 200 seconds

  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
!
!R4#show ipv6 interface fastEthernet0/1 prefix

IPv6 Prefix Advertisements FastEthernet0/1
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default
       N - Not advertised, C - Calendar

PD default [LA] Valid lifetime 2592000, preferred lifetime 604800
 AD 2004:44::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

Verify the IPv6 RA guard on SW4:

```
SW4#show ipv6 snooping features

Feature name   priority state RA guard          192   READY
!
!SW4#show ipv6 snooping policies
```

https://t.me/learningnets

```
Target               Type  Policy               Feature        Target range
Gi1/0/1              PORT  ROUTER               RA guard       vlan all
vlan 44              VLAN  HOST_INSPECT         RA guard       vlan all

!
!SW4#show ipv6 snooping capture-policy
HW Policy DB:
        HW Policy 0000001C #targets:2
                Target Gi1/0/1 type 0 handle 1
                Target vlan 44   type 1 handle 2C0000
Target DB: HW Target Gi1/0/1 HW policy signature 0000001C policies#:1 rules#:3 sig 0000001C
 SW policy ROUTER feature RA guard

                Rule RS Protocol ICMPV6 mask 00000004 action PUNT match 133 #feat:1
                        feature RA guard
                Rule RA Protocol ICMPV6 mask 00000008 action PUNT match 134 #feat:1
                        feature RA guard
                Rule REDIR Protocol ICMPV6 mask 00000010 action PUNT match 137 #feat:1
                        feature RA guard
HW Target vlan 44   HW policy signature 0000001C policies#:1 rules#:3 sig 0000001C
 SW policy HOST_INSPECT feature RA guard


                Rule RS Protocol ICMPV6 mask 00000004 action PUNT match 133 #feat:1
                        feature RA guard
                Rule RA Protocol ICMPV6 mask 00000008 action PUNT match 134 #feat:1
                        feature RA guard
                Rule REDIR Protocol ICMPV6 mask 00000010 action PUNT match 137 #feat:1
                        feature RA guard
```

Verify that IPV6 RA messages have been received on SW4's Gi1/0/1 interface, but not dropped because of the configured policy:

https://t.me/learningnets

```
SW4#show ipv6 snooping counters interface gigabitEthernet1/0/1

Received messages on Gi1/0/1:
Protocol        Protocol message NDP               RA[6]

DHCPv6

Bridged messages from Gi1/0/1:
Protocol        Protocol message NDP               RA[6]

DHCPv6

Dropped messages on Gi1/0/1:
Feature         Protocol Msg [Total dropped]
```

Task 6.3 Solution

```
SW1:

spanning-tree portfast bpduguard default
!
interface range fastEthernet 1/0/23 - 24
 spanning-tree guard root
```

Task 6.3 Verification

Verify that BPDU Guard is globally enabled and activated on portfast-enabled ports:

```
SW1#show spanning-tree summary

Switch is in pvst mode
Root bridge for: VLAN0001, VLAN0003, VLAN0006, VLAN0009, VLAN0011, VLAN0013
  VLAN0015-VLAN0019, VLAN0022-VLAN0023, VLAN0044, VLAN0051, VLAN0054-VLAN0055
  VLAN0066, VLAN0069, VLAN0076, VLAN0081, VLAN0091, VLAN0099
Extended system ID           is enabled
Portfast Default             is disabled PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
```

https://t.me/learningnets

```
Configured Pathcost method used is short
!
!SW1#show  spanning-tree interface fastEthernet1/0/2 detail

 Port 4 (FastEthernet1/0/2) of VLAN0023 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.4.
   Designated root has priority 16407, address 001b.d58b.2180
   Designated bridge has priority 16407, address 001b.d58b.2180
   Designated port id is 128.4, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1 The port is in the portfast mode
   Link type is point-to-point by default Bpdu guard is enabled by default

   BPDU: sent 24077, received 0
```

Verify that Root Guard is enabled on trunk links to SW5 and SW6; for example, check VLAN 44:

```
SW1#show spanning-tree vlan 44 interface fastEthernet1/0/23 detail

 Port 25 (FastEthernet1/0/23) of VLAN0044 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.25.
   Designated root has priority 16428, address 001b.d58b.2180
   Designated bridge has priority 16428, address 001b.d58b.2180
   Designated port id is 128.25, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default Root guard is enabled on the port
   BPDU: sent 24143, received 0
!
!SW1#show spanning-tree vlan 44 interface fastEthernet1/0/24 detail

 Port 26 (FastEthernet1/0/24) of VLAN0044 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.26.
   Designated root has priority 16428, address 001b.d58b.2180
   Designated bridge has priority 16428, address 001b.d58b.2180
   Designated port id is 128.26, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default Root guard is enabled on the port

   BPDU: sent 24165, received 1
```

https://t.me/learningnets

Task 6.4 Solution

```
SW3:

interface GigabitEthernet1/0/9
  spanning-tree bpdufilter enable
```

Task 6.4 Verification

Verify that BPDU Filter is applied on IPS port so that STP messages are no longer sent to the IPS, but the port is still in STP FW mode:

```
SW3#show spanning-tree interface gigabitEthernet1/0/9

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
VLAN0023            Desg FWD 4         128.9    P2p
VLAN0032            Desg FWD 4         128.9    P2p
!
!SW3#show spanning-tree interface gigabitEthernet 1/0/9 detail
 Port 9 (GigabitEthernet1/0/9) of VLAN0023 is designated forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.9.
   Designated root has priority 16407, address 001b.d58b.2180
   Designated bridge has priority 32791, address 44d3.ca63.9980
   Designated port id is 128.9, designated path cost 19
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default Bpdu filter is enabled
   BPDU: sent 84172, received 21
 Port 9 (GigabitEthernet1/0/9) of VLAN0032 is designated forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.9.
   Designated root has priority 16416, address 001b.d58b.2180
   Designated bridge has priority 32800, address 44d3.ca63.9980
   Designated port id is 128.9, designated path cost 19
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default Bpdu filter is enabled

   BPDU: sent 21, received 84171
```

https://t.me/learningnets

Verify that IPS no longer receives the STP packets:

```
IPS# packet display gigabitEthernet0/1

Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
05:50:45.306000 IP 130.1.32.2 > 224.0.0.5: OSPFv2, Hello, length: 60
05:50:45.307000 IP 130.1.32.2 > 224.0.0.5: OSPFv2, Hello, length: 60
05:50:45.967000 IP 150.1.2.2 > 150.1.4.4: ESP(spi=0x72df3401,seq=0x245), length 116
05:50:45.967000 IP 150.1.2.2 > 150.1.4.4: ESP(spi=0x72df3401,seq=0x245), length 116
05:50:47.030000 IP 150.1.4.4 > 150.1.2.2: ESP(spi=0x49f4ebd0,seq=0x246), length 116
05:50:47.030000 IP 150.1.4.4 > 150.1.2.2: ESP(spi=0x49f4ebd0,seq=0x246), length 116
05:50:48.090000 IP 150.1.6.6.179 > 150.1.2.2.57557: P 1599786044:1599786063(19) ack 3361277668 win 15709: BGP, lengt
05:50:48.090000 IP 150.1.6.6.179 > 150.1.2.2.57557: P 0:19(19) ack 1 win 15709: BGP, length: 19
05:50:48.287000 IP 150.1.2.2.57557 > 150.1.6.6.179: . ack 19 win 15752
05:50:48.287000 IP 150.1.2.2.57557 > 150.1.6.6.179: . ack 19 win 15752
05:50:50.584000 IP 150.1.2.2 > 150.1.4.4: ESP(spi=0x72df3401,seq=0x246), length 116
05:50:50.585000 IP 150.1.2.2 > 150.1.4.4: ESP(spi=0x72df3401,seq=0x246), length 116
05:50:51.081000 IP 130.1.32.3 > 224.0.0.5: OSPFv2, Hello, length: 60
05:50:51.082000 IP 130.1.32.3 > 224.0.0.5: OSPFv2, Hello, length: 60
05:50:51.506000
05:50:51.515000 IP 150.1.4.4 > 150.1.2.2: ESP(spi=0x49f4ebd0,seq=0x247), length 116
05:50:51.515000 IP 150.1.4.4 > 150.1.2.2: ESP(spi=0x49f4ebd0,seq=0x247), length 116
17 packets captured
17 packets received by filter
0 packets dropped by kernel
```

Task 6.5 Solution

```
R1:

ip cef
!
access-list 100 permit ip 130.1.91.0 0.0.0.255 any
access-list 100 permit ip any 130.1.91.0 0.0.0.255
!
interface GigabitEthernet0/0.17
  ip verify unicast source reachable-via rx allow-self-ping 100
```

https://t.me/learningnets

Task 6.5 Verification

Verify that output is being matched:

```
R1#ping 130.1.76.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 130.1.76.1, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Verify that uRPF strict mode is configured on R1's VLAN 17 interface:

```
R1#show ip interface gigabitEthernet0/0.17 | b IP verify
 IP verify source reachable-via RX, allow self-ping, ACL 100

    0 verification drops
    46 suppressed verification drops
    0 verification drop-rate
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 3

CCIE SCv4 Lab 3 Introduction

Lab Guidelines

The following scenarios are practice labs designed to test your readiness for the Cisco Systems CCIE Security Lab Exam. However, remember that in addition to being designed as a simulation of the actual CCIE lab exam, these practice labs should be used as a learning tool. Instead of rushing through the labs to complete all the configuration steps, take the time to research the networking technology and gain a deeper understanding of the principles behind its operation. For each lab of the CCIE Security Practice Labs Workbook, follow these guidelines:

- Read the entire lab exam before starting the configuration, and correlate tasks within a section to get a complete overview of the lab objectives.
- There are dependencies between tasks of the same section and between tasks from different sections. Carefully read throughout the lab to identify and make notes of it
- The lab consists of six sections that don't necessarily need to be completed in the presented order. However some tasks must be completed before others (such as initialization of ASA firewalls).
- All sections total 100 points, and you must earn a minimum of 80 points to receive a passing grade. To earn the points assigned to each task, you must fulfill all requirements and conform to all restrictions.
- No partial credit is awarded. You will earn all points or zero points for each task; if multiple solutions are available for a task, choose the one that technically best meets the requirements.
- Some tasks present a set of requirements for implementing a technology, and some tasks present outputs to be matched.
- Labs include both configuration and troubleshooting tasks; the number of faults relevant to each troubleshooting task may or not be specified.
- Before starting the exam, verify that all equipment is functional, powered up and that you can access it at the console.
- Routers and switches are preconfigured, do not change it unless specifically allowed

https://t.me/learningnets

by the task. On troubleshooting tickets, you may change any of the initial configurations.

- IPv4/IPv6 static and default routes are allowed to complete any task, but only if this is the only available option, and unless otherwise stated in any task.
- Make sure you do not to lock yourself out of any device, because password recovery or device reset is not available in the lab.
- At the end of the exam, ensure that all devices are accessible at the console by using preconfigured credentials or the ones from specific task requirements.
- For IPv4/IPv6 addressing configuration, the following variables will be used as a reference:
  - **X** is the rack number; the value for **Rack1** will be **1**.
  - **Y** is the device number, with routers ranging from one (1) to seven (7), switches from nine (9) to fourteen (14), and ASA firewalls from fifteen (15) to eighteen (18); the value for **Router1** will be **1**, **Switch1** will be **9**, and **ASA1** will be **15**.

All routers and switches are accessible at the console without requiring any authentication; do not change this. To access other devices within the lab, use the following tables as a reference:

Device	Username	Password
TESTPC-A	ineadmin	ciscoccie
TESTSRV-A	Administrator	Cisco1234
TESTPC-B	ineadmin	ciscoccie
TESTSRV-B	Administrator	Cisco1234
TESTPC-WIFI	ineadmin	ciscoccie

Device	Username	Password
WSA CLI&GUI	admin	default1A

https://t.me/learningnets

Device	Username	Password
ACS1 CLI	admin	default1A
ACS1 GUI	acsadmin	default1A
ACS2 CLI	admin	default1A
ACS2 GUI	acsadmin	default1A
ISE1 CLI&GUI	admin	default1A
ISE2 CLI&GUI	admin	default1A
WLC CLI&GUI	admin	default1A
LAP CLI	cisco	Cisco
IPS CLI&GUI	cisco	ciscoips4240

Lab Instructions

Before you begin, make sure that the initial configuration scripts for each lab have been applied. If you have any questions related to the scenario solutions, visit our CCIE support forum at http://IEOC.com. Refer to the attached physical and logical diagrams on each lab for interface and protocol assignments; you may access these by clicking the **Resources** button in the upper-right corner. Upon lab completion, end-to-end IPv4/IPv6 connectivity is not a requirement unless specifically asked for, but you are required to meet task requirements and restrictions.

Lab Restrictions

Each lab scenario contains explicit general restrictions that you must conform to while configuring the lab. These restrictions are defined in the introductory section for each scenario. Examples of such restrictions include, but are not limited to, not adding additional IP addressing, not changing the default authentication methods,

https://t.me/learningnets

etc. There may also be certain restrictions for particular tasks within a lab scenario. Examples of these restrictions include, but are not limited to, not issuing a particular configuration command, not using the legacy configuration for a technology, etc.

TIP

You may do whatever is necessary to complete a task unless the general requirements for the lab scenario or the specific requirements for the task explicitly prohibit you from doing so. This may include using static routing, NAT statements, ACL exceptions, IPsec/GRE tunneling, etc.

Difficulty Rating

Each lab scenario has been assigned a difficulty rating. Ratings are on a scale of one (1) to ten (10), with 10 being the most difficult. Labs are designed to be more technically challenging than the actual CCIE Security Lab Exam. Do not be discouraged if you score low or do not understand a particular set of technologies. If you are having trouble with a certain area, do not hesitate to read the explanation contained within the solutions guide and study the respective technology using the Technologies Workbook or the Advanced Technologies video course. Remember that these labs are designed to teach you required skills for implementing and troubleshooting a complex network with several technologies mixed together, just as much as they are intended to test your current technical knowledge.

Point Values

As in the actual CCIE Lab exam, each task within a lab is assigned a specific point value. Points are awarded only if the presented solution meets all the given requirements and does not violate any restrictions. No partial credit is awarded for any task. A minimum score of 80 points is required to pass a particular scenario. Some tasks have multiple solutions; as long as the presented solution meets the given requirements, points will be awarded for that task. However, certain solutions may negatively affect previous or future tasks. Make sure that you carefully read all presented requirements and try your best to come up with a technically appropriate solution.

TIP

https://t.me/learningnets

Points will never be awarded for a task in which you have violated the requirements. However, remember the relative point value of the task in question as compared to future tasks. If you cannot find an appropriate solution for a particular task, it is advisable to solve the task by whatever means necessary to complete the future tasks that depend on it.

Loading Initial Config

Each lab contains a set of initial configuration scripts for routers and switches. These configuration scripts include basic Layer 2 and Layer 3 routing connectivity (as well as possible more advanced functionalities for troubleshooting tickets), and must be loaded on your rack before beginning the configuration of the scenario. These are available to be loaded from the Rack Rental Control Panel, or if you are using your own rack, they are attached to each individual lab and available for download. Initial configurations and physical and logical diagrams of each lab are attached to this Introduction; you may access these by clicking the **Resources** button in the upper-right corner.

Rack Rentals

INE has designed the CCIE Security Practice Labs Workbook based around the publicly stated hardware specification used in the actual CCIE Lab exam. To eliminate the cost of buying all the equipment used in the workbook, INE offers cost-effective equipment rentals specifically designed to be used with this and other self-paced training product lines. For more information on rack rentals. visit http://INE.com.

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 3

CCIE SCv4 Lab 3 Tasks

1. Perimeter Security and Services
2. Intrusion Prevention and Content Security
3. Confidentiality and Secure Access
4. Identity Management
5. System Hardening and Availability
6. Threat Identification and Mitigation

Difficulty Rating (10 highest): 8

Point Values

The point values for each section are as follows:

Section	Point Value
Perimeter Security and Services	26
Intrusion Prevention and Content Security	18
Confidentiality and Secure Access	15
Identity Management	14
System Hardening and Availability	14

https://t.me/learningnets

Section	Point Value
Threat Identification and Mitigation	13

GOOD LUCK!

TIP

When taking the CCIE lab exam, you will be provided with a few sheets of scratch paper for notes and diagrams. You should create two diagrams at a minimum: one for the logical Layer 2 topology and one for the logical Layer 3 topology. Note that the physical diagram and the logical Layer 2 diagram are not the same.

Although you are provided with the logical Layer 3 diagram in the lab, it will be in electronic format, which means that you cannot add notes to it and may need to switch between windows to see it on the computer. By having your own diagram, you will be able to take notes on it and quickly reference it as you work through the configuration section. Finally, drawing the Layer 2 and Layer 3 topologies will help you become familiar with a complex network toplogy at first sight.

---

1. Perimeter Security and Services

1.1 ASA Routed Mode (3 points)

- Configure ASA4 in routed single mode with a hostname of **ASA4**, using the information from the table:

Interface1	Nameif	Security Level	IPv4 Address
Gi0/0	OUTSIDE	60	190.1.96.Y/24
Gi0/1	INSIDE	100	190.1.26.Y/24

https://t.me/learningnets

- Enable OSPF and EIGRP as shown in the diagram.
- Configure mutual redistribution between the routing domains, but do not advertise VLAN 29 prefix into OSPF.
- Do not use any access-lists for this task.

1.2 ASA Transparent Mode (3 points)

- Configure ASA3 in transparent single mode with a hostname of **ASA3**, using the information from the table:

Interface	Nameif	Security Level	Bridge-Group
Gi0/0.42	VLAN42	0	42
Gi0/0.56	VLAN56	40	56
Gi0/1.24	VLAN24	0	42
Gi0/1.65	VLAN65	80	56

- Ensure that OSPF is functional between routers in area 12; if required, use interface-level filtering.
- Use the IPv4 address 190.1.24.Y/24 for BVI42 and 190.1.56.Y/24 for BVI56.

1.3 ASA Transparent Security (2 points)

- To protect from CAM table overflow, do not allow ASA3 to dynamically learn MAC addresses.
  - Do not use the **mac-address-table static** command for this task.

1.4 ASA Multiple Context Routed (3 points)

- Configure ASA1 in routed multiple mode with a hostname of **ASA12**, using the information from the table:

https://t.me/learningnets

Interface	Nameif	Security Level	IPv4 Adress	Context Name	Context File
Ma0/0.47	OUTSIDE	50	190.1.47.Y/24	ASA1	ASA1.cfg
Ma0/0.58	OUTSIDE	50	190.1.58.Y/24	ASA2	ASA2.cfg
Red1.37	INSIDE	100	172.16.10.1/24	ASA1	ASA1.cfg
Red1.38	INSIDE	100	190.1.38.Y/24	ASA2	ASA2.cfg

- Remote management for all contexts should be available from within **ASA1** context.
- Match the following output for the redundant interface:

```
ASA12# show interface redundant1 | b Redundancy

      Redundancy Information:
            Member Ethernet0/0(Active), Ethernet0/2
            Last switchover at 10:09:45 UTC Apr 4 2014
```

1.5 ASA Active-Active Failover (4 points)

- Configure ASA1 and ASA2 for stateful failover so that ASA1 is forwarding for context **ASA1** and ASA2 for context **ASA2**.
- Use the following information for both contexts:
  - replicate all possible session states.
  - interface health-check is performed every 2 seconds.
  - detect interface failure within 10 seconds.

- Using VLAN 100 for failover, match the output from ASA1:

```
ASA12# show failover interface

            interface FAILOVER Ethernet0/1
                  System IP Address: 190.1.100.15 255.255.255.0
                  My IP Address    : 190.1.100.15
```

https://t.me/learningnets

```
                    Other IP Address : 190.1.100.16
```

- Match the following output from ASA1:

```
ASA12/ASA1# show failover

    Failover On
    Last Failover at: 12:30:45 UTC Apr 4 2014
            This context: Active
                    Active time: 1447 (sec)
                      Interface INSIDE (172.16.10.1): Normal (Monitored)
                      Interface OUTSIDE (190.1.47.15): Normal (Monitored)
            Peer context: Standby Ready
                    Active time: 0 (sec)
                      Interface INSIDE (172.16.10.2): Normal (Monitored)
                      Interface OUTSIDE (190.1.47.16): Normal (Monitored)
```

- Match the following output from ASA2:

```
ASA12/ASA2# show failover

    Failover On
    Last Failover at: 12:34:50 UTC Apr 4 2014
            This context: Active
                    Active time: 516 (sec)
                      Interface INSIDE (190.1.38.15): Normal (Monitored)
                      Interface OUTSIDE (190.1.58.15): Normal (Monitored)
            Peer context: Standby Ready
                    Active time: 981 (sec)
                      Interface INSIDE (190.1.38.16): Normal (Monitored)
                      Interface OUTSIDE (190.1.58.16): Normal (Monitored)
```

1.6 ASA Application Inspection (2 points)

- Configure ASA4 to deny MSN Instant Messenger traffic for games and webcam services.
- Yahoo and all other MSN services should not be affected.

https://t.me/learningnets

1.7 ZBPF Routed (3 points)

- Configure ZBPF on R1 to match the following requirements:
  - Gi0/1.12 and Loopback0 interfaces are members of the **INSIDE** zone, and Gi0/1.23 is a member of the **OUTSIDE** zone.
  - inspect telnet, icmp, udp, and tcp connections initiated from **INSIDE**.
  - inspect telnet, icmp, and udp traffic initiated from **OUTSIDE**.

- To reduce SPAM messages, drop and log SMTP traffic on ports 25 and 125 initiated from **OUTSIDE** if the following conditions are true:
  - the sender is **brutus@spam.com**
  - the recipient is **ccie@inelab.local**

- Do not use any access-lists for this task.

1.8 ZBPF High Availability (4 points)

- Configure R1 and R2 in active/standby mode for ZBPF functionality, with R1 always preferred as the active forwarder:
  - use a priority of **150** on R1.
  - use GigabitEthernet0/1 for both **control** and **data** interfaces.
  - use IPv4 addressing in the format of **190.1.200.Y/24** for GigabitEthernet0/1.

- Match the following output on both routers:

```
R2#show redundancy application if-mgr group 1

     RG ID: 1
     Interface       VIP         VMAC        Shut   Decrement
     ============================================================
     GigabitEthernet0/1.12 190.1.12.12 0007.b421.000c  shut    0

     WAN Interface
     Interface                    Decrement
     ========================================
```

https://t.me/learningnets

```
R2#show redundancy rii

      No. of RIIs in database: 2
      Interface                          RII Id     decrement
       GigabitEthernet0/1.12         :    12            0
       GigabitEthernet0/1.24         :    24            0
```

1.9 IOS Network Address Translation (2 points)

- Configure NAT on R1 and R2 to translate VLAN 12 subnet into pool of **190.1.88.0/24** as it exits the **OUTSIDE** interface.
  - no simple translation entries should be created.

- R4 has been preconfigured with a static route; do not change it.

2. Intrusion Prevention and Content Security

2.1 IPS Initialization (3 points)

- Initialize the IPS using the information from the table:

Variables	Values
Hostname	IPS4240
IPv4 Address	190.1.44.100/24
Default Gateway	190.1.44.4
Telnet	Disabled
Management Access	190.1.12.0/24
Management Type	HTTPS Port 4443

https://t.me/learningnets

- Ensure that administrators from VLAN 12 can access and manage the IPS via HTTPS without modifying the above management ACL.
- For troubleshooting purposes, enable debug logging for **sensorApp** events.

2.2 IPS Inline VLAN-Pair (3 points)

- Configure the IPS inline between R4 and **ASA1** context, and between R5 and **ASA2** context.
- Ensure that signature changes for a context do not affect the other context.

2.3 IPS Custom Signature (3 points)

- Configure the IPS to block an attacker inline when it detects the case-insensitive substring **cmd.exe** in HTTP URLs:
  - it should apply only for traffic between R4 and **ASA1** context.
  - do not use any **STRING** engines for that task.
  - the signature should have a medium severity and fidelity rating.
  - to protect against various evasion techniques, assume that the server may listen on ports 80 and 8080.
  - fire an event on every signature match.
  - use a signature ID of **60005** and subsignature ID of **0**.

2.4 WSA Initialization (3 points)

- Initialize the WSA using the information from the table:

Variables	Values
Hostname	wsa.inelab.local
DNS Server	150.1.4.4
NTP Server	150.1.4.4
Proxy Ports	M1 and P1

https://t.me/learningnets

Variables	Values
M1 IPv4 Address	172.16.6.100/24
M1 Default Gateway	172.16.6.1
Admin Password	default1A
Email Address	ccielab@inelab.local
Senderbase Participation	Minimum

- Assign **TEST-PC-B** an IPv4 address from VLAN 12 for this scope.
- Ensure that VLAN 12 administrators can manage the WSA over HTTPS; do not configure any NAT exemptions.

2.5 WSA WCCP Integration (3 points)

- Configure R1 and R2 to redirect HTTP traffic from VLAN 12 as it exits on the **OUTSIDE** interface to the WSA.
  - use M1 port of the WSA for this scope.

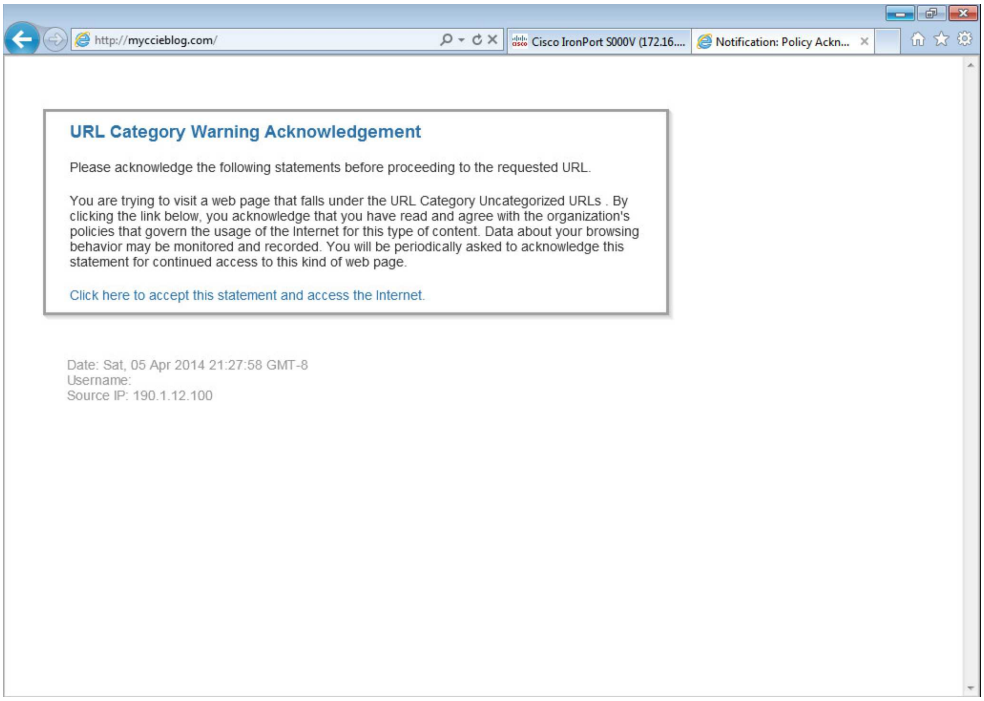
- R1 and R2 should allow only WSA's M1 IP address as the WCCP client.

2.6 WSA Traffic Policies (3 points)

- Configure WSA with the following policies:
  - block non-safe content from being displayed by search engines.
  - block access to search engines that do not support safe search functionality.
  - block access to any content rated as adult.

https://t.me/learningnets

- R4 has been preconfigured as a DNS server. Configure **TEST-PC-B** with a DNS server of 150.1.4.4.
- ensure to match the following output when accessing **www.myccieblog.com** from **TEST-PC-B**:



3. Confidentiality and Secure Access

3.1 VRF-Aware IPv6 IKEv2 SVTI Troubleshooting (3 points)

- IKEv2 SVTI has been configured between R1 and R2 with the scope of protecting IPV6 traffic inside vrf **SVTI**.
- IPv6 is used as both transport and payload protocol.
- Fix the configuration to achieve the match output:

```
R1#show crypto ikev2 sa detailed | i inelab.local

          Local id: R1.inelab.local
          Remote id: R2.inelab.local
```

https://t.me/learningnets

- When the IPsec tunnel is negotiated, match the following output:

```
R1#ping vrf SVTI 2001::2 source loopback12

    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 2001::2, timeout is 2 seconds:
    Packet sent with a source address of 2001::1%SVTI
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

3.2 IKEv1 Crypto Map Troubleshooting (3 points)

- A crypto map-based IKEv1 IPsec tunnel has been configured between R3 and R7 for protecting traffic between VLAN 33 and VLAN 11 subnets.
- Tunnel negotiation is between Loopback0 IPv4 addresses, and both routers should be able to perform the role of initiator.
- Fix the configuration to match the following output:

```
R7#show crypto ipsec sa


    interface: FastEthernet0/0.27
        Crypto map tag: VPN, local addr 150.1.7.7

       protected vrf: (none)
       local  ident (addr/mask/prot/port): (172.16.5.0/255.255.255.0/0/0)
       remote ident (addr/mask/prot/port): (190.1.33.0/255.255.255.0/0/0)
       current_peer 190.1.58.3 port 4500
```

- When the IPsec tunnel is negotiated, match the following output:

https://t.me/learningnets

```
R3#ping 172.16.5.1 source fastEthernet0/0.33


    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 172.16.5.1, timeout is 2 seconds:
    Packet sent with a source address of 190.1.33.3
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
```

3.3 EzVPN Server on ASA (3 points)

- Configure ASA4 as EzVPN server; use **cisco** for all required passwords.
- Enable DHCP server on SW2 for IPv4 address assignment; use 190.1.50.0/24 subnet.
- Your configuration should allow all users from VLAN 12 to connect.
- Tunnel only traffic for VLAN 29, and match the following output for a connected client:

```
ASA4# show vpn-sessiondb detail ra-ikev1-ipsec


    Session Type: IKEv1 IPsec Detailed

    Username     : ezvpnuser             Index        : 16
    Assigned IP  : 190.1.50.12           Public IP    : 190.1.12.100
    Protocol     : IKEv1 IPsecOverUDP
    License      : Other VPN
    Encryption   : 3DES                  Hashing      : MD5
    Bytes Tx     : 300                   Bytes Rx     : 300
    Pkts Tx      : 5                     Pkts Rx      : 5
    Pkts Tx Drop : 0                     Pkts Rx Drop : 0
    Group Policy : EZVPN_POLICY          Tunnel Group : EZVPN_TUNNEL
    Login Time   : 20:10:49 UTC Sat Apr 5 2014
    Duration     : 0h:04m:28s
    Inactivity   : 0h:00m:00s
    NAC Result   : Unknown
    VLAN Mapping : N/A                   VLAN         : none

    IKEv1 Tunnels: 1
    IPsecOverUDP Tunnels: 1

    IKEv1:
```

https://t.me/learningnets

```
      Tunnel ID    : 16.1
      UDP Src Port : 63505                  UDP Dst Port : 500
      IKE Neg Mode : Aggressive             Auth Mode    : preSharedKeys
      Encryption   : 3DES                   Hashing      : MD5
      Rekey Int (T): 86400 Seconds          Rekey Left(T): 86135 Seconds
      D/H Group    : 2
      Filter Name  :
      Client OS    : WinNT                  Client OS Ver: 5.0.07.0410

    IPsecOverUDP:
      Tunnel ID    : 16.2
      Local Addr   : 0.0.0.0/0.0.0.0/0/0
      Remote Addr  : 190.1.50.12/255.255.255.255/0/0
      Encryption   : 3DES                   Hashing      : MD5
      Encapsulation: Tunnel                 UDP Dst Port : 9500
      Rekey Int (T): 28800 Seconds          Rekey Left(T): 28530 Seconds
      Idle Time Out: 30 Minutes             Idle TO Left : 27 Minutes
      Bytes Tx     : 300                    Bytes Rx     : 300
      Pkts Tx      : 5                      Pkts Rx      : 5

    NAC:
      Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
      SQ Int (T)   : 0 Seconds              EoU Age(T)   : 270 Seconds
      Hold Left (T): 0 Seconds              Posture Token:
      Redirect URL :
```

- Do not disable NAT-T on ASA4 using the command **no crypto isakmp nat-traversal**.

3.4 IKev1 PKI IPsec (3 points)

- Configure a PKI-based authentication IKEv1 IPsec VPN between ASA4 and R5 to protect traffic between R5 and SW2 Loopback0 subnets.
- R3 has been preconfigured as NTP and PKI server; synchronize time and perform certificate enrollment for both R5 and ASA4.
- Ensure that session can be initiated only by ASA4.
- Use of the command **peer-id-validate** on ASA4 or ACL modifications on ASA3 is restricted.
- Match the following output:

```
ASA4# show vpn-sessiondb detail l2l
```

https://t.me/learningnets

```
Session Type: LAN-to-LAN Detailed

Connection   : CCIELAB
Index        : 54                    IP Addr      : 190.1.56.5
Protocol     : IKEv1 IPsec
Encryption   : AES256                Hashing      : SHA1
Bytes Tx     : 400                   Bytes Rx     : 400
Login Time   : 22:57:49 UTC Sat Apr 5 2014
Duration     : 0h:04m:43s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 54.1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Main                  Auth Mode    : rsaCertificate
  Encryption   : AES256                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 86117 Seconds
  D/H Group    : 5
  Filter Name  :
  IPv6 Filter  :

IPsec:
  Tunnel ID    : 54.2
  Local Addr   : 150.1.10.10/255.255.255.255/0/0
  Remote Addr  : 150.1.5.5/255.255.255.255/0/0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 3600 Seconds          Rekey Left(T): 3317 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 25 Minutes
  Bytes Tx     : 400                   Bytes Rx     : 400
  Pkts Tx      : 4                     Pkts Rx      : 4

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 286 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

3.5 WLC Local Web Authentication (3 points)

https://t.me/learningnets

- Configure a WLAN on the WLC with the following parameters:

Variables	Values
Profile	CCIELAB
SSID	CCIELAB-RACK-X
Authentication	Web Authentication
Encryption	None
Authentication Server	LDAP
Authentication Username	USER1
Authentication Password	1qaz@WSX
Interface Name	CCIELAB
Interface VLAN	111
Interface Port	1
Interface IPv4 Address	190.1.111.100
Interface DHCP	190.1.111.13
IPv4 Subnet	190.1.111.0/24
Default Gateway	190.1.111.13

https://t.me/learningnets

- Ensure that administrators from VLAN 12 can manage the WLC via HTTPS.
- Integrate with the **TEST-SRV-A** LDAP server on 190.1.47.100 using **ldapuser** with a password of **1qaz@WSX**, member of **Users** organization unit in the **inelab.local** domain.
- SW5 has been preconfigured to assign IPv4 addresses to WiFi clients.
- **WIFI-PC** should successfully authenticate to the SSID and ping its default gateway.

4. Identity Management

4.1 ASA Cut-Through Proxy (4 points)

- Configure **ASA2** context to transparently enforce authentication for HTTP traffic inbound on its VLAN 58 interface.
  - use the RADIUS server from ACS for this scope, with a shared key of **ciscoasa** and a username/password pair of **httpuser/httppass**.
  - authorize users for HTTP/HTTPS traffic through the use of proxy-acl.

- Test the authentication process from VLAN 12 to R3's NAT'ed Loopback0 address of 190.1.58.3.
- Ensure that administrators from VLAN 12 can manage ACS via HTTPS.

4.2 IOS RADIUS Authentication (3 points)

- Configure R4 to authenticate telnet sessions with a user named **ADMIN** along with the password **CISCO** with the ACS server via RADIUS.
  - If the ACS server is not available, the user should be authenticated against the local database.
  - User should be automatically placed into privilege-level 15; do not modify the default privilege-level on VTY lines for this.

- Additionally, all privilege-level 15 commands should be accounted for on the ACS server.
- For integration with ACS server, use Loopback0 interface and the shared key of **cisco**.

4.3 IOS TACACS+ Authentication (3 points)

https://t.me/learningnets

- Configure R7 to authenticate telnet sessions against the ACS server using TACACS+:
  - source the TACACS+ connections off the reliable interface and use a shared key of **tacacskey**.

- Upon authentication, user **USER1** with a password of **CISCO** should be placed into privilege-level 9:
  - disconnect the user if inactive for 10 minutes.
  - allow the user access to any **snmp-server**-related configurations.

4.4 EAP-FAST 802.1x Authentication (4 points)

- Configure SW3 to authenticate **TEST-PC-B** using ISE server at 190.1.96.100, to match the output:

```
SW3#show authentication sessions interface gigabitEthernet1/0/5

               Interface:  GigabitEthernet1/0/5
             MAC Address:  48f8.b32e.2532
              IP Address:  Unknown
               User-Name:  iseuser
                  Status:  Authz Success
                  Domain:  DATA
         Security Policy:  Must Secure
         Security Status:  Secured
          Oper host mode:  single-host
        Oper control dir:  both
           Authorized By:  Authentication Server
             Vlan Policy:  N/A
         Session timeout:  N/A
            Idle timeout:  N/A
       Common Session ID:  00000000000069AB0FBE61F9
         Acct Session ID:  0x000000F6
                  Handle:  0x50000A73

    Runnable methods list:
           Method   State
           dot1x    Authc Success
```

- Use the Cisco proprietary EAP method, with the username/password pair of **iseuser/Cisco123**

https://t.me/learningnets

.

- Use the shared key of **isekey** for RADIUS integration and source RADIUS packets from Loopback0 address.
- Ensure that administrators from VLAN 12 can manage ISE via HTTPS.
- Use the following 802.1x timers:
  - wait 15 seconds for EAP answer to an EAP Identity Request frame.
  - resend each EAP Identity Request 5 times if no answer is received from the client.
  - restart the EAP authentication process 3 times.

5. System Hardening and Availability

5.1 Remotely Triggered Blackhole (3 points)

- An attack has been detected in the network, sourced from a WiFi user in VLAN 111 with the IP address of 190.1.111.99.
- Consider R3 as the trigger router using BGP in AS 357 to instruct edge routers of R5 and R7 to drop malicious traffic.
- Configure BGP peering based on Loopback0 IPv4 addresses.
- Ensure that R5 and R7 can initiate the BGP session.

5.2 IOS Netflow (3 points)

- Configure netflow data collection on R1's VLAN 12 interface to match the following requirements:
  - export version 9 statistics to the collection server at 172.16.1.99 on port 8000.
  - use Loopback0 interface as the source and include the interface name in the export.
  - randomly sample packets at a rate of one out of 20 packets.
  - collect information about packet-length, VLAN number, and TTL value.

5.3 IOS OSPFv2 Neighbor Authentication (3 points)

- To prevent OSPF spoofed packets being injected from VLAN 45, enable OSPF authentication between R4 and R5 with the most secure method using the string of **ospf**.

https://t.me/learningnets

- Do not use the command **ip ospf authentication** on R4's VLAN 45 interface.

5.4 IOS Traffic Classification and QoS (3 points)

- Configure R6 with the following traffic policy outbound on its VLAN 65 interface:
  - guarantee 10% of the interface bandwidth to OSPF.
  - limit ICMP traffic to 10% of the bandwidth.
  - mark telnet traffic with the DSCP value of AF43.

5.5 IOS CPU Monitoring (2 points)

- Configure R5 to generate a syslog message when the total CPU utilization rises above 95% for 10 seconds.
- Configure R5 to generate a syslog message when the CPU goes below 20% for at least 20 seconds.
- Send a version 2 SNMP trap to 172.16.1.44 using the community name of **cpu** when the above thresholds are reached.
  - use a source of Loopback0 for this.

6. Threat Identification and Mitigation

6.1 IPv6 DHCP Guard Troubleshooting (3 points)

- R6 is configured as a IPv6 DHCP server on VLAN 69 and SW3 as a client.
- IPv6 DHCP Guard has been configured on SW3 to protect from spoofed DHCP servers.
- Fix the configuration to match the following output:

```
SW3#ping 2001:69:69::6

    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 2001:69:69::6, timeout is 2 seconds:
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/9 ms
```

6.2 Layer 2 Security (2 points)

https://t.me/learningnets

- Configure ports Fa1/0/10 and Fa1/0/11 of SW1 into VLAN 12.
- Configure SW1 so that servers connected on these two ports are not allowed to communicate directly at layer 2.
- Additionally, SW1 should not flood unknown unicast frames from VLAN 12 out on these ports.

6.3 IOS Control-Plane Logging (3 points)

- Configure R5 to log packets destined to itself.
- Do not use any access-lists for this task.

6.4 OSPF Security (3 points)

- An OSPF DoS attack has been detected in VLAN 45.
- Configure the network to ensure that R4 and R5 receive OSPF packets only from each other.

6.5 IOS Control-Plane Policing (2 points)

- Configure R6 to police all ICMP traffic destined to itself to 100Kbps, unless sourced from Loopback0 range of 150.1.0.0/16.
- Do not use any interface-level configuration for this scope.

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 3

CCIE SCv4 Lab 3 Solutions Section 1

1. Task 1.1 Solution
2. Task 1.2 Solution
3. Task 1.3 Solution
4. Task 1.4 Solution
5. Task 1.5 Solution
6. Task 1.6 Solution
7. Task 1.7 Solution
8. Task 1.8 Solution
9. Task 1.9 Solution

Task 1.1 Solution

SW1:

```
 interface FastEthernet1/0/19
  switchport mode access
  switchport access vlan 26
  no shutdown
```

SW2:

```
 interface FastEthernet1/0/18
  switchport mode access
  switchport access vlan 96
  no shutdown
```

ASA4:

```
hostname ASA4
!
interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 60
 ip address 190.1.96.18 255.255.255.0
 ospf authentication message-digest
```

https://t.me/learningnets

```
 ospf message-digest-key 1 md5 ospfkey
 no shutdown
!
interface GigabitEthernet0/1
 nameif INSIDE
 security-level 100
 ip address 190.1.26.18 255.255.255.0
 no shutdown
!
prefix-list EIGRP_TO_OSPF seq 5 deny 172.16.3.0/24
prefix-list EIGRP_TO_OSPF seq 10 permit 0.0.0.0/0 le 32
!
route-map EIGRP_TO_OSPF permit 10
 match ip address prefix-list EIGRP_TO_OSPF
!
router ospf 300
 network 190.1.96.0 255.255.255.0 area 0
 redistribute eigrp 300 subnets route-map EIGRP_TO_OSPF
!
router eigrp 300
 no auto-summary
 network 190.1.26.0 255.255.255.0
 redistribute ospf 300 metric 100000 100 255 1 1500
```

Task 1.1 Verification

Verify that switch intrefaces are in access mode in required VLANs:

```
SW1#show interfaces fastEthernet1/0/19 trunk


Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/19    off              negotiate      not-trunking  1

Port        Vlans allowed on trunk
Fa1/0/19    26

Port        Vlans allowed and active in management domain
Fa1/0/19    26

Port        Vlans in spanning tree forwarding state and not prunedFa1/0/19    26
!
!SW2#show interfaces fastEthernet1/0/18 trunk
```

https://t.me/learningnets

```
Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/18    off              negotiate      not-trunking  1


Port        Vlans allowed on trunk
Fa1/0/18    96

Port        Vlans allowed and active in management domain
Fa1/0/18    96

Port        Vlans in spanning tree forwarding state and not prunedFa1/0/18    96
```

Verify security-level, nameif, and IPv4 addressing:

```
ASA4# show nameif

Interface               Name                    Security
GigabitEthernet0/0      OUTSIDE                  60
GigabitEthernet0/1      INSIDE                  100
!
!ASA4# show ip address

System IP Addresses:
Interface               Name                    IP address      Subnet mask     Method
GigabitEthernet0/0      OUTSIDE                 190.1.96.18     255.255.255.0   manual
GigabitEthernet0/1      INSIDE                  190.1.26.18     255.255.255.0   manual
Current IP Addresses:
Interface               Name                    IP address      Subnet mask     Method
GigabitEthernet0/0      OUTSIDE                 190.1.96.18     255.255.255.0   manual
GigabitEthernet0/1      INSIDE                  190.1.26.18     255.255.255.0   manual
```

Verify the EIGRP and OSPF neighbors, as well as routing table entries:

```
ASA4# show ospf neighbor



Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.10.10       1   FULL/BDR        0:00:31     190.1.96.11     OUTSIDE
!
!ASA4# show eigrp neighbors

EIGRP-IPv4 neighbors for process 300
```

https://t.me/learningnets

```
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   190.1.26.10             Gi0/1            10  00:11:59 1    200   0   23

!
!
ASA4# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O IA 190.1.56.0 255.255.255.0 [110/12] via 190.1.96.11, 0:04:40, OUTSIDE
D    190.1.27.0 255.255.255.0 [90/3072] via 190.1.26.10, 0:12:05, INSIDE
C    190.1.26.0 255.255.255.0 is directly connected, INSIDE
D    190.1.23.0 255.255.255.0 [90/3072] via 190.1.26.10, 0:12:05, INSIDE
D    190.1.7.0 255.255.255.0 [90/28672] via 190.1.26.10, 0:12:05, INSIDE
D    190.1.111.0 255.255.255.0 [90/3328] via 190.1.26.10, 0:12:05, INSIDE
C    190.1.96.0 255.255.255.0 is directly connected, OUTSIDE
O    190.1.69.0 255.255.255.0 [110/11] via 190.1.96.11, 0:04:40, OUTSIDE
D    172.16.5.0 255.255.255.0 [90/3328] via 190.1.26.10, 0:12:05, INSIDE
O    172.16.6.0 255.255.255.0 [110/11] via 190.1.96.11, 0:04:40, OUTSIDE
O IA 172.16.1.0 255.255.255.0 [110/12] via 190.1.96.11, 0:04:40, OUTSIDE
D    172.16.3.0 255.255.255.0 [90/3328] via 190.1.26.10, 0:12:05, INSIDE
O    150.1.6.6 255.255.255.255 [110/12] via 190.1.96.11, 0:04:40, OUTSIDE
O    150.1.11.11 255.255.255.255 [110/11] via 190.1.96.11, 0:04:40, OUTSIDE
D    150.1.7.7 255.255.255.255 [90/131072] via 190.1.26.10, 0:12:06, INSIDE
D    150.1.13.13 255.255.255.255 [90/131072] via 190.1.26.10, 0:12:06, INSIDE
D    150.1.10.10 255.255.255.255 [90/130816] via 190.1.26.10, 0:12:06, INSIDE
```

Verify that OSPF MD5 authentication is configured:

```
ASA4# show ospf interface OUTSIDE


OUTSIDE is up, line protocol is up
  Internet Address 190.1.96.18 mask 255.255.255.0, Area 0
  Process ID 300, Router ID 190.1.96.18, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
```

https://t.me/learningnets

```
  Designated Router (ID) 190.1.96.18, Interface address 190.1.96.18
  Backup Designated router (ID) 150.1.10.10, Interface address 190.1.96.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 0:00:07
  Index 1/1, flood queue length 0
  Next 0x0000000000000000(0)/0x0000000000000000(0)
  Last flood scan length is 2, maximum is 8
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 150.1.10.10  (Backup Designated Router)
  Suppress hello for 0 neighbor(s) Message digest authentication enabled
Youngest key id is 1
```

Verify that VLAN 29 prefix is not injected in the OSPF database, and therefore not advertised into the OSPF domain:

```
ASA4# show ospf database | b External

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
150.1.7.7       190.1.96.18     866         0x80000001 0xd6f1 0
150.1.10.10     190.1.96.18     866         0x80000001 0x972b 0
150.1.13.13     190.1.96.18     866         0x80000001 0x5864 0
172.16.5.0      190.1.96.18     866         0x80000001 0x5f4d 0
190.1.7.0       190.1.96.18     866         0x80000001 0x1394 0
190.1.23.0      190.1.96.18     866         0x80000001 0x6235 0
190.1.26.0      190.1.96.18     868         0x80000001 0x4153 0
190.1.27.0      190.1.96.18     866         0x80000001 0x365d 0
190.1.111.0     190.1.96.18     866         0x80000001 0x96a8 0
!
!SW3#show ip route 172.16.3.0
% Subnet not in table
```

Task 1.2 Solution

```
SW1:
interface FastEthernet1/0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 24,65
```

https://t.me/learningnets

```
 no shutdown
```

SW2:

```
interface FastEthernet1/0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 42,56
 no shutdown
```

ASA3:

```
firewall transparent
!
hostname ASA3
!
interface GigabitEthernet0/0
 no shutdown
!
interface GigabitEthernet0/0.42
 vlan 42
 nameif VLAN42
 security-level 0
 bridge-group 42
!
interface GigabitEthernet0/0.56
 vlan 56
 nameif VLAN56
 security-level 40
 bridge-group 56
!
interface GigabitEthernet0/1
 no shutdown
!
interface GigabitEthernet0/1.24
 vlan 24
 nameif VLAN24
 security-level 0
 bridge-group 42
!
interface GigabitEthernet0/1.65
 vlan 65
 nameif VLAN65
 security-level 80
 bridge-group 56
!
interface Bvi42
```

https://t.me/learningnets

```
 ip address 190.1.24.17 255.255.255.0
!
interface Bvi56
 ip address 190.1.56.17 255.255.255.0
!
same-security-traffic permit inter-interface
!
access-list VLAN56_IN extended permit ospf host 190.1.56.5 host 190.1.56.6
access-group VLAN56_IN in interface VLAN56
```

Task 1.2 Verification

Verify that switch interfaces are in trunk mode and required VLANs are allowed:

https://t.me/learningnets

```
SW1#show interfaces fastEthernet1/0/17 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/17    on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa1/0/17    24,65

Port        Vlans allowed and active in management domain
Fa1/0/17    24,65

Port        Vlans in spanning tree forwarding state and not pruned Fa1/0/17    24,65

!
!SW2#show interfaces fastEthernet1/0/16 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/16    on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa1/0/16    42,56

Port        Vlans allowed and active in management domain
Fa1/0/16    42,56

Port        Vlans in spanning tree forwarding state and not pruned Fa1/0/16    42,56
```

Verify security-level and nameif:

```
ASA3# show nameif

Interface                Name                   Security
GigabitEthernet0/0.42    VLAN42                   0
GigabitEthernet0/0.56    VLAN56                  40
GigabitEthernet0/1.24    VLAN24                   0
GigabitEthernet0/1.65    VLAN65                  80
```

https://t.me/learningnets

Verify the bridge-group interface allocation and IP addressing:

```
ASA3# show bridge-group 56
 Interfaces:  GigabitEthernet0/0.56
 GigabitEthernet0/1.65

 Management System IP Address:  190.1.56.17 255.255.255.0
 Management Current IP Address: 190.1.56.17 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 2
!
!ASA3# show bridge-group 42
 Interfaces:  GigabitEthernet0/0.42
 GigabitEthernet0/1.24

 Management System IP Address:  190.1.24.17 255.255.255.0
 Management Current IP Address: 190.1.24.17 255.255.255.0

 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 3
```

Verify that OSPF traffic is allowed by the firewall:

```
R6#show ip ospf neighbor fastEthernet0/1

Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.5.5         1   FULL/BDR        00:01:32    190.1.56.5      FastEthernet0/1
!
!R4#show ip ospf neighbor fastEthernet0/0.42


Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.1.1         1   FULL/DROTHER    00:00:38    190.1.24.1      FastEthernet0/0.42
150.1.2.2         1   FULL/BDR        00:00:37    190.1.24.2      FastEthernet0/0.42
```

Task 1.3 Solution

https://t.me/learningnets

Ping all connected devices to learn the MAC addresses:

```
ASA3# ping 190.1.24.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.1.24.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
!ASA3# ping 190.1.24.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.1.24.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
!ASA3# ping 190.1.24.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.1.24.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
!ASA3# ping 190.1.56.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.1.56.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
!ASA3# ping 190.1.56.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.1.56.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Verify the IP to MAC mappings; this may differ based on the rack being assigned:

```
ASA3# show arp

        VLAN42 190.1.24.4 0019.0653.2a18 19
        VLAN56 190.1.56.5 0017.e04a.9678 9
        VLAN24 190.1.24.2 d867.d9e0.bbc1 23
        VLAN24 190.1.24.1 d48c.b5da.d549 25
        VLAN65 190.1.56.6 0017.5aed.28b1 5
```

Configure static MAC entries by using ARP, and disable MAC learning:

```
ASA3:

mac-learn VLAN42 disable
```

https://t.me/learningnets

```
mac-learn VLAN56 disable
mac-learn VLAN24 disable
mac-learn VLAN65 disable
!
arp VLAN42 190.1.24.4 0019.0653.2a18
arp VLAN65 190.1.56.6 0017.5aed.28b1
arp VLAN56 190.1.56.5 0017.e04a.9678
arp VLAN24 190.1.24.1 d48c.b5da.d549
arp VLAN24 190.1.24.2 d867.d9e0.bbc1
```

Task 1.3 Verification

Verify that MAC learning has been disabled:

```
ASA3# show mac-learn

interface                          mac learn
-----------------------------------------
 VLAN42                              disabled
 VLAN56                              disabled
 VLAN24                              disabled
 VLAN65                              disabled
```

Verify that static MAC entries have been populated through the ARP configuration:

```
ASA3# show mac-address-table static

interface                  mac  address          type      Age(min)   bridge-group
-------------------------------------------------------------------------------
VLAN24                     d867.d9e0.bbc1          static                42
VLAN42                     0019.0653.2a18          static                42
VLAN56                     0017.e04a.9678          static                56
VLAN24                     d48c.b5da.d549          static                42
VLAN65                     0017.5aed.28b1          static                56
```

Task 1.4 Solution

```
SW1:
interface FastEthernet1/0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 47,58
```

https://t.me/learningnets

```
 no shutdown

SW2:

interface range FastEthernet1/0/12 - 13
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 37,38
 no shutdown
```

Convert ASA1 into multiple-context mode:

```
ciscoasa(config)# mode multiple

WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]

ASA1 System Context:
hostname ASA12
!
interface Ethernet0/0
 no shutdown
!
interface Management0/0
 no shutdown
!
interface Ethernet0/2
 no shutdown
!
interface Redundant1
 member-interface ethernet0/0
 member-interface ethernet0/2
!
interface Redundant1.37
 vlan 37
!
interface Redundant1.38
 vlan 38
!
interface Management0/0.47
 vlan 47
!
interface Management0/0.58
```

https://t.me/learningnets

```
 vlan 58
!
delete /noconfirm disk0:/*.cfg
!
!
context ASA1
 allocate-interface Redundant1.37
 allocate-interface Management0/0.47
 config-url disk0:/ASA1.cfg
!
context ASA2
 allocate-interface Redundant1.38
 allocate-interface Management0/0.58
 config-url disk0:/ASA2.cfg
!
no context admin
admin-context ASA1
```

ASA1 ASA1 Context:

```
interface Redundant1.37
 nameif INSIDE
 security-level 100
 ip address 172.16.10.1 255.255.255.0
!
interface Management0/0.47
 nameif OUTSIDE
 security-level 50
 no  management-only
 ip address 190.1.47.15 255.255.255.0
```

ASA1 ASA2 Context:

```
interface Redundant1.38
 nameif INSIDE
 security-level 100
 ip address 190.1.38.15 255.255.255.0
!
interface Management0/0.58
 nameif OUTSIDE
 security-level 50
 no  management-only
 ip address 190.1.58.15 255.255.255.0
```

https://t.me/learningnets

Task 1.4 Verification

Verify that switch ports are trunking correct VLANs:

```
SW1#show interfaces fastEthernet1/0/12 trunk


Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/12    on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa1/0/12    47,58

Port        Vlans allowed and active in management domain
Fa1/0/12    47,58

Port        Vlans in spanning tree forwarding state and not prunedFa1/0/12    47,58
!
!SW2#show spanning-tree interface fastEthernet1/0/12

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
VLAN0037            Desg FWD 19        128.14   P2p
VLAN0038            Desg FWD 19        128.14   P2p
!
!SW2#show spanning-tree interface fastEthernet1/0/13

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
VLAN0037            Desg FWD 19        128.15   P2p
VLAN0038            Desg FWD 19        128.15   P2p
```

Verify context interface allocation and that **ASA1** context is the admin context:

https://t.me/learningnets

```
ASA12# show context

Context Name      Class      Interfaces           URL
*ASA1             default    Management0/0.47,    disk0:/ASA1.cfg
 Redundant1.37

 ASA2             default    Management0/0.58,    disk0:/ASA2.cfg
                             Redundant1.38

Total active Security Contexts: 2
```

Verify that requested output for the redundant interface is matched:

```
ASA12# show interface redundant1 | b Redundancy
  Redundancy Information: Member Ethernet0/0(Active), Ethernet0/2

        Last switchover at 10:09:45 UTC Apr 4 2014
```

Verify the nameif, security-level, and IPv4 addressing for context **ASA1**:

```
ASA12/ASA1# show nameif
Interface                 Name                    Security
Redundant1.37             INSIDE                  100
Management0/0.47          OUTSIDE                  50
!
!ASA12/ASA1# show ip address

System IP Addresses:
Interface                 Name                    IP address      Subnet mask     Method
Redundant1.37             INSIDE                  172.16.10.1     255.255.255.0   manual
Management0/0.47          OUTSIDE                 190.1.47.15     255.255.255.0   manual
Current IP Addresses:
Interface                 Name                    IP address      Subnet mask     Method
Redundant1.37             INSIDE                  172.16.10.1     255.255.255.0   manual
Management0/0.47          OUTSIDE                 190.1.47.15     255.255.255.0   manual
```

Verify the nameif, security-level, and IPv4 addressing for context **ASA2**:

```
ASA12/ASA2# show nameif
Interface                 Name                    Security
Redundant1.38             INSIDE                  100
```

https://t.me/learningnets

```
Management0/0.58         OUTSIDE                  50
!
!ASA12/ASA2# show ip address

System IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
Redundant1.38            INSIDE                 190.1.38.15     255.255.255.0   manual
Management0/0.58         OUTSIDE                190.1.58.15     255.255.255.0   manual
Current IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
Redundant1.38            INSIDE                 190.1.38.15     255.255.255.0   manual
Management0/0.58         OUTSIDE                190.1.58.15     255.255.255.0   manual
```

Task 1.5 Solution

SW1:

```
interface FastEthernet1/0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 47,58
 no shutdown
!
interface range FastEthernet1/0/13 , FastEthernet1/0/15
 switchport mode access
 switchport access vlan 100
 no shutdown
```

SW2:

```
interface range FastEthernet1/0/14 - 15
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 37,38
 no shutdown
```

ASA1 System Context:

```
failover group 1
 primary
 preempt
 replication http
 polltime interface 2 holdtime 10
!
failover group 2
 secondary
```

https://t.me/learningnets

```
 preempt
 replication http
 polltime interface 2 holdtime 10
!
context ASA1
 join-failover-group 1
!
context ASA2
 join-failover-group 2
!
interface Ethernet0/1
 no shutdown
!
failover lan unit primary
failover lan interface FAILOVER Ethernet0/1
failover link failover Ethernet0/1
failover interface ip FAILOVER 190.1.100.15 255.255.255.0 standby 190.1.100.16
failover

ASA1 ASA1 Context:
interface Redundant1.37
 ip address 172.16.10.1 255.255.255.0 standby 172.16.10.2
!
interface Management0/0.47
 ip address 190.1.47.15 255.255.255.0 standby 190.1.47.16
!
monitor-interface INSIDE
monitor-interface OUTSIDE

ASA1 ASA2 Context:

interface Redundant1.38
 ip address 190.1.38.15 255.255.255.0 standby 190.1.38.16
!
interface Management0/0.58
 ip address 190.1.58.15 255.255.255.0 standby 190.1.58.16
!
monitor-interface INSIDE
monitor-interface OUTSIDE
```

First, convert ASA2 into multiple-context mode:

```
ciscoasa(config)# mode multiple
 WARNING: This command will change the behavior of the device
```

https://t.me/learningnets

```
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]

ASA2 System Context:

delete /noconfirm disk0:/*.cfg
!
interface Ethernet0/1
 no shutdown
!
failover lan unit secondary
failover lan interface FAILOVER Ethernet0/1
failover link failover Ethernet0/1
failover interface ip FAILOVER 190.1.100.15 255.255.255.0 standby 190.1.100.16
failover
```

Task 1.5 Verification

Verify that requested output is matched on both ASA1 and ASA2:

```
ASA12# show failover interface

        interface FAILOVER Ethernet0/1
                System IP Address: 190.1.100.15 255.255.255.0
                My IP Address    : 190.1.100.15
                Other IP Address : 190.1.100.16
!
!ASA12/ASA1# show failover

Failover On
Last Failover at: 12:30:45 UTC Apr 4 2014
        This context: Active
                Active time: 1598 (sec)
                  Interface INSIDE (172.16.10.1): Normal (Monitored)
                  Interface OUTSIDE (190.1.47.15): Normal (Monitored)
        Peer context: Standby Ready
                Active time: 0 (sec)
                  Interface INSIDE (172.16.10.2): Normal (Monitored)
                  Interface OUTSIDE (190.1.47.16): Normal (Monitored)
!
!ASA12/ASA2# show failover

Failover On
Last Failover at: 12:34:50 UTC Apr 4 2014
```

https://t.me/learningnets

```
        This context: Active
                Active time: 630 (sec)
                  Interface INSIDE (190.1.38.15): Normal (Monitored)
                  Interface OUTSIDE (190.1.58.15): Normal (Monitored)
        Peer context: Standby Ready
                Active time: 981 (sec)
                  Interface INSIDE (190.1.38.16): Normal (Monitored)
                  Interface OUTSIDE (190.1.58.16): Normal (Monitored)
```

Verify that HTTP replication is configured and interface failure timers have been modified:

```
ASA12# show running-config failover

failover
failover lan unit primary
failover lan interface FAILOVER Ethernet0/1
failover link FAILOVER Ethernet0/1
failover interface ip FAILOVER 190.1.100.15 255.255.255.0 standby 190.1.100.16failover group 1
  preempt replication http
 polltime interface 2 holdtime 10
failover group 2
  secondary
  preempt replication http
 polltime interface 2 holdtime 10
```

Task 1.6 Solution

https://t.me/learningnets

ASA4:

```
class-map type inspect im match-all MSN_DROP
 match protocol msn-im
 match service games webcam
!
 policy-map type inspect im MSN_DROP
 class MSN_DROP
  drop-connection
!
policy-map global_policy
 class inspection_default
 inspect im MSN_DROP
```

Task 1.6 Verification

Verify the configured settings:

```
ASA4# show service-policy global inspect im


Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: im MSN_DROP, packet 0, lock fail 0, drop 0, reset-drop 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
        class MSN_DROP
          drop-connection, packet 0
```

Task 1.7 Solution

R1:

```
class-map type inspect match-any INSIDE_TO_OUTSIDE
 match protocol icmp
 match protocol tcp
 match protocol telnet
 match protocol udp
!
class-map type inspect match-any OUTSIDE_TO_INSIDE
 match protocol icmp
 match protocol telnet
```

https://t.me/learningnets

```
 match protocol udp
!
ip port-map smtp port tcp 125
!
class-map type inspect match-any SMTP_PROTOCOL
 match protocol smtp
!
parameter-map type regex SMTP_RECIPIENT_REGEX
 pattern "ccie@inelab\.local"
!
parameter-map type regex SMTP_SENDER_REGEX
 pattern "brutus@spam\.com"
!
class-map type inspect smtp match-all SMTP_APPLICATION
 match sender address regex SMTP_SENDER_REGEX
 match recipient address regex SMTP_RECIPIENT_REGEX
!
policy-map type inspect smtp SMTP_APPLICATION
 class type inspect smtp SMTP_APPLICATION
  reset
  log
!
policy-map type inspect INSIDE_TO_OUTSIDE
 class INSIDE_TO_OUTSIDE
  inspect
!
policy-map type inspect OUTSIDE_TO_INSIDE
 class OUTSIDE_TO_INSIDE
  inspect
 class SMTP_PROTOCOL
  inspect
  service-policy smtp SMTP_APPLICATION
!
zone security INSIDE
zone security OUTSIDE
!
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE_TO_OUTSIDE
!
zone-pair security OUTSIDE_TO_INSIDE source OUTSIDE destination INSIDE
 service-policy type inspect OUTSIDE_TO_INSIDE
!
interface GigabitEthernet0/1.12
 zone-member security INSIDE
!
interface Loopback0
```

https://t.me/learningnets

```
 zone-member security INSIDE
!
interface GigabitEthernet0/1.24
 zone-member security OUTSIDE

R2:

interface gigabitEthernet 0/1.12
 ip ospf cost 100
```

Task 1.7 Verification

Configure **TEST-PC-B** with IPv4 address from VLAN 12 (for example, 190.1.12.100) and default gateway of R1, to verify basic connectivity through the firewall:

```
R4#ping 190.1.12.100

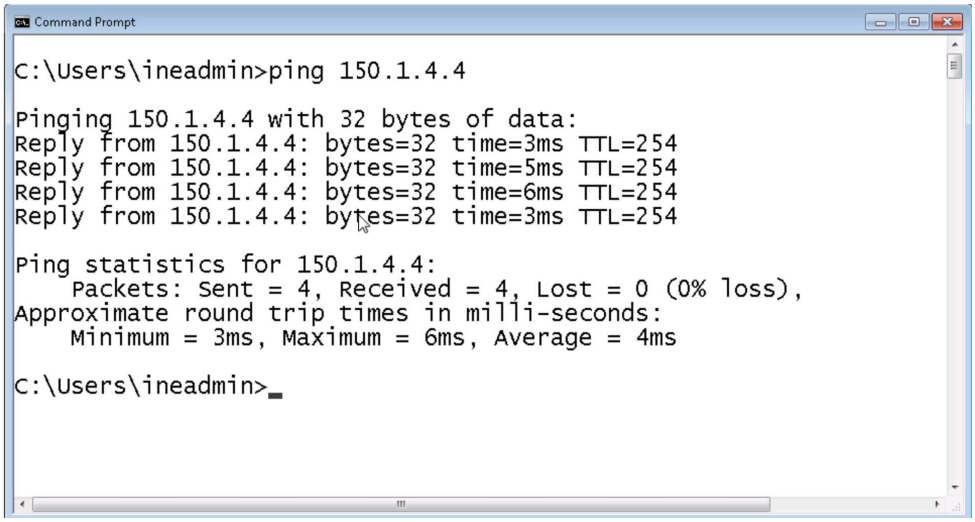
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.1.12.100, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
!
!R1#show policy-firewall session zone-pair OUTSIDE_TO_INSIDE

 Zone-pair: OUTSIDE_TO_INSIDE
  Service-policy inspect : OUTSIDE_TO_INSIDE
    Class-map : OUTSIDE_TO_INSIDE(match-any) Established Sessions =  1
 Session 2CEFC2A0 (190.1.24.4:8)=>(190.1.12.100:0) icmp SIS_OPEN
          Created 00:00:03, Last heard 00:00:03 ECHO request

          Bytes sent (initiator:responder) [360:360]
    Class-map : SMTP_PROTOCOL(match-any)
    Class-map : class-default(match-any)
```

Initiate traffic also from **INSIDE** to **OUTSIDE**:

https://t.me/learningnets




```
R1#show policy-firewall session zone-pair INSIDE_TO_OUTSIDE


 Zone-pair: INSIDE_TO_OUTSIDE
  Service-policy inspect : INSIDE_TO_OUTSIDE
    Class-map : INSIDE_TO_OUTSIDE(match-any) Established Sessions =  1
 Session 2CEFD420 (190.1.12.100:8)=>(150.1.4.4:0) icmp SIS_OPEN
          Created 00:00:04, Last heard 00:00:01 ECHO request


          Bytes sent (initiator:responder) [128:128]
    Class-map : class-default(match-any)
```

Verify correct interface zone allocation:

https://t.me/learningnets

```
R1#show policy-firewall config zone

Zone: self
  Description: System defined zone
Zone: INSIDE
Member Interfaces:
GigabitEthernet0/1.12
Loopback0

  Member of Zone-pairs:
    Zone INSIDE is source of Zone-pair INSIDE_TO_OUTSIDE
    Zone INSIDE is destination of Zone-pair OUTSIDE_TO_INSIDE
Zone: OUTSIDE
Member Interfaces:
GigabitEthernet0/1.24

  Member of Zone-pairs:
    Zone OUTSIDE is destination of Zone-pair INSIDE_TO_OUTSIDE
    Zone OUTSIDE is source of Zone-pair OUTSIDE_TO_INSIDE
```

Verify correct firewall configuration, in both directions:

```
R1#show policy-firewall config zone-pair INSIDE_TO_OUTSIDE

Zone-pair              : INSIDE_TO_OUTSIDE
Source Zone            : INSIDE
Destination Zone       : OUTSIDE
Service-policy inspect : INSIDE_TO_OUTSIDE Class-map : INSIDE_TO_OUTSIDE(match-any)
Match protocol icmp
Match protocol tcp
Match protocol telnet
Match protocol udp
Action : inspect
   Parameter-map : Default

  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default
!
!R1#show policy-firewall config zone-pair OUTSIDE_TO_INSIDE
Zone-pair              : OUTSIDE_TO_INSIDE
Source Zone            : OUTSIDE
Destination Zone       : INSIDE
```

https://t.me/learningnets

```
Service-policy inspect : OUTSIDE_TO_INSIDE Class-map : OUTSIDE_TO_INSIDE(match-any)
Match protocol icmp
Match protocol telnet
Match protocol udp
Action : inspect
   Parameter-map : Default
 Class-map : SMTP_PROTOCOL(match-any)
Match protocol smtp
Action : inspect
   Parameter-map : Default Service Policy: smtp SMTP_APPLICATION

  Class-map : class-default(match-any)
   Match any  Action : drop log

   Parameter-map : Default
```

Verify that SMTP is inspected on both TCP port 25 and 125:

```
R1#show ip port-map smtp

Default mapping:  smtp                tcp port 25                    system defined
Default mapping:  smtp                tcp port 125                   user defined
```

Task 1.8 Solution

```
R2:
class-map type inspect match-any INSIDE_TO_OUTSIDE
 match protocol icmp
 match protocol tcp
 match protocol telnet
 match protocol udp
!
class-map type inspect match-any OUTSIDE_TO_INSIDE
 match protocol icmp
 match protocol telnet
 match protocol udp
!
ip port-map smtp port tcp 125
!
class-map type inspect match-any SMTP_PROTOCOL
 match protocol smtp
!
parameter-map type regex SMTP_RECIPIENT_REGEX
```

https://t.me/learningnets

```
 pattern ccie@inelab.local
!
parameter-map type regex SMTP_SENDER_REGEX
 pattern brutus@spam.com
!
class-map type inspect smtp match-all SMTP_APPLICATION
 match sender address regex SMTP_SENDER_REGEX
 match recipient address regex SMTP_RECIPIENT_REGEX
!
policy-map type inspect smtp SMTP_APPLICATION
 class type inspect smtp SMTP_APPLICATION
  reset
  log
!
policy-map type inspect INSIDE_TO_OUTSIDE
 class INSIDE_TO_OUTSIDE
  inspect
!
policy-map type inspect OUTSIDE_TO_INSIDE
 class OUTSIDE_TO_INSIDE
  inspect
 class SMTP_PROTOCOL
  inspect
  service-policy smtp SMTP_APPLICATION
!
zone security INSIDE
zone security OUTSIDE
!
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE_TO_OUTSIDE
!
zone-pair security OUTSIDE_TO_INSIDE source OUTSIDE destination INSIDE
 service-policy type inspect OUTSIDE_TO_INSIDE
!
interface GigabitEthernet0/1.12
 zone-member security INSIDE
!
interface Loopback0
 zone-member security INSIDE
!
interface GigabitEthernet0/1.24
 zone-member security OUTSIDE
```

R1:

```
interface GigabitEthernet0/1
 ip address 190.1.200.1 255.255.255.0
```

https://t.me/learningnets

```
!
parameter-map type inspect global
 redundancy
 exit
!
redundancy
 application redundancy
  group 1
   name ZBPF_HA
   preempt
   priority 150
   control GigabitEthernet0/1 protocol 1
   data GigabitEthernet0/1
!
interface GigabitEthernet0/1.24
 redundancy rii 24
!
interface GigabitEthernet0/1.12
 redundancy rii 12
 redundancy group 1 ip 190.1.12.12 exclusive
```

R2:

```
interface GigabitEthernet0/1
 ip address 190.1.200.2 255.255.255.0
!
parameter-map type inspect global
 redundancy
 exit
!
redundancy
 application redundancy
  group 1
   name ZBPF_HA
   preempt
   priority 100
   control GigabitEthernet0/1 protocol 1
   data GigabitEthernet0/1
!
interface GigabitEthernet0/1.24
 redundancy rii 24
!
interface GigabitEthernet0/1.12
 redundancy rii 12
 redundancy group 1 ip 190.1.12.12 exclusive
```

SW2:

https://t.me/learningnets

```
interface range fastEthernet 1/0/1 - 2
 switchport trunk allowed vlan add 1
```

Task 1.8 Verification

Verify that requested output is being matched:

```
R2#show redundancy application if-mgr group 1
 RG ID: 1
 Interface       VIP         VMAC        Shut   Decrement
 ============================================================
 GigabitEthernet0/1.12 190.1.12.12 0007.b421.000c  shut    0

 WAN Interface
 Interface                    Decrement
 ========================================
!
!R2#show redundancy rii

 No. of RIIs in database: 2
 Interface                         RII Id     decrement
  GigabitEthernet0/1.12         :   12            0
  GigabitEthernet0/1.24         :   24            0
```

Verify the router states, active and standby:

```
R1#show redundancy application group 1
Group ID:1
Group Name:ZBPF_HA

Administrative State: No Shutdown
Aggregate operational state : Up My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: STANDBY HOT
!
!R2#show redundancy application group 1
Group ID:1
Group Name:ZBPF_HA
```

https://t.me/learningnets

```
Administrative State: No Shutdown
Aggregate operational state : Up My Role: STANDBY
Peer Role: ACTIVE

Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
         RF state: STANDBY HOT
         Peer RF state: ACTIVE
```

Verify the interface used for **control**, configured priority, and IPv4 addressing:

```
R1#show redundancy application protocol group 1

RG Protocol RG 1
------------------
        Role: Active
        Negotiation: Enabled Priority: 150
        Protocol state: Active
        Ctrl Intf(s) state: Up
        Active Peer: Local Standby Peer: address 190.1.200.2, priority 100, intf Gi0/1
        Log counters:
                role change to active: 1
                role change to standby: 0
                disable events: rg down state 0, rg shut 0
                ctrl intf events: up 1, down 0, admin_down 0
                reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default Control Interface: GigabitEthernet0/1

        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 392, Bytes 24304, HA Seq 0, Seq Number 392, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
```

https://t.me/learningnets

```
                Resign: TX 0, RX 1
        Standby Peer: Present. Hold Timer: 10000
                Pkts 312, Bytes 10608, HA Seq 0, Seq Number 373, Pkt Loss 0
```

Initiate a telnet session from **TEST-PC-B** to R4 and verify that session state is replicated from R1 (the active router) to R2 (the standby router):

```
R1#show policy-firewall session ha
 Session 2CEFECA0 (190.1.12.100:6198)=>(150.1.4.4:23) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:12, Last heard 00:00:09
          Bytes sent (initiator:responder) [45:82] HA State: ACTIVE, RG ID: 1
Established Sessions = 1
!
!R2#show policy-firewall session ha
 Session 2C8A4040 (190.1.12.100:6198)=>(150.1.4.4:23) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:23, Last heard never
          Bytes sent (initiator:responder) [0:0] HA State: STANDBY, RG ID: 1
Established Sessions = 1
```

Task 1.9 Solution

```
R1:
interface GigabitEthernet0/1.12
 ip nat inside
!
interface GigabitEthernet0/1.24
 ip nat outside
!
ip access-list extended NAT_ACL
 permit ip 190.1.12.0 0.0.0.255 any
!
ip nat pool NAT_POOL 190.1.88.1 190.1.88.254 prefix-length 24
!
ip nat inside source list NAT_ACL pool NAT_POOL overload

R2:
interface GigabitEthernet0/1.12
 ip nat inside
!
interface GigabitEthernet0/1.24
 ip nat outside
!
```

https://t.me/learningnets

```
ip access-list extended NAT_ACL
 permit ip 190.1.12.0 0.0.0.255 any
!
ip nat pool NAT_POOL 190.1.88.1 190.1.88.254 prefix-length 24
!
ip nat inside source list NAT_ACL pool NAT_POOL overload

ASA3:

arp permit-nonconnected
```

Task 1.9 Verification

Initiate traffic from **TEST-PC-B** and verify that it is functional; check the NAT and firewall tables:

```
R1#show policy-firewall session zone-pair INSIDE_TO_OUTSIDE

 Zone-pair: INSIDE_TO_OUTSIDE
  Service-policy inspect : INSIDE_TO_OUTSIDE
    Class-map : INSIDE_TO_OUTSIDE(match-any)
      Established Sessions =  1
        Session 2C6B9B00 (190.1.12.100:8)=>(150.1.4.4:0) icmp SIS_OPEN
          Created 00:00:03, Last heard 00:00:00
          ECHO request
          Bytes sent (initiator:responder) [128:128]
    Class-map : class-default(match-any)
!
!R1#show ip nat translations icmp

Pro Inside global      Inside local       Outside local      Outside global
icmp 190.1.88.1:1      190.1.12.100:1     150.1.4.4:1        150.1.4.4:1
```

Verify the NAT configuration and NAT pool, on R1 for example:

```
R1#show ip nat statistics

Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 6, occurred 00:05:22 agoOutside interfaces:
 GigabitEthernet0/1.24
Inside interfaces:
 GigabitEthernet0/1.12
Hits: 276  Misses: 0
CEF Translated packets: 230, CEF Punted packets: 74
```

https://t.me/learningnets

```
Expired translations: 12
Dynamic mappings:
-- Inside Source
[Id: 7] access-list NAT_ACL pool NAT_POOL refcount 0 pool NAT_POOL: netmask 255.255.255.0
 start 190.1.88.1 end 190.1.88.254

        type generic, total addresses 254, allocated 0 (0%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 3

CCIE SCv4 Lab 3 Solutions Section 2

1. Task 2.1 Solution
2. Task 2.2 Solution
3. Task 2.3 Solution
4. Task 2.4 Solution
5. Task 2.5 Solution
6. Task 2.6 Solution

Task 2.1 Solution

SW3:

```
interface GigabitEthernet1/0/10
 switchport mode access
 switchport access vlan 44
 no shutdown
```

IPS:

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# host-name IPS4240
sensor(config-hos-net)# host-ip 190.1.44.100/24,190.1.44.4
sensor(config-hos-net)# telnet-option disabled
sensor(config-hos-net)# access-list 190.1.12.0/24
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes?[yes]:
!
!
sensor(config)# service web-server
sensor(config-web)# port 4443
sensor(config-web)# exit
Apply Changes?[yes]:
!
```

https://t.me/learningnets

```
!
sensor(config)# service logger
sensor(config-log)# master-control
sensor(config-log-mas)# individual-zone-control true
sensor(config-log-mas)# exit
sensor(config-log)# zone-control sensorApp severity debug
sensor(config-log)# exit
Apply Changes?[yes]:
```

R1:

```
ip access-list extended NAT_ACL
 1 deny tcp 190.1.12.0 0.0.0.255 host 190.1.44.100 eq 4443
!
ip access-list resequence NAT_ACL 10 10
```

R2:

```
ip access-list extended NAT_ACL
 1 deny tcp 190.1.12.0 0.0.0.255 host 190.1.44.100 eq 4443
!
ip access-list resequence NAT_ACL 10 10
```

Task 2.1 Verification

Verify the configured host settings:

```
sensor(config-hos-net)# show settings

   network-settings
   ------------------------------------------------
host-ip: 190.1.44.100/24,190.1.44.4 default: 192.168.1.2/24,192.168.1.1
 host-name: IPS4240 default: sensor
telnet-option: disabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------ network-address: 190.1.12.0/24

         ------------------------------------------------
```

Verify that the default HTTPS port has been modified:

```
sensor(config-web)# show settings
  enable-tls: true <defaulted>
port: 4443 default: 443
```

https://t.me/learningnets

```
    server-id: HTTP/1.1 compliant <defaulted>
    configurable-service (min: 0, max: 99, current: 0)
    ------------------------------------------------
    ------------------------------------------------
```

Verify the debug logging configuration:

```
sensor(config-log)# show settings | begin master
    master-control
    ------------------------------------------------
       enable-debug: false <defaulted> individual-zone-control: true default: false
    ------------------------------------------------
    zone-control (min: 0, max: 999999999, current: 20)
    ------------------------------------------------
       <protected entry>
       zone-name: AD <defaulted>
       severity: warning <defaulted>
       <protected entry>
       zone-name: AuthenticationApp <defaulted>
       severity: warning <defaulted>
       <protected entry>
       zone-name: Cid <defaulted>
       severity: debug <defaulted>
       <protected entry>
       zone-name: Cli <defaulted>
       severity: warning <defaulted>
       <protected entry>
       zone-name: IdapiCtlTrans <defaulted>
       severity: warning <defaulted>
       <protected entry>
       zone-name: IdsEventStore <defaulted>
       severity: warning <defaulted>
       <protected entry>
       zone-name: Monitor <defaulted>
       severity: warning <defaulted>
       <protected entry>
       zone-name: MpInstaller <defaulted>
       severity: warning <defaulted>
       <protected entry>
       zone-name: cmgr <defaulted>
       severity: warning <defaulted>
       <protected entry>
       zone-name: cplane <defaulted>
       severity: warning <defaulted>
       <protected entry>
```

https://t.me/learningnets

```
      zone-name: csi <defaulted>
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransImpl <defaulted>
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource <defaulted>
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc <defaulted>
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac <defaulted>
      severity: warning <defaulted>
      <protected entry>
      zone-name: rep <defaulted>
      severity: warning <defaulted>
      <protected entry>
      zone-name: sched <defaulted>
      severity: warning <defaulted>
      <protected entry> zone-name: sensorApp
severity: debug default: warning

      <protected entry>
      zone-name: tls <defaulted>
      severity: warning <defaulted>
      <protected entry>
      zone-name: watchdog <defaulted>
      severity: warning <defaulted>
   ------------------------------------------------
```

Task 2.2 Solution

SW4:

```
interface GigabitEthernet1/0/9
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 47,74
 switchport mode trunk
 no shutdown
!
interface GigabitEthernet1/0/10
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 58,85
 switchport mode trunk
```

https://t.me/learningnets

```
 no shutdown
```

IPS:

```
sensor(config)# service interface
sensor(config-int)# physical-interfaces gigabitEthernet0/2
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# subinterface-type inline-vlan-pair
sensor(config-int-phy-inl)# subinterface 1
sensor(config-int-phy-inl-sub)# vlan1 47
sensor(config-int-phy-inl-sub)# vlan2 74
sensor(config-int-phy-inl-sub)# exit
sensor(config-int-phy-inl)# exit
sensor(config-int-phy)# exit
!
!
sensor(config-int)# physical-interfaces gigabitEthernet0/3
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# subinterface-type inline-vlan-pair
sensor(config-int-phy-inl)# subinterface 2
sensor(config-int-phy-inl-sub)# vlan1 58
sensor(config-int-phy-inl-sub)# vlan2 85
sensor(config-int-phy-inl-sub)# exit
sensor(config-int-phy-inl)# exit
sensor(config-int-phy)# exit
sensor(config-int)# exit
Apply Changes?[yes]:
!
!
sensor# copy signature-definition sig0 sig1
sensor(config)# service analysis-engine
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)# physical-interface gigabitEthernet0/2 subinterface-number 1
sensor(config-ana-vir)# exit
sensor(config-ana)# virtual-sensor vs1
sensor(config-ana-vir)# physical-interface gigabitEthernet0/3 subinterface-number 2
sensor(config-ana-vir)# signature-definition sig1
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
Apply Changes?[yes]:
```

Task 2.2 Verification

https://t.me/learningnets

Verify the physical and logical interface states:

```
sensor# show interfaces brief

CC   Interface            Sensing State   Link   Inline Mode        Pair Status
     GigabitEthernet0/0   Disabled        Down   Unpaired           N/A
*    Management0/0        Disabled        Up
     GigabitEthernet0/1   Disabled        Down   Unpaired           N/A
GigabitEthernet0/2   Enabled          Up     Inline-vlan-pair   N/A
          GigabitEthernet0/3   Enabled          Up     Inline-vlan-pair   N/A

!
!sensor(config-int-phy)# show settings

   <protected entry>
   name: GigabitEthernet0/2
   ------------------------------------------------
      media-type: tx <protected>
      description:  <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      default-vlan: 0 <defaulted>
      alt-tcp-reset-interface
      ------------------------------------------------
         none
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------ subinterface-type
      ------------------------------------------------ inline-vlan-pair
         ------------------------------------------------ subinterface (min: 1, max: 255, current: 1)
            ------------------------------------------------ subinterface-number: 1
               ------------------------------------------------
                  description:  <defaulted> vlan1: 47
vlan2: 74
               ------------------------------------------------
!
!sensor(config-int-phy)# show settings

   <protected entry>
   name: GigabitEthernet0/3
   ------------------------------------------------
      media-type: tx <protected>
      description:  <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
```

https://t.me/learningnets

```
      speed: auto <defaulted>
      default-vlan: 0 <defaulted>
      alt-tcp-reset-interface
      ------------------------------------------------
         none
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------ subinterface-type
      ------------------------------------------------ inline-vlan-pair
         ------------------------------------------------ subinterface (min: 1, max: 255, current: 1)
            ------------------------------------------------ subinterface-number: 2
               ------------------------------------------------
                  description:  <defaulted> vlan1: 58
vlan2: 85


               ------------------------------------------------
```

Verify that traffic flows between **ASA1** context and R4:

```
ASA12/ASA1# ping 190.1.47.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.1.47.4, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
!
!
sensor# packet display gigabitEthernet0/2
Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_2: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_2, link-type EN10MB (Ethernet), capture size 65535 bytes
00:07:02.979000 01:00:0c:cc:cc:cd (oui Unknown) > 70:81:05:39:fe:89 (oui Unknown) SNAP Unnumbered, ui, Flags [Comman
00:07:02.979000 01:00:0c:cc:cc:cd (oui Unknown) > 70:81:05:39:fe:89 (oui Unknown) SNAP Unnumbered, ui, Flags [Comman
00:07:04.323000
00:07:04.545000 IP 190.1.47.15 > 190.1.47.4: ICMP echo request, id 15263, seq 8510, length 80
00:07:04.546000 IP 190.1.47.15 > 190.1.47.4: ICMP echo request, id 15263, seq 8510, length 80
00:07:04.547000 IP 190.1.47.4 > 190.1.47.15: ICMP echo reply, id 15263, seq 8510, length 80
00:07:04.547000 IP 190.1.47.4 > 190.1.47.15: ICMP echo reply, id 15263, seq 8510, length 80

00:07:04.548000 IP 190.1.47.15 > 190.1.47.4: ICMP echo request, id 15263, seq 8510, length 80
00:07:04.548000 IP 190.1.47.15 > 190.1.47.4: ICMP echo request, id 15263, seq 8510, length 80
00:07:04.549000 IP 190.1.47.4 > 190.1.47.15: ICMP echo reply, id 15263, seq 8510, length 80
00:07:04.549000 IP 190.1.47.4 > 190.1.47.15: ICMP echo reply, id 15263, seq 8510, length 80
00:07:04.550000 IP 190.1.47.15 > 190.1.47.4: ICMP echo request, id 15263, seq 8510, length 80
00:07:04.550000 IP 190.1.47.15 > 190.1.47.4: ICMP echo request, id 15263, seq 8510, length 80
00:07:04.551000 IP 190.1.47.4 > 190.1.47.15: ICMP echo reply, id 15263, seq 8510, length 80
```

https://t.me/learningnets

```
00:07:04.552000 IP 190.1.47.4 > 190.1.47.15: ICMP echo reply, id 15263, seq 8510, length 80
00:07:04.552000 IP 190.1.47.15 > 190.1.47.4: ICMP echo request, id 15263, seq 8510, length 80
00:07:04.552000 IP 190.1.47.15 > 190.1.47.4: ICMP echo request, id 15263, seq 8510, length 80
00:07:04.553000 IP 190.1.47.4 > 190.1.47.15: ICMP echo reply, id 15263, seq 8510, length 80
00:07:04.554000 IP 190.1.47.4 > 190.1.47.15: ICMP echo reply, id 15263, seq 8510, length 80
00:07:04.554000 IP 190.1.47.15 > 190.1.47.4: ICMP echo request, id 15263, seq 8510, length 80
00:07:04.555000 IP 190.1.47.15 > 190.1.47.4: ICMP echo request, id 15263, seq 8510, length 80
00:07:04.555000 IP 190.1.47.4 > 190.1.47.15: ICMP echo reply, id 15263, seq 8510, length 80
00:07:04.556000 IP 190.1.47.4 > 190.1.47.15: ICMP echo reply, id 15263, seq 8510, length 80
29 packets captured
29 packets received by filter
0 packets dropped by kernel
```

Verify that traffic flows between **ASA2** context and R5:

```
ASA12/ASA2# ping 190.1.58.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.1.58.5, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
!
!sensor# packet display
gigabitEthernet0/0  gigabitEthernet0/1  gigabitEthernet0/2  gigabitEthernet0/3
sensor# packet display gigabitEthernet0/3
Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_3: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_3, link-type EN10MB (Ethernet), capture size 65535 bytes
00:09:01.538000 01:00:0c:cc:cc:cd (oui Unknown) > 70:81:05:39:fe:8a (oui Unknown) SNAP Unnumbered, ui, Flags [Comman
00:09:01.538000 01:00:0c:cc:cc:cd (oui Unknown) > 70:81:05:39:fe:8a (oui Unknown) SNAP Unnumbered, ui, Flags [Comman
00:09:02.450000 IP 190.1.58.15 > 190.1.58.5: ICMP echo request, id 59133, seq 1876, length 80
00:09:02.451000 IP 190.1.58.15 > 190.1.58.5: ICMP echo request, id 59133, seq 1876, length 80
00:09:02.452000 IP 190.1.58.5 > 190.1.58.15: ICMP echo reply, id 59133, seq 1876, length 80
00:09:02.453000 IP 190.1.58.5 > 190.1.58.15: ICMP echo reply, id 59133, seq 1876, length 80

00:09:02.453000 IP 190.1.58.15 > 190.1.58.5: ICMP echo request, id 59133, seq 1876, length 80
00:09:02.454000 IP 190.1.58.15 > 190.1.58.5: ICMP echo request, id 59133, seq 1876, length 80
00:09:02.456000 IP 190.1.58.5 > 190.1.58.15: ICMP echo reply, id 59133, seq 1876, length 80
00:09:02.457000 IP 190.1.58.5 > 190.1.58.15: ICMP echo reply, id 59133, seq 1876, length 80
00:09:02.457000 IP 190.1.58.15 > 190.1.58.5: ICMP echo request, id 59133, seq 1876, length 80
00:09:02.458000 IP 190.1.58.15 > 190.1.58.5: ICMP echo request, id 59133, seq 1876, length 80
00:09:02.459000 IP 190.1.58.5 > 190.1.58.15: ICMP echo reply, id 59133, seq 1876, length 80
00:09:02.460000 IP 190.1.58.5 > 190.1.58.15: ICMP echo reply, id 59133, seq 1876, length 80
00:09:02.460000 IP 190.1.58.15 > 190.1.58.5: ICMP echo request, id 59133, seq 1876, length 80
00:09:02.461000 IP 190.1.58.15 > 190.1.58.5: ICMP echo request, id 59133, seq 1876, length 80
00:09:02.462000 IP 190.1.58.5 > 190.1.58.15: ICMP echo reply, id 59133, seq 1876, length 80
```

https://t.me/learningnets

```
00:09:02.462000 IP 190.1.58.5 > 190.1.58.15: ICMP echo reply, id 59133, seq 1876, length 80
00:09:02.462000 IP 190.1.58.15 > 190.1.58.5: ICMP echo request, id 59133, seq 1876, length 80
00:09:02.463000 IP 190.1.58.15 > 190.1.58.5: ICMP echo request, id 59133, seq 1876, length 80
00:09:02.464000 IP 190.1.58.5 > 190.1.58.15: ICMP echo reply, id 59133, seq 1876, length 80
00:09:02.464000 IP 190.1.58.5 > 190.1.58.15: ICMP echo reply, id 59133, seq 1876, length 80
00:09:03.170000 IP 190.1.58.5 > 224.0.0.5: OSPFv2, Hello, length: 56
29 packets captured
29 packets received by filter
0 packets dropped by kernel
```

Task 2.3 Solution

IPS:

```
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 60005 0
sensor(config-sig-sig)# engine service-http
sensor(config-sig-sig-ser)# event-action deny-attacker-inline
sensor(config-sig-sig-ser)# service-ports 80,8080
sensor(config-sig-sig-ser)# regex
sensor(config-sig-sig-ser-reg)# specify-uri-regex yes
sensor(config-sig-sig-ser-reg-yes)# uri-regex [Cc][Mm][Dd]\.[Ee][Xx][Ee]
sensor(config-sig-sig-ser-reg-yes)# exit
sensor(config-sig-sig-ser-reg)# exit
sensor(config-sig-sig-ser)# exit
sensor(config-sig-sig)# alert-severity medium
sensor(config-sig-sig)# sig-fidelity-rating 50
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-all
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes?[yes]:
```

Task 2.3 Verification

Verify the signature settings:

```
sensor(config-sig-sig)# show settings | b alert
 alert-severity: medium default: medium
```

https://t.me/learningnets

```
sig-fidelity-rating: 50 default: 75

      promisc-delta: 0 <defaulted>
      sig-description
      -----------------------------------------------
         sig-name: My Sig <defaulted>
         sig-string-info: My Sig Info <defaulted>
         sig-comment: Sig Comment <defaulted>
         alert-traits: 0 <defaulted>
         release: custom <defaulted>
         sig-creation-date: 20000101 <defaulted>
         sig-type: Other <defaulted>
      ------------------------------------------------ engine
      ------------------------------------------------ service-http
         ------------------------------------------------
event-action: deny-attacker-inline default: produce-alert
            de-obfuscate: true default: true
            max-field-sizes
            ------------------------------------------------
!
!sensor(config-sig-sig)# show settings | b regex
            regex
            ------------------------------------------------ specify-uri-regex
               ------------------------------------------------ yes
                  ------------------------------------------------ uri-regex: [Cc][Mm][Dd]\.[Ee][Xx][Ee]
                  ------------------------------------------------
!
!sensor(config-sig-sig)# show settings | b alert-frequency
      alert-frequency
      ------------------------------------------------ summary-mode
         ------------------------------------------------ fire-all
            ------------------------------------------------
               specify-summary-threshold
               ------------------------------------------------
                  no
                  ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------
               summary-key: Axxx <defaulted>
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------ status
      ------------------------------------------------ enabled: true <defaulted>
retired: false <defaulted>

         obsoletes (min: 0, max: 65535, current: 0)
```

https://t.me/learningnets

```
---------------------------------------------
```

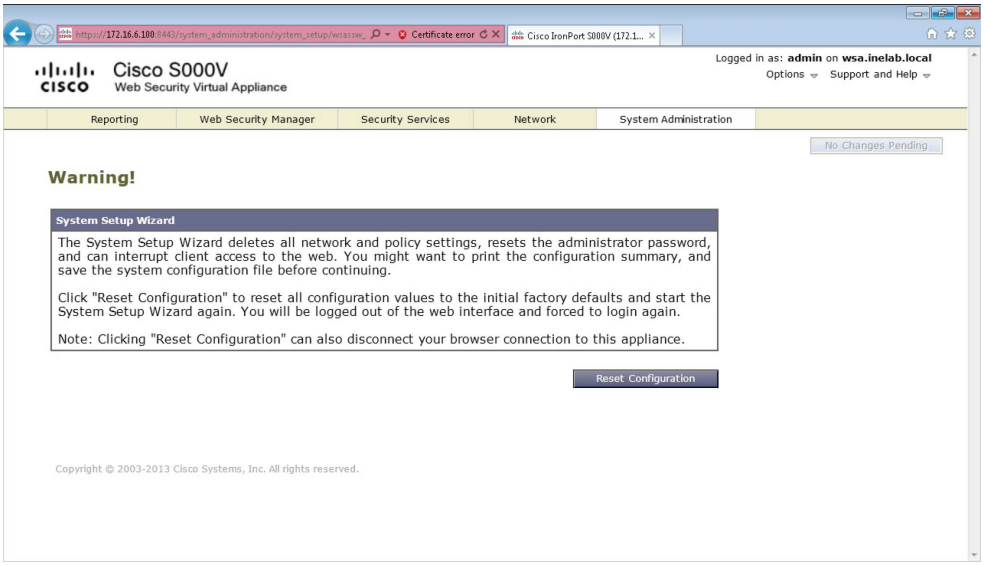
Task 2.4 Solution

```
SW6:
interface FastEthernet1/0/10
 switchport mode access
 switchport access vlan 99
 no shutdown

ASA3:

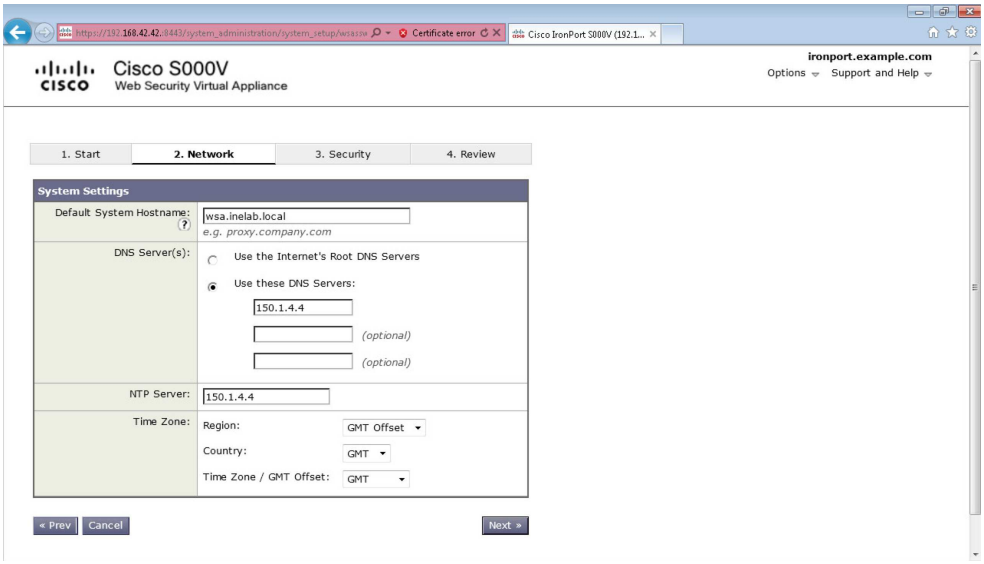
access-list VLAN56_IN permit tcp 190.1.88.0 255.255.255.0 host 172.16.6.100 eq 8443
```

Using Internet Explorer from **TEST-PC-B**, navigate to **https://172.16.6.100:8443** authenticate and browse to **System Administration -> System Setup Wizard**; click **Reset Configuration**:

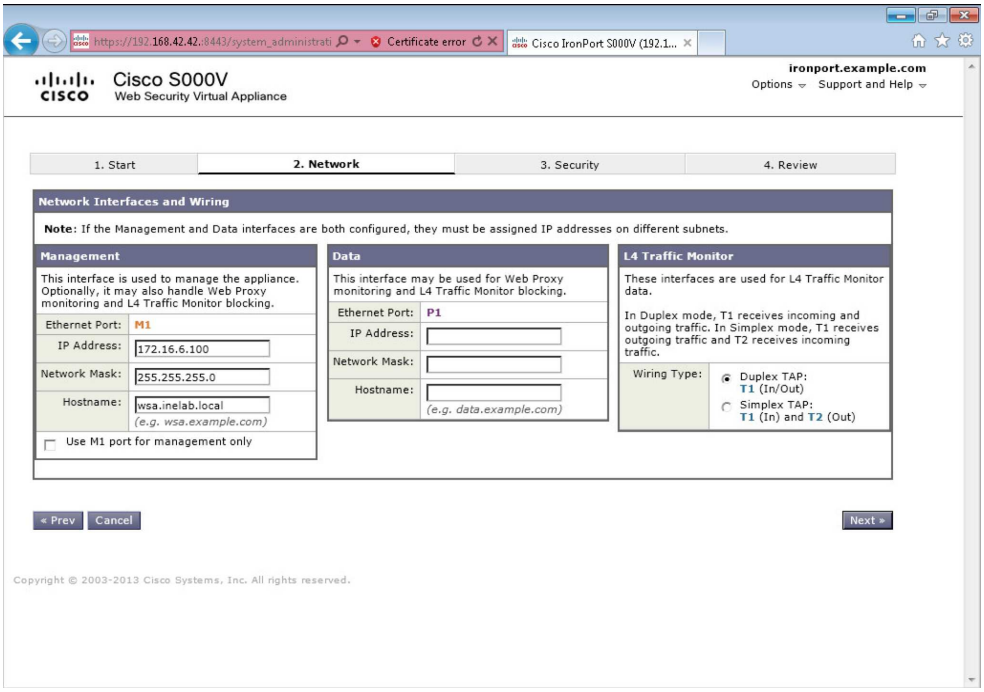


Configure **TEST-PC-B** with IPv4 address from subnet 192.168.42.0/24 , allocate its switchport in the same VLAN as WSA, and using Internet Explorer navigate to **https://192.168.42.42:8443**. Authenticate with the default credentials of **admin/ironport** and browse to **System Administration -> System Setup Wizard**. Configure hostname, DNS, and NTP server:

https://t.me/learningnets

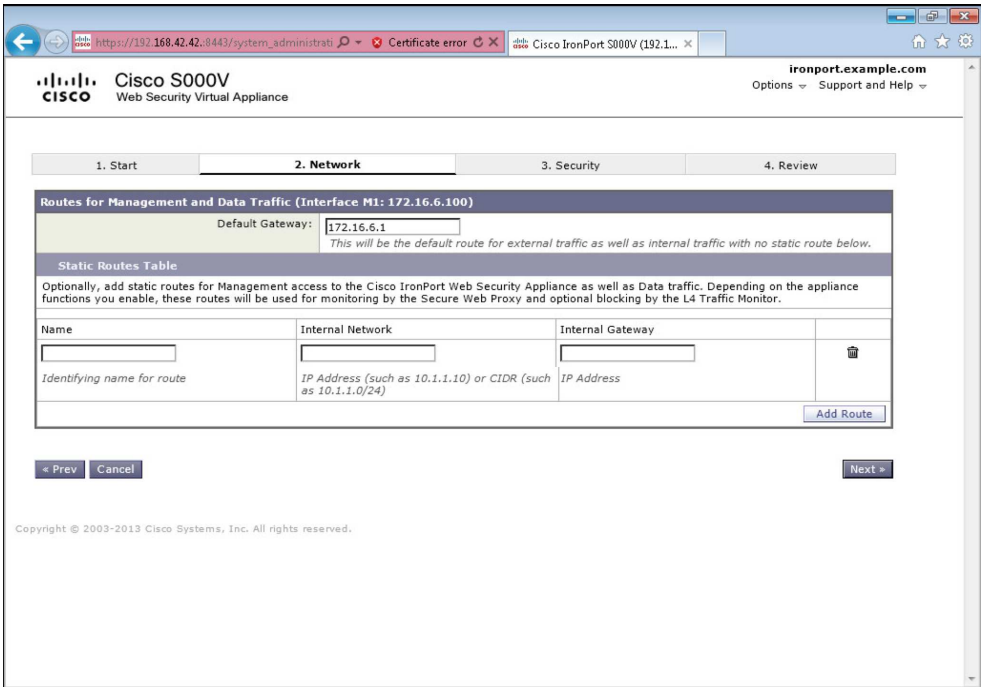


Configure the M1 interface for both proxy and management:

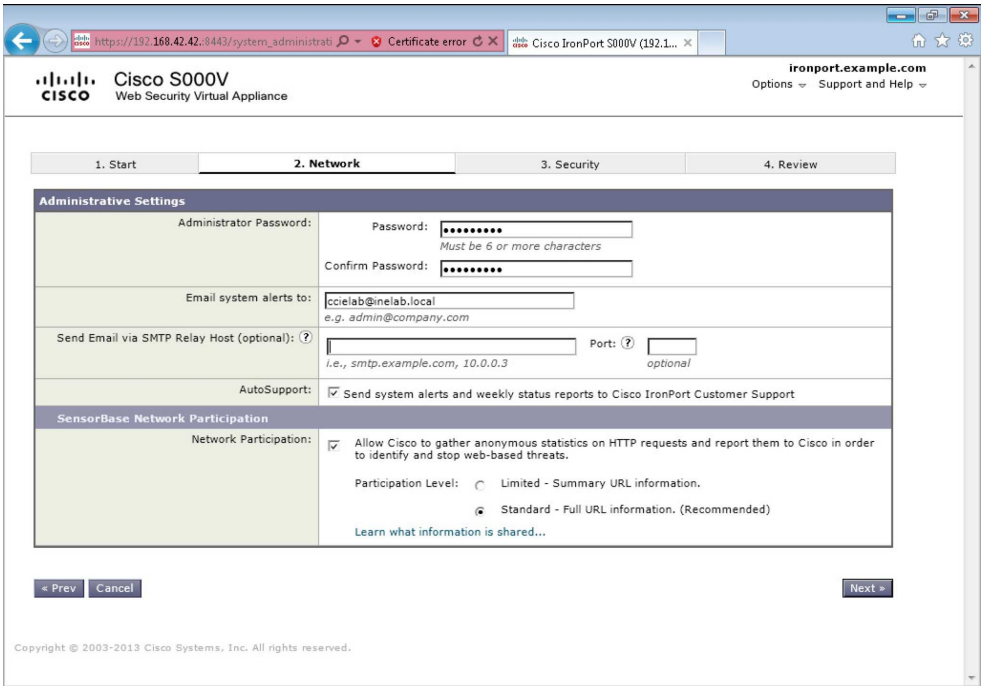


Configure the default gateway for M1 port:

https://t.me/learningnets



Configure the administrator password and email address:



All other settings are left at their default values, so screens are missing from the complete **System Setup Wizard**.

Task 2.4 Verification

Use Internet Explorer to manage the WSA. When the sessions is successful, check the connection table on ASA3 and the NAT table on R1:

https://t.me/learningnets

```
ASA3# show conn protocol tcp address 172.16.6.100

24 in use, 33 most used
TCP VLAN56 190.1.88.1:6583 VLAN65 172.16.6.100:8443, idle 0:00:00, bytes 1355, flags UfIOB
TCP VLAN56 190.1.88.1:6582 VLAN65 172.16.6.100:8443, idle 0:00:00, bytes 1355, flags UfIOB
TCP VLAN56 190.1.88.1:6581 VLAN65 172.16.6.100:8443, idle 0:00:00, bytes 1355, flags UfrIOB
TCP VLAN24 190.1.88.1:6583 VLAN42 172.16.6.100:8443, idle 0:00:00, bytes 1355, flags UfIOB
TCP VLAN24 190.1.88.1:6582 VLAN42 172.16.6.100:8443, idle 0:00:00, bytes 1355, flags UfIOB
TCP VLAN24 190.1.88.1:6581 VLAN42 172.16.6.100:8443, idle 0:00:00, bytes 1355, flags UfFrIOB
!
!R1#show ip nat translations tcp global
Pro Inside global      Inside local       Outside local      Outside global
tcp 190.1.88.1:6586    190.1.12.100:6586  172.16.6.100:8443  172.16.6.100:8443

tcp 190.1.88.1:6587    190.1.12.100:6587  172.16.6.100:8443  172.16.6.100:8443
```

Task 2.5 Solution

R1:

```
ip access-list extended REDIRECTED_TRAFFIC
 permit tcp 190.1.12.0 0.0.0.255 any eq 80
!
ip access-list standard WSA_GROUP
 permit host 172.16.6.100
!
ip wccp version 2
ip wccp 93 redirect-list REDIRECTED_TRAFFIC group-list WSA_GROUP
!
interface GigabitEthernet0/1.24
 ip wccp 93 redirect out
```

R2:

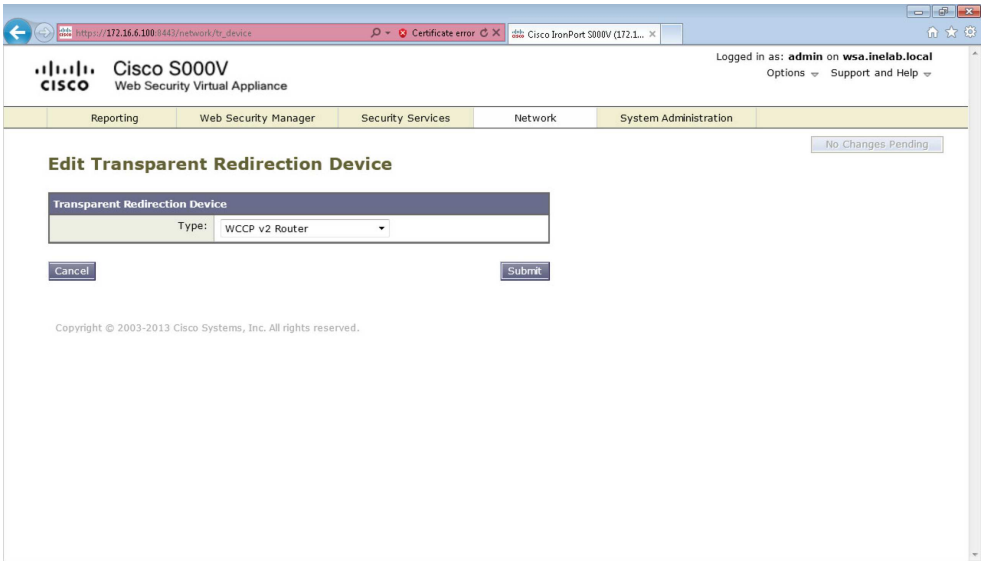
```
ip access-list extended REDIRECTED_TRAFFIC
 permit tcp 190.1.12.0 0.0.0.255 any eq 80
!
ip access-list standard WSA_GROUP
 permit host 172.16.6.100
!
ip wccp version 2
ip wccp 93 redirect-list REDIRECTED_TRAFFIC group-list WSA_GROUP
!
interface GigabitEthernet0/1.24
 ip wccp 93 redirect out
```

https://t.me/learningnets

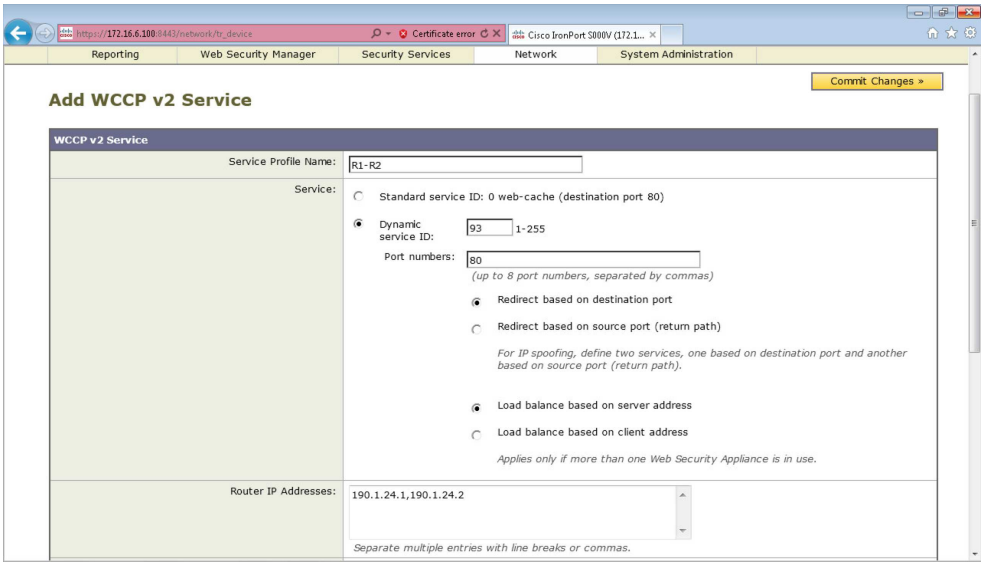
ASA3:

```
access-list VLAN56_IN permit gre host 150.1.1.1 host 172.16.6.100
access-list VLAN56_IN permit gre host 150.1.2.2 host 172.16.6.100
```

Browse to **Network -> Transparent Redirection** and select **WCCP v2 Router**:

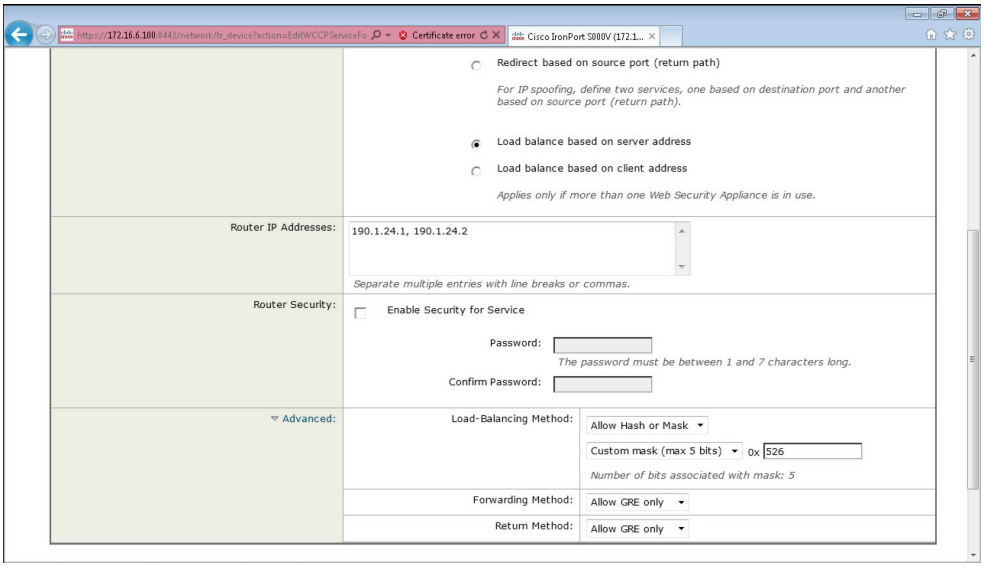


Click **Add Service**, configure the same service-id as on the routers, and enable it only for HTTP traffic:



Enable the service for GRE; otherwise WSA will try L2, fail, and not negotiate GRE:

https://t.me/learningnets



Task 2.5 Verification

Verify that UDP WCCP communication has been established between R1, R2, and WSA:

```
ASA3# show conn address 172.16.6.100

22 in use, 34 most used
UDP VLAN24 190.1.24.1:2048 VLAN42 172.16.6.100:2048, idle 0:00:01, bytes 17260, flags -
UDP VLAN24 190.1.24.2:2048 VLAN42 172.16.6.100:2048, idle 0:00:01, bytes 17260, flags -
UDP VLAN56 190.1.24.1:2048 VLAN65 172.16.6.100:2048, idle 0:00:01, bytes 17260, flags -
UDP VLAN56 190.1.24.2:2048 VLAN65 172.16.6.100:2048, idle 0:00:01, bytes 17260, flags -
```

Messages similar to the following should be logged on both R1 and R2, confirming that the GRE tunnel is established:

```
%WCCP-5-SERVICEFOUND: Service 93 acquired on WCCP client 172.16.6.100
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
```

Verify the tunnel encapsulation:

```
R1#show interfaces tunnel0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of Loopback0 (150.1.1.1)
  MTU 17912 bytes, BW 10000 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
```

https://t.me/learningnets

```
  Keepalive not set
  Tunnel source 150.1.1.1 Tunnel protocol/transport multi-GRE/IP

    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1472 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
```

Verify the WCCP service state:

```
R1#show ip wccp 93 clients

WCCP Client information: WCCP Client ID:          172.16.6.100
        Protocol Version:        2.00 State:                   Usable
 Redirection:             GRE
 Packet Return:           GRE
        Assignment:              MASK
        Connect Time:            00:04:37
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Mask Allotment:          32 of 32 (100.00%)
!
!R1#show ip wccp 93

Global WCCP information:
    Router information: Router Identifier:                   150.1.1.1
 Service Identifier: 93
        Protocol Version:                   2.00
        Number of Service Group Clients:    1
        Number of Service Group Routers:    2
        Total Packets Redirected:           0
          Process:                          0
          CEF:                              0
        Service mode:                       Open
        Service Access-list:                -none-
        Total Packets Dropped Closed:       0 Redirect access-list:               REDIRECTED_TRAFFIC
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           0 Group access-list:                  WSA_GROUP
```

https://t.me/learningnets

```
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total GRE Bypassed Packets Received: 0
          Process:                           0
          CEF:                               0 GRE tunnel interface:                Tunnel0
```

Task 2.6 Solution

R1:

```
ip access-list extended HTTP_OUTSIDE_TO_INSIDE
 permit tcp any eq 80 190.1.12.0 0.0.0.255
!
class-map type inspect match-any HTTP_OUTSIDE_TO_INSIDE
 match access-group name HTTP_OUTSIDE_TO_INSIDE
!
policy-map type inspect OUTSIDE_TO_INSIDE
 class HTTP_OUTSIDE_TO_INSIDE
  pass
```

R2:

```
ip access-list extended HTTP_OUTSIDE_TO_INSIDE
 permit tcp any eq 80 190.1.12.0 0.0.0.255
!
class-map type inspect match-any HTTP_OUTSIDE_TO_INSIDE
 match access-group name HTTP_OUTSIDE_TO_INSIDE
!
policy-map type inspect OUTSIDE_TO_INSIDE
 class HTTP_OUTSIDE_TO_INSIDE
  pass
```

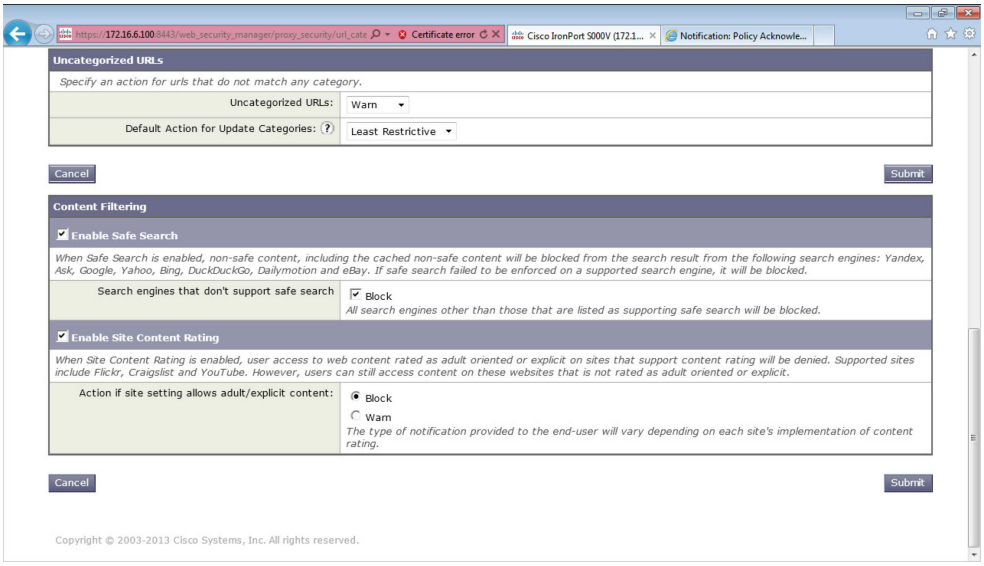
ASA3:

```
access-list WCCP_RETURN permit tcp any eq 80 190.1.12.0 255.255.255.0
!
class-map WCCP_RETURN
 match access-list WCCP_RETURN
!
policy-map global_policy
 class WCCP_RETURN
  set connection advanced-options tcp-state-bypass
```

Using Internet Explorer from **TEST-PC-B**, access the WSA and browse to **Web Security Manager -> Access Policies**

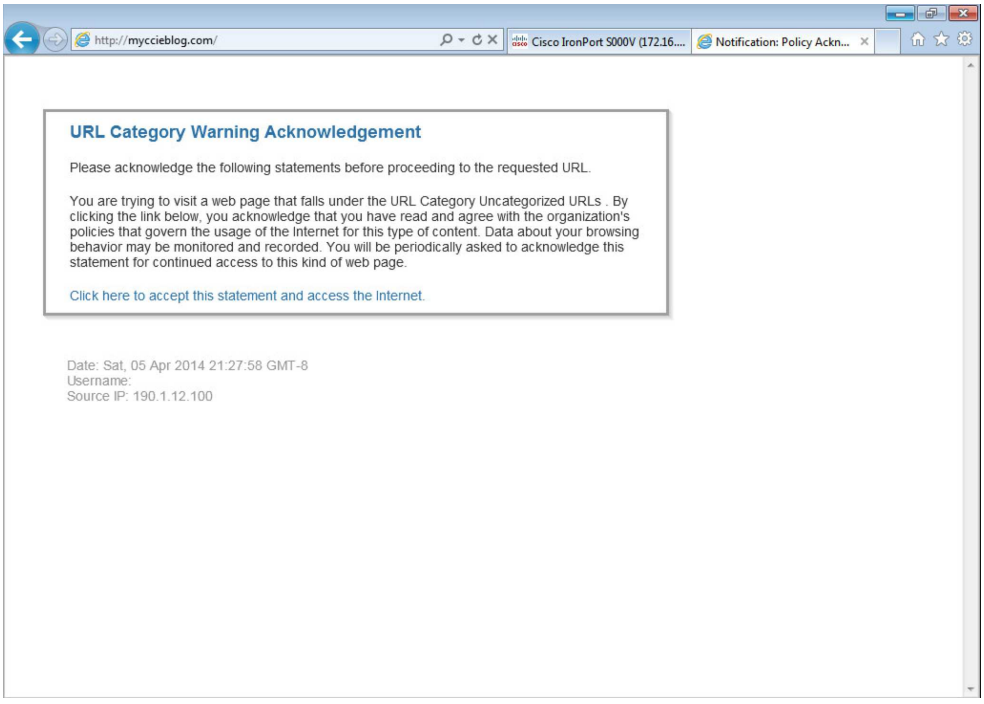
https://t.me/learningnets

; edit the URL Filtering settings for the default Global Policy. Set the action for uncategorized URLs to **warn**, and set the action for content filtering to **block**:



Task 2.6 Verification

From **TEST-PC-B**, use Internet Explorer to access **www.myccieblog.com** and verify that the EUN page is presented; accept the statement to be redirected to R4's HTTP server.



Verify the access logs on the WSA; note that initially access is denied because of EUN message being displayed. After a message is acknowledged, access is allowed:

https://t.me/learningnets

```
1396705491.488 17
190.1.12.100 TCP_DENIED/403 0 GET http://myccieblog.com/ - DIRECT/myccieblog.com text/plain BLOCK_CONTINUE_WEBCAT_12
-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup <nc,ns,0,"-",0,0,0,1,"-",-,-,-,"-",-,-,"-","-",-,-,nc,nc,"Unk
1396705495.693 23
190.1.12.100 TCP_MISS/401 253 GET http://myccieblog.com/ - DIRECT/myccieblog.com text/plain MONITOR_CONTINUE_WEBCAT_
-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup <nc,ns,0,"-",0,0,0,1,"-",-,-,-,"-",0,262686,"-","-",-,-,nc,nc
```

Verify the HTTP logs on R4, and note that the session was initiated by the WSA that spoofed the client IP:

```
R4#show ip http server history


HTTP server history:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes  end-time
150.1.4.4:80        172.16.6.100:44711 477         192         13:56:55 04/05

      150.1.4.4:80       172.16.6.100:60233 510         192         13:57:00 04/05
      150.1.4.4:80       172.16.6.100:9294  353         137         13:59:23 04/05
```

Verify the session state on ASA3, and note that the **b** flag is present because TCP state-bypass was configured:

```
ASA3# show conn protocol tcp address 172.16.6.100 detail

68 in use, 72 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service moduleTCP VLAN24:190.1.12.100/8268 VLAN42:172.16.6.100/80,
 flags b, idle 5m31s, uptime 5m31s, timeout 1h0m, bytes 1998

TCP VLAN56:190.1.12.100/8268 VLAN65:172.16.6.100/80,
    flags b, idle 5m31s, uptime 5m31s, timeout 1h0m, bytes 1998
```

https://t.me/learningnets

Because of the **pass** action, there is no information in R1's state table; verify that packets matched the configured class-map:

```
R1#show policy-firewall stats zone-pair OUTSIDE_TO_INSIDE | section HTTP


    Class-map: HTTP_OUTSIDE_TO_INSIDE (match-any)
      Match: access-group name HTTP_OUTSIDE_TO_INSIDE 107 packets, 12882 bytes
        30 second rate 0 bps Pass
 107 packets, 12882 bytes
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 3

CCIE SCv4 Lab 3 Solutions Section 3

1. Task 3.1 Solution
2. Task 3.2 Solution
3. Task 3.3 Solution
4. Task 3.4 Solution
5. Task 3.5 Solution

Task 3.1 Solution

```
R1:
crypto ikev2 profile R1_R2_PROFILE
 identity local fqdn R1.inelab.local
 keyring local R1_R2_KEYRING
!
interface Tunnel12
 tunnel mode ipsec ipv6

R2:

crypto ikev2 profile R1_R2_PROFILE
 identity local fqdn R2.inelab.local
 keyring local R1_R2_KEYRING
!
interface Tunnel12
 tunnel mode ipsec ipv6
```

Task 3.1 Verification

Verify that the requested output is matched:

```
R1#ping vrf SVTI 2001::2 source loopback12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::2, timeout is 2 seconds:
```

https://t.me/learningnets

```
Packet sent with a source address of 2001::1%SVTI
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Verify the IKEv2 SA tunnel state:

```
R2#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status 1              none/none                READY

Local  2001:24:24::2/500
Remote  2001:24:24::1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/76 sec
```

Verify the IPsec SA tunnel state and that packets flow bidirectionally through the tunnel:

```
R2#show crypto ipsec sa peer 2001:24:24::1

interface: Tunnel12
    Crypto map tag: Tunnel12-head-0, local addr 2001:24:24::2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer 2001:24:24::1 port 500
     PERMIT, flags={origin_is_acl,} #pkts encaps: 50, #pkts encrypt: 50, #pkts digest: 50
 #pkts decaps: 56, #pkts decrypt: 56, #pkts verify: 56
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 2001:24:24::2,
     remote crypto endpt.: 2001:24:24::1
     path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet0/1.24
     current outbound spi: 0x9D7924D4(2641962196)
     PFS (Y/N): N, DH group: none
 inbound esp sas:
```

https://t.me/learningnets

```
      spi: 0x44A94C84(1151945860)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2015, flow_id: Onboard VPN:15, sibling_flags 80000041, crypto map: Tunnel12-head-0
        sa timing: remaining key lifetime (k/sec): (4362046/3475)
        IV size: 16 bytes
        replay detection support: Y Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:
 outbound esp sas:
      spi: 0x9D7924D4(2641962196)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2016, flow_id: Onboard VPN:16, sibling_flags 80000041, crypto map: Tunnel12-head-0
        sa timing: remaining key lifetime (k/sec): (4362047/3475)
        IV size: 16 bytes
        replay detection support: Y Status: ACTIVE(ACTIVE)


     outbound ah sas:

     outbound pcp sas:
```

Task 3.2 Solution

R3:

```
crypto ipsec nat-transparency udp-encapsulation
```

R7:

```
crypto ipsec nat-transparency udp-encapsulation
!
crypto map VPN 100 ipsec-isakmp
 no set peer 190.1.58.33
 set peer 190.1.58.3
```

SW6:

```
ip access-list extended 100
 no 10
```

ASA1 ASA2 Context:

```
access-list OUTSIDE_IN permit udp host 150.1.7.7 host 190.1.58.3 eq 500
access-list OUTSIDE_IN permit udp host 150.1.7.7 host 190.1.58.3 eq 4500
```

https://t.me/learningnets

```
!
access-group OUTSIDE_IN in interface OUTSIDE
!
static (INSIDE,OUTSIDE) 190.1.58.3 150.1.3.3 netmask 255.255.255.255
!
route OUTSIDE 150.1.7.7 255.255.255.255 190.1.58.5
route INSIDE 150.1.3.3 255.255.255.255 190.1.38.3 1

ASA3:
access-list VLAN56_IN permit udp host 190.1.58.3 host 150.1.7.7 eq 500
access-list VLAN56_IN permit udp host 190.1.58.3 host 150.1.7.7 eq 4500

ASA4:

access-list OUTSIDE_IN permit udp host 190.1.58.3 host 150.1.7.7 eq 500
access-list OUTSIDE_IN permit udp host 190.1.58.3 host 150.1.7.7 eq 4500
!
access-group OUTSIDE_IN in interface OUTSIDE
```

Task 3.2 Verification

Verify that the requested output is matched:

https://t.me/learningnets

```
R3#ping 172.16.5.1 source fastEthernet0/0.33


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.5.1, timeout is 2 seconds:
Packet sent with a source address of 190.1.33.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
!
!
R7#show crypto ipsec sa

interface: FastEthernet0/0.27
    Crypto map tag: VPN, local addr 150.1.7.7

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.5.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (190.1.33.0/255.255.255.0/0/0)
   current_peer 190.1.58.3 port 4500
```

Verify the IPsec tunnel state and that packets are bidirectionally flowing through the tunnel:

```
R7#show crypto ipsec sa

interface: FastEthernet0/0.27
    Crypto map tag: VPN, local addr 150.1.7.7

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.5.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (190.1.33.0/255.255.255.0/0/0)
   current_peer 190.1.58.3 port 4500
     PERMIT, flags={origin_is_acl,} #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 150.1.7.7, remote crypto endpt.: 190.1.58.3
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0.27
     current outbound spi: 0xB58A4603(3045737987)
     PFS (Y/N): N, DH group: none
```

https://t.me/learningnets

```
 inbound esp sas:
      spi: 0xA7FDA9BA(2818419130)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        conn id: 2019, flow_id: NETGX:19, sibling_flags 80000046, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4462128/3496)
        IV size: 8 bytes
        replay detection support: Y Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:
 outbound esp sas:
      spi: 0xB58A4603(3045737987)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        conn id: 2020, flow_id: NETGX:20, sibling_flags 80000046, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4462128/3496)
        IV size: 8 bytes
        replay detection support: Y Status: ACTIVE


     outbound ah sas:

     outbound pcp sas:
```

Task 3.3 Solution

ASA4:

```
crypto ikev1 enable OUTSIDE
crypto ikev1 policy 100
 authentication pre-share
 encryption 3des
 hash md5
 group 2
!
access-list SPLIT_TUNNEL standard permit 172.16.3.0 255.255.255.0
!
username ezvpnuser password cisco
!
group-policy EZVPN_POLICY internal
group-policy EZVPN_POLICY attributes
 ipsec-udp enable
 ipsec-udp-port 9500
```

https://t.me/learningnets

```
 dhcp-network-scope 190.1.50.18
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT_TUNNEL
!
tunnel-group EZVPN_TUNNEL type remote-access
tunnel-group EZVPN_TUNNEL general-attributes
 authentication-server-group LOCAL
 default-group-policy EZVPN_POLICY
 dhcp-server 190.1.26.10
!
tunnel-group EZVPN_TUNNEL ipsec-attributes
 ikev1 pre-shared-key cisco
!
crypto ipsec ikev1 transform-set 3DES_MD5 esp-3des esp-md5-hmac
crypto dynamic-map DYNAMIC 100 set ikev1 transform-set 3DES_MD5
crypto dynamic-map DYNAMIC 100 set reverse-route
crypto map VPN 100 ipsec-isakmp dynamic DYNAMIC
crypto map VPN interface OUTSIDE
!
router eigrp 300
 redistribute static metric 100000 100 255 1 1500
```

R1:

```
ip access-list extended NAT_ACL
 1 deny udp 190.1.12.0 0.0.0.255 host 190.1.96.18 eq 500
 2 deny udp 190.1.12.0 0.0.0.255 host 190.1.96.18 eq 9500
!
ip access-list resequence NAT_ACL 10 10
```

R2:

```
ip access-list extended NAT_ACL
 1 deny udp 190.1.12.0 0.0.0.255 host 190.1.96.18 eq 500
 2 deny udp 190.1.12.0 0.0.0.255 host 190.1.96.18 eq 9500
!
ip access-list resequence NAT_ACL 10 10
```

ASA3:

```
access-list VLAN56_IN permit udp 190.1.12.0 255.255.255.0 host 190.1.96.18 eq 500
access-list VLAN56_IN permit udp 190.1.12.0 255.255.255.0 host 190.1.96.18 eq 9500
```

SW2:

```
ip dhcp excluded-address 190.1.50.18 190.1.50.18
ip dhcp pool EZVPN_TUNNEL
 network 190.1.50.0 /24
!
```

https://t.me/learningnets

```
ip route 190.1.50.18 255.255.255.255 190.1.26.18
```

Task 3.3 Verification

Configure the VPN Client on **TEST-PC-B**, initiate the connection, and authenticate using the username/password **ezvpnuser/cisco**. When the connection is established, verify that the requested output is matched:

```
ASA4# show vpn-sessiondb detail ra-ikev1-ipsec


Session Type: IKEv1 IPsec Detailed

Username     : ezvpnuser              Index        : 55
Assigned IP  : 190.1.50.15            Public IP    : 190.1.12.100
Protocol     : IKEv1 IPsecOverUDP
License      : Other VPN
Encryption   : 3DES                   Hashing      : MD5
Bytes Tx     : 0                      Bytes Rx     : 0
Pkts Tx      : 0                      Pkts Rx      : 0
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : EZVPN_POLICY           Tunnel Group : EZVPN_TUNNEL
Login Time   : 23:05:04 UTC Sat Apr 5 2014
Duration     : 0h:00m:30s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv1 Tunnels: 1
IPsecOverUDP Tunnels: 1

IKEv1:
  Tunnel ID    : 55.1
  UDP Src Port : 54245                  UDP Dst Port : 500
  IKE Neg Mode : Aggressive             Auth Mode    : preSharedKeys
  Encryption   : 3DES                   Hashing      : MD5
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86374 Seconds
  D/H Group    : 2
  Filter Name  :
  Client OS    : WinNT                  Client OS Ver: 5.0.07.0410

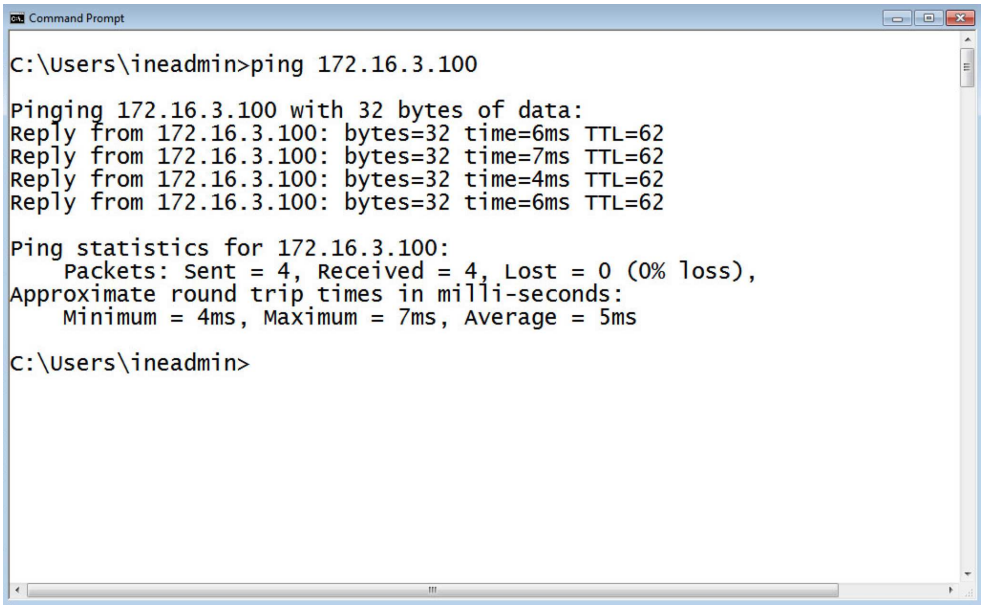
IPsecOverUDP:
  Tunnel ID    : 55.2
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
```

https://t.me/learningnets

```
  Remote Addr  : 190.1.50.15/255.255.255.255/0/0
  Encryption   : 3DES                    Hashing      : MD5
  Encapsulation: Tunnel                  UDP Dst Port : 9500
  Rekey Int (T): 28800 Seconds           Rekey Left(T): 28773 Seconds
  Idle Time Out: 30 Minutes              Idle TO Left : 29 Minutes
  Bytes Tx     : 0                       Bytes Rx     : 0
  Pkts Tx      : 0                       Pkts Rx      : 0

NAC:
  Reval Int (T): 0 Seconds               Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds               EoU Age(T)   : 27 Seconds
  Hold Left (T): 0 Seconds               Posture Token:
  Redirect URL :
```

Send traffic through the tunnel, and verify that it is functional:



Verify the IPsec tunnel counters:

```
ASA4#  show crypto ipsec sa peer 190.1.12.100
peer address: 190.1.12.100
    Crypto map tag: DYNAMIC, seq num: 100, local addr: 190.1.96.18

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (190.1.50.15/255.255.255.255/0/0)
      current_peer: 190.1.12.100, username: ezvpnuser
      dynamic allocated peer ip: 190.1.50.15
 #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
```

https://t.me/learningnets

```
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 190.1.96.18/9500, remote crypto endpt.: 190.1.12.100/9500
      path mtu 1500, ipsec overhead 66, media mtu 1500
      current outbound spi: 3C92DEE3
      current inbound spi : 3B04FC1C

    inbound esp sas:
      spi: 0x3B04FC1C (990182428)
         transform: esp-3des esp-md5-hmac no compression
         in use settings ={RA, Tunnel,  UDP-Encaps, }
         slot: 0, conn_id: 225280, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28575
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x3C92DEE3 (1016258275)
         transform: esp-3des esp-md5-hmac no compression
         in use settings ={RA, Tunnel,  UDP-Encaps, }
         slot: 0, conn_id: 225280, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28575
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Verify that both control-plane and data-plane sessions are inspected by the ZBPF:

```
R1#show policy-firewall session zone-pair INSIDE_TO_OUTSIDE
 Zone-pair: INSIDE_TO_OUTSIDE
  Service-policy inspect : INSIDE_TO_OUTSIDE
    Class-map : INSIDE_TO_OUTSIDE(match-any) Established Sessions =  2
 Session 31BDB160 (190.1.12.100:54245)=>(190.1.96.18:500) udp SIS_OPEN
          Created 00:06:07, Last heard 00:00:06
          Bytes sent (initiator:responder) [5288:3880]
          HA State: ACTIVE, RG ID: 1
Session 31BDC660 (190.1.12.100:9500)=>(190.1.96.18:9500) udp SIS_OPEN

          Created 00:00:06, Last heard 00:00:03
          Bytes sent (initiator:responder) [368:368]
          HA State: ACTIVE, RG ID: 1
```

https://t.me/learningnets

```
    Class-map : class-default(match-any)
```

Verify the assigned IPv4 addresses by the DDHCP server on SW2:

```
SW2#show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
190.1.50.15         0063.6973.636f.2d61.    Mar 04 1993 08:35 AM    Automatic
                    3439.332e.3463.6161.
                    2e66.3738.372d.5465.
                    7374.2d50.432d.4231.
                    392d.494e.5349.4445.
                    00
```

Task 3.4 Solution

```
ASA4:
ntp server 190.1.58.3
crypto key generate rsa general-keys modulus 1024 noconfirm
!
crypto ca trustpoint VPN
 enrollment url http://190.1.58.3
!
crypto ca authenticate VPN
crypto ca enroll VPN
!
crypto ikev1 policy 200
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 5
!
tunnel-group CCIELAB type ipsec-l2l
!
crypto ipsec ikev1 transform-set AES256_SHA esp-aes-256 esp-sha-hmac
!
access-list LOSW2_LOR5 permit ip host 150.1.10.10 host 150.1.5.5
!
crypto map VPN 50 match address LOSW2_LOR5
crypto map VPN 50 set peer 190.1.56.5
```

https://t.me/learningnets

```
crypto map VPN 50 set ikev1 transform-set AES256_SHA
crypto map VPN 50 set trustpoint VPN
```

R5:

```
ntp server 190.1.58.3
!
crypto pki trustpoint VPN
 subject-name CN=R5.inelab.local,OU=CCIELAB
 enrollment url http://190.1.58.3
!
crypto pki authenticate VPN
crypto pki enroll VPN
!
crypto isakmp policy 200
 encryption aes 256
 authentication rsa-sig
 hash sha
 group 5
!
crypto ipsec transform-set AES256_SHA esp-aes 256 esp-sha-hmac
crypto isakmp identity dn
!
ip access-list extended LOR5_LOSW2
 permit ip host 150.1.5.5 host 150.1.10.10
!
crypto map VPN 50 ipsec-isakmp
 match address LOR5_LOSW2
 set transform AES256_SHA
 set peer 190.1.96.18
!
interface FastEthernet0/0.56
 crypto map VPN
```

ASA1 ASA2 Context:

```
access-list OUTSIDE_IN permit tcp host 190.1.96.18 host 190.1.58.3 eq 80
access-list OUTSIDE_IN permit tcp host 190.1.58.5 host 190.1.58.3 eq 80
access-list OUTSIDE_IN permit udp host 190.1.96.18 host 190.1.58.3 eq 123
access-list OUTSIDE_IN permit udp host 190.1.58.5 host 190.1.58.3 eq 123
!
route OUTSIDE 190.1.96.18 255.255.255.255 190.1.58.5
```

ASA3:

```
policy-map global_policy
 class inspection_default
```

https://t.me/learningnets

```
  inspect ipsec-pass-thru
```

Task 3.4 Verification

Verify that both R5 and ASA4 have synchronized time with R3:

```
ASA4# show ntp status

Clock is synchronized, stratum 9, reference is 190.1.58.3
nominal freq is 99.9984 Hz, actual freq is 99.9967 Hz, precision is 2**6
reference time is d6eb0ca1.c93aeed4 (23:13:37.786 UTC Sat Apr 5 2014)
clock offset is 18.6232 msec, root delay is 3.57 msec
root dispersion is 34.87 msec, peer dispersion is 15.81 msec
!
!R5#show ntp status

Clock is synchronized, stratum 9, reference is 190.1.58.3
nominal freq is 250.0000 Hz, actual freq is 249.9998 Hz, precision is 2**24
reference time is D6EB0B8C.1471DE2B (23:09:00.079 UTC Sat Apr 5 2014)
clock offset is 18.5253 msec, root delay is 3.47 msec
root dispersion is 26.85 msec, peer dispersion is 3.21 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000576 s/s
system poll interval is 64, last update was 340 sec ago.
```

Initiate traffic from SW2 to trigger the IKE negotiation:

```
SW2#ping 150.1.5.5 source loopback0


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.5.5, timeout is 2 seconds:
Packet sent with a source address of 150.1.10.10 .!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/9/25 ms
```

Verify that the requested output is matched, and note that traffic flows bidirectionally through the tunnel:

```
ASA4# show vpn-sessiondb detail l2l


Session Type: LAN-to-LAN Detailed
```

https://t.me/learningnets

```
Connection    : CCIELAB

Index         : 56                    IP Addr      : 190.1.56.5
Protocol      : IKEv1 IPsec
Encryption    : AES256                Hashing      : SHA1
Bytes Tx      : 400                   Bytes Rx     : 400
Login Time    : 23:16:01 UTC Sat Apr 5 2014
Duration      : 0h:00m:43s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 56.1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Main                  Auth Mode    : rsaCertificate
  Encryption   : AES256                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 86356 Seconds
  D/H Group    : 5
  Filter Name  :
  IPv6 Filter  :
IPsec:
  Tunnel ID    : 56.2
  Local Addr   : 150.1.10.10/255.255.255.255/0/0
  Remote Addr  : 150.1.5.5/255.255.255.255/0/0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 3600 Seconds          Rekey Left(T): 3556 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
  Bytes Tx     : 400                   Bytes Rx     : 400
Pkts Tx       : 4                     Pkts Rx      : 4


NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 45 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

Task 3.5 Solution

R3:

```
ip access-list extended R3_TO_R7_FILTER
 permit udp 190.1.33.0 0.0.0.255 host 172.16.5.100 eq 5246
```

https://t.me/learningnets

```
 permit udp 190.1.33.0 0.0.0.255 host 172.16.5.100 eq 5247

R7:
ip access-list extended R7_TO_R3_FILTER
 permit udp host 172.16.5.100 eq 5246 190.1.33.0 0.0.0.255
 permit udp host 172.16.5.100 eq 5247 190.1.33.0 0.0.0.255

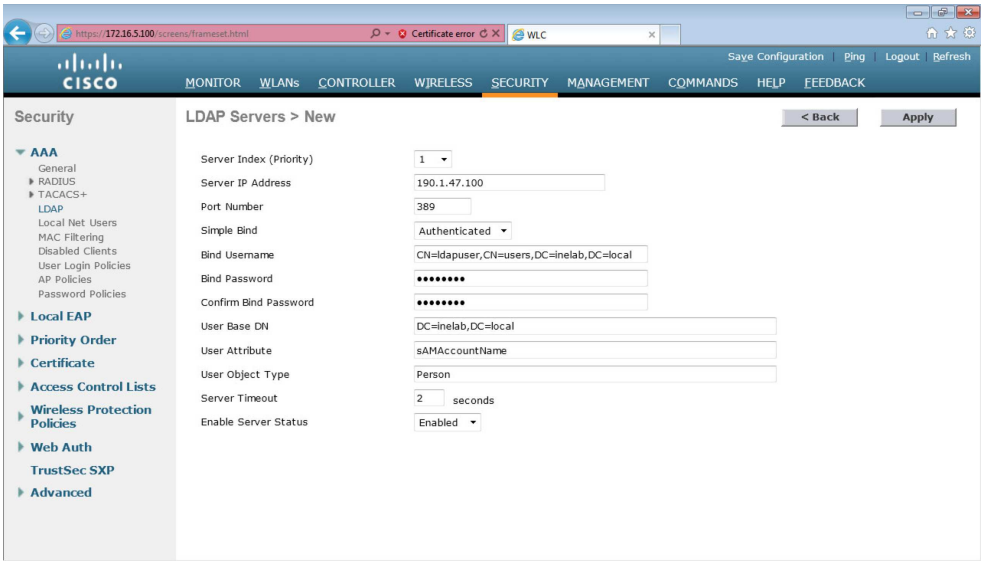
ASA1:
static (INSIDE,OUTSIDE) 190.1.47.100 172.16.10.100 netmask 255.255.255.255
route OUTSIDE 172.16.5.100 255.255.255.255 190.1.47.4
!
access-list OUTSIDE_IN permit tcp host 172.16.5.100 host 190.1.47.100 eq 389

ASA3:
access-list VLAN56_IN extended permit tcp 190.1.88.0 255.255.255.0 host 172.16.5.100 eq 443

ASA4:

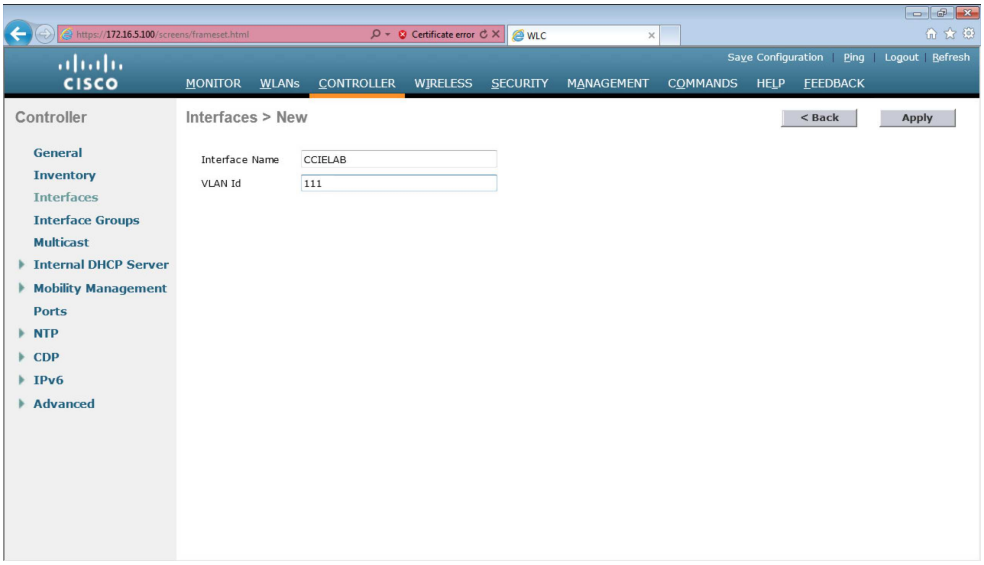
access-list OUTSIDE_IN extended permit tcp 190.1.88.0 255.255.255.0 host 172.16.5.100 eq 443
```

From **TEST-PC-B**, use Internet Explorer to navigate through WLC GUI; go to **Security -> AAA -> LDAP**, click **New**, and configure the LDAP parameters:

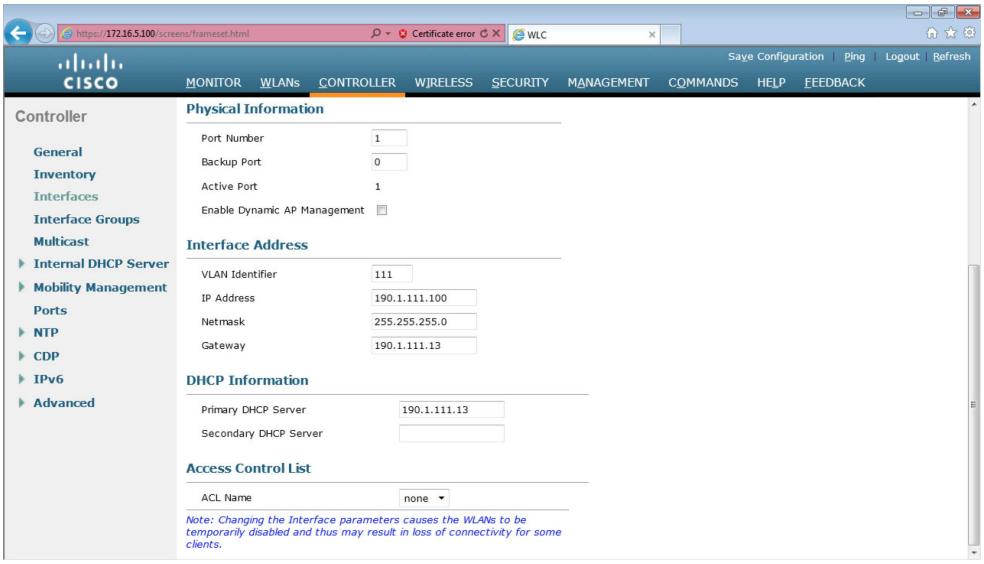


Navigate to **Controller -> Interfaces** and click **New** to add the dynamic interface:

https://t.me/learningnets

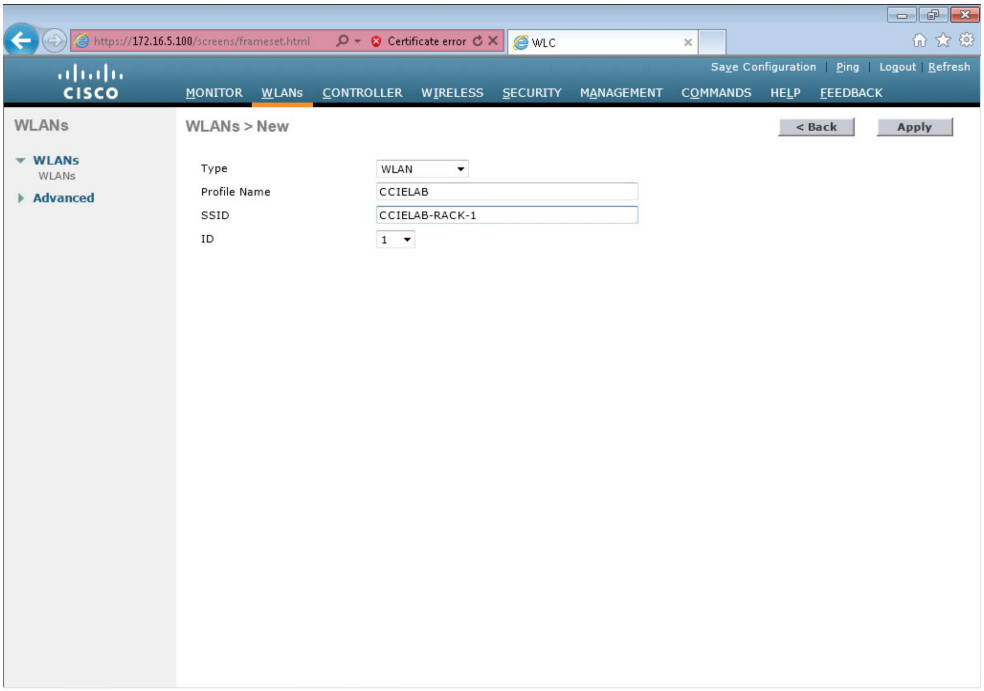


Configure the parameters for the dynamic interface:

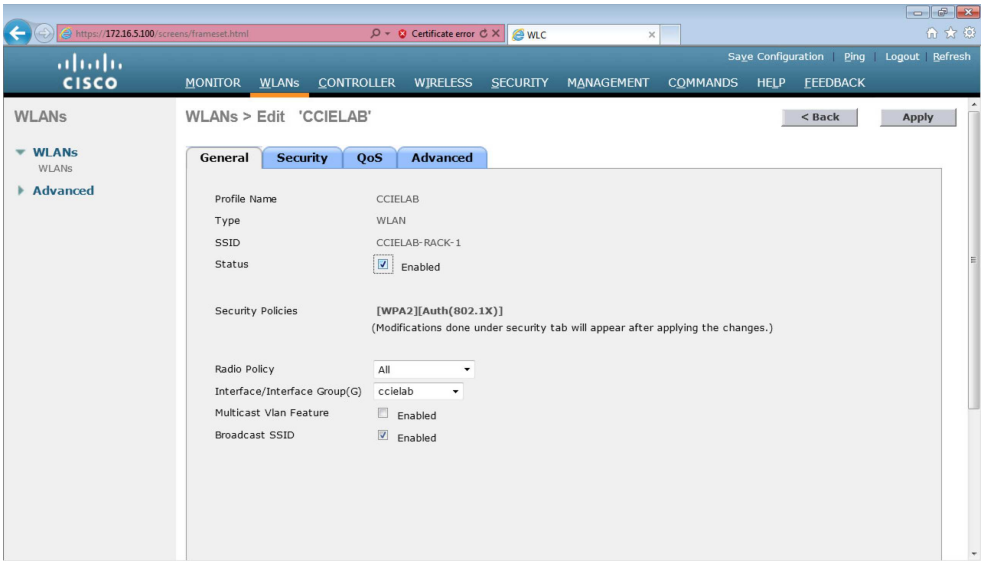


Navigate to the **WLANs** tab, select **Create New**, and click **Go**:

https://t.me/learningnets

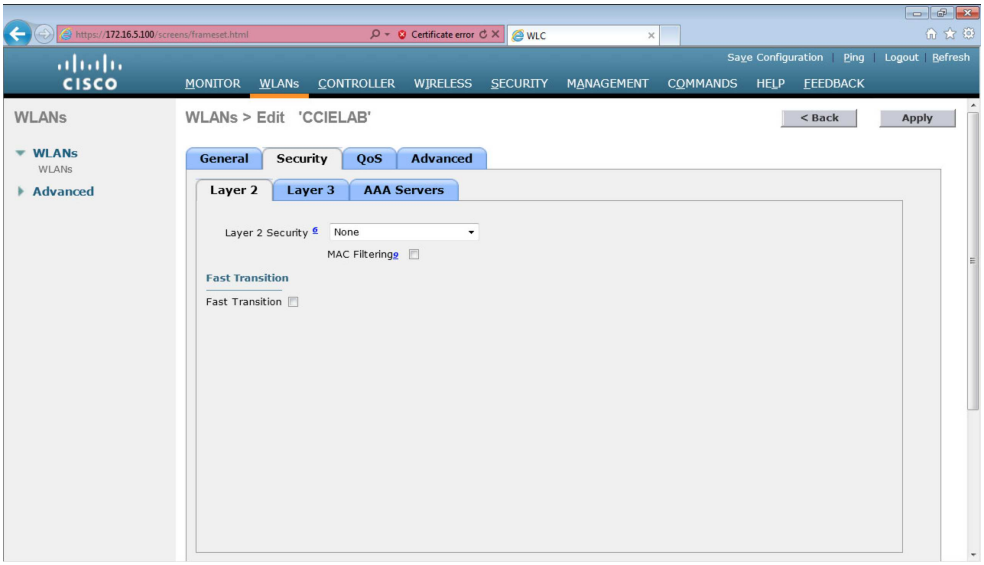


In the **General** section, enable the SSID and assign the created dynamic interface:

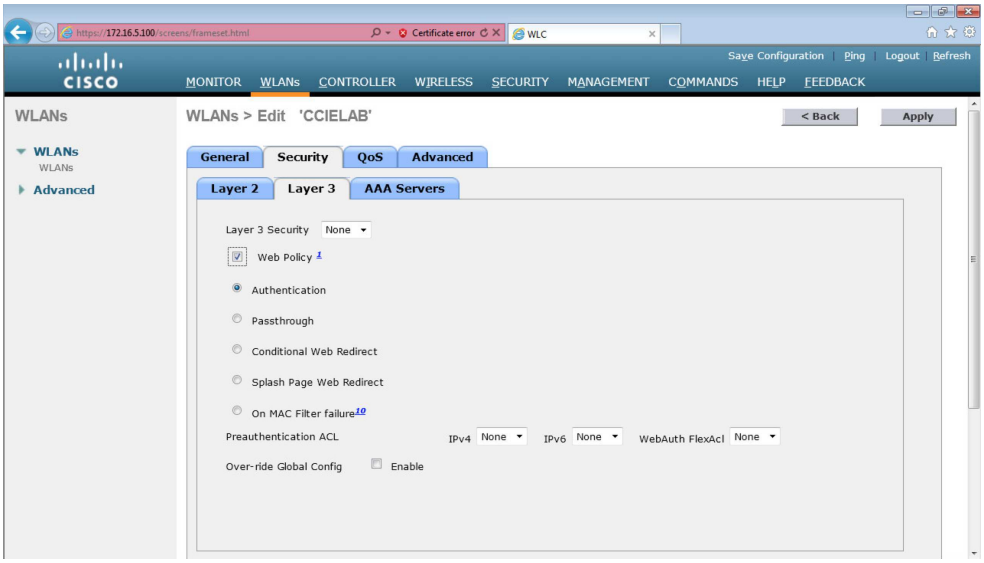


In **Security -> Layer2**, select **none**:

https://t.me/learningnets



In **Security -> Layer3**, enable **Web Policy** and leave the default method of **Authentication**:



Task 3.5 Verification

Verify that the LAP joined the WLC:

https://t.me/learningnets

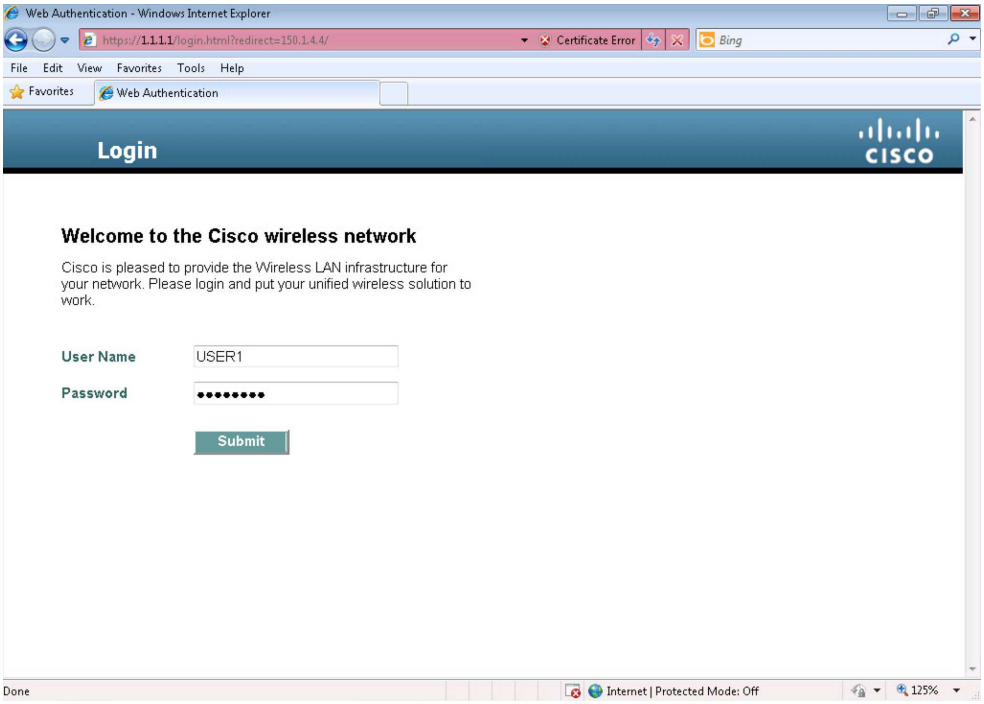
```
(Cisco Controller) >show ap summary


Number of APs.................................... 1

Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model              Ethernet MAC       Location          Port  Country  Priority
------------------  -----  --------------------  -----------------  ----------------  ----  -------  --------
RACK1-AP            2      AIR-LAP1262N-A-K9     00:06:f6:3b:9a:da  default location  1     US       1
```

From **WiFi-PC**, associate to the configured SSID and open Internet Explorer, navigate to any HTTP URL (for example, **http://150.1.4.4**); WLC should present the portal for authentication:



The client should be authenticated successfully; verify its status on WLC:

https://t.me/learningnets

```
(Cisco Controller) >show client summary


Number of Clients.............................. 1

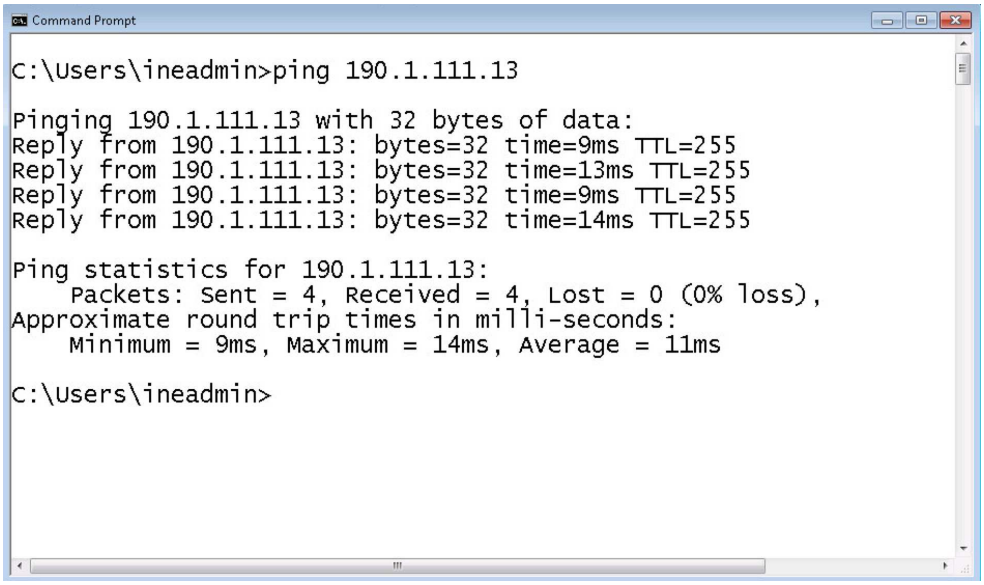
MAC Address       AP Name           Status        WLAN/RLAN      Auth Protocol         Port Wired
----------------- ----------------- ------------- -------------- ---- ---------------- ---- -----
ac:f1:df:13:bd:8f RACK2-AP          Associated    1              Yes  802.11n(2.4 GHz) 1    N/A
```

Verify that the client received IPv4 address from SW5:

```
SW5#show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
190.1.111.1         01ac.f1df.13bd.8f       Mar 04 1993 10:00 AM    Automatic
```

Verify that the client has IP connectivity with its default gateway:



https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 3

CCIE SCv4 Lab 3 Solutions Section 4

1. Task 4.1 Solution
2. Task 4.2 Solution
3. Task 4.3 Solution
4. Task 4.4 Solution

Task 4.1 Solution

```
ASA1 ASA2 Context:
aaa-server ACS_RADIUS protocol radius
aaa-server ACS_RADIUS (OUTSIDE) host 172.16.1.100
 key ciscoasa
!
access-list AUTH_RADIUS deny tcp host 190.1.96.18 host 190.1.58.3 eq 80
access-list AUTH_RADIUS deny tcp host 190.1.58.5 host 190.1.58.3 eq 80
access-list AUTH_RADIUS permit tcp any any eq 80
!
aaa authentication match AUTH_RADIUS OUTSIDE ACS_RADIUS
!
access-list OUTSIDE_IN permit tcp any any eq 80
access-group OUTSIDE_IN in interface OUTSIDE per-user-override
!
route OUTSIDE 172.16.1.100 255.255.255.255 190.1.58.5
route OUTSIDE 172.16.6.100 255.255.255.255 190.1.58.5

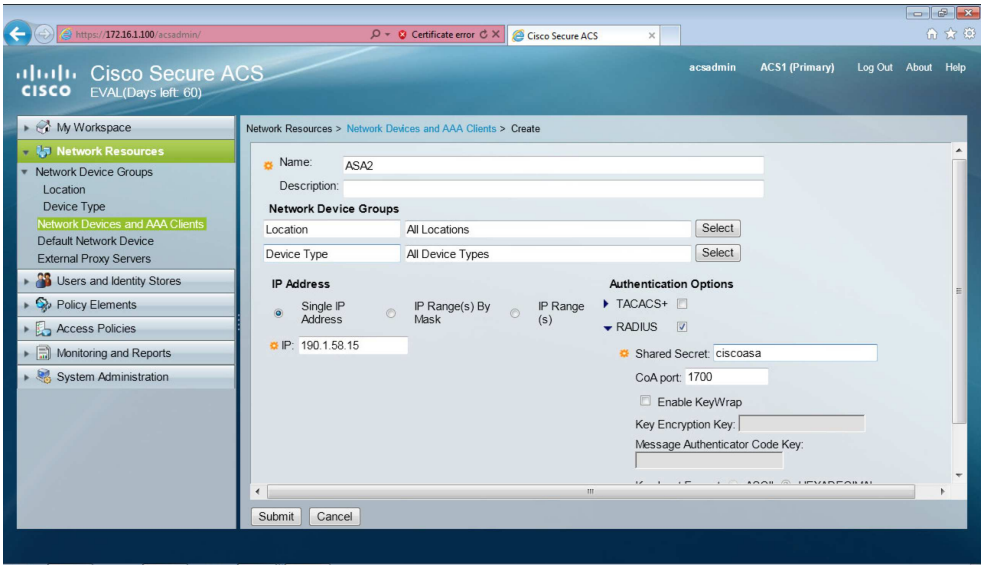
ASA3:

access-list VLAN56_IN permit udp host 190.1.58.15 host 172.16.1.100 eq 1645
access-list VLAN56_IN permit udp host 190.1.58.15 host 172.16.1.100 eq 1812
access-list VLAN56_IN permit tcp 190.1.88.0 255.255.255.0 host 172.16.1.100 eq 443
```

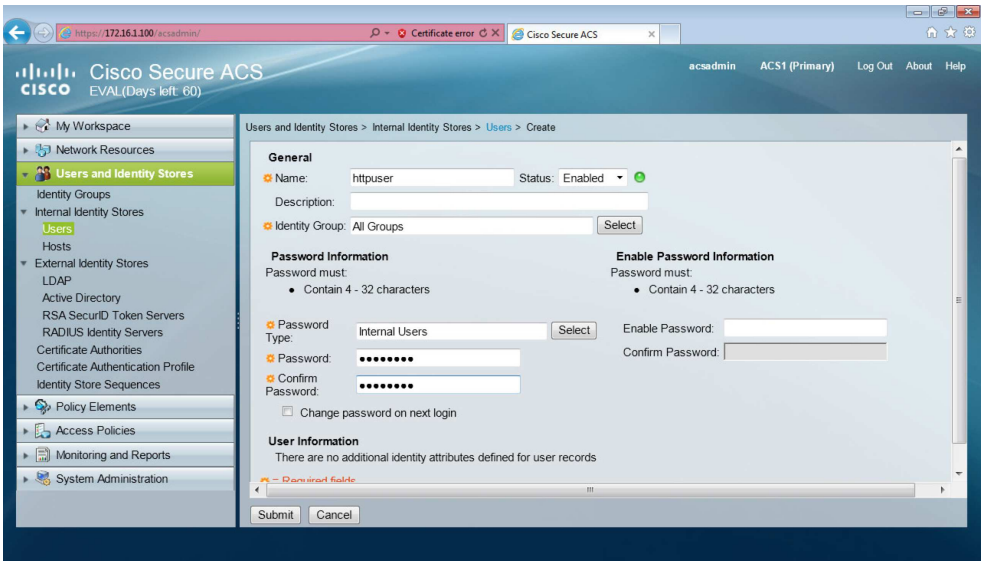
From **TEST-PC-B**, use Internet Explorer to browse to ACS and navigate to **Network Resources -> Network Devices and AAA Clients**; click **Create** to add

https://t.me/learningnets

ASA failover pair as NAD client:

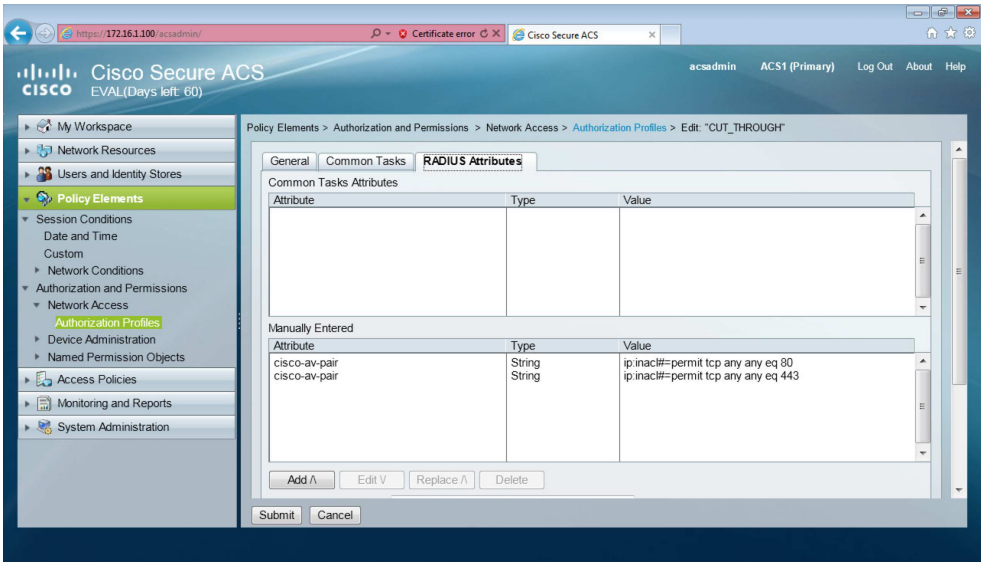


Navigate to **Users and Identity Stores- > Internal Identity Stores -> Users** and click **Create** to add the authentication username/password pair:

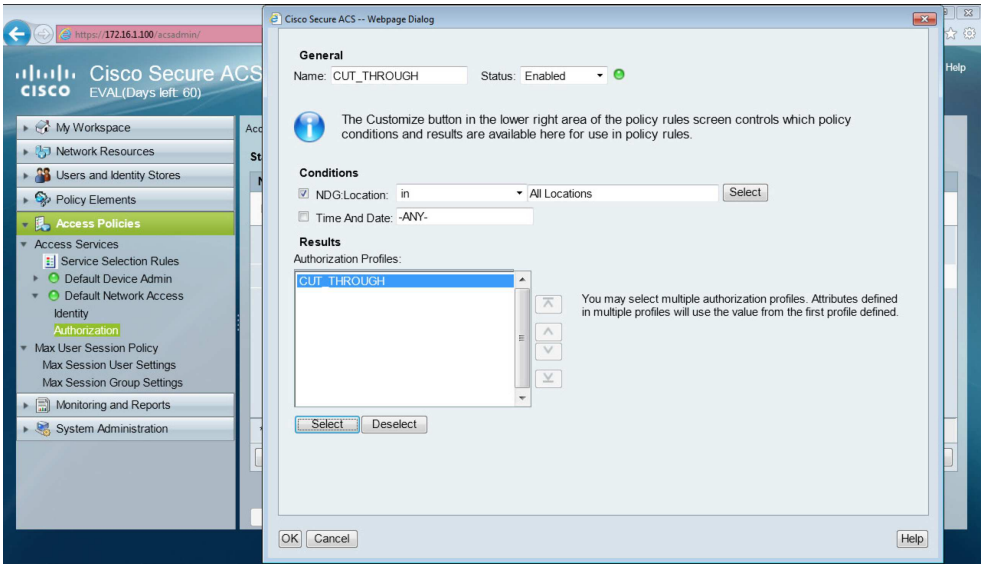


Navigate to **Policy Elements -> Authorization and Permissions -> Network Access ->Authorization Profiles** and click **Create** to add the authorization ACL entries as a profile:

https://t.me/learningnets



Navigate to **Access Policies -> Default Network Access -> Authorization** and click **Create** to add the authorization rule:



Task 4.1 Verification

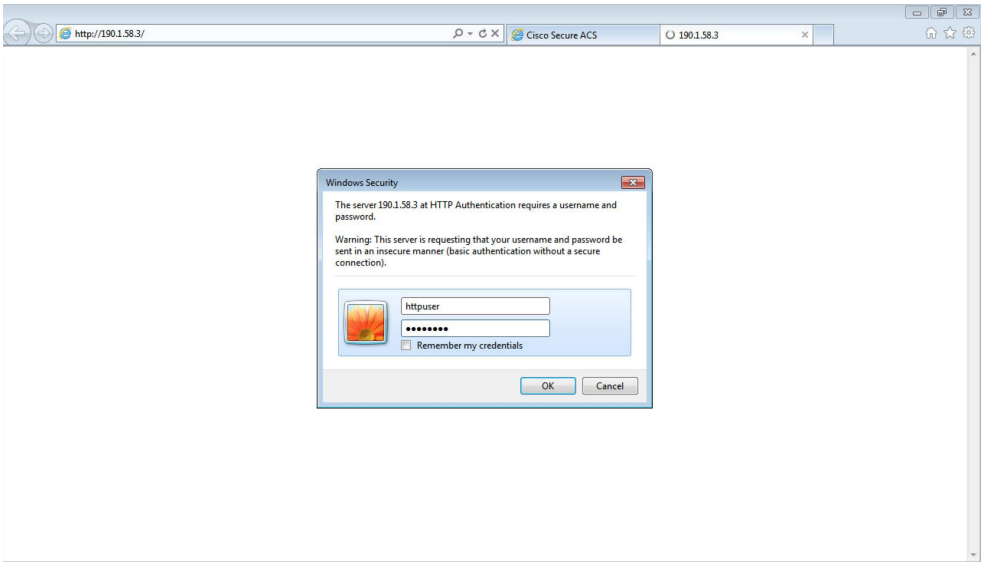
Test from the ASA that authentication is successful:

```
ASA12/ASA2# test aaa-server authentication ACS_RADIUS username httpuser password httppass
Server IP Address or name: 172.16.1.100
INFO: Attempting Authentication test to IP address <172.16.1.100> (timeout: 12 seconds)
INFO: Authentication Successful
```

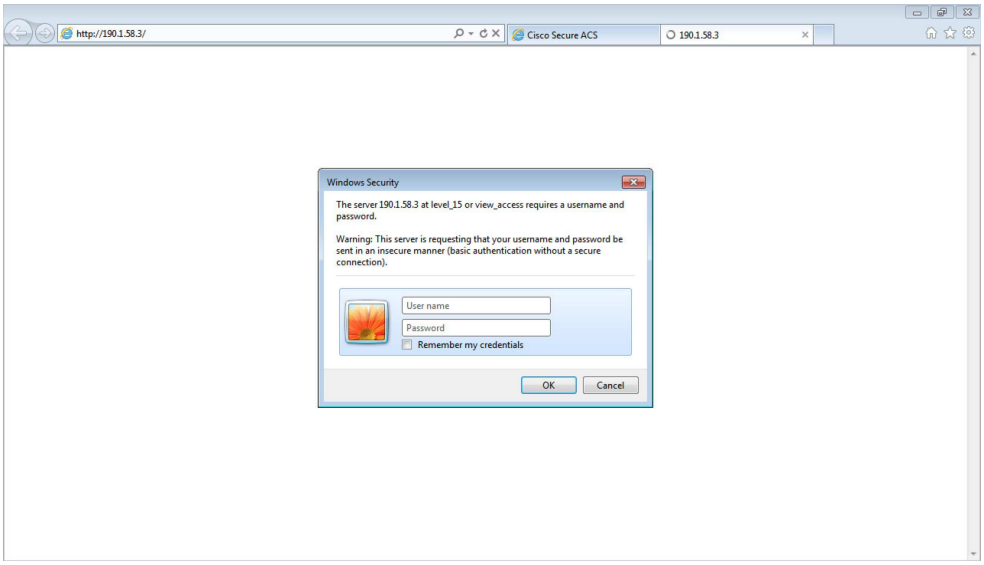
From **TEST-PC-B**, use Internet Explorer to navigate to **http://190.1.58.3**; ASA will

https://t.me/learningnets

intercept the session and request for authentication:



If authentication is successful, ASA will allow the session and the router will ask for authentication:



Verify that ACL was downloaded from the ACS server:

```
ASA12/ASA2# show uauth

                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          4
user 'httpuser' at 172.16.6.100, authenticated
   access-list AAA-user-httpuser-734C0000 (*)
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
!
```

https://t.me/learningnets

```
!ASA12/ASA2# show access-list AAA-user-httpuser-734C0000

access-list AAA-user-httpuser-734C0000; 2 elements; name hash: 0xf49c17da (dynamic)
access-list AAA-user-httpuser-734C0000 line 1 extended permit tcp any any eq www (hitcnt=1) 0x7e1ec84d
access-list AAA-user-httpuser-734C0000 line 2 extended permit tcp any any eq https (hitcnt=0) 0x407b5910
```

Verify that the session was proxied by the WSA:

```
1396787669.142 2039190.1.12.100 TCP_MISS/401 261 GET http://190.1.58.3/ - DIRECT/190.1.58.3 text/plain
 DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup <IW_infr,-5.9,0,"-",0,0,0,1,"-",-,-,-,"-",0,2
```

Task 4.2 Solution

R4:

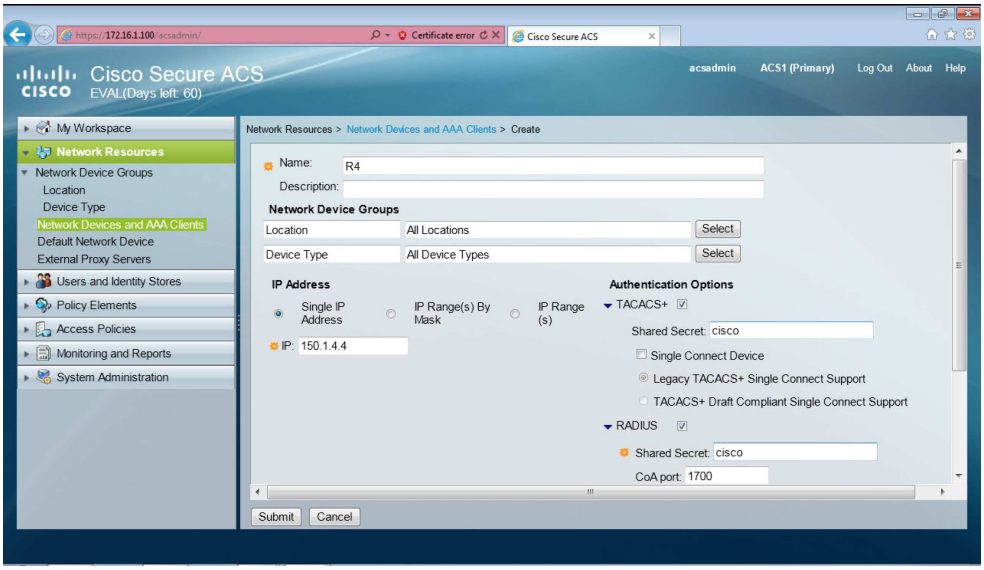
```
aaa new-model
!
aaa group server radius ACS_RADIUS
 server-private 172.16.1.100 key cisco
 ip radius source-interface Loopback0
!
aaa group server tacacs+ ACS_TACACS
 server-private 172.16.1.100 key cisco
 ip tacacs source-interface Loopback0
!
aaa authentication login VTY group ACS_RADIUS local
aaa authorization exec VTY group ACS_RADIUS local
aaa accounting commands 15 VTY start-stop group ACS_TACACS
!
username ADMIN privilege 15 password CISCO
!
line vty 0 15
 login authentication VTY
 accounting commands 15 VTY
 authorization exec VTY
```

ASA3:

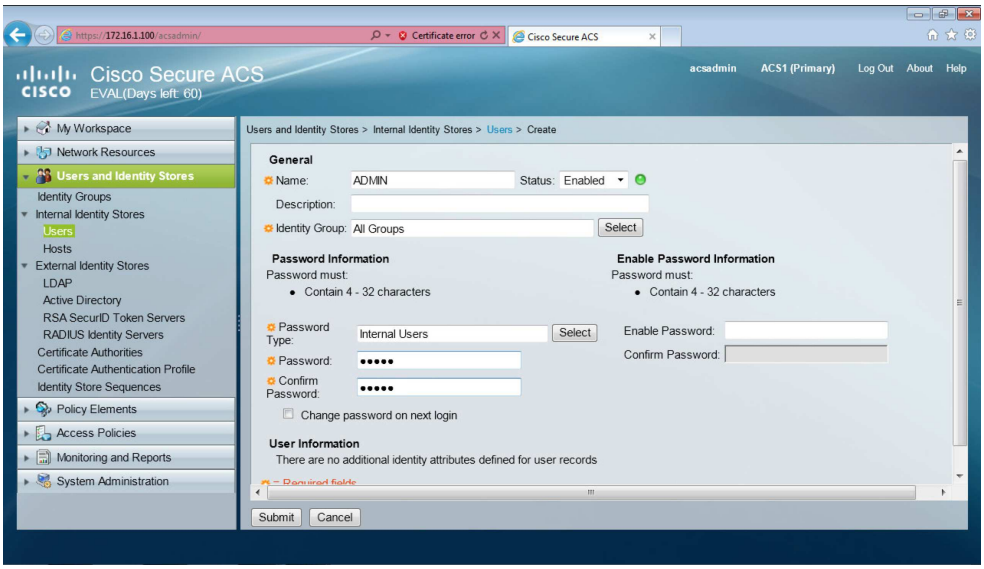
```
access-list VLAN56_IN permit udp host 150.1.4.4 host 172.16.1.100 eq 1645
access-list VLAN56_IN permit udp host 150.1.4.4 host 172.16.1.100 eq 1812
access-list VLAN56_IN permit tcp host 150.1.4.4 host 172.16.1.100 eq 49
```

https://t.me/learningnets

From **TEST-PC-B**, use Internet Explorer to browse to ACS and navigate to **Network Resources -> Network Devices and AAA Clients**; click **Create** to add R4 as NAD client for both RADIUS and TACACS:

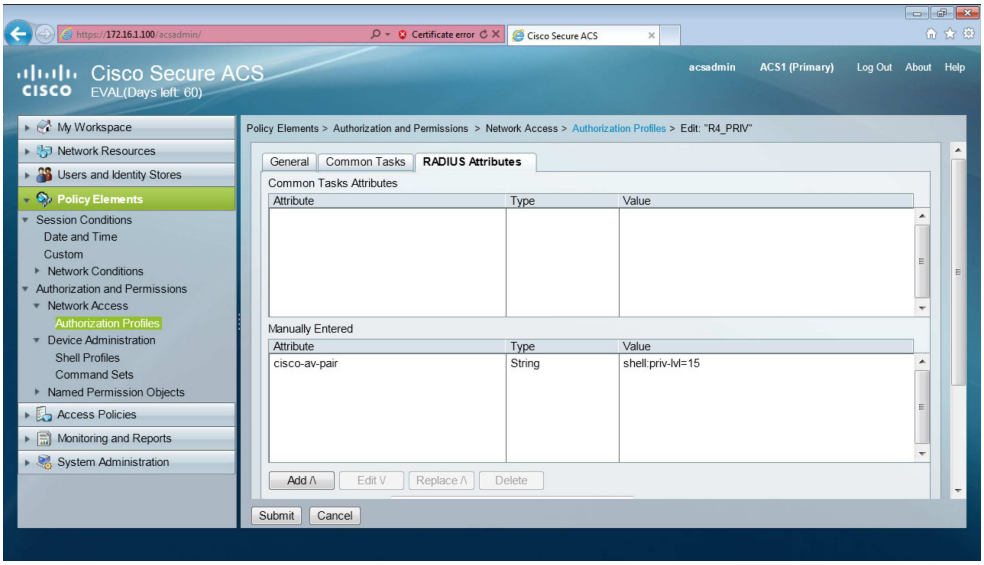


Navigate to **Users and Identity Stores- > Internal Identity Stores -> Users** and click **Create** to add the authentication username/password pair:

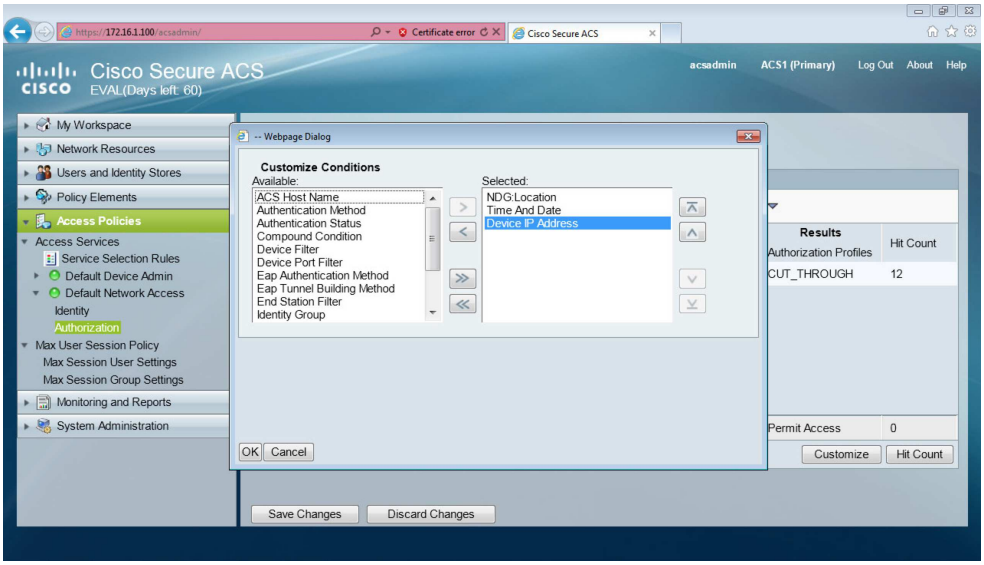


Navigate to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click **Create** to configure privilege-level assignment:

https://t.me/learningnets

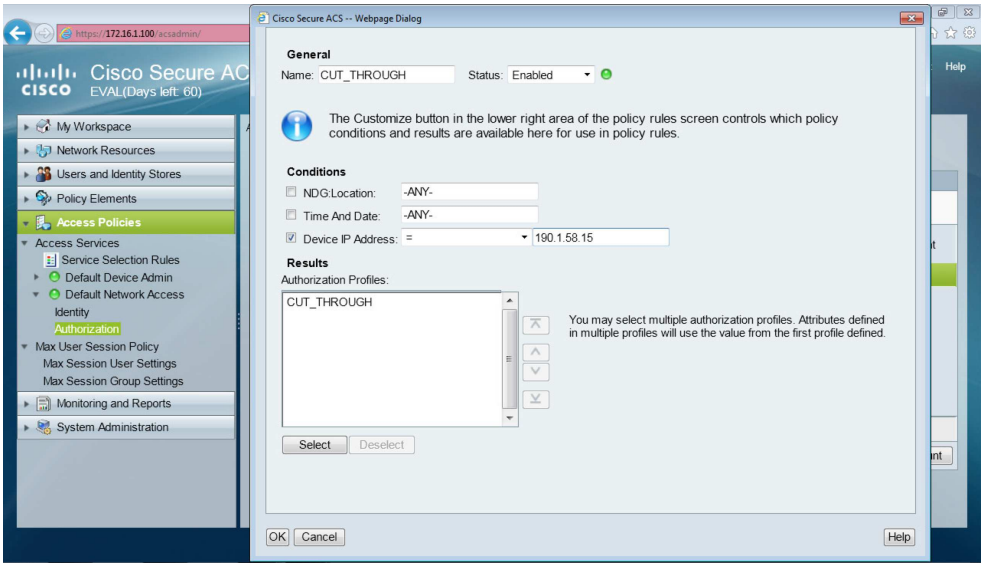


Navigate to **Access Policies -> Default Network Access -> Authorization** and click **Customize** to add conditions to the rules; for example, **Device IP Address**:

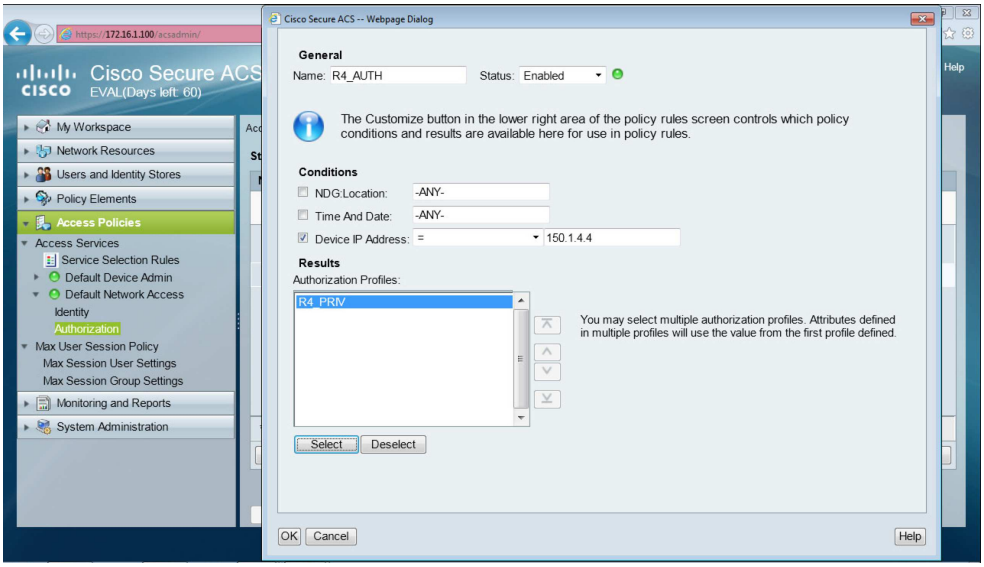


Navigate to **Access Policies -> Default Network Access -> Authorization**, select the rule from the previous task, click **Edit**, and change the conditions:

https://t.me/learningnets



Navigate to **Access Policies -> Default Network Access -> Authorization** and click **Create** to add the authorization rule for R4:



Task 4.2 Verification

Test from R4 that authentication via RADIUS is successful:

```
R4#test aaa group ACS_RADIUS ADMIN CISCO legacy

Attempting authentication test to server-group ACS_RADIUS using radius
User was successfully authenticated.
```

Telnet to R4 and verify that privilege-level 15 is assigned:

https://t.me/learningnets

```
R4#telnet 150.1.4.4

Trying 150.1.4.4 ... Open



User Access Verification

Username: ADMIN
Password:
R4#show privilege
      Current privilege level is 15
```

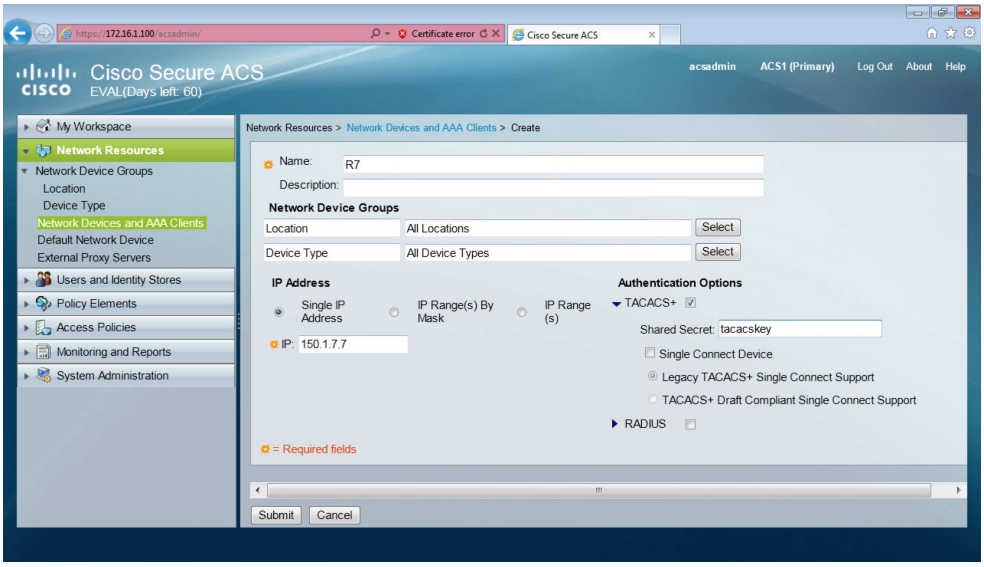
Task 4.3 Solution

```
R7:

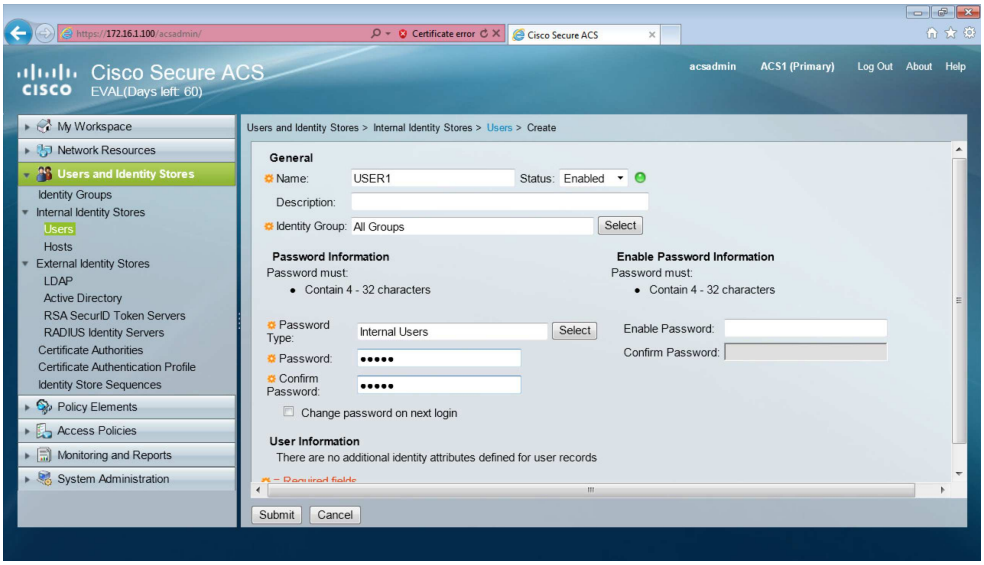
aaa new-model
!
aaa group server tacacs+ ACS_TACACS
 server-private 172.16.1.100 key tacacskey
 ip tacacs source-interface Loopback0
!
aaa authentication login VTY group ACS_TACACS
aaa authorization exec VTY group ACS_TACACS
!
privilege exec level 9 configure terminal
privilege configure all level 7 snmp-server
!
line vty 0 15
 login authentication VTY
 authorization exec VTY
```

From **TEST-PC-B**, use Internet Explorer to browse to ACS and navigate to **Network Resources -> Network Devices and AAA Clients**; click **Create** to add R7 as NAD client for TACACS:

https://t.me/learningnets

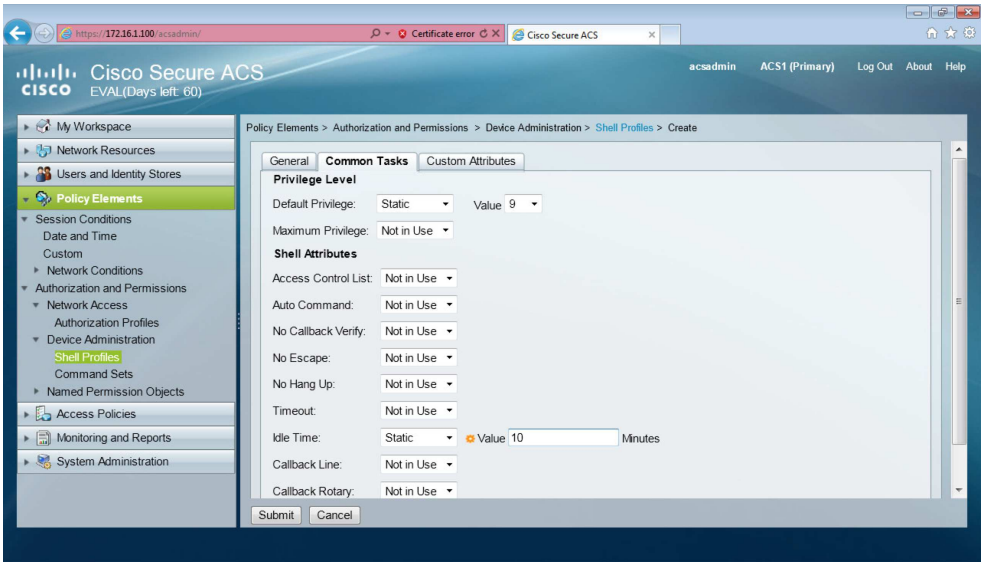


Navigate to **Users and Identity Stores- > Internal Identity Stores -> Users** and click **Create** to add the authentication username/password pair:

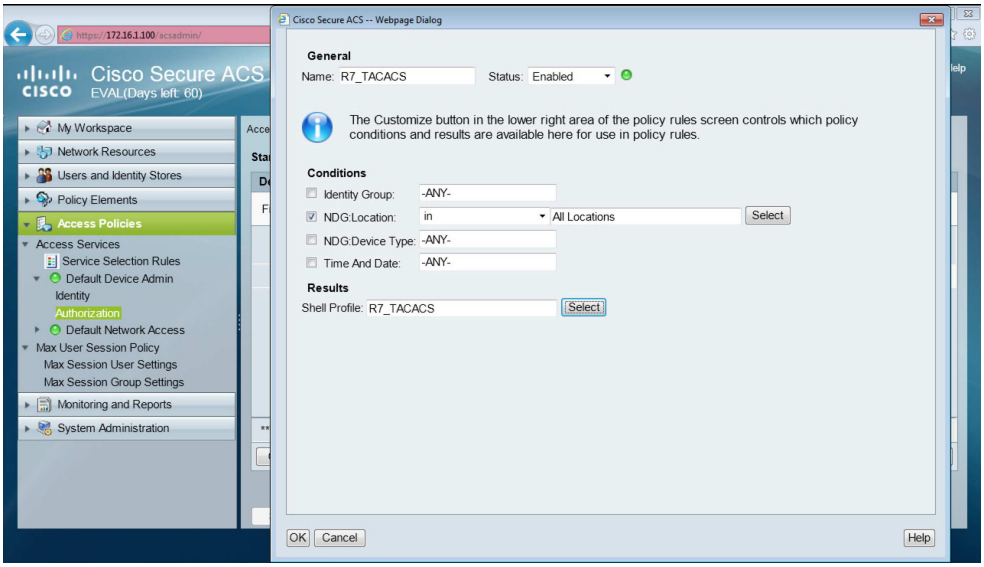


Navigate to **Policy Elements -> Authorization and Permissions -> Device Administration -> Shell Profiles** and click **Create** to configure privilege-level and idle-timeout assignment:

https://t.me/learningnets



Navigate to **Access Policies -> Default Device Admin -> Authorization**, click **Customize**, and click **Create** to add the authorization rule for R7:



Task 4.3 Verification

Test from R7 that authentication via TACACS+ is successful:

```
R7#test aaa group ACS_TACACS USER1 CISCO legacy

Attempting authentication test to server-group ACS_TACACS using tacacs+
User was successfully authenticated.
```

https://t.me/learningnets

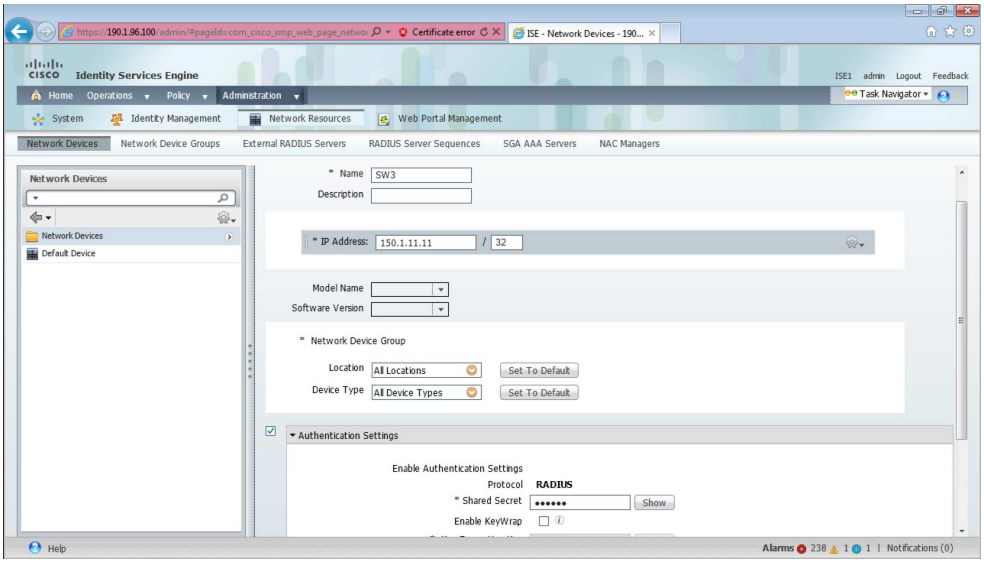
Telnet to R7 and verify that privilege-level 9 is assigned and that access to only **snmp-server** configure mode-related commands is allowed:

```
R7#telnet 150.1.7.7
Trying 150.1.7.7 ... Open

username: USER1
password:
R7#show privilege
Current privilege level is 9
R7#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.R7(config)#router ospf eigrp 300
           ^% Invalid input detected at '^' marker.
R7(config)#snmp-server enable traps vtp
R7(config)#no snmp-server enable traps vtp
```

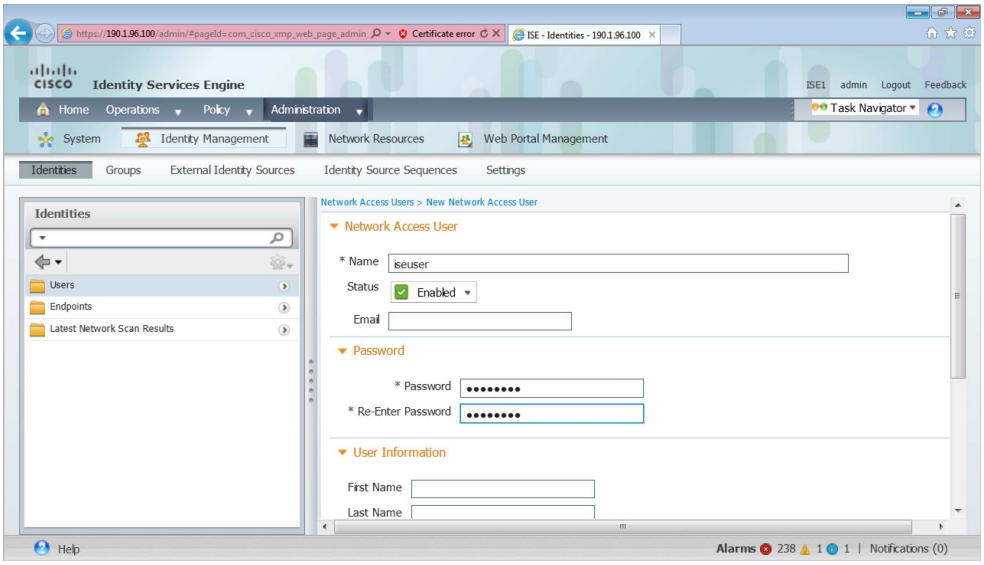
Task 4.4 Solution

From **TEST-PC-B**, use Internet Explorer to navigate to ISE, **Administration -> Network Resources -> Network Devices**, and click **Add** to add SW3 as a NAD client:

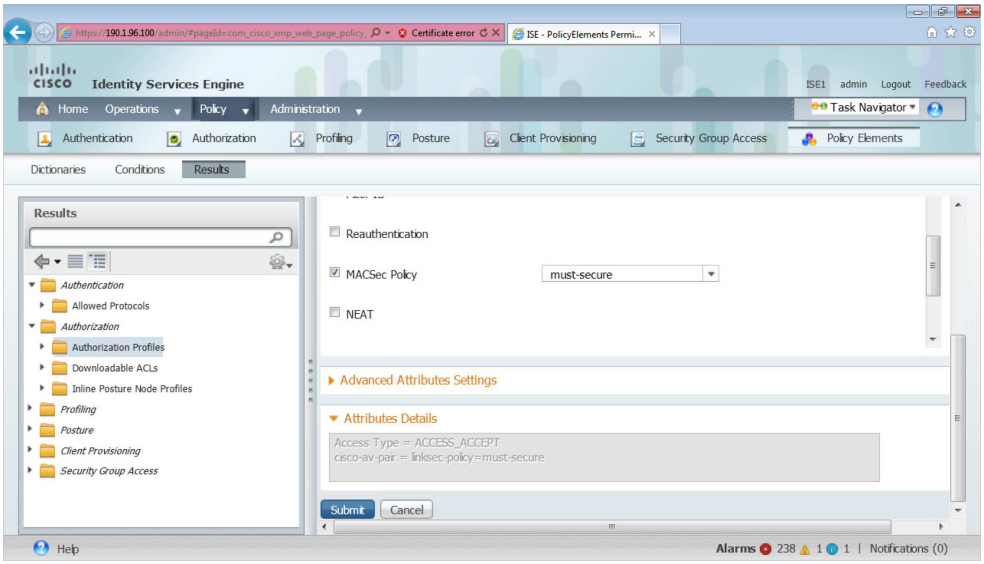


Navigate to **Administration -> Identity Management -> Identities -> Users** and click **Add** to configure the required username/password pair:

https://t.me/learningnets

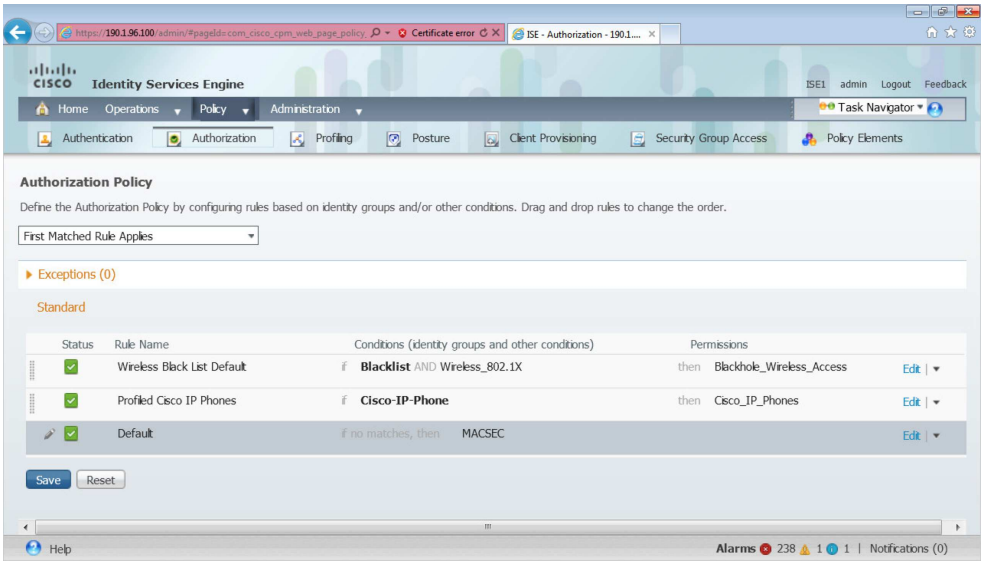


Navigate to **Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles** and click **Add** to configure the authorization profile for MACSec:



Navigate to **Policy -> Authorization** and modify the default rule by applying the configured authorization profile of **MACSEC**:

https://t.me/learningnets



SW3:

```
aaa new-model
aaa authentication dot1x default group ISE_RADIUS
aaa authorization network default group ISE_RADIUS
!
aaa group server radius ISE_RADIUS
 server-private 190.1.96.100 key isekey
 ip radius source-interface Loopback0
!
dot1x system-auth-control
!
interface GigabitEthernet1/0/5
 authentication host-mode single-host
 authentication port-control auto
 dot1x pae authenticator
 dot1x timeout tx-period 15
 dot1x max-reauth-req 3
 dot1x max-req 5
 macsec
 authentication event linksec fail action authorize vlan 12
 mka default-policy
```

ASA3:

```
access-list VLAN56_IN permit tcp 190.1.88.0 255.255.255.0 host 190.1.96.100 eq 443
```

ASA4:

```
object network ISE_REAL
 host 172.16.3.100
 nat (INSIDE,OUTSIDE) static 190.1.96.100
```

https://t.me/learningnets

```
!
access-list OUTSIDE_IN permit udp host 150.1.11.11 host 172.16.3.100 eq 1645
access-list OUTSIDE_IN permit udp host 150.1.11.11 host 172.16.3.100 eq 1812
access-list OUTSIDE_IN permit tcp 190.1.88.0 255.255.255.0 host 172.16.3.100 eq 443
```

Task 4.4 Verification

Test from SW3 that authentication via RADIUS is successful:

```
SW3#test aaa group ISE_RADIUS iseuser Cisco123 legacy
Attempting authentication test to server-group ISE_RADIUS using radius
User was successfully authenticated.
```

Configure AnyConnect supplicant for EAP-FAST with MACsec, and when prompted use the usernmae/password pair configured on ISE. The client should be authenticated and authorized; verify that the requested output is matched:

```
SW3#show authentication sessions interface gigabitEthernet1/0/5

            Interface:  GigabitEthernet1/0/5
          MAC Address:  48f8.b32e.2532
           IP Address:  Unknown
            User-Name:  iseuser
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Must Secure
      Security Status:  Secured
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  00000000000069AB0FBE61F9
      Acct Session ID:  0x000000F6
               Handle:  0x50000A73

Runnable methods list:
       Method   State
       dot1x    Authc Success
```

https://t.me/learningnets

Verify the configured 802.1x timers:

```
SW3#show dot1x interface gigabitEthernet1/0/5
Dot1x Info for GigabitEthernet1/0/5
-----------------------------------
PAE                     = AUTHENTICATOR
QuietPeriod             = 60
ServerTimeout           = 0
SuppTimeout             = 30 ReAuthMax                  = 3
MaxReq                  = 5
TxPeriod                = 15
```

Verify that MACsec has been negotiated on the port:

```
SW3#show macsec summary

Interface                   Transmit SC         Receive SC
GigabitEthernet1/0/5              1                   1
!
!SW3#show macsec interface gigabitEthernet1/0/5
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128 Transmit Secure Channels
 SCI : 44D3CA6399850002
   Elapsed time : 00:15:27
   Current AN: 0   Previous AN: -
   SC Statistics
    Auth-only (0 / 0)
    Encrypt (1950 / 0) Receive Secure Channels
 SCI : 48F8B32E25320000

   Elapsed time : 00:15:27
   Current AN: 0   Previous AN: -
   SC Statistics
    Notvalid pkts 0      Invalid pkts 0
```

https://t.me/learningnets

```
  Valid pkts 1198         Late pkts 0
  Uncheck pkts 0       Delay pkts 0
Port Statistics
 Ingress untag pkts  0        Ingress notag pkts 99983
 Ingress badtag pkts 0        Ingress unknownSCI pkts 0
 Ingress noSCI pkts 0         Unused pkts 0
 Notusing pkts 0              Decrypt bytes 238478
 Ingress miss pkts 99983
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 3

CCIE SCv4 Lab 3 Solutions Section 5

1. Task 5.1 Solution
2. Task 5.2 Solution
3. Task 5.3 Solution
4. Task 5.4 Solution
5. Task 5.5 Solution

Task 5.1 Solution

R3:

```
router bgp 357
 neighbor 150.1.5.5 remote-as 357
 neighbor 150.1.5.5 update-source Loopback0
 neighbor 150.1.5.5 send-community
 neighbor 150.1.7.7 remote-as 357
 neighbor 150.1.7.7 update-source Loopback0
 neighbor 150.1.7.7 send-community
 redistribute static route-map STATIC_TO_BGP
!
route-map STATIC_TO_BGP permit 10
 match tag 357
 set local-preference 200
 set origin igp
 set community no-export
 set ip next-hop 192.0.2.1
!
ip route 192.0.2.1 255.255.255.255 Null0
ip route 190.1.111.99 255.255.255.255 Null0 tag 357
```

R5:

```
router bgp 357
 neighbor 190.1.58.3 remote-as 357
 neighbor 190.1.58.3 update-source Loopback0
!
ip route 192.0.2.1 255.255.255.255 Null0
```

https://t.me/learningnets

```
 !
 interface FastEthernet0/0.56
  ip verify unicast source reachable-via any

R7:
 router bgp 357
  neighbor 190.1.58.3 remote-as 357
  neighbor 190.1.58.3 update-source Loopback0
 !
 ip route 192.0.2.1 255.255.255.255 Null0
 !
 interface FastEthernet0/0.27
  ip verify unicast source reachable-via any

ASA1 ASA2 Context:

 access-list OUTSIDE_IN permit tcp host 150.1.5.5 host 190.1.58.3 eq 179
 access-list OUTSIDE_IN permit tcp host 150.1.7.7 host 190.1.58.3 eq 179
 !
 route OUTSIDE 150.1.5.5 255.255.255.255 190.1.58.5
```

Task 5.1 Verification

Verify that both BGP sessions have been established:

https://t.me/learningnets

```
R3#show ip bgp summary

BGP router identifier 150.1.3.3, local AS number 357
BGP table version is 3, main routing table version 3
1 network entries using 136 bytes of memory
1 path entries using 52 bytes of memory
1/1 BGP path/bestpath attribute entries using 124 bytes of memory
1 BGP community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 336 total bytes of memory
BGP activity 2/1 prefixes, 2/1 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
150.1.5.5       4          357       2       4        3    0    0 00:00:06        0
150.1.7.7       4          357       5       6        3    0    0 00:02:29        0
```

Verify that R5 and R7 receive the BGP update from R3:

```
R5#show ip bgp 190.1.111.99
BGP routing table entry for 190.1.111.99/32, version 2
Paths: (1 available, best #1, table default, not advertised to EBGP peer)
  Not advertised to any peer
  Local 192.0.2.1 from 190.1.58.3 (150.1.3.3)
 Origin IGP, metric 0, localpref 200, valid, internal, best
 Community: no-export
!
!R7#show ip bgp 190.1.111.99
BGP routing table entry for 190.1.111.99/32, version 2
Paths: (1 available, best #1, table default, not advertised to EBGP peer)
  Not advertised to any peer
  Local 192.0.2.1 from 190.1.58.3 (150.1.3.3)
 Origin IGP, metric 0, localpref 200, valid, internal, best
 Community: no-export
```

Verify that uRPF in loose mode is configured on both R5 and R7 and that the route to the attacker points to Null0; if inbound traffic is received from the attacker, it is dropped:

```
R5#show ip interface fastEthernet0/0.56 | b verify
```

https://t.me/learningnets

```
IP verify source reachable-via ANY

   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
!
!R7#show ip interface fastEthernet0/0.27 | b verify
IP verify source reachable-via ANY
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
!
!R5#show ip cef 190.1.111.99
190.1.111.99/32 nexthop 192.0.2.1 Null0
!
!R7#show ip cef 190.1.111.99
190.1.111.99/32 nexthop 192.0.2.1 Null0
```

Task 5.2 Solution

```
R1:
flow-sampler-map NETFLOW
 mode random one-out-of 20
!
ip flow-export version 9
ip flow-export source loopback0
ip flow-export destination 172.16.1.99 8000
!
ip flow-capture packet-length
ip flow-capture vlan-id
ip flow-capture ttl
!
interface gigabitEthernet0/1.12
 flow-sampler NETFLOW

ASA3:

access-list VLAN56_IN permit udp host 150.1.1.1 host 172.16.1.99 eq 8000
```

https://t.me/learningnets

Task 5.2 Verification

Verify the flow-sampler configuration:

```
R1#show flow-sampler
 Sampler : NETFLOW, id : 1, packets matched : 207, mode : random sampling mode
sampling interval is : 20
```

Verify the flow-export configuration:

```
R1#show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default Source(1)       150.1.1.1 (Loopback0)
Destination(1)  172.16.1.99 (8000)

  Version 9 flow records
  178 flows exported in 20 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Verify which interfaces have netflow activated:

```
R1#show ip flow interface
GigabitEthernet0/1.12
 flow-sampler NETFLOW
```

Verify that statistics are being collected:

```
R1#show ip cache flow

IP packet size distribution (389 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .442 .143 .015 .000 .007 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

https://t.me/learningnets

```
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .390 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 46 added
  1104 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  8 active, 1016 inactive, 92 added, 46 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-other           40      0.0         8   342      0.0      11.4      13.0
IP-other             2      0.0         1    80      0.0       0.0      15.8
Total:              42      0.0         8   340      0.0      10.9      13.1

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/1.12      190.1.12.100    Gi0/1.24      190.1.96.100    06 2635 01BB    10
Gi0/1.12      190.1.12.100    Gi0/1.24      190.1.96.100    06 2634 01BB    13

Gi0/1.12      190.1.12.100    Gi0/1.24      190.1.96.100    06 2637 01BB     1
Gi0/1.12      190.1.12.100    Gi0/1.24      190.1.96.100    06 2636 01BB     7
```

Task 5.3 Solution

R4:

```
router ospf 300
 area 12 authentication message-digest
!
interface FastEthernet0/0.45
 ip ospf message-digest-key 1 md5 ospf
!
interface FastEthernet0/0.42
 ip ospf authentication null
```

R5:

```
interface FastEthernet0/0.45
 ip ospf authentication message-digest
```

https://t.me/learningnets

```
 ip ospf message-digest-key 1 md5 ospf
```

Task 5.3 Verification

Verify that R4 is still OSPF neighbor with R1, R2, and R5:

```
R4#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.5.5         1   FULL/DR         00:00:34    190.1.45.5      FastEthernet0/0.45
150.1.1.1         1   FULL/DROTHER    00:00:39    190.1.24.1      FastEthernet0/0.42
150.1.2.2         1   FULL/BDR        00:00:36    190.1.24.2      FastEthernet0/0.42
```

Verify that OSFP authentication is enabled at the area level and that it is active between R4 and R5, but not between R4 and R1/R2:

```
R4#show ip ospf | b Area 12
    Area 12
        Number of interfaces in this area is 5 (1 loopback) Area has message digest authentication
        SPF algorithm last executed 00:01:54.572 ago
        SPF algorithm executed 27 times
        Area ranges are
        Number of LSA 15. Checksum Sum 0x08BC83
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
!
!R4#show ip ospf interface fastEthernet0/0.45 | b Message
 Message digest authentication enabled
 Youngest key id is 1
!
!R4#show ip ospf interface fastEthernet0/0.42

FastEthernet0/0.42 is up, line protocol is up
  Internet Address 190.1.24.4/24, Area 12
  Process ID 300, Router ID 150.1.4.4, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 150.1.4.4, Interface address 190.1.24.4
```

https://t.me/learningnets

```
  Backup Designated router (ID) 150.1.2.2, Interface address 190.1.24.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 14
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 150.1.1.1
    Adjacent with neighbor 150.1.2.2  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

Task 5.4 Solution

R6:

```
class-map match-any OSPF
 match protocol ospf
!
class-map match-any ICMP
 match protocol icmp
!
class-map match-any TELNET
 match protocol telnet
!
policy-map VLAN65_OUTBOUND
 class OSPF
  bandwidth percent 10
 class ICMP
  police rate percent 10
 class TELNET
  set dscp af43
!
interface FastEthernet0/1
 service-policy output VLAN65_OUTBOUND
```

https://t.me/learningnets

Task 5.4 Verification

Generate some ICMP/telnet traffic through R6, and then verify policy-map statistics:

```
R6#show policy-map interface fastEthernet0/1
 FastEthernet0/1

  Service-policy output: VLAN65_OUTBOUND
 Class-map: OSPF (match-any)
 6 packets, 468 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol ospf
        6 packets, 468 bytes
        5 minute rate 0 bps
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 6/564 bandwidth 10% (10000 kbps)
 Class-map: ICMP (match-any)
      5 packets, 570 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol icmp 5 packets, 570 bytes
        5 minute rate 0 bps police:
 rate 10 %
          rate 10000000 bps, burst 312500 bytes
        conformed 5 packets, 570 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps
 Class-map: TELNET (match-any)
      8 packets, 461 bytes
      5 minute offered rate 0 bps, drop rate 0 bps Match: protocol telnet
 8 packets, 461 bytes
        5 minute rate 0 bps QoS Set
 dscp af43
 Packets marked 8


    Class-map: class-default (match-any)
      4477 packets, 1050330 bytes
      5 minute offered rate 33000 bps, drop rate 0 bps
      Match: any
```

https://t.me/learningnets

```
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 4224/988885
```

Task 5.5 Solution

```
R5:
snmp-server source-interface traps loopback0
snmp-server enable traps cpu threshold
snmp-server host 172.16.1.44  version 2c traps cpu cpu
!
process cpu threshold type total rising 95 interval 10 falling 20 interval 20

ASA3:

access-list VLAN56_IN permit udp host 150.1.5.5 host 172.16.1.44 eq 162
```

Task 5.5 Verification

Verify the SNMP host being notified, SNNMP version and community:

```
R5#show snmp host
 Notification host: 172.16.1.44  udp-port: 162   type: trap
user: cpu        security model: v2c
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 3

CCIE SCv4 Lab 3 Solutions Section 6

1. Task 6.1 Solution
2. Task 6.2 Solution
3. Task 6.3 Solution
4. Task 6.4 Solution
5. Task 6.5 Solution

Task 6.1 Solution

```
SW3:

ipv6 dhcp guard policy DHCP_SERVER
 device-role server
!
interface GigabitEthernet1/0/3
 ipv6 dhcp guard attach-policy DHCP_SERVER
```

Task 6.1 Verification

Verify that the requested output is matched:

```
SW3#ping 2001:69:69::6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:69:69::6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Verify that SW3 has been assigned an IPv6 address via DHCP:

```
SW3#show ipv6 interface vlan69
```

https://t.me/learningnets

```
Vlan69 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::46D3:CAFF:FE63:99C1
  No Virtual link-local address(es):
  Global unicast address(es):
2001:69:69:0:D59C:ECC8:B143:4FAE, subnet is 2001:69:69:0:D59C:ECC8:B143:4FAE/128
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF43:4FAE
    FF02::1:FF63:99C1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  Output features: Check hwidb
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
!
!R6#show ipv6 dhcp binding

Client: FE80::46D3:CAFF:FE63:99C1
  DUID: 0003000144D3CA639980
  Username : unassigned
  IA NA: IA ID 0x08590001, T1 43200, T2 69120 Address: 2001:69:69:0:D59C:ECC8:B143:4FAE

            preferred lifetime 86400, valid lifetime 172800
            expires at Apr 08 2014 08:24 PM (172638 seconds)
```

Task 6.2 Solution

https://t.me/learningnets

```
SW1:

interface range FastEthernet1/0/10 - 11
 switchport mode access
 switchport access vlan 12
 switchport protected
 switchport block unicast
 no shutdown
```

Task 6.2 Verification

Verify that both features are enabled on the ports:

```
SW1#show interfaces fastEthernet1/0/10 switchport | i Protected|Unknown
Protected: true
Unknown unicast blocked: enabled
Unknown multicast blocked: disabled
!
!SW1#show interfaces fastEthernet1/0/11 switchport | i Protected|Unknown
Protected: true
Unknown unicast blocked: enabled

Unknown multicast blocked: disabled
```

Task 6.3 Solution

```
R5:

class-map type logging match-any VLAN45
 match ipv4 destination-address 190.1.45.5
!
class-map type logging match-any VLAN56
 match ipv4 destination-address 190.1.56.5
!
class-map type logging match-any VLAN58
 match ipv4 destination-address 190.1.58.5
!
class-map type logging match-any LOOPBACK
 match ipv4 destination-address 150.1.5.5
!
policy-map type logging LOGGING
```

https://t.me/learningnets

```
 class VLAN45
  log
 class VLAN56
  log
 class VLAN58
  log
 class LOOPBACK
  log
!
control-plane host
 service-policy type logging input LOGGING
```

Task 6.3 Verification

Verify that the feature is activated:

```
R5#show control-plane features

Total 1 features configured

Control plane host path features :

------------------------------------------------------
Control-plane Logging activated Apr 06 2014 18:3

------------------------------------------------------
!
!R5#show control-plane host counters

Control plane host path counters :

Feature                  Packets Processed/Dropped/Errors

----------------------------------------------------------Control-plane Logging          37/0/0



------------------------------------------------------
```

Verify statistics for the configured policy-map:

```
R5#show policy-map type logging control-plane host


 Control Plane Host
```

https://t.me/learningnets

```
  Service-policy logging input: LOGGING

    Class-map: VLAN45 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  ipv4 destination-address 190.1.45.5
        0 packets, 0 bytes
        5 minute rate 0 bps
      log

    Class-map: VLAN56 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  ipv4 destination-address 190.1.56.5
        0 packets, 0 bytes
        5 minute rate 0 bps
      log
 Class-map: VLAN58 (match-any)
5 packets, 450 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  ipv4 destination-address 190.1.58.5
        0 packets, 0 bytes
        5 minute rate 0 bps
      log
 Class-map: LOOPBACK (match-any)
12 packets, 798 bytes

      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  ipv4 destination-address 150.1.5.5
        0 packets, 0 bytes
        5 minute rate 0 bps
      log

    Class-map: class-default (match-any)
      20 packets, 2360 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Because of BGP session and NTP server configuration, the following messages will start to appear at R5's console:

https://t.me/learningnets

```
%CP-6-TCP: PERMIT  190.1.58.3(179) -> 150.1.5.5(45882)
%CP-6-UDP: PERMIT  190.1.58.3(123) -> 190.1.58.5(123)
```

Task 6.4 Solution

SW3:

```
ip access-list extended OSPF_ALLOW
 permit ospf host 190.1.45.4 any
 permit ospf host 190.1.45.5 any
!
ip access-list extended OSPF_DROP
 permit ospf any any
!
vlan access-map VLAN45_VACL 10
 match ip address OSPF_ALLOW
 action forward
!
vlan access-map VLAN45_VACL 20
 match ip address OSPF_DROP
 action drop
!
vlan access-map VLAN45_VACL 30
 action forward
!
vlan filter VLAN45_VACL vlan-list 45
```

Task 6.4 Verification

Verify that R4 and R5 are still OSPF neighbors:

```
R4#show ip ospf neighbor fastEthernet0/0.45

Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.5.5         1   FULL/BDR        00:00:33    190.1.45.5      FastEthernet0/0.45
```

Verify the VACL configuration:

https://t.me/learningnets

```
SW3#show vlan access-map

Vlan access-map "VLAN45_VACL"  10
  Match clauses:
    ip  address: OSPF_ALLOW
  Action:
    forward
Vlan access-map "VLAN45_VACL"  20
  Match clauses:
    ip  address: OSPF_DROP
  Action:
    drop
Vlan access-map "VLAN45_VACL"  30
  Match clauses:
  Action:
    forward
!
!SW3#show vlan filter access-map VLAN45_VACL
VLAN Map VLAN45_VACL is filtering VLANs: 45
```

Task 6.5 Solution

```
R6:

ip access-list extended ICMP_POLICING
 deny icmp 150.1.0.0 0.0.255.255 any
 permit icmp any any
!
class-map ICMP_POLICING
 match access-group name ICMP_POLICING
!
policy-map ICMP_POLICING
 class ICMP_POLICING
  police 100000 conform-action transmit exceed-action drop
!
control-plane host
 service-policy input ICMP_POLICING
```

Task 6.5 Verification

https://t.me/learningnets

Verify that the feature has been enabled:

```
R6#show control-plane features

Total 1 features configured

Control plane host path features :

------------------------------------------------------
Control-plane Policing activated Apr 06 2014 21:2



------------------------------------------------------
```

Verify that ICMP traffic is policed only if not sourced from Loopback0 range:

```
SW3#ping 150.1.6.6 size 1500 repeat 10
Type escape sequence to abort.
Sending 10, 1500-byte ICMP Echos to 150.1.6.6, timeout is 2 seconds:!!.!!.!!.!
Success rate is 70 percent (7/10), round-trip min/avg/max = 1/1/1 ms
!
!SW3#ping 150.1.6.6 size 1500 repeat 10 source loopback0
Type escape sequence to abort.
Sending 10, 1500-byte ICMP Echos to 150.1.6.6, timeout is 2 seconds:
Packet sent with a source address of 150.1.11.11 !!!!!!!!!!

Success rate is 100 percent (10/10), round-trip min/avg/max = 1/5/17 ms
```

Verify the policy-map statistics:

```
R6#show policy-map control-plane host input

 Control Plane Host

  Service-policy input: ICMP_POLICING
 Class-map: ICMP_POLICING (match-all)
      10 packets, 15180 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name ICMP_POLICING
      police:
          cir 100000 bps, bc 3125 bytes conformed 7 packets, 10626 bytes; actions:
          transmit  exceeded 3 packets, 4554 bytes; actions:

          drop
```

https://t.me/learningnets

```
      conformed 0 bps, exceed 0 bps

  Class-map: class-default (match-any)
    11 packets, 15274 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 5

CCIE SCv4 Lab 5 Introduction

Lab Guidelines

The following scenarios are practice labs designed to test your readiness for the Cisco Systems CCIE Security Lab Exam. However, remember that in addition to being designed as a simulation of the actual CCIE lab exam, these practice labs should be used as a learning tool. Instead of rushing through the labs to complete all the configuration steps, take the time to research the networking technology and gain a deeper understanding of the principles behind its operation. For each lab of the CCIE Security Practice Labs Workbook, follow these guidelines:

- Read the entire lab exam before starting the configuration, and correlate tasks within a section to get a complete overview of the lab objectives.
- There are dependencies between tasks of the same section and between tasks from different sections. Carefully read throughout the lab to identify and make notes of it
- The lab consists of six sections that don't necessarily need to be completed in the presented order. However some tasks must be completed before others (such as initialization of ASA firewalls).
- All sections total 100 points, and you must earn a minimum of 80 points to receive a passing grade. To earn the points assigned to each task, you must fulfill all requirements and conform to all restrictions.
- No partial credit is awarded. You will earn all points or zero points for each task; if multiple solutions are available for a task, choose the one that technically best meets the requirements.
- Some tasks present a set of requirements for implementing a technology, and some tasks present outputs to be matched.
- Labs include both configuration and troubleshooting tasks; the number of faults relevant to each troubleshooting task may or not be specified.
- Before starting the exam, verify that all equipment is functional, powered up and that you can access it at the console.
- Routers and switches are preconfigured, do not change it unless specifically allowed

https://t.me/learningnets

by the task. On troubleshooting tickets, you may change any of the initial configurations.

- IPv4/IPv6 static and default routes are allowed to complete any task, but only if this is the only available option, and unless otherwise stated in any task.
- Make sure you do not to lock yourself out of any device, because password recovery or device reset is not available in the lab.
- At the end of the exam, ensure that all devices are accessible at the console by using preconfigured credentials or the ones from specific task requirements.
- For IPv4/IPv6 addressing configuration, the following variables will be used as a reference:
  - **X** is the rack number; the value for **Rack1** will be **1**.
  - **Y** is the device number, with routers ranging from one (1) to seven (7), switches from nine (9) to fourteen (14), and ASA firewalls from fifteen (15) to eighteen (18); the value for **Router1** will be **1**, **Switch1** will be **9**, and **ASA1** will be **15**.

All routers and switches are accessible at the console without requiring any authentication; do not change this. To access other devices within the lab, use the following tables as a reference:

Device	Username	Password
TESTPC-A	ineadmin	ciscoccie
TESTSRV-A	Administrator	Cisco1234
TESTPC-B	ineadmin	ciscoccie
TESTSRV-B	Administrator	Cisco1234
TESTPC-WIFI	ineadmin	ciscoccie

Device	Username	Password
WSA CLI&GUI	admin	default1A

https://t.me/learningnets

Device	Username	Password
ACS1 CLI	admin	default1A
ACS1 GUI	acsadmin	default1A
ACS2 CLI	admin	default1A
ACS2 GUI	acsadmin	default1A
ISE1 CLI&GUI	admin	default1A
ISE2 CLI&GUI	admin	default1A
WLC CLI&GUI	admin	default1A
LAP CLI	cisco	Cisco
IPS CLI&GUI	cisco	ciscoips4240

Lab Instructions

Before you begin, make sure that the initial configuration scripts for each lab have been applied. If you have any questions related to the scenario solutions, visit our CCIE support forum at http://IEOC.com. Refer to the attached physical and logical diagrams on each lab for interface and protocol assignments; you may access these by clicking the **Resources** button in the upper-right corner. Upon lab completion, end-to-end IPv4/IPv6 connectivity is not a requirement unless specifically asked for, but you are required to meet task requirements and restrictions.

Lab Restrictions

Each lab scenario contains explicit general restrictions that you must conform to while configuring the lab. These restrictions are defined in the introductory section for each scenario. Examples of such restrictions include, but are not limited to, not adding additional IP addressing, not changing the default authentication methods,

https://t.me/learningnets

etc. There may also be certain restrictions for particular tasks within a lab scenario. Examples of these restrictions include, but are not limited to, not issuing a particular configuration command, not using the legacy configuration for a technology, etc.

TIP

You may do whatever is necessary to complete a task unless the general requirements for the lab scenario or the specific requirements for the task explicitly prohibit you from doing so. This may include using static routing, NAT statements, ACL exceptions, IPsec/GRE tunneling, etc.

Difficulty Rating

Each lab scenario has been assigned a difficulty rating. Ratings are on a scale of one (1) to ten (10), with 10 being the most difficult. Labs are designed to be more technically challenging than the actual CCIE Security Lab Exam. Do not be discouraged if you score low or do not understand a particular set of technologies. If you are having trouble with a certain area, do not hesitate to read the explanation contained within the solutions guide and study the respective technology using the Technologies Workbook or the Advanced Technologies video course. Remember that these labs are designed to teach you required skills for implementing and troubleshooting a complex network with several technologies mixed together, just as much as they are intended to test your current technical knowledge.

Point Values

As in the actual CCIE Lab exam, each task within a lab is assigned a specific point value. Points are awarded only if the presented solution meets all the given requirements and does not violate any restrictions. No partial credit is awarded for any task. A minimum score of 80 points is required to pass a particular scenario. Some tasks have multiple solutions; as long as the presented solution meets the given requirements, points will be awarded for that task. However, certain solutions may negatively affect previous or future tasks. Make sure that you carefully read all presented requirements and try your best to come up with a technically appropriate solution.

TIP

https://t.me/learningnets

Points will never be awarded for a task in which you have violated the requirements. However, remember the relative point value of the task in question as compared to future tasks. If you cannot find an appropriate solution for a particular task, it is advisable to solve the task by whatever means necessary to complete the future tasks that depend on it.

Loading Initial Config

Each lab contains a set of initial configuration scripts for routers and switches. These configuration scripts include basic Layer 2 and Layer 3 routing connectivity (as well as possible more advanced functionalities for troubleshooting tickets), and must be loaded on your rack before beginning the configuration of the scenario. These are available to be loaded from the Rack Rental Control Panel, or if you are using your own rack, they are attached to each individual lab and available for download. Initial configurations and physical and logical diagrams of each lab are attached to this Introduction; you may access these by clicking the **Resources** button in the upper-right corner.

Rack Rentals

INE has designed the CCIE Security Practice Labs Workbook based around the publicly stated hardware specification used in the actual CCIE Lab exam. To eliminate the cost of buying all the equipment used in the workbook, INE offers cost-effective equipment rentals specifically designed to be used with this and other self-paced training product lines. For more information on rack rentals. visit http://INE.com.

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 5

CCIE SCv4 Lab 5 Tasks

1. Perimeter Security and Services
2. Intrusion Prevention and Content Security
3. Confidentiality and Secure Access
4. Identity Management
5. System Hardening and Availability
6. Threat Identification and Mitigation

Difficulty Rating (10 highest): 8

Point Values

The point values for each section are as follows:

Section	Point Value
Perimeter Security and Services	24
Intrusion Prevention and Content Security	18
Confidentiality and Secure Access	17
Identity Management	17
System Hardening and Availability	14

https://t.me/learningnets

Section	Point Value
Threat Identification and Mitigation	10

GOOD LUCK!

TIP

When taking the CCIE lab exam, you will be provided with a few sheets of scratch paper for notes and diagrams. You should create two diagrams at a minimum: one for the logical Layer 2 topology and one for the logical Layer 3 topology. Note that the physical diagram and the logical Layer 2 diagram are not the same.

Although you are provided with the logical Layer 3 diagram in the lab, it will be in electronic format, which means that you cannot add notes to it and may need to switch between windows to see it on the computer. By having your own diagram, you will be able to take notes on it and quickly reference it as you work through the configuration section. Finally, drawing the Layer 2 and Layer 3 topologies will help you become familiar with a complex network toplogy at first sight.

---

1. Perimeter Security and Services

1.1 ASA Routed Mode (3 points)

- Configure ASA1 in routed single mode with a hostname of **ASA12**, using the information from the table:

Interface1	Nameif	Security Level	IPv4 Address
Red1	INSIDE	90	172.16.6.1/24
Red1.15	DMZ	50	155.1.15.Y/24

https://t.me/learningnets

Interface1	Nameif	Security Level	IPv4 Address
Red1.25	OUTSIDE	10	155.1.25.Y/241

- Enable OSPF and EIGRP in AS 500 according to the diagram.
- Redistribute OSPF into EIGRP, and advertise 150.1.0.0/16 and 155.1.0.0/16 into area 55.
- Without redistributing OSPF into EIGRP, ensure that there is IP connectivity between the routing domains.
- No static routes are allowed for this task.
- Match the following output:

```
ASA12# show interface redundant1 | b Redundancy

      Redundancy Information:
            Member Ethernet0/0(Active), Ethernet0/2
            Last switchover at 07:03:31 UTC Apr 11 2014
```

1.2 ASA Active-Standby Failover (3 points)

- Configure ASA1 and ASA2 for stateful failover, matching the following output from ASA1:

```
ASA12/act# show failover

    Failover On
    Failover unit Primary
    Failover LAN Interface: FAILOVER Redundant2 (up)
    Unit Poll frequency 1 seconds, holdtime 15 seconds
    Interface Poll frequency 5 seconds, holdtime 25 seconds
    Interface Policy 1
    Monitored Interfaces 3 of 110 maximum
    failover replication http
    Version: Ours 8.2(5), Mate 8.2(5)
    Last Failover at: 08:13:18 UTC Apr 11 2014
            This host: Primary - Active
                    Active time: 1314 (sec)
```

https://t.me/learningnets

```
                slot 0: ASA5510 hw/sw rev (1.1/8.2(5)) status (Up Sys)
                  Interface DMZ (155.1.15.15): Normal (Waiting)
                  Interface OUTSIDE (155.1.25.15): Normal (Waiting)
                  Interface INSIDE (172.16.6.1): Normal (Waiting)
                slot 1: empty
        Other host: Secondary - Failed
                Active time: 0 (sec)
                slot 0: ASA5510 hw/sw rev (2.0/8.2(5)) status (Up Sys)
                  Interface DMZ (155.1.15.16): No Link (Waiting)
                  Interface OUTSIDE (155.1.25.16): No Link (Waiting)
                  Interface INSIDE (172.16.6.2): No Link (Waiting)
                slot 1: empty

Stateful Failover Logical Update Statistics
        Link : FAILOVER Redundant2 (up)
```

- Use VLAN 202 for failover with IPv4 addressing in the format 155.1.202.Y/24.

1.3 ASA Multiple Context Routed (3 points)

- Configure ASA3 in routed multiple mode with a hostname of **ASA34**, using the information from the table:

Interface	Nameif	Security Level	IPv4 Address	Context Name	Context File
Po1.34	OUTSIDE	20	155.1.34.18/24	ACS	ACS.cfg
Po1.34	OUTSIDE	20	155.1.34.17/24	ISE	ISE.cfg
Po1.110	INSIDE	80	172.16.1.1/24	ACS	ACS.cfg
Po1.130	INSIDE	80	172.16.3.1/24	ISE	ISE.cfg

- Match the following output:

https://t.me/learningnets

```
ASA34/ACS# show interface | i Interface|System

    Interface OUTSIDE "OUTSIDE", is up, line protocol is up
            System name Port-channel1.34, VLAN identifier 34
    Interface INSIDE "INSIDE", is up, line protocol is up
            System name Port-channel1.110, VLAN identifier 110
    !
    !ASA34/ISE# show interface | i Interface|System

    Interface OUTSIDE "OUTSIDE", is up, line protocol is up
            System name Port-channel1.34, VLAN identifier 34
    Interface INSIDE "INSIDE", is up, line protocol is up
            System name Port-channel1.130, VLAN identifier 130
```

- Configure ASA3 and SW2 to match the output:

```
ASA34# show port-channel 1

    Ports: 2   Maxports = 16
    Port-channels: 1 Max Port-channels = 48
    Protocol: LACP/ active
    Minimum Links: 2
    Maximum Bundle: 8
    Load balance: src-dst-ip-port
```

1.4 ASA Active-Active Failover (3 points)

- Configure ASA3 and ASA4 for stateful failover so that ASA3 is forwarding for context **ISE** and ASA4 for context **ACS**.
- Match the following output:

```
ASA34/pri/ISE/act# show failover

    Failover On
    Last Failover at: 10:21:09 UTC Apr 11 2014
            This context: Active
                    Active time: 69 (sec)
                      Interface OUTSIDE (155.1.34.17): Normal (Monitored)
                      Interface INSIDE (172.16.3.1): Normal (Monitored)
            Peer context: Standby Ready
                    Active time: 0 (sec)
```

https://t.me/learningnets

```
                    Interface OUTSIDE (155.1.34.200): Normal (Monitored)
                    Interface INSIDE (172.16.3.2): Normal (Monitored)


ASA34/sec/ACS/act# show failover

    Failover On
    Last Failover at: 10:21:05 UTC Apr 11 2014
            This context: Active
                    Active time: 116 (sec)
                      Interface OUTSIDE (155.1.34.18): Normal (Monitored)
                      Interface INSIDE (172.16.1.1): Normal (Monitored)
            Peer context: Standby Ready
                    Active time: 0 (sec)
                      Interface OUTSIDE (155.1.34.100): Normal (Monitored)
                      Interface INSIDE (172.16.1.2): Normal (Monitored)
```

- Use VLAN 101 for failover with IPv4 addressing in the format 155.1.101.Y/24.
- Configure SW1 to match the following output on both ASA3 and ASA4:

```
ASA34/pri/act# show port-channel 2

    Ports: 2   Maxports = 16
    Port-channels: 2 Max Port-channels = 48
    Protocol: ON
    Minimum Links: 1
    Load balance: src-dst-ip
```

1.5 ASA Multiple Context Resource Management (1 points)

- To protect from resource exemption, configure the following limits for the two contexts:
  - allow a maximum of 1000 new connections per second.
  - allow a maximum of 5000 concurrent connections for **ISE** and 10000 for **ACS** .
  - allow a maximum of 50 concurrent hosts for **ISE** and 100 for **ACS**.

https://t.me/learningnets

1.6 IOS ZBPF Routed (3 points)

- Configure ZBPF on R4 to match the following requirements:
  - Fa0/0.41 interface is a member of the **TRUSTED** zone while Fa0/0.15, Fa0/1.43, and Fa0/1.48 interfaces are members of the **UNTRUSTED** zone.
  - all TCP/ICMP/UDP traffic passing through the router should create entries in the firewall state table.
  - all PING/TELNET/SSH traffic from the **UNTRUSTED** zone destined to the router should create entries in the firewall state table.
  - all firewall rules required for other tasks should create entries in the firewall state table if supported.
  - ensure that policy from **TRUSTED** to **UNTRUSTED** applies only for VLAN 41 subnet and that FTP/TFTP is functional.
  - log a message for packets dropped by the inspection engine.

1.7 IOS Network Address Translation (3 points)

- Configure NAT for **TEST-SRV-A** on R4 to match the output:

```
R4#show ip nat translations

    Pro Inside global      Inside local       Outside local      Outside global
    --- 155.1.43.100       172.16.10.100      ---                ---
    --- 155.1.15.100       172.16.10.100      ---                ---
    --- 155.1.48.100       172.16.10.100      ---                ---
```

- Configure ZBPF rules on R4 to allow telnet, http, and https sessions from the **UNTRUSTED** zone to **TEST-SRV-A** only if sourced from 155.1.99.0/24, 172.16.5.0/24, or 155.1.10.0/24.
- For testing purposes, match the output:

```
SW3#telnet 155.1.43.100 /source-interface vlan99

    Trying 155.1.43.100 ... Open
    Kerberos: No default realm defined for Kerberos!
    Welcome to Microsoft Telnet Service

    login: Administrator
```

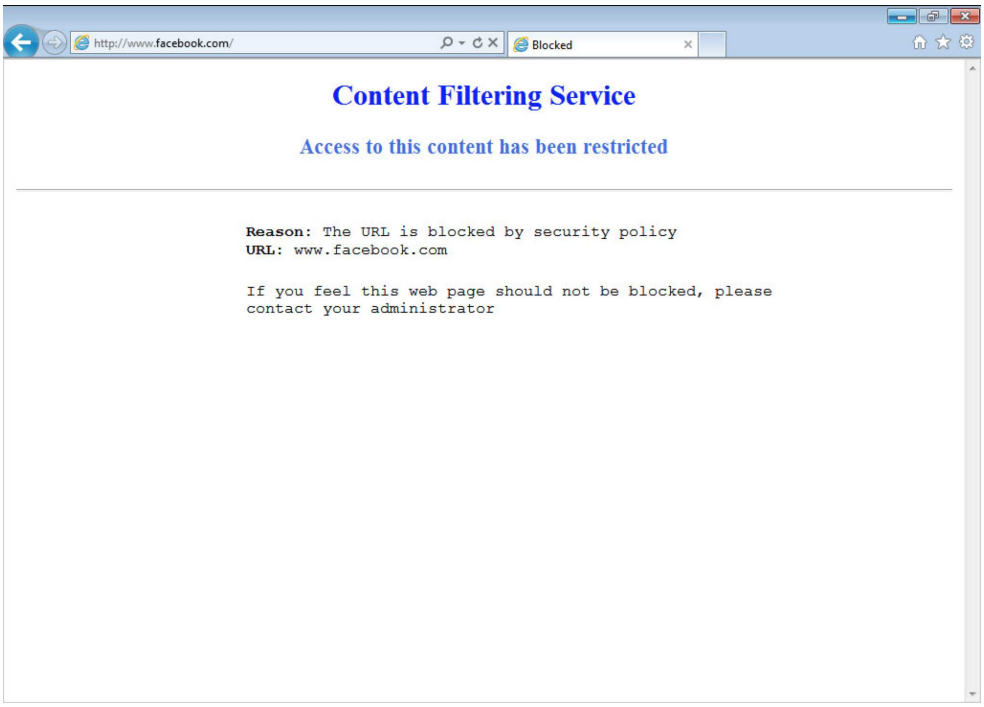
https://t.me/learningnets

```
password:


*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\Administrator>
```

1.8 IOS ZBPF Local URL Filtering (4 points)

- Configure R4 to deny HTTP traffic on port 80 and 8080 from the **UNTRUSTED** zone to the **TRUSTED** zone if the requested URL is for **.reddit.com** or **.facebook.com**.
- Additionally, log a message and present the following answer to the user for either of the two destinations:



- For testing purposes, configure **TEST-PC-B** in VLAN 99 with a DNS server of **150.1.1.1** and access **www.facebook.com** or **www.reddit.com**.

1.9 ASA URL Filtering (1 points)

- Configure **ISE** context for HTTP/HTTPS URL filtering for its **INSIDE** users using a WebSense server located at **172.16.3.99**.
  - if the filtering server is down, all HTTP/HTTPS requests should be allowed.
  - ensure that users accessing websites via external proxies are blocked by

https://t.me/learningnets

this policy.

2. Intrusion Prevention and Content Security

2.1 IPS Initialization (2 points)

- Initialize the IPS using the information from the table:

Variables	Values
Hostname	IPS4240
IPv4 Address	155.1.99.100/24
Default Gateway	155.1.99.11
Telnet	Enable
Management Access	155.1.99.0/24
Management Type	HTTPS Port 443

- Enable automatic IP logging for the default signature definition set as follows:
  - 500 packets
  - 2 minutes
  - 16000 bytes

2.2 IPS Promiscuous Mode (2 points)

- Configure SW3 to send a copy of VLAN 41 traffic to the Gi0/0 interface of IPS for inspection.
  - IPS should send dot1q-tagged TCP resets for this traffic, if required.

- Configure SW5 to send a copy of WiFi user traffic to the Gi0/1 interface of IPS for

https://t.me/learningnets

inspection.
    - use VLAN 150 for this scope.
    - do not accept inbound TCP resets from Gi0/1, but IPS should be able to generate TCP resets.

- All traffic should be inspected with the default signature set.

2.3 IPS Blocking (4 points)

- Configure IPS to block malicious WiFi hosts from subnet 172.16.5.0/24 through integration with WLC and ASA3 **ISE** Context.
    - use SSH for ASA communication and the username/password pair of **asauser/asapass**.
    - for WLC communication use the username/password pair of **wlcuser/1qaz2wsx**.

- Manually configure WiFi client 172.16.5.150 to be permanently blocked by the sensor.
- For testing purposes, tune the **ICMP Echo** signature with following actions:
    - produce alert.
    - block host.
    - log attacker packets.

2.4 WSA Initialization (2 points)

- Initialize the WSA using the information from the table:

Variables	Values
Hostname	wsa.inelab.local
DNS Server	150.1.4.4
NTP Server	150.1.4.4
Proxy Ports	M1 and P1

https://t.me/learningnets

Variables	Values
M1 IPv4 Address	172.16.6.100/24
M1 Default Gateway	172.16.6.1
Admin Password	default1A
Email Address	ccielab@inelab.local
Senderbase Participation	Minimum
Global Policy Action	Block
Global Policy WBRS	Disabled

- Assign **TEST-PC-B** an IPv4 address from VLAN 99 for this scope.
- Ensure that all hosts from VLAN 99 can manage the WSA over HTTPS on port 8883.
- Do not configure any NAT statements for this task.

2.5 WSA WCCP Integration (3 points)

- Configure R4 to redirect all HTTP and HTTPS traffic on ports 443 and 4443 from users in VLAN 99 to the WSA as it exits its VLAN 48 interface.
- Restrict the WCCP clients accepted by R4 and match the following output:

```
R4#show tunnel groups wccp

     WCCP : service group 351 in "Default", ver v2, assgnmnt: mask-value set
       intf: Tunnel0, locally sourced
```

2.6 WSA Traffic Policies (3 points)

- Define an HTTP Access Policy with the following conditions:

https://t.me/learningnets

- match on default identity.
- it applies only for users in VLAN 99 if protocol is HTTP/HTTPS.

- Ensure that users in VLAN 99 have access to **http://www.linkedin.com** and **https://www.linkedin.com:4443**.
- For testing purposes, on **TEST-PC-B** use a DNS server of 150.1.4.4 and match the output:

```
R1#show ip http server history


    HTTP server history:
    local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes  end-time
          150.1.1.1:4443     172.16.6.100:24990 0          0          09:45:22 04/13
          150.1.1.1:80       172.16.6.100:63593 355        137        09:45:58 04/13
```

2.7 WSA Application Control (2 points)

- Configure the WSA to restrict file upload to Google Mail service:
  - enable accurate detection of applications using HTTPS protocol.

- The above configured policy causes Google Talk service to stop working:
  - fix this by configuring WSA to not decrypt sessions destined for the **talk.google.com** domain or any of its sub-domains.

3. **Confidentiality and Secure Access**

3.1 IOS PKI Server (3 points)

https://t.me/learningnets

- Configure a PKI infrastructure with R4 as ROOT-CA and R3 as a SUB-CA:
  - use RSA keys of 2048 bits and generate new keys for each re-enrollment.
  - use SHA1 as signature algorithm.
  - use a lifetime of 1095 days for all certificates.
  - store the SN and Subject Name for each issued certificate in the database.
  - use **ccielabpassword** as the password to protect the CA certificate and key.
  - automatically renew all certificates 72 days prior to expiry date.
  - automatically grant client certificates.

- Use R4 as the NTP server.
- If additional firewall rules are required, use only Loopback0 IP addresses.

3.2 IKEv1 VPN Address Overlapping (3 points)

- Using the default IKEv1/IPsec policies, configure an IPsec tunnel between R3 and R5 to protect traffic between VLAN 33 and VLAN 55.
- Use RSA-SIG authentication, and consider R3 as the CA server.
- Both routers should be able to initiate the session.
- Match the following output:

https://t.me/learningnets

```
R5#show crypto session

    Crypto session current status

    Interface: FastEthernet0/0.60
    Session status: UP-ACTIVE
    Peer: 150.1.3.3 port 500
      IKEv1 SA: local 150.1.5.5/500 remote 150.1.3.3/500 Active
      IPSEC FLOW: permit ip 155.1.55.0/255.255.255.0 155.1.33.0/255.255.255.0
            Active SAs: 2, origin: crypto map

R3#ping 155.1.55.5 source fastEthernet0/1.33

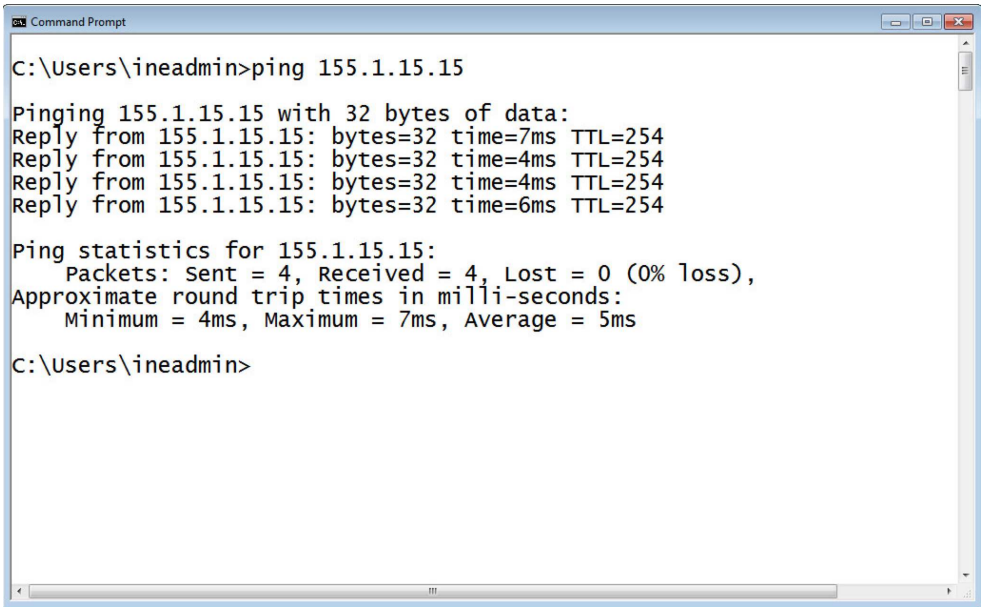

    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 155.1.55.5, timeout is 2 seconds:
    Packet sent with a source address of 155.1.35.3
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

3.3 IKEv1 VPN Remote Access (3 points)

- Configure R4 as EzVPN server for clients in VLAN 99 as follows:
  - use Loopback0 interface of R4 for the VPN session.
  - use AES 128 bits, SHA1, DH group 2, a PSK of **CISCO**, and group name of **EZVPN_CLIENT**.
  - allocate IPv4 addresses from 155.1.130.0/24 subnet.
  - tunnel only traffic destined to VLAN 15.
  - for XAUTH, use the username/password pair **EZVPN_USER/EZVPN_PASSWORD**.

- Without using any static routes or RRI, match the following output after the VPN session is established successfully:

https://t.me/learningnets



3.4 VRF Aware DMVPN Phase3 Troubleshooting (4 points)

- R4 is the HUB for two DMVPN Phase3 clouds:
  - cloud with network-id of **124** between R1, R2, and R4; R1 and R2 source the tunnel interface from a VRF named **MGMT**.
  - cloud with network-id of **345** between R3, R4, and R5.
  - between spokes of both DMVPN clouds, Loopback1 prefixes in the format of Y.Y.Y.Y/32 are advertised through EIGRP AS 124 in cloud **124** and EIGRP AS 345 in cloud **345**.

- Without using ISAKMP profiles on the hub, fix the configuration so that spoke-to-spoke tunnels are established.
- For verification, match the following output on R1:

```
R1#ping 2.2.2.2 source loopback1 repeat 10
    Type escape sequence to abort.
    Sending 10, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
    Packet sent with a source address of 1.1.1.1
    !!!!!!!!!!
    Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/4 ms

R1#show dmvpn

    Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
            N - NATed, L - Local, X - No Socket
            # Ent --> Number of NHRP entries with same NBMA peer
```

https://t.me/learningnets

```
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
    ==========================================================================

    Interface: Tunnel124, IPv4 NHRP Details
    Type:Spoke, NHRP Peers:2,

     # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
     ----- --------------- --------------- ----- -------- -----
         2       150.1.2.2      31.31.31.2    UP 00:02:59   DT2
                                31.31.31.2    UP 00:02:59     D
         1       150.1.4.4      31.31.31.4    UP 00:04:28     S
```

- For verification, match the following output on R3:

```
R3#ping 5.5.5.5 source loopback1 repeat 10

    Type escape sequence to abort.
    Sending 10, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
    Packet sent with a source address of 3.3.3.3
    !!!!!!!!!!
    Success rate is 100 percent (10/10), round-trip min/avg/max = 8/16/36 ms

R3#show dmvpn

    Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
            N - NATed, L - Local, X - No Socket
            # Ent --> Number of NHRP entries with same NBMA peer
            NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
            UpDn Time --> Up or Down Time for a Tunnel
    ==========================================================================

    Interface: Tunnel345, IPv4 NHRP Details
    Type:Spoke, NHRP Peers:2,

     # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
     ----- --------------- --------------- ----- -------- -----
         2       150.1.5.5      41.41.41.5   IKE 00:02:46     D
                                41.41.41.5   IKE 00:02:46     D
         1       150.1.4.4      41.41.41.4    UP 00:03:21     S
```

https://t.me/learningnets

3.5 VRF-Aware GETVPN Deployment (4 points)

- There is a GET VPN deployment between R1, R2 and R4:
  - R1 and R2 must be configured as GMs to encrypt traffic in VRF **RED** and **GREEN**.
  - R4 has been pre-configured as the KS for each VRF; do not modify the GET VPN configuration on it.

- Configure R1 and R2 to match the output after successful registration to the KS:

```
R1#show crypto gdoi ipsec sa


    SA created for group VRF_RED_GROUP:
      GigabitEthernet0/1.11:
        protocol = ip
          local ident  = 150.1.0.0/16, port = 0
          remote ident = 150.1.0.0/16, port = 0
          direction: Both, replay: Disabled

    SA created for group VRF_GREEN_GROUP:
      GigabitEthernet0/1.22:
        protocol = ip
          local ident  = 150.11.0.0/16, port = 0
          remote ident = 150.11.0.0/16, port = 0
          direction: Both, replay: Disabled

R2#show crypto gdoi ipsec sa


    SA created for group VRF_RED_GROUP:
      GigabitEthernet0/1.33:
        protocol = ip
          local ident  = 150.1.0.0/16, port = 0
          remote ident = 150.1.0.0/16, port = 0
          direction: Both, replay: Disabled

    SA created for group VRF_GREEN_GROUP:
      GigabitEthernet0/1.44:
        protocol = ip
          local ident  = 150.11.0.0/16, port = 0
          remote ident = 150.11.0.0/16, port = 0
```

https://t.me/learningnets

```
          direction: Both, replay: Disabled
```

- Ensure that PING works between R1, R2, an SW6 on both VRF **RED** and **GREEN**.
- For example, the following should be functional on R1:

```
R1#ping vrf RED 150.1.1.14
    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 150.1.1.14, timeout is 2 seconds:
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping vrf RED 150.1.2.2

    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping vrf GREEN 150.11.1.14
    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 150.11.1.14, timeout is 2 seconds:
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping vrf GREEN 150.11.2.2

    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 150.11.2.2, timeout is 2 seconds:
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

4. Identity Management

4.1 ASA LDAP Authentication (3 points)

- Configure ASA1 to authenticate telnet sessions via LDAP server on **TEST-SRV-A**.
  - use **ldapuser** with the password **1qaz@WSX**, which resides in the **Users** organizational unit, to query the LDAP server.

https://t.me/learningnets

- For testing purposes, allow telnet sessions from R5's Loopback0:
  - authenticate with user **USER3** and the password **1qaz@WSX**.
  - **USER3** has the LDAP attribute of **Department** with a value of **CCIELAB**.
  - authorize the user for **show nameif** and **show route** commands at privilege-level 11.

4.2 IOS TACACS Command Authorization and Accounting (3 points)

- Configure R1 to authenticate, authorize, and account for VTY lines access with the ACS server as follows:
  - use a multiplexed connection with source of **Loopback0** and a key of **cisco**.
  - upon successful authentication, user **ADMIN** should be assigned privilege-level **8** but allowed access to privilege-level **15**.
  - allow the user **ADMIN** with the password **CISCO** unrestricted access to all privilege-level 15 commands except routing protocol configuration.
  - all privilege-level 15 commands issued by the user should be accounted for on the ACS server.

- Ensure that administrators from VLAN 99 can manage the ACS via HTTPS.
- Match the following output:

```
ASA34/sec/ACS/act# show xlate

    1 in use, 1 most used
    Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
    NAT from INSIDE:172.16.1.100 to OUTSIDE:155.1.34.110
        flags s idle 0:00:25 timeout 0:00:00
```

4.3 IOS RADIUS Authentication and Accounting (3 points)

- Configure R4 to authenticate and authorize exec sessions for VTY lines access with the ACS server as follows:
  - use RADIUS with source of **Loopback0** and a key of **cisco**.
  - upon successful authentication, user **RADIUS** should be assigned privilege-level **8** but allowed access to privilege-level **15**.

https://t.me/learningnets

- allow the user **RADIUS** with the password **CISCO** unrestricted access to all commands and account for exec sessions.

4.4 IOS User-Based Firewall (3 points)

- Configure R4 to authenticate users before allowing access from the **TRUSTED** zone to the **UNTRUSTED** zone.
- Use RADIUS server from ACS for this scope and match the output:

```
R4#show user-group

    Usergroup : ZBPF_GROUP
    ------------------------------------------------------------------------
    User Name       Type     Interface              Learn         Age (min)
    ------------------------------------------------------------------------
    172.16.10.100   IPv4     FastEthernet0/0.41     Dynamic         4
```

4.5 ISE 802.1x Wireless Authentication (5 points)

- Configure a WLAN on the WLC with the following parameters:

Variables	Values
Profile	CCIELAB
SSID	CCIE-TEST-RACK-X
Hide SSID	Yes
Authentication	WPA+WPA2 PSK
Encryption	AES and TKIP
Authentication Server	ISE

https://t.me/learningnets

Variables	Values
Authentication Username	WIFIUSER
Authentication Password	Cisco123!
Interface Name	Management
Interface IPv4 Address	190.1.111.100
WLC DHCP Server	No
IPv4 Subnet	172.16.5.0/24
Default Gateway	172.16.5.1

- Configure RADIUS for secure delivery of the derived PMK (pairwise master key).
- Authentication against ISE server should be performed using PEAP(EAP-MSCHAPv2).
- Upon successful authentication, ISE should authorize the user for full access through the use of ACL.
- Ensure that administrators from VLAN 99 can manage ISE and WLC via HTTPS.
- Match the following output:

```
ASA34/pri/ISE/act# show xlate

    1 in use, 1 most used
    Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
    NAT from INSIDE:172.16.3.100 to OUTSIDE:155.1.34.130
        flags s idle 0:00:04 timeout 0:00:00
```

5. System Hardening and Availability

https://t.me/learningnets

5.1 IOS RMON Alarms (3 points)

- Configure R3 to monitor the rate of packets entering its interface connecting to VLAN 33 based on the total input packet counter **ifEntry.11**.
  - if the rate is above 100 packets per minute, generate the log message **VLAN33 Interface Congested** and send a trap to the management host at 172.16.6.55.
  - use the SNMP community string **CISCO** and a source of Loopback0.
  - when the packet rate falls below 50 packets per minute, generate another log message **VLAN33 Interface UnCongested** and send a corresponding trap.
  - the owner of events should be set to **CISCO**.

5.2 IP Options Security (3 points)

- Configure R3 to drop all packets with IP options enabled, without using ACL filtering.
- Configure ASA1 to clear IP options from packets between VLAN 50 and VLAN 70.

5.3 IOS Selective Packet Discard (2 points)

- Configure Selective Packet Discard on R3 as follows:
  - enable SPD aggressive mode.
  - increase R3's input queue size on its link to VLAN 33 to twice the default.
  - increase the amount of the memory headroom for IGP packets to 150 buffers.
  - set the headroom for BGP packets to 120 packets.
  - start dropping low-priority packets randomly when the input queue is 50% full.

5.4 IOS Netflow Sampling (3 points)

- Configure R3 to collect Netflow statistics outbound on its VLAN 39 interface:
  - it samples every tenth packet in each flow.
  - it samples every packet for traffic between VLAN 70 and VLAN 20.

5.5 IOS Control Plane Security (3 points)

https://t.me/learningnets

- Configure the following on R3:
  - drop packets going to all closed ports, except TCP 4040 and 5050.
  - to reduce the effect of broadcast storms, limit the rate of input non-IP packets to 150 per second with a burst value of 30 packets.
  - limit the rate of ICMP packets destined to R3 to 20 per second with a burst value of 5 packets.
  - ensure that all fragmented packets transiting the router are limited to 1 Mpps with a burst value of 0.2Mpps.

6. Threat Identification and Mitigation

6.1 ASA IP Spoofing Prevention (2 points)

- Configure ASA firewalls to drop all IP packets with spoofed sources not matching the routing table.

6.2 IOS ARP Spoofing Prevention (2 points)

- Configure SW1 to defend against ARP spoofing in VLAN 10:
  - do not check the DHCP snooping table.
  - validate MAC addresses from the ARP payload against MAC addresses from the Ethernet header.

- A log message similar to the following should be triggered for ARP traffic from R1:

```
%SW_DAI-6-ACL_PERMIT: 1 ARPs (Res) on Fa1/0/1, vlan 10.([d48c.b5da.d548/155.1.10.1/001b.d58b.21c1/155.1.10.9/19:
```

6.3 IOS TCP DoS Prevention (3 points)

- A TCP SYN flooding attack has been detected against hosts in VLAN 50.
- Configure R5 to watch TCP sessions destined for hosts in this VLAN:
  - reset the TCP session if the connection has not established within 15 seconds.
  - start dropping partial connections when there are more than 1500 and stop dropping them when the number of partial connections falls below 1200.

https://t.me/learningnets

    - randomly drop sessions.

6.4 Layer 2 Security (2 points)

- VLAN 41 has been flooded with spoofed IP packets and non-IP packets from **TEST-SRV-A**.
- Configure interface Fa1/0/4 to drop all malicious traffic.

6.5 ASA ICMP Flooding (1 points)

- ASA3 has been flooded with ICMP Echo Request packets destined to itself on the **OUTSIDE** interface.
- Configure it so that it drops all inbound ICMP Echo Request traffic.

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 5

CCIE SCv4 Lab 5 Solutions Section 1

1. Task 1.1 Solution
2. Task 1.2 Solution
3. Task 1.3 Solution
4. Task 1.4 Solution
5. Task 1.5 Solution
6. Task 1.6 Solution
7. Task 1.7 Solution
8. Task 1.8 Solution
9. Task 1.9 Solution

Task 1.1 Solution

SW2:

```
 interface range FastEthernet1/0/12 - 13
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 15,25,60
  switchport trunk native vlan 15
  switchport mode trunk
  no shutdown
```

ASA1:

```
hostname ASA12
!
interface Ethernet0/0
 no shutdown
!
interface Ethernet0/2
 no shutdown
!
interface Redundant1
 member-interface Ethernet0/0
 member-interface Ethernet0/2
```

https://t.me/learningnets

```
!
interface Redundant1
 nameif DMZ
 security-level 50
 ip address 155.1.15.15 255.255.255.0
 ospf message-digest-key 1 md5 ospfkey
 ospf authentication message-digest
!
interface Redundant1.25
 vlan 25
 nameif OUTSIDE
 security-level 10
 ip address 155.1.25.15 255.255.255.0
 ospf authentication-key ospfkey
 ospf authentication
!
interface Redundant1.60
 vlan 60
 nameif INSIDE
 security-level 90
 ip address 172.16.6.1 255.255.255.0
!
router ospf 500
 network 155.1.15.0 255.255.255.0 area 0
 network 155.1.25.0 255.255.255.0 area 55
 area 0 range 150.1.0.0 255.255.0.0
 area 0 range 155.1.0.0 255.255.0.0
 default-information originate always
!
router eigrp 500
 no auto-summary
 network 172.16.6.0 255.255.255.0
 redistribute ospf 500 metric 100000 100 255 1 1500
```

Task 1.1 Verification

Verify that switch interfaces are in trunk with the correct native VLAN:

```
SW2#show interfaces fastEthernet1/0/12 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/12    on               802.1q         trunking      15

Port        Vlans allowed on trunk
```

https://t.me/learningnets

```
Fa1/0/12    15,25,60

Port        Vlans allowed and active in management domain
Fa1/0/12    15,25,60

Port        Vlans in spanning tree forwarding state and not pruned Fa1/0/12     15,25,60
!
!SW2#show interfaces fastEthernet1/0/13 trunk


Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/13    on               802.1q         trunking      15

Port        Vlans allowed on trunk
Fa1/0/13    15,25,60

Port        Vlans allowed and active in management domain
Fa1/0/13    15,25,60

Port        Vlans in spanning tree forwarding state and not pruned Fa1/0/13     15,25,60
```

Verify security-level, nameif, and IPv4 addressing:

https://t.me/learningnets

```
ASA12# show nameif

Interface               Name                    Security
Redundant1              DMZ                      50
Redundant1.25           OUTSIDE                  10
Redundant1.60           INSIDE                   90
!
!ASA12# show ip address

System IP Addresses:
Interface               Name                    IP address      Subnet mask     Method
Redundant1              DMZ                     155.1.15.15     255.255.255.0   manual
Redundant1.25           OUTSIDE                 155.1.25.15     255.255.255.0   manual
Redundant1.60           INSIDE                  172.16.6.1      255.255.255.0   manual
Current IP Addresses:
Interface               Name                    IP address      Subnet mask     Method
Redundant1              DMZ                     155.1.15.15     255.255.255.0   manual
Redundant1.25           OUTSIDE                 155.1.25.15     255.255.255.0   manual
Redundant1.60           INSIDE                  172.16.6.1      255.255.255.0   manual
```

Verify the EIGRP and OSPF neighbors, as well as routing table entries:

```
ASA12# show ospf neighbor



Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.4.4         1   FULL/BDR        0:00:37     155.1.15.4      DMZ
150.1.3.3         1   FULL/BDR        0:00:37     155.1.25.3      OUTSIDE
!
!ASA12# show eigrp neighbors

EIGRP-IPv4 neighbors for process 500
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   172.16.6.5              Red1.60          14  00:35:37 2    200   0   8
!
!ASA12# show route INSIDE



Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

https://t.me/learningnets

```
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
D    172.16.5.0 255.255.255.0 [90/28416] via 172.16.6.5, 0:35:49, INSIDE
C    172.16.6.0 255.255.255.0 is directly connected, INSIDE
D    150.1.5.5 255.255.255.255 [90/130816] via 172.16.6.5, 0:35:49, INSIDE
!
!ASA12# show route OUTSIDE


Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    155.1.25.0 255.255.255.0 is directly connected, OUTSIDE
O    155.1.20.0 255.255.255.0 [110/12] via 155.1.25.3, 0:30:25, OUTSIDE
O    155.1.34.0 255.255.255.0 [110/12] via 155.1.25.3, 0:30:25, OUTSIDE
O    155.1.39.0 255.255.255.0 [110/11] via 155.1.25.3, 0:30:25, OUTSIDE
O    150.1.10.10 255.255.255.255 [110/12] via 155.1.25.3, 0:30:25, OUTSIDE
O    150.1.3.3 255.255.255.255 [110/11] via 155.1.25.3, 0:30:25, OUTSIDE
O    150.1.2.2 255.255.255.255 [110/13] via 155.1.25.3, 0:30:25, OUTSIDE
!
!ASA12# show route DMZ

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
O    155.1.10.0 255.255.255.0 [110/12] via 155.1.15.4, 0:31:49, DMZ

C    155.1.15.0 255.255.255.0 is directly connected, DMZ
O    155.1.48.0 255.255.255.0 [110/11] via 155.1.15.4, 0:31:49, DMZ
```

https://t.me/learningnets

```
O    155.1.43.0 255.255.255.0 [110/11] via 155.1.15.4, 0:31:49, DMZ
O    155.1.70.0 255.255.255.0 [110/12] via 155.1.15.4, 0:31:49, DMZ
O    155.1.99.0 255.255.255.0 [110/12] via 155.1.15.4, 0:31:49, DMZ
O    172.16.10.0 255.255.255.0 [110/11] via 155.1.15.4, 0:31:49, DMZ
O    150.1.11.11 255.255.255.255 [110/12] via 155.1.15.4, 0:31:49, DMZ
O    150.1.9.9 255.255.255.255 [110/12] via 155.1.15.4, 0:31:49, DMZ
O    150.1.4.4 255.255.255.255 [110/11] via 155.1.15.4, 0:31:49, DMZ
O    150.1.1.1 255.255.255.255 [110/13] via 155.1.15.4, 0:31:49, DMZ
```

Verify that OSPF authentication is enabled:

```
ASA12# show ospf interface OUTSIDE


OUTSIDE is up, line protocol is up
  Internet Address 155.1.25.15 mask 255.255.255.0, Area 55
  Process ID 500, Router ID 172.16.6.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.6.1, Interface address 155.1.25.15
  Backup Designated router (ID) 150.1.3.3, Interface address 155.1.25.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 0:00:03
  Index 1/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 11
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 150.1.3.3  (Backup Designated Router)
  Suppress hello for 0 neighbor(s) Simple password authentication enabled
!
!ASA12# show ospf interface DMZ


DMZ is up, line protocol is up
  Internet Address 155.1.15.15 mask 255.255.255.0, Area 0
  Process ID 500, Router ID 172.16.6.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.6.1, Interface address 155.1.15.15
  Backup Designated router (ID) 150.1.4.4, Interface address 155.1.15.4
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 0:00:07
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 7
  Last flood scan time is 0 msec, maximum is 0 msec
```

https://t.me/learningnets

```
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 150.1.4.4  (Backup Designated Router)
  Suppress hello for 0 neighbor(s) Message digest authentication enabled
Youngest key id is 1
```

Verify that OSPF prefixes are redistributed into EIGRP:

```
R5#show ip route eigrp

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      150.1.0.0/16 is variably subnetted, 9 subnets, 2 masks
D EX     150.1.0.0/16 [170/53760] via 172.16.6.1, 00:34:39, FastEthernet0/0.60
D EX     150.1.1.1/32 [170/53760] via 172.16.6.1, 00:34:39, FastEthernet0/0.60
D EX     150.1.2.2/32 [170/53760] via 172.16.6.1, 00:33:09, FastEthernet0/0.60
D EX     150.1.3.3/32 [170/53760] via 172.16.6.1, 00:33:09, FastEthernet0/0.60
D EX     150.1.4.4/32 [170/53760] via 172.16.6.1, 00:34:39, FastEthernet0/0.60
D EX     150.1.9.9/32 [170/53760] via 172.16.6.1, 00:34:39, FastEthernet0/0.60
```

Verify that the default route is originated into OSPF, and that the requested summaries are present in area 55:

```
R3#show ip route ospf

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 155.1.25.15 to network 0.0.0.0
```

https://t.me/learningnets

```
O*E2  0.0.0.0/0 [110/1] via 155.1.25.15, 00:35:49, FastEthernet0/0.25

      150.1.0.0/16 is variably subnetted, 4 subnets, 2 masks
O IA     150.1.0.0/16 [110/12] via 155.1.25.15, 00:35:49, FastEthernet0/0.25
O        150.1.2.2/32 [110/3] via 155.1.39.10, 10:52:42, FastEthernet0/0.39
O        150.1.10.10/32 [110/2] via 155.1.39.10, 10:52:42, FastEthernet0/0.39
      155.1.0.0/16 is variably subnetted, 9 subnets, 3 masks
O IA     155.1.0.0/16 [110/11] via 155.1.25.15, 00:35:49, FastEthernet0/0.25
O        155.1.20.0/24 [110/2] via 155.1.39.10, 10:52:42, FastEthernet0/0.39
O        155.1.34.0/24 [110/2] via 155.1.39.10, 10:52:42, FastEthernet0/0.39
      172.16.0.0/24 is subnetted, 1 subnets
O IA     172.16.10.0 [110/12] via 155.1.25.15, 00:35:49, FastEthernet0/0.25
!
!R4#show ip route ospf | i 0.0.0.0
Gateway of last resort is 155.1.15.15 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 155.1.15.15, 00:38:00, FastEthernet0/0.15
```

Verify that the requested output is being matched:

```
ASA12/act# show interface redundant1 | b Redundancy

  Redundancy Information:
        Member Ethernet0/0(Active), Ethernet0/2
        Last switchover at 07:03:31 UTC Apr 11 2014
```

Task 1.2 Solution

```
SW2:
 interface range FastEthernet1/0/14 - 15
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 15,25,60
  switchport trunk native vlan 15
  switchport mode trunk
  no shutdown

SW1:
vlan 202
!
interface range FastEthernet1/0/12 - 15
 switchport mode access
 switchport access vlan 202
 no shutdown
```

https://t.me/learningnets

ASA1:

```
prompt hostname state
!
interface Ethernet0/1
 no shutdown
!
interface Redundant2
 member-interface Ethernet0/1
!
interface Redundant1
 ip address 155.1.15.15 255.255.255.0 standby 155.1.15.16
!
interface Redundant1.25
 ip address 155.1.25.15 255.255.255.0 standby 155.1.25.16
!
interface Redundant1.60
 ip address 172.16.6.1 255.255.255.0 standby 172.16.6.2
!
failover lan unit primary
failover lan interface FAILOVER Redundant2
failover link FAILOVER Redundant2
failover interface ip FAILOVER 155.1.202.15 255.255.255.0 standby 155.1.202.16
failover replication http
failover
!
monitor-interface INSIDE
monitor-interface DMZ
monitor-interface OUTSIDE
```

ASA2:

```
interface Ethernet0/1
 no shutdown
!
interface Redundant2
 member-interface Ethernet0/1
!
failover lan unit secondary
failover lan interface FAILOVER Redundant2
failover link FAILOVER Redundant2
failover interface ip FAILOVER 155.1.202.15 255.255.255.0 standby 155.1.202.16
failover replication http
```

https://t.me/learningnets

```
failover
```

Task 1.2 Verification

Verify that switch interfaces are in access mode in VLAN 202:

```
SW1#show interfaces fastEthernet1/0/12 trunk


Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/12    off              negotiate      not-trunking  1

Port        Vlans allowed on trunk
Fa1/0/12    202

Port        Vlans allowed and active in management domain
Fa1/0/12    202

Port        Vlans in spanning tree forwarding state and not prunedFa1/0/12    202
!
!SW1#show spanning-tree vlan 202

VLAN0202
  Spanning tree enabled protocol ieee
  Root ID    Priority    16586
             Address     001b.d58b.2180
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    16586  (priority 16384 sys-id-ext 202)
             Address     001b.d58b.2180
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa1/0/12            Desg FWD 19        128.14   P2p
Fa1/0/13            Desg FWD 19        128.15   P2p
Fa1/0/14            Desg FWD 19        128.16   P2p
Fa1/0/15            Desg FWD 19        128.17   P2p

Fa1/0/20            Desg FWD 19        128.22   P2p
Fa1/0/21            Desg FWD 19        128.23   P2p
Fa1/0/22            Desg FWD 19        128.24   P2p
Fa1/0/23            Desg FWD 19        128.25   P2p
```

https://t.me/learningnets

```
Fa1/0/24            Desg FWD 19        128.26   P2p
```

Verify the IPv4 addressing for the failover interface:

```
ASA12/act(config)# show failover interface


        interface FAILOVER Redundant2
                System IP Address: 155.1.202.15 255.255.255.0 My IP Address     : 155.1.202.15
 Other IP Address : 155.1.202.16
```

Verify that the requested output is being matched:

https://t.me/learningnets

```
ASA12/act# show failover

Failover On
Failover unit Primary
Failover LAN Interface: FAILOVER Redundant2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 110 maximum
failover replication http
Version: Ours 8.2(5), Mate 8.2(5)
Last Failover at: 08:13:18 UTC Apr 11 2014
        This host: Primary - Active
                Active time: 1205 (sec)
                slot 0: ASA5510 hw/sw rev (1.1/8.2(5)) status (Up Sys)
                  Interface DMZ (155.1.15.15): Normal (Waiting)
                  Interface OUTSIDE (155.1.25.15): Normal (Waiting)
                  Interface INSIDE (172.16.6.1): Normal (Waiting)
                slot 1: empty
        Other host: Secondary - Failed
                Active time: 0 (sec)
                slot 0: ASA5510 hw/sw rev (2.0/8.2(5)) status (Up Sys)
                  Interface DMZ (155.1.15.16): No Link (Waiting)
                  Interface OUTSIDE (155.1.25.16): No Link (Waiting)
                  Interface INSIDE (172.16.6.2): No Link (Waiting)
                slot 1: empty

Stateful Failover Logical Update Statistics
        Link : FAILOVER Redundant2 (up)
```

Task 1.3 Solution

```
SW2:

interface range FastEthernet1/0/16 - 17
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 34,110,130
 switchport mode trunk
 channel-group 1 mode active
 no shutdown
```

https://t.me/learningnets

Convert ASA3 to multiple mode:

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]

ASA3 System Context:
hostname ASA34
!
interface GigabitEthernet0/0
 no shutdown
 channel-group 1 mode active
!
interface GigabitEthernet0/2
 no shutdown
 channel-group 1 mode active
!
interface Port-channel1
 port-channel load-balance src-dst-ip-port
 port-channel min-bundle 2
!
interface Port-Channel1.34
 vlan 34
!
interface Port-Channel1.110
 vlan 110
!
interface Port-Channel1.130
 vlan 130
!
delete /noconfirm disk0:/*.cfg
!
context ACS
 allocate-interface Port-Channel1.34 OUTSIDE visible
 allocate-interface Port-Channel1.110 INSIDE visible
 config-url disk0:/ACS.cfg
!
context ISE
 allocate-interface Port-Channel1.34 OUTSIDE visible
 allocate-interface Port-Channel1.130 INSIDE visible
 config-url disk0:/ISE.cfg

ASA3 ACS Context:
```

https://t.me/learningnets

```
interface OUTSIDE
 nameif OUTSIDE
 security-level 20
 ip address 155.1.34.18 255.255.255.0
!
interface INSIDE
 nameif INSIDE
 security-level 80
 ip address 172.16.1.1 255.255.255.0
```

ASA3 ISE Context:

```
interface OUTSIDE
 nameif OUTSIDE
 security-level 20
 ip address 155.1.34.17 255.255.255.0
!
interface INSIDE
 nameif INSIDE
 security-level 80
 ip address 172.16.3.1 255.255.255.0
```

Task 1.3 Verification

Verify that switch interfaces are in trunk mode and that LACP negotiated successfully:

```
SW2#show etherchannel summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1
```

https://t.me/learningnets

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa1/0/16(P) Fa1/0/17(P)
!
!SW2#show interfaces port-channel 1 trunk


Port        Mode             Encapsulation  Status        Native vlan
Po1         on               802.1q         trunking      1

Port        Vlans allowed on trunk
Po1         34,110,130

Port        Vlans allowed and active in management domain
Po1         34,110,130

Port        Vlans in spanning tree forwarding state and not pruned Po1          34,110,130
```

Verify context interface allocation and configuration file:

```
ASA34# show context

Context Name      Class      Interfaces           URL
*admin            default                         disk0:/admin.cfg
ACS               default    Port-channel1.34,110 disk0:/ACS.cfg
 ISE              default    Port-channel1.34,130 disk0:/ISE.cfg


Total active Security Contexts: 3
```

Verify security-level, nameif, and IPv4 addressing in both contexts:

```
ASA34/ACS# show nameif
Interface               Name                    Security
OUTSIDE                 OUTSIDE                  20
INSIDE                  INSIDE                   80
!
!ASA34/ACS# show ip address

System IP Addresses:
Interface               Name                  IP address      Subnet mask     Method
OUTSIDE                 OUTSIDE               155.1.34.18     255.255.255.0   manual
INSIDE                  INSIDE                172.16.1.1      255.255.255.0   manual
Current IP Addresses:
```

https://t.me/learningnets

```
Interface                  Name                   IP address      Subnet mask     Method
OUTSIDE                    OUTSIDE                155.1.34.18     255.255.255.0   manual
INSIDE                     INSIDE                 172.16.1.1      255.255.255.0   manual

!
!ASA34/ISE# show nameif
Interface                  Name                     Security
OUTSIDE                    OUTSIDE                    20
INSIDE                     INSIDE                     80
!
!ASA34/ISE# show ip address

System IP Addresses:
Interface                  Name                   IP address      Subnet mask     Method
OUTSIDE                    OUTSIDE                155.1.34.17     255.255.255.0   manual
INSIDE                     INSIDE                 172.16.3.1      255.255.255.0   manual
Current IP Addresses:
Interface                  Name                   IP address      Subnet mask     Method
OUTSIDE                    OUTSIDE                155.1.34.17     255.255.255.0   manual
INSIDE                     INSIDE                 172.16.3.1      255.255.255.0   manual
```

Verify that the requested interface output from each context is being matched:

```
ASA34/ACS# show interface | i Interface|System
Interface OUTSIDE "OUTSIDE", is up, line protocol is up
        System name Port-channel1.34, VLAN identifier 34
Interface INSIDE "INSIDE", is up, line protocol is up
        System name Port-channel1.110, VLAN identifier 110
!
!ASA34/ISE# show interface | i Interface|System

Interface OUTSIDE "OUTSIDE", is up, line protocol is up
        System name Port-channel1.34, VLAN identifier 34
Interface INSIDE "INSIDE", is up, line protocol is up
        System name Port-channel1.130, VLAN identifier 130
```

Verify that port-channel configuration is being matched:

```
ASA34# show port-channel 1

Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
```

https://t.me/learningnets

```
Minimum Links: 2
Maximum Bundle: 8
Load balance: src-dst-ip-port
```

Task 1.4 Solution

SW2:

```
interface range FastEthernet1/0/18 - 19
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 34,110,130
 switchport mode trunk
 channel-group 2 mode active
 no shutdown
```

SW1:

```
vlan 101
!
interface range FastEthernet1/0/16 - 17
 switchport mode access
 switchport access vlan 101
 channel-group 1 mode on
 no shutdown
!
!
interface range FastEthernet1/0/18 - 19
 switchport mode access
 switchport access vlan 101
 channel-group 2 mode on
 no shutdown
```

ASA3 System Context:

```
prompt hostname priority context state
!
interface GigabitEthernet0/1
 no shutdown
 channel-group 2 mode on
!
interface gabitEthernet0/3
 no shutdown
 channel-group 2 mode on
!
failover group 1
 primary
 preempt
```

https://t.me/learningnets

```
!
failover group 2
 secondary
 preempt
!
context ISE
 join-failover-group 1
!
context ACS
 join-failover-group 2
!
failover lan unit primary
failover lan interface FAILOVER Port-Channel2
failover link failover Port-Channel2
failover interface ip FAILOVER 155.1.101.17 255.255.255.0 standby 155.1.101.18
failover

ASA3 ACS Context:
interface OUTSIDE
 ip address 155.1.34.18 255.255.255.0 standby 155.1.34.100
!
interface INSIDE
 ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2
!
monitor-interface INSIDE
monitor-interface OUTSIDE

ASA3 ISE Context:

interface OUTSIDE
 ip address 155.1.34.17 255.255.255.0 standby 155.1.34.200
!
interface INSIDE
 ip address 172.16.3.1 255.255.255.0 standby 172.16.3.2
!
monitor-interface INSIDE
monitor-interface OUTSIDE
```

Convert ASA4 to multiple mode:

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
```

https://t.me/learningnets

```
ASA4 System Context:

interface GigabitEthernet0/1
 no shutdown
 channel-group 2 mode on
!
interface GigabitEthernet0/3
 no shutdown
 channel-group 2 mode on
!
failover lan unit secondary
failover lan interface FAILOVER Port-Channel2
failover link failover Port-Channel2
failover interface ip FAILOVER 155.1.101.17 255.255.255.0 standby 155.1.101.18
failover
```

Task 1.4 Verification

Verify that the requested failover output from each context is being matched:

```
ASA34/pri/ISE/act# show failover

Failover On
Last Failover at: 10:21:09 UTC Apr 11 2014
        This context: Active
                Active time: 381 (sec)
                  Interface OUTSIDE (155.1.34.17): Normal (Monitored)
                  Interface INSIDE (172.16.3.1): Normal (Monitored)
        Peer context: Standby Ready
                Active time: 0 (sec)
                  Interface OUTSIDE (155.1.34.200): Normal (Monitored)
                  Interface INSIDE (172.16.3.2): Normal (Monitored)
!
!ASA34/sec/ACS/act# show failover

Failover On
Last Failover at: 10:21:05 UTC Apr 11 2014
        This context: Active
                Active time: 402 (sec)
                  Interface OUTSIDE (155.1.34.18): Normal (Monitored)
                  Interface INSIDE (172.16.1.1): Normal (Monitored)
        Peer context: Standby Ready
                Active time: 0 (sec)
                  Interface OUTSIDE (155.1.34.100): Normal (Monitored)
```

https://t.me/learningnets

```
                Interface INSIDE (172.16.1.2): Normal (Monitored)
```

Verify that the failover port-channel requested output is being matched, and check EtherChannel status on both the switch and ASA:

```
ASA34/pri/act# show port-channel 2
Ports: 2   Maxports = 16
Port-channels: 2 Max Port-channels = 48
Protocol: ON
Minimum Links: 1
Load balance: src-dst-ip
!
!ASA34/sec/stby#  show port-channel 2
Ports: 2   Maxports = 16
Port-channels: 2 Max Port-channels = 48
Protocol: ON
Minimum Links: 1
Load balance: src-dst-ip
!
!SW1#show etherchannel summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)           -        Fa1/0/16(P) Fa1/0/17(P)
2      Po2(SU)           -        Fa1/0/18(P) Fa1/0/19(P)
!
!SW2#show etherchannel summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
```

https://t.me/learningnets

```
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          LACP      Fa1/0/16(P) Fa1/0/17(P)
2      Po2(SU)          LACP      Fa1/0/18(P) Fa1/0/19(P)
!
!ASA34/pri/act# show port-channel summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        U - in use      N - not in use, no aggregation/nameif
        M - not in use, no aggregation due to minimum links not met
        w - waiting to be aggregated
Number of channel-groups in use: 2
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(U)             LACP    Gi0/0(P)   Gi0/2(P)
2      Po2(U)              -      Gi0/1(P)   Gi0/3(P)
!
!ASA34/sec/stby# show port-channel summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        U - in use      N - not in use, no aggregation/nameif
        M - not in use, no aggregation due to minimum links not met
        w - waiting to be aggregated
Number of channel-groups in use: 2
Group  Port-channel  Protocol    Ports
```

https://t.me/learningnets

```
------+------------+-----------+--------------------------------------------
1      Po1(U)             LACP      Gi0/0(P)    Gi0/2(P)
2      Po2(U)              -        Gi0/1(P)    Gi0/3(P)
```

Task 1.5 Solution

```
ASA3 System Context:

class ACS-RESOURCES
  limit-resource rate Conns 1000
  limit-resource Conns 10000
  limit-resource Hosts 100
!
class ISE-RESOURCES
  limit-resource rate Conns 1000
  limit-resource Conns 5000
  limit-resource Hosts 50
!
context ACS
 member ACS-RESOURCES
!
context ISE
 member ISE-RESOURCES
```

Task 1.5 Verification

Verify the allocated resources for the two contexts:

```
ASA34/pri/act# show resource allocation detail


Resource Origin:
        A       Value was derived from the resource 'all'
        C       Value set in the definition of this class
        D       Value set in default class
Resource          Class          Mmbrs  Origin      Limit      Total     Total %
Conns [rate]      default            all      CA  unlimited
                      ISE-RESOURCES      1       C       1000       1000       0.00%
 ACS-RESOURCES       1       C       1000       1000       0.00%
                  All Contexts:      3                          2000       0.00%
```

https://t.me/learningnets

```
Inspects [rate]  default          all      CA  unlimited
                 ISE-RESOURCES      1      DA  unlimited
                 ACS-RESOURCES      1      DA  unlimited
                 All Contexts:      3

Syslogs [rate]   default          all      CA  unlimited
                 ISE-RESOURCES      1      DA  unlimited
                 ACS-RESOURCES      1      DA  unlimited
                 All Contexts:      3
Conns            default          all      CA  unlimited
                      ISE-RESOURCES      1       C       5000       5000      1.99%
ACS-RESOURCES      1       C      10000      10000      3.98%
                 All Contexts:      3                          15000      5.97%
Hosts            default          all      CA  unlimited
                      ISE-RESOURCES      1       C         50         50      0.00%
ACS-RESOURCES      1       C        100        100      0.00%

                 All Contexts:      3                            150      0.00%

IPSec            default          all      CA  unlimited
                 ISE-RESOURCES      1      DA  unlimited
                 ACS-RESOURCES      1      DA  unlimited
                 All Contexts:      3

Mac-addresses    default          all      CA  unlimited
                 ISE-RESOURCES      1      DA  unlimited
                 ACS-RESOURCES      1      DA  unlimited
                 All Contexts:      3

ASDM             default          all       C          5
                 ISE-RESOURCES      1       D          5          5      2.50%
                 ACS-RESOURCES      1       D          5          5      2.50%
                 All Contexts:      3                            15      7.50%

SSH              default          all       C          5
                 ISE-RESOURCES      1       D          5          5      5.00%
                 ACS-RESOURCES      1       D          5          5      5.00%
                 All Contexts:      3                            15     15.00%

Telnet           default          all       C          5
                 ISE-RESOURCES      1       D          5          5      5.00%
                 ACS-RESOURCES      1       D          5          5      5.00%
                 All Contexts:      3                            15     15.00%

Xlates           default          all      CA  unlimited
                 ISE-RESOURCES      1      DA  unlimited
```

https://t.me/learningnets

```
                ACS-RESOURCES       1       DA  unlimited
                All Contexts:       3
```

Task 1.6 Solution

R4:

```
ip access-list extended TRUSTED_ZONE_ACL
 permit ip 172.16.10.0 0.0.0.255 any
!
ip access-list extended SELF_ZONE_INSPECT_ACL
 permit tcp any any eq 22
 permit tcp any any eq 23
 permit icmp any any echo
!
ip access-list extended SELF_ZONE_PASS_ACL
 permit ospf any any
!
class-map type inspect match-all TRUSTED_TCP_UDP
 match access-group name TRUSTED_ZONE_ACL
!
class-map type inspect match-any TRUSTED_TO_UNTRUSTED
 match protocol icmp
 match protocol ftp
 match protocol tftp
 match class-map TRUSTED_TCP_UDP
!
class-map type inspect match-any UNTRUSTED_TO_TRUSTED
 match protocol tcp
 match protocol udp
 match protocol icmp
!
class-map type inspect match-any UNTRUSTED_TO_UNTRUSTED
 match protocol tcp
 match protocol udp
 match protocol icmp
!
class-map type inspect match-any INSPECT_UNTRUSTED_TO_SELF
 match access-group name SELF_ZONE_INSPECT_ACL
!
class-map type inspect match-any PASS_UNTRUSTED_TO_SELF
 match access-group name SELF_ZONE_PASS_ACL
!
policy-map type inspect TRUSTED_TO_UNTRUSTED
```

https://t.me/learningnets

```
 class TRUSTED_TO_UNTRUSTED SELF_ZONE_ACL
  inspect
!
policy-map type inspect UNTRUSTED_TO_TRUSTED
 class UNTRUSTED_TO_TRUSTED
  inspect
!
policy-map type inspect UNTRUSTED_TO_UNTRUSTED
 class UNTRUSTED_TO_UNTRUSTED
  inspect
!
policy-map type inspect UNTRUSTED_TO_SELF
 class INSPECT_UNTRUSTED_TO_SELF
  inspect
 class PASS_UNTRUSTED_TO_SELF
  pass
!
zone security TRUSTED
zone security UNTRUSTED
!
zone-pair security TRUSTED_TO_UNTRUSTED source TRUSTED destination UNTRUSTED
 service-policy type inspect TRUSTED_TO_UNTRUSTED
!
zone-pair security UNTRUSTED_TO_TRUSTED source UNTRUSTED destination TRUSTED
 service-policy type inspect UNTRUSTED_TO_TRUSTED
!
zone-pair security UNTRUSTED_TO_UNTRUSTED source UNTRUSTED destination UNTRUSTED
 service-policy type inspect UNTRUSTED_TO_UNTRUSTED
!
zone-pair security UNTRUSTED_TO_SELF source UNTRUSTED destination self
 service-policy type inspect UNTRUSTED_TO_SELF
!
interface FastEthernet0/0.41
 zone-member security TRUSTED
!
interface FastEthernet0/0.15
 zone-member security UNTRUSTED
!
interface FastEthernet0/1.43
 zone-member security UNTRUSTED
!
interface FastEthernet0/1.48
 zone-member security UNTRUSTED
!
parameter-map type inspect global
```

https://t.me/learningnets

```
log dropped-packets enable
```

Task 1.6 Verification

Verify that traffic between zones and intra-zone creates entries in the firewall state table:

https://t.me/learningnets

```
SW1#ping 150.1.11.11


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.11.11, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
!
!R4#show  policy-firewall session zone-pair UNTRUSTED_TO_UNTRUSTED

 Zone-pair: UNTRUSTED_TO_UNTRUSTED
  Service-policy inspect : UNTRUSTED_TO_UNTRUSTED
    Class-map : UNTRUSTED_TO_UNTRUSTED(match-any) Established Sessions =  1
 Session 4A579900 (155.1.48.9:8)=>(150.1.11.11:0) icmp SIS_OPEN

          Created 00:00:02, Last heard 00:00:02
          ECHO request
          Bytes sent (initiator:responder) [360:360]
    Class-map : class-default(match-any)
!
!SW1#ping 172.16.10.100


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
!
!R4#show policy-firewall session zone-pair UNTRUSTED_TO_TRUSTED

 Zone-pair: UNTRUSTED_TO_TRUSTED
  Service-policy inspect : UNTRUSTED_TO_TRUSTED
    Class-map : UNTRUSTED_TO_TRUSTED(match-any) Established Sessions =  1
 Session 4A57A380 (155.1.48.9:8)=>(172.16.10.100:0) icmp SIS_OPEN

          Created 00:00:01, Last heard 00:00:01
          ECHO request
          Bytes sent (initiator:responder) [360:360]
    Class-map : class-default(match-any)
```

Verify that traffic allowed to self zone from the **UNTRUSTED** zone creates entries in the firewall state table:

https://t.me/learningnets

```
SW1#ping 155.1.48.4


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.48.4, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
!
!R4#show policy-firewall session zone-pair UNTRUSTED_TO_SELF

 Zone-pair: UNTRUSTED_TO_SELF
  Service-policy inspect : UNTRUSTED_TO_SELF
    Class-map : INSPECT_UNTRUSTED_TO_SELF(match-any) Established Sessions =  1
 Session 4A57B880 (155.1.48.9:8)=>(155.1.48.4:0) icmp SIS_OPEN
          Created 00:00:02, Last heard 00:00:02
          ECHO request
          Bytes sent (initiator:responder) [360:360]
    Class-map : PASS_UNTRUSTED_TO_SELF(match-any)
    Class-map : class-default(match-any)
!
!SW1#telnet 155.1.48.4
Trying 155.1.48.4 ... Open


Password required, but none set
 [Connection to 155.1.48.4 closed by foreign host]
!
!R4#show policy-firewall session zone-pair UNTRUSTED_TO_SELF

 Zone-pair: UNTRUSTED_TO_SELF
  Service-policy inspect : UNTRUSTED_TO_SELF
    Class-map : INSPECT_UNTRUSTED_TO_SELF(match-any) Established Sessions =  1
 Session 4A57BC00 (155.1.48.9:28416)=>(155.1.48.4:23) tcp SIS_OPEN/TCP_ESTAB

          Created 00:00:01, Last heard 00:00:00
          Bytes sent (initiator:responder) [27:49]
    Class-map : PASS_UNTRUSTED_TO_SELF(match-any)
    Class-map : class-default(match-any)
```

Verify that logging for firewall inspection dropped packets is enabled:

```
R4#show policy-firewall config parameter-map global

  alert on
  sessions maximum 2147483647
  waas disabled
```

https://t.me/learningnets

```
  l2-transparent dhcp-passthrough disabled log dropped-packets enabled

  log summary disabled
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  tcp reset-PSH disabled
```

Verify the firewall configuration for the **TRUSTED** to **UNTRUSTED** zone:

```
R4#show policy-firewall config zone-pair TRUSTED_TO_UNTRUSTED

Zone-pair              : TRUSTED_TO_UNTRUSTED
Source Zone            : TRUSTED
Destination Zone       : UNTRUSTED
Service-policy inspect : TRUSTED_TO_UNTRUSTED Class-map : TRUSTED_TO_UNTRUSTED(match-any)
 Match protocol ftp
 Match protocol tftp
 Match class-map TRUSTED_TCP_UDP
 Action : inspect

   Parameter-map : Default

  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default
```

Verify the firewall configuration for the **UNTRUSTED** to **TRUSTED** zone:

```
R4#show policy-firewall config zone-pair UNTRUSTED_TO_TRUSTED

Zone-pair              : UNTRUSTED_TO_TRUSTED
Source Zone            : UNTRUSTED
Destination Zone       : TRUSTED
Service-policy inspect : UNTRUSTED_TO_TRUSTED Class-map : UNTRUSTED_TO_TRUSTED(match-any)
 Match protocol tcp
 Match protocol udp
 Match protocol icmp
 Action : inspect

   Parameter-map : Default

  Class-map : class-default(match-any)
```

https://t.me/learningnets

```
   Match any
  Action : drop log
   Parameter-map : Default
```

Verify the firewall configuration for the **UNTRUSTED** to **UNTRUSTED** zone:

```
R4#show policy-firewall config zone-pair UNTRUSTED_TO_UNTRUSTED

Zone-pair               : UNTRUSTED_TO_UNTRUSTED
Source Zone             : UNTRUSTED
Destination Zone        : UNTRUSTED
Service-policy inspect  : UNTRUSTED_TO_UNTRUSTED Class-map : UNTRUSTED_TO_UNTRUSTED(match-any)
 Match protocol tcp
 Match protocol udp
 Match protocol icmp
 Action : inspect

   Parameter-map : Default

  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default
```

Verify the firewall configuration for the **UNTRUSTED** to **SELF** zone:

https://t.me/learningnets

```
R4#show policy-firewall config zone-pair UNTRUSTED_TO_SELF

Zone-pair               : UNTRUSTED_TO_SELF
Source Zone             : UNTRUSTED
Destination Zone        : self
Service-policy inspect  : UNTRUSTED_TO_SELF Class-map : INSPECT_UNTRUSTED_TO_SELF(match-any)
 Match access-group name SELF_ZONE_INSPECT_ACL
 Action : inspect

    Parameter-map : Default
 Class-map : PASS_UNTRUSTED_TO_SELF(match-any)
 Match access-group name SELF_ZONE_PASS_ACL
 Action : pass log

    Parameter-map : Default

  Class-map : class-default(match-any)
    Match any
  Action : drop log
    Parameter-map : Default
```

Clear the OSPF process and verify that R4 still has all three neighbors established:

```
R4#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.9.9         1   FULL/DR         00:00:37    155.1.48.9      FastEthernet0/1.48
150.1.11.11       1   FULL/DR         00:00:35    155.1.43.11     FastEthernet0/1.43
172.16.6.1        1   FULL/DR         00:00:38    155.1.15.15     FastEthernet0/0.15
```

Task 1.7 Solution

```
R4:

ip nat inside source static 172.16.10.100 155.1.15.100 extendable
ip nat inside source static 172.16.10.100 155.1.43.100 extendable
ip nat inside source static 172.16.10.100 155.1.48.100 extendable
!
interface fastEthernet 0/0.41
 ip nat inside
```

https://t.me/learningnets

```
!
interface FastEthernet0/1.43
 ip nat outside
!
interface FastEthernet0/0.15
 ip nat outside
!
interface FastEthernet0/1.48
 ip nat outside
!
ip access-list extended TELNET_ALLOW_ACL
 permit tcp 155.1.99.0 0.0.0.255 host 172.16.10.100 eq 23
 permit tcp 172.16.5.0 0.0.0.255 host 172.16.10.100 eq 23
 permit tcp 155.1.10.0 0.0.0.255 host 172.16.10.100 eq 23
 permit tcp 155.1.99.0 0.0.0.255 host 172.16.10.100 eq 80
 permit tcp 172.16.5.0 0.0.0.255 host 172.16.10.100 eq 80
 permit tcp 155.1.10.0 0.0.0.255 host 172.16.10.100 eq 80
 permit tcp 155.1.99.0 0.0.0.255 host 172.16.10.100 eq 443
 permit tcp 172.16.5.0 0.0.0.255 host 172.16.10.100 eq 443
 permit tcp 155.1.10.0 0.0.0.255 host 172.16.10.100 eq 443
!
ip access-list extended TELNET_DROP_ACL
 permit tcp any host 172.16.10.100 eq 23
!
class-map type inspect match-any TELNET_ALLOW_TO_TRUSTED
 match access-group name TELNET_ALLOW_ACL
!
class-map type inspect match-any TELNET_DROP_TO_TRUSTED
 match access-group name TELNET_DROP_ACL
!
policy-map type inspect UNTRUSTED_TO_TRUSTED
 no class type inspect UNTRUSTED_TO_TRUSTED
 class TELNET_ALLOW_TO_TRUSTED
  inspect
 class TELNET_DROP_TO_TRUSTED
  drop
 class type inspect UNTRUSTED_TO_TRUSTED
  inspect
```

Task 1.7 Verification

https://t.me/learningnets

Verify the static-extendable NAT entries matching the requested output, and NAT configuration:

```
R4#show ip nat translations

Pro Inside global      Inside local       Outside local      Outside global
--- 155.1.43.100       172.16.10.100      ---                ---
--- 155.1.15.100       172.16.10.100      ---                ---
--- 155.1.48.100       172.16.10.100      ---                ---
!
!R4#show ip nat statistics

Total active translations: 3 (3 static, 0 dynamic; 0 extended)
Peak translations: 0, occurred 1d00h agoOutside interfaces:
 FastEthernet0/0.15, FastEthernet0/1.43, FastEthernet0/1.48
Inside interfaces:
 FastEthernet0/0.41

Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Verify that telnet access is allowed only from configured sources:

```
SW3#telnet 155.1.43.100

Trying 155.1.43.100 ... % Connection timed out; remote host not responding
!
!SW3#telnet 155.1.43.100 /source-interface vlan99
Trying 155.1.43.100 ... Open
Kerberos: No default realm defined for Kerberos!
Welcome to Microsoft Telnet Service

login: Administrator
password:

*===============================================================
Microsoft Telnet Server.
```

https://t.me/learningnets

```
*============================================================C:\Users\Administrator>

!
!R5#telnet 155.1.15.100
Trying 155.1.15.100 ... % Connection timed out; remote host not responding
!
!R5#telnet 155.1.15.100 /source-interface fastEthernet0/0.55
Trying 155.1.15.100 ... Open
Welcome to Microsoft Telnet Service

login: Administrator
password:

*============================================================
Microsoft Telnet Server.
*============================================================C:\Users\Administrator>
!
!R4#show policy-firewall session zone-pair UNTRUSTED_TO_TRUSTED

 Zone-pair: UNTRUSTED_TO_TRUSTED
  Service-policy inspect : UNTRUSTED_TO_TRUSTED
    Class-map : HTTP_PROTOCOL(match-any)
    Class-map : TELNET_ALLOW_TO_TRUSTED(match-any) Established Sessions =  2
 Session 4A586080 (155.1.99.11:42116)=>(172.16.10.100:23) tcp SIS_OPEN/TCP_ESTAB
          Created 00:09:13, Last heard 00:08:48
          Bytes sent (initiator:responder) [69:287]
 Session 4A586780 (172.16.5.1:35714)=>(172.16.10.100:23) tcp SIS_OPEN/TCP_ESTAB

          Created 00:00:39, Last heard 00:00:17
          Bytes sent (initiator:responder) [69:287]
    Class-map : TELNET_DROP_TO_TRUSTED(match-any)
    Class-map : UNTRUSTED_TO_TRUSTED(match-any)
    Class-map : class-default(match-any)
```

Task 1.8 Solution

R4:

```
ip port-map http port 8080
!
class-map type inspect match-any HTTP_PROTOCOL
 match protocol http
!
parameter-map type urlf-glob BLOCK_URL
```

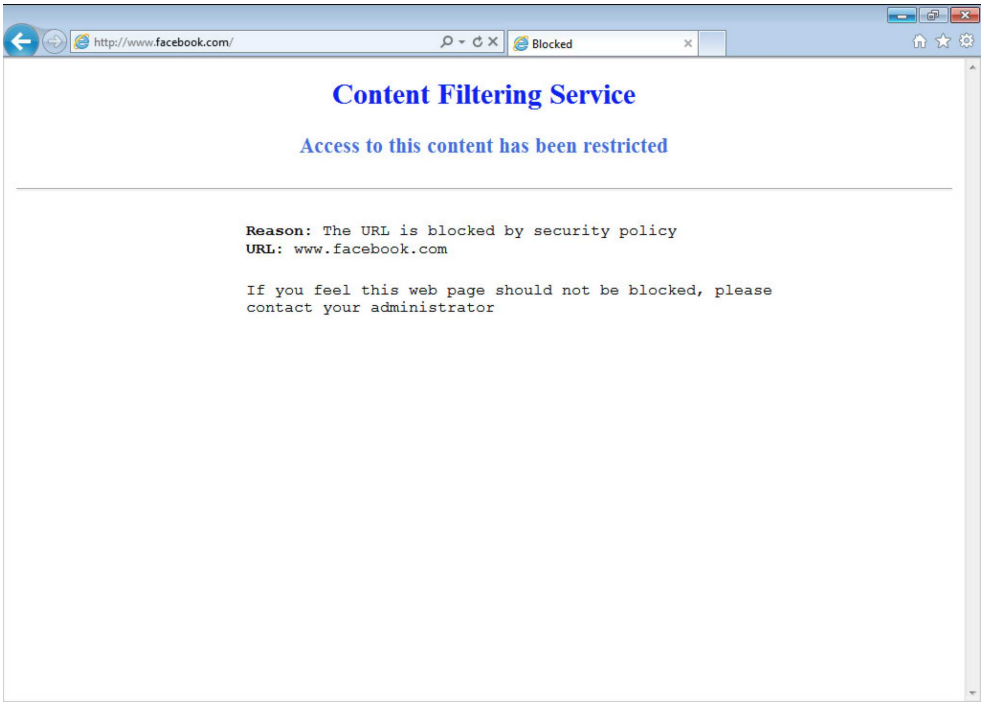
https://t.me/learningnets

```
 pattern *.reddit.com
 pattern *.facebook.com
!
parameter-map type urlf-glob ALLOW_URL
 pattern *
!
class-map type urlfilter match-any BLOCK_MAP
 match server-domain urlf-glob BLOCK_URL
!
class-map type urlfilter match-any ALLOW_MAP
 match server-domain urlf-glob ALLOW_URL
!
parameter-map type urlfpolicy local BANNER
 block-page message "Access to this content has been restricted"
!
policy-map type inspect urlfilter HTTP_POLICY
 parameter type urlfpolicy local BANNER
 class type urlfilter BLOCK_MAP
  reset
  log
 class type urlfilter ALLOW_MAP
  allow
!
policy-map type inspect UNTRUSTED_TO_TRUSTED
 no  class type inspect UNTRUSTED_TO_TRUSTED
 class HTTP_PROTOCOL
  inspect
  service-policy urlfilter HTTP_POLICY
 class type inspect UNTRUSTED_TO_TRUSTED
  inspect
```

Task 1.8 Verification

Configure **TEST-PC-B** in VLAN 99 with a default gateway of SW3 and a DNS server of R1. Access **www.facebook.com** and **www.reddit.com** and verify that access is rejected by R4 and requested messages are displayed:

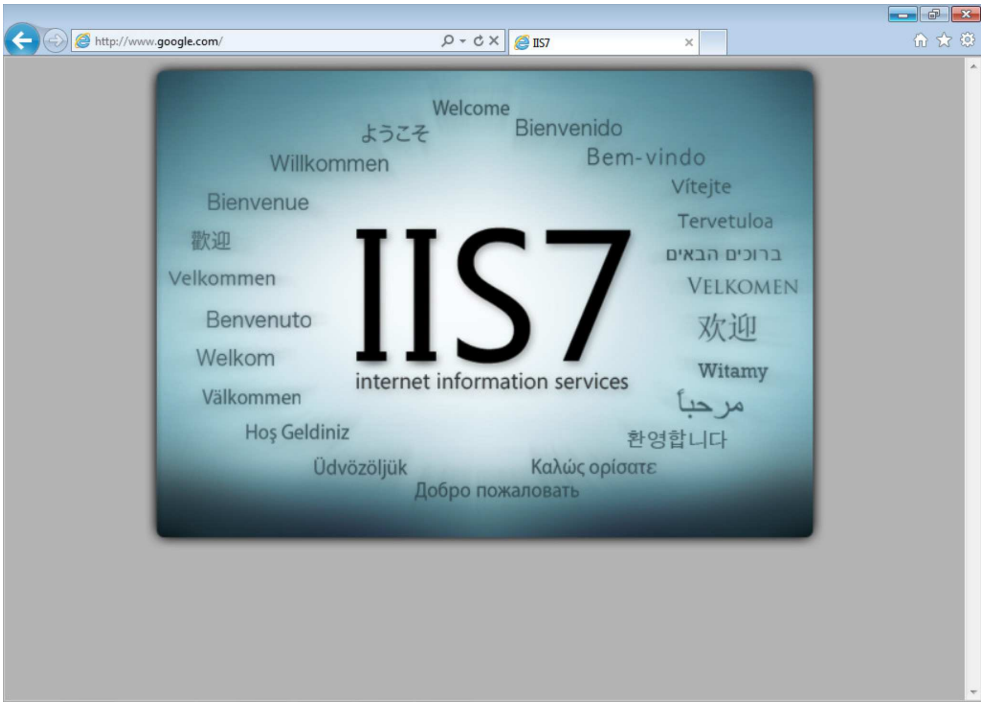
https://t.me/learningnets



Verify that a log message has also been generated by R4:

```
%URLF-4-SITE_BLOCKED: (target:class)-(UNTRUSTED_TO_TRUSTED:HTTP_PROTOCOL):Access denied for the site 'www.facebook.c
%URLF-4-SITE_BLOCKED: (target:class)-(UNTRUSTED_TO_TRUSTED:HTTP_PROTOCOL):Access denied for the site 'www.reddit.com
```

Verify that access to other URLs, such as **www.google.com**, is not restricted:



https://t.me/learningnets

Verify the configuration and that packets are matching the configured policy:

```
R4#show policy-map type inspect urlfilter

  Policy Map type inspect urlfilter HTTP_POLICY
    Parameter BANNER Class BLOCK_MAP
 reset
 log
 Class ALLOW_MAP
 allow
!
!R4#show parameter-map type urlfpolicy local

parameter map type urlfpolicy local BANNER
  alert on
  allow-mode off block-page message "Access to this content has been restricted"
!
!R4#show parameter-map type urlf-glob
 parameter-map type urlf-glob BLOCK_URL
 pattern *.reddit.com
 pattern *.facebook.com
 parameter-map type urlf-glob ALLOW_URL
 pattern *
!
!R4#show policy-firewall config zone-pair UNTRUSTED_TO_TRUSTED

Zone-pair              : UNTRUSTED_TO_TRUSTED
Source Zone            : UNTRUSTED
Destination Zone       : TRUSTED
Service-policy inspect : UNTRUSTED_TO_TRUSTED Class-map : HTTP_PROTOCOL(match-any)
 Match protocol http
 Action : inspect
   Parameter-map : Default Service Policy: urlfilter HTTP_POLICY

  Class-map : UNTRUSTED_TO_TRUSTED(match-any)
   Match protocol tcp
   Match protocol udp
   Match protocol icmp
  Action : inspect
   Parameter-map : Default

  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default
```

https://t.me/learningnets

```
!
!R4#show policy-firewall stats zone-pair UNTRUSTED_TO_TRUSTED


policy exists on zp UNTRUSTED_TO_TRUSTED
 Zone-pair: UNTRUSTED_TO_TRUSTED

  Service-policy inspect : UNTRUSTED_TO_TRUSTED
 Class-map: HTTP_PROTOCOL (match-any)
 Match: protocol http
 14 packets, 448 bytes

        30 second rate 0 bps

   Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [33:371]

        Session creations since subsystem startup or last reset 14
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [2:1:0]
        Last session created 00:02:23
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 4
        Last half-open session total 0
        TCP reassembly statistics
        received 0 packets out-of-order; dropped 0
        peak memory usage 0 KB; current usage: 0 KB
        peak queue length 0
```

Task 1.9 Solution

```
ASA3 ISE Context:

url-server (INSIDE) vendor websense host 172.16.3.99 protocol udp
filter url http 172.16.3.0 255.255.255.0 0.0.0.0 0.0.0.0 allow proxy-block
filter url 443 172.16.3.0 255.255.255.0 0.0.0.0 0.0.0.0 allow proxy-block
```

Task 1.9 Verification

https://t.me/learningnets

Verify the URL Filtering configuration:

```
ASA34/pri/ISE/act# show url-server statistics


Global Statistics:
--------------------
URLs total/allowed/denied         0/0/0
URLs allowed by cache/server      0/0
URLs denied by cache/server       0/0
HTTPSs total/allowed/denied       0/0/0
HTTPSs allowed by cache/server    0/0
HTTPSs denied by cache/server     0/0
FTPs total/allowed/denied         0/0/0
FTPs allowed by cache/server      0/0
FTPs denied by cache/server       0/0
Requests dropped                  0
Server timeouts/retries           0/0
Processed rate average 60s/300s   0/0 requests/second
Denied rate average 60s/300s      0/0 requests/second
Dropped rate average 60s/300s     0/0 requests/second

Server Statistics:
--------------------172.16.3.99                          DOWN
Vendor                            websense

  Port                            15868
  Requests total/allowed/denied   0/0/0
  Server timeouts/retries         0/0
  Responses received              0
  Response time average 60s/300s  0/0

URL Packets Sent and Received Stats:
------------------------------------
Message                 Sent    Received
STATUS_REQUEST          15      0
LOOKUP_REQUEST          0       0
LOG_REQUEST             0       NA

Errors:
-------
RFC noncompliant GET method     0
URL buffer update failure       0
```

https://t.me/learningnets

Verify that URL Filtering is performed for HTTP/HTTPS traffic:

```
ASA34/pri/ISE/act#packet-tracer input INSIDE tcp 172.16.3.30 2000 155.1.34.50 80 detailed

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fff31ab9000, priority=1, domain=permit, deny=false
        hits=10851, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0100.0000.0000
        input_ifc=INSIDE, output_ifc=any

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   155.1.34.0      255.255.255.0   OUTSIDE

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fff31abe040, priority=0, domain=inspect-ip-options, deny=true
        hits=2, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=INSIDE, output_ifc=any
Phase: 4
Type: FILTER
Subtype: filter-url
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fff3124ece0, priority=69, domain=filter-url, deny=false
```

https://t.me/learningnets

```
        hits=1, user_data=0x7fff31ae64f0, cs_id=0x0, use_real_addr, flags=0x2000, protocol=6
        src ip/id=172.16.3.0, mask=255.255.255.0, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=80, dscp=0x0
        input_ifc=INSIDE, output_ifc=any
!
!ASA34/pri/ISE/act# packet-tracer input INSIDE tcp 172.16.3.30 2000 155.1.34.50 443 detailed

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fff31ab9000, priority=1, domain=permit, deny=false
        hits=10868, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0100.0000.0000
        input_ifc=INSIDE, output_ifc=any

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   155.1.34.0      255.255.255.0   OUTSIDE

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fff31abe040, priority=0, domain=inspect-ip-options, deny=true
        hits=3, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=INSIDE, output_ifc=any
 Phase: 4
Type: FILTER
Subtype: filter-url
Result: ALLOW
```

https://t.me/learningnets

```
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fff23e21ab0, priority=69, domain=filter-url, deny=false
        hits=1, user_data=0x7fff31ae64f0, cs_id=0x0, use_real_addr, flags=0x2000, protocol=6
        src ip/id=172.16.3.0, mask=255.255.255.0, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, dscp=0x0
        input_ifc=INSIDE, output_ifc=any
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 5

CCIE SCv4 Lab 5 Solutions Section 2

1. Task 2.1 Solution
2. Task 2.2 Solution
3. Task 2.3 Solution
4. Task 2.4 Solution
5. Task 2.5 Solution
6. Task 2.6 Solution
7. Task 2.7 Solution

Task 2.1 Solution

SW3:

```
interface GigabitEthernet1/0/10
 switchport mode access
 switchport access vlan 99
 no shutdown
```

IPS:

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# host-name IPS4240
sensor(config-hos-net)# host-ip 155.1.99.100/24,155.1.99.11
sensor(config-hos-net)# access-list 155.1.99.0/24
sensor(config-hos-net)# telnet-option enabled
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes?[yes]:
!
!
sensor(config)# service signature-definition sig0
sensor(config-sig)# ip-log
sensor(config-sig-ip)# ip-log-packets 500
```

https://t.me/learningnets

```
sensor(config-sig-ip)# ip-log-time 120
sensor(config-sig-ip)# ip-log-bytes 16000
sensor(config-sig-ip)# exit
sensor(config-sig)# exit
Apply Changes?[yes]:
```

Task 2.1 Verification

Verify the configured host settings:

```
sensor(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
host-ip: 155.1.99.100/24,155.1.99.11 default: 192.168.1.2/24,192.168.1.1
 host-name: IPS4240 default: sensor
 telnet-option: enabled default: disabled
 access-list (min: 0, max: 512, current: 1)
      ----------------------------------------------- network-address: 155.1.99.0/24
         -----------------------------------------------
      -----------------------------------------------
!
!sensor(config-sig-ip)# show settings

   ip-log
   ----------------------------------------------- ip-log-packets: 500 default: 0
 ip-log-time: 120 default: 30
 ip-log-bytes: 16000 default: 0

   -----------------------------------------------
```

Task 2.2 Solution

```
SW3:
interface range GigabitEthernet 1/0/8 - 9
 no shutdown
!
monitor session 1 source vlan 41
monitor session 1 destination interface Gi1/0/8 encapsulation dot1q ingress dot1q vlan 50
monitor session 2 source remote vlan 150
monitor session 2 destination interface GigabitEthernet1/0/9

SW5:
```

https://t.me/learningnets

```
vlan 150
 remote-span
!
monitor session 2 source interface FastEthernet1/0/10
monitor session 2 destination remote vlan 150
```

IPS:

```
sensor(config)# service interface
sensor(config-int)# physical-interfaces gigabitEthernet0/0
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# exit
sensor(config-int)# physical-interfaces gigabitEthernet0/1
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# alt-tcp-reset-interface interface-name gigabitEthernet0/0
sensor(config-int-phy)# exit
sensor(config-int)# exit
Apply Changes?[yes]:
!
!
sensor(config)# service analysis-engine
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)# physical-interface gigabitEthernet0/0
sensor(config-ana-vir)# physical-interface gigabitEthernet0/1
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
Apply Changes?[yes]:
```

Task 2.2 Verification

Verify the SPAN and RSPAN configuration:

```
SW3#show monitor
 Session 1
---------
Type                   : Local Session
Source VLANs           : Both                : 41
Destination Ports      : Gi1/0/8
 Encapsulation      : DOT1Q
 Ingress       : Enabled, default VLAN = 50
 Ingress encap : DOT1Q

 Session 2
---------
Type                   : Remote Destination Session Source RSPAN VLAN       : 150
Destination Ports      : Gi1/0/9
```

https://t.me/learningnets

```
Encapsulation      : Native
 Ingress       : Disabled
!
!SW3#show vlan id 150

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
150  VLAN0150                         active    Gi1/0/20

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
150  enet  100150     1500  -      -      -        -    -        0      0
 Remote SPAN VLAN
----------------Enabled


Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------
```

Verify the IPS interface status:

```
sensor# show interfaces brief

CC   Interface            Sensing State   Link   Inline Mode   Pair Status
GigabitEthernet0/0   Enabled          Up     Unpaired      N/A

*    Management0/0        Disabled        Up
GigabitEthernet0/1   Enabled          Up     Unpaired      N/A

     GigabitEthernet0/2   Disabled        Down   Unpaired      N/A
     GigabitEthernet0/3   Disabled        Down   Unpaired      N/A
!
!sensor(config-int-phy)# show settings

   <protected entry> name: GigabitEthernet0/1
   ----------------------------------------------
      media-type: tx <protected>
      description:  <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      default-vlan: 0 <defaulted> alt-tcp-reset-interface
      ---------------------------------------------- interface-name: GigabitEthernet0/0

      ----------------------------------------------
```

https://t.me/learningnets

```
      subinterface-type
      ------------------------------------------------
         none
         ------------------------------------------------
```

Verify that both SPAN and RSPAN traffic is inspected by IPS:

```
sensor(config-ana-vir)# show settings

   <protected entry> name: vs0
   ------------------------------------------------
      description: default virtual sensor <defaulted>
      signature-definition: sig0 <protected>
      event-action-rules: rules0 <protected>
      anomaly-detection
      ------------------------------------------------
         anomaly-detection-name: ad0 <protected>
         operational-mode: inactive <defaulted>
      ------------------------------------------------
physical-interface (min: 0, max: 999999999, current: 2)
      ------------------------------------------------ name: GigabitEthernet0/0
         subinterface-number: 0 <defaulted>
         ------------------------------------------------ name: GigabitEthernet0/1

         subinterface-number: 0 <defaulted>
         ------------------------------------------------
```

Task 2.3 Solution

This task should be completed after the wireless configuration from the **Identity Management** section.

```
ASA1:
access-list DMZ_IN permit tcp host 155.1.99.100 host 155.1.34.17 eq 22

ASA3 System Context:
delete /noconfirm disk0:/admin.cfg
admin-context ISE
no context admin

ASA3 ISE Context:
crypto key generate rsa general-keys modulus 1024
!
```

https://t.me/learningnets

```
ssh 155.1.99.100 255.255.255.255 OUTSIDE
username asauser password asapass
aaa authentication ssh console LOCAL
!
route OUTSIDE 172.16.5.0 255.255.255.0 155.1.34.10
```

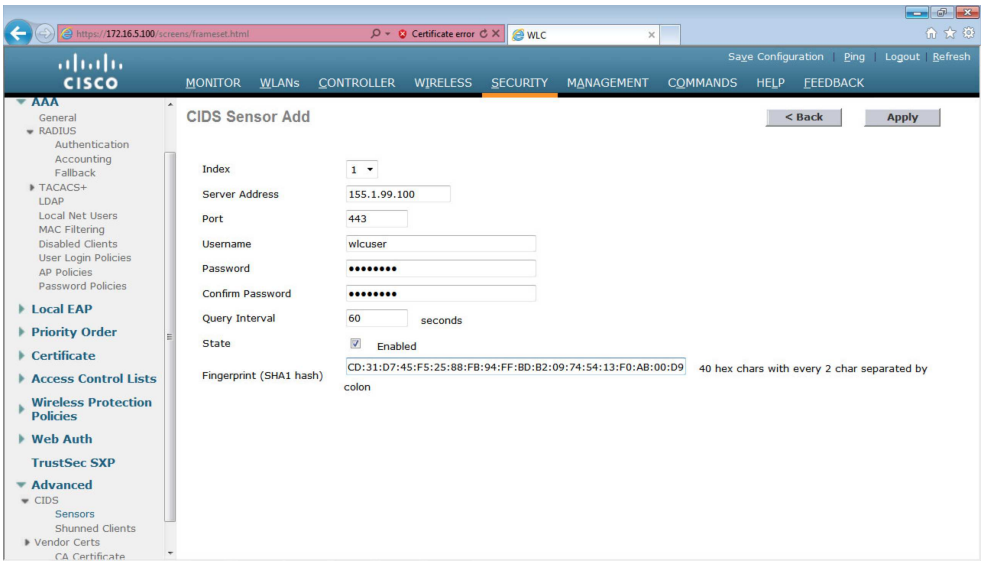
IPS:

```
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 2004 0
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# enabled true
sensor(config-sig-sig-sta)# exit
sensor(config-sig-sig)# engine atomic-ip
sensor(config-sig-sig-ato)# event-action request-block-host|produce-alert|log-attacker-packets
sensor(config-sig-sig-ato)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes?[yes]:
!
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# access-list 172.16.5.100/32
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes?[yes]:
!
sensor(config)# username wlcuser password 1qaz2wsx privilege viewer
!
sensor(config)# service network-access
sensor(config-net)# user-profiles ASA3
sensor(config-net-use)# username asauser
sensor(config-net-use)# password
Enter password[]: *******
Re-enter password: *******
sensor(config-net-use)# enable-password
Enter enable-password[]:
Re-enter enable-password:
sensor(config-net-use)# exit
sensor(config-net)# exit
Apply Changes?[yes]:
!
sensor(config)# service network-access
sensor(config-net)# firewall-devices 155.1.34.17
sensor(config-net-fir)# communication ssh-3des
sensor(config-net-fir)# profile-name ASA3
```

https://t.me/learningnets

```
sensor(config-net-fir)# exit
sensor(config-net)# exit
Apply Changes?[yes]:
!
sensor(config)# ssh host-key 155.1.34.17
MD5 fingerprint is 1A:3C:08:A5:45:1D:85:C0:47:50:8E:BC:44:4E:91:38
Bubble Babble is xidah-sofyf-sumom-bafon-movik-kegyc-kunok-kokok-vynam-nunob-gyxix
Would you like to add this to the known hosts table for this host?[yes]:
!
sensor# block host 172.16.5.150
!
sensor# show tls fingerprint
MD5: AC:27:34:BB:F4:B0:16:A0:04:18:31:23:70:06:A0:98
SHA1: CD:31:D7:45:F5:25:88:FB:94:FF:BD:B2:09:74:54:13:F0:AB:00:D9
```

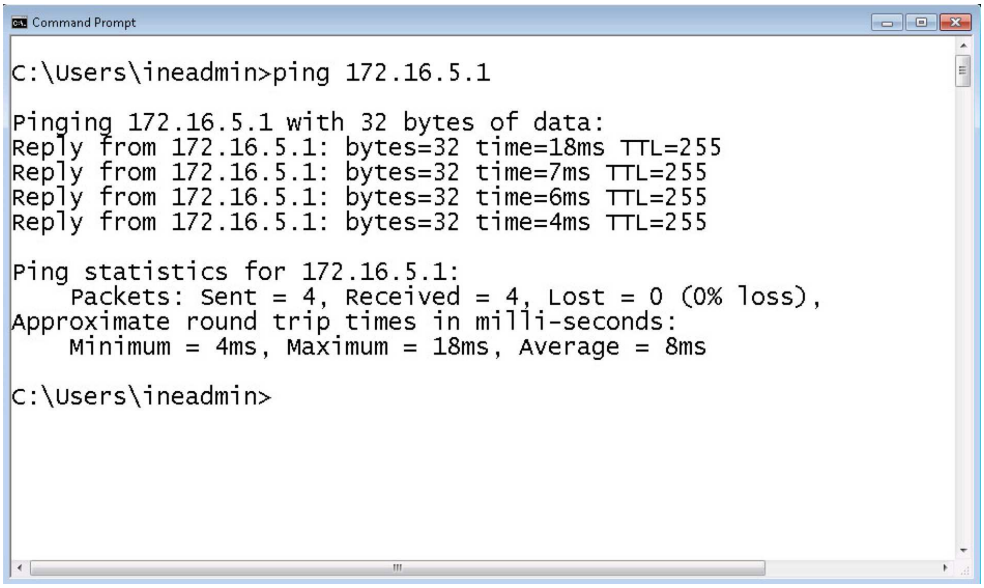
From **TEST-PC-B**, use Internet Explorer to navigate to **Security -> Advanced -> CIDS -> Sensors**, click **New**, and configure it for IPS integration:



Task 2.3 Verification

From the connected WiFi client, generate ICMP Echo packets to the default gateway:

https://t.me/learningnets



Traffic should trigger the IPS signature and the client should be added to the shun list, and therefore blocked by the WLC and ASA:

https://t.me/learningnets

```
sensor# show events


evIdsAlert: eventId=1395329437431000949 severity=informational vendor=Cisco
  originator:
    hostId: IPS4240
    appName: sensorApp
    appInstanceId: 1202
  time: 2014/04/14 12:19:49 2014/04/14 12:19:49 UTC
signature: description=ICMP Echo Request id=2004 created=20001127 type=other version=S666

    subsigId: 0 sigDetails: ICMP Echo Request

  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 172.16.5.2
    target:
      addr: locality=OUT 172.16.5.1
      os: idSource=unknown relevance=relevant type=unknown  actions:
 logPacketsActivated: true
 blockRequested: true
 logAttackerPacketsActivated: true
 ipLogIds:
 ipLogId: 1441800

  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
  threatRatingValue: 15
  interface: ge0_1
  protocol: icmp
```

Verify that IPS is connected to the ASA and the manually blocked host is shunned, as well as the WiFi client:

https://t.me/learningnets

```
ASA34/pri/ISE/act# show ssh sessions


SID Client IP       Version Mode Encryption Hmac     State            Username
0   155.1.99.100    1.5     -    3DES       -        SessionStarted   asauser

!
!ASA34/pri/ISE/act# show shun
 shun (OUTSIDE) 172.16.5.2 0.0.0.0 0 0 0
shun (OUTSIDE) 172.16.5.150 0.0.0.0 0 0 0
```

Verify that WLC successfully connected to IPS, and check the shunned client list:

```
(Cisco Controller) >show wps cids-sensor summary


Configured IDS Sensors

Index  Server Address    Port    State      Intvl   Last Query
-----  ----------------  ------  ---------  ------  --------------
1      155.1.99.100      443     Enabled    60      Success
!
!(Cisco Controller) >show wps  shun-list

Total number of Entries ......................... 2

IP Address        Last MAC address     Expire     Sensor IP/Index
---------------   -------------------  ---------  ----------------
172.16.5.2        ac:f1:df:13:bd:8f    30         155.1.99.100/1
172.16.5.150                           -          155.1.99.100/1
```

Task 2.4 Solution

```
SW6:
interface FastEthernet1/0/10
 switchport mode access
 switchport access vlan 60
 no shutdown

ASA1:
```

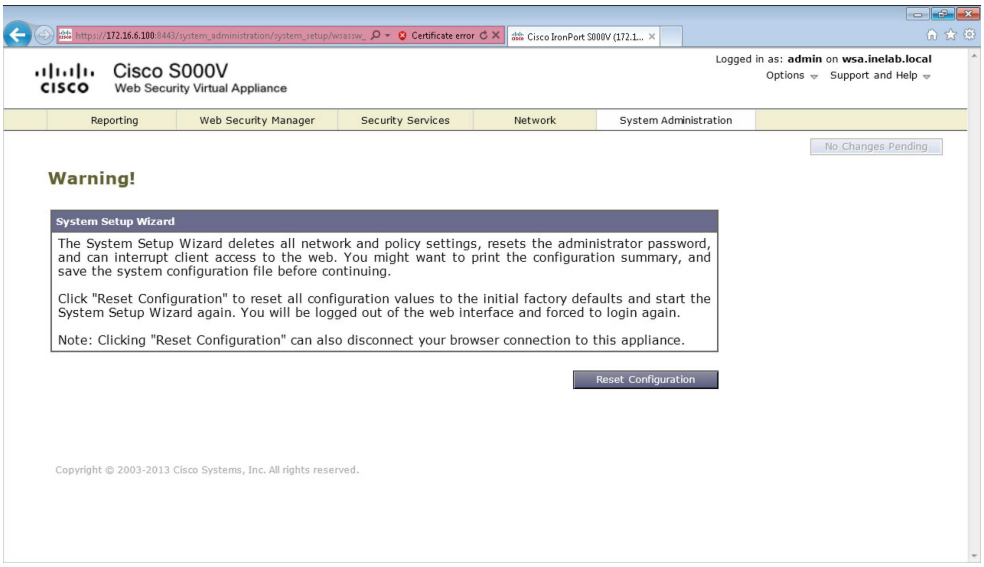
https://t.me/learningnets

```
access-list DMZ_IN permit tcp 155.1.99.0 255.255.255.0 host 172.16.6.100 eq 8883
!
access-group DMZ_IN in interface DMZ
```

R4:

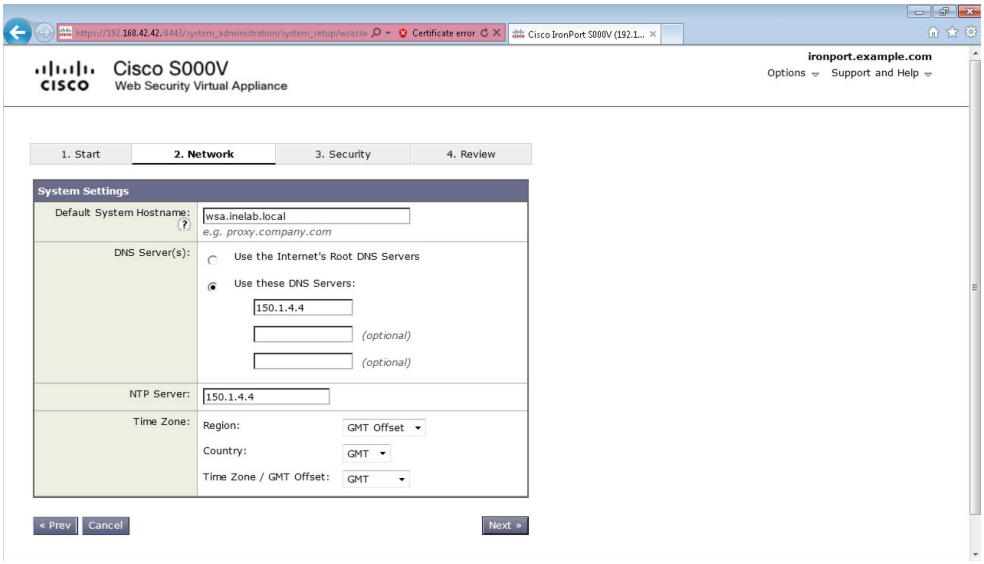
```
ip access-list extended SELF_ZONE_INSPECT_ACL
 permit udp host 172.16.6.100 host 150.1.4.4 eq 53
 permit udp host 172.16.6.100 host 150.1.4.4 eq 123
```

Using Internet Explorer from **TEST-PC-B**, navigate to **https://172.16.6.100:8443**, authenticate and browse to **System Administration -> System Setup Wizard**, and click **Reset Configuration**:

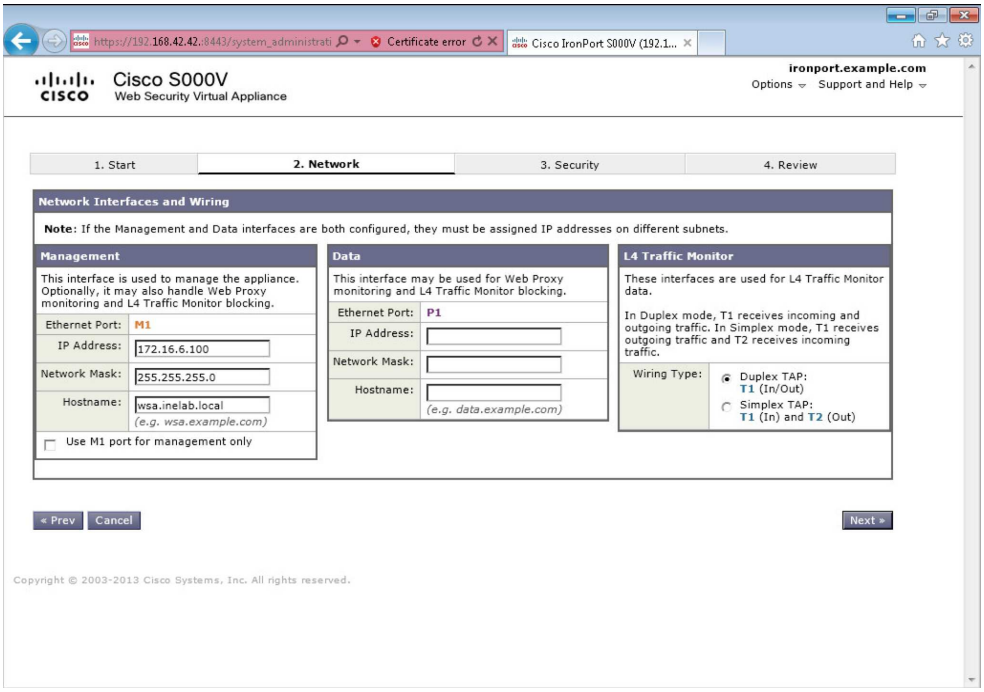


Configure **TEST-PC-B** with IPv4 address from subnet 192.168.42.0/24, and use Internet Explorer to navigate to **https://192.168.42.42:8443**. Authenticate with the default credentials of **admin/ironport** and browse to **System Administration -> System Setup Wizard**. Configure hostname, DNS, and NTP server:

https://t.me/learningnets

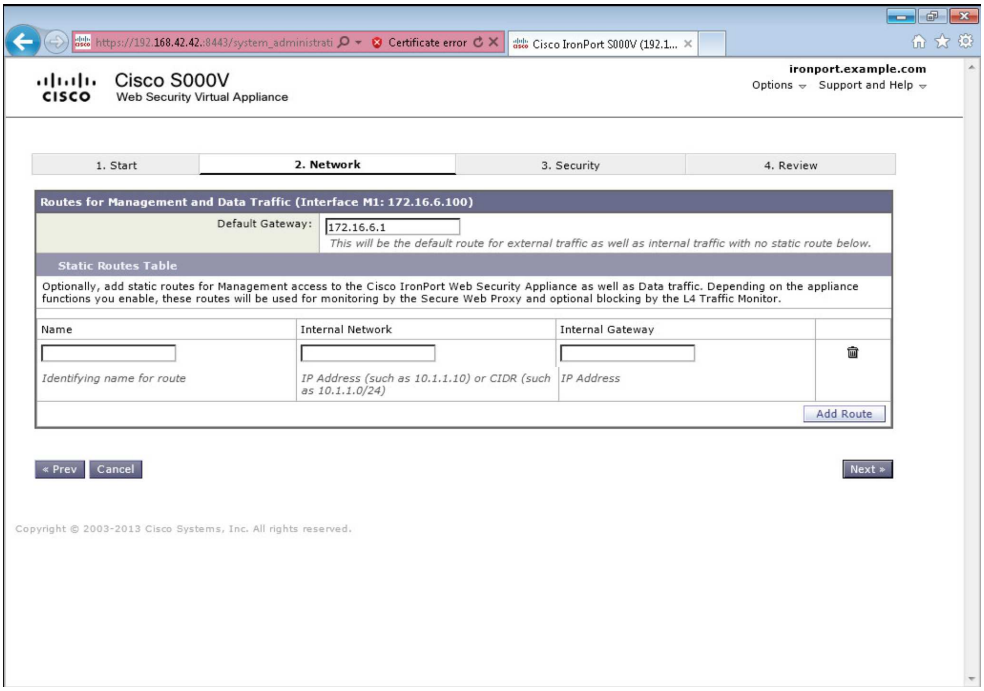


Configure the M1 interface for both proxy and management:

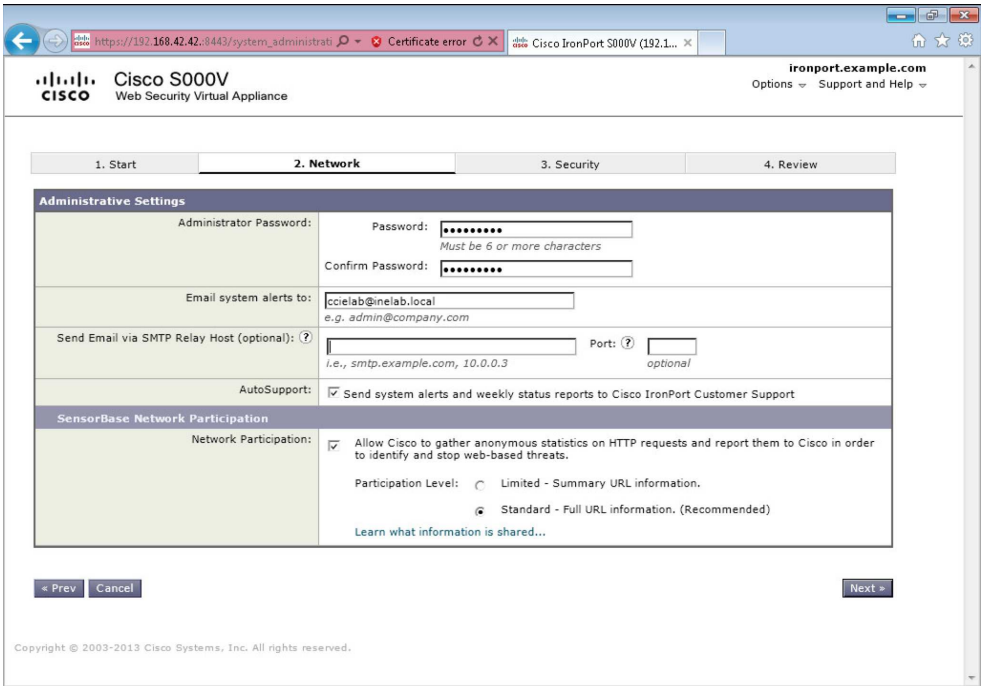


Configure the default gateway for M1 port:

https://t.me/learningnets

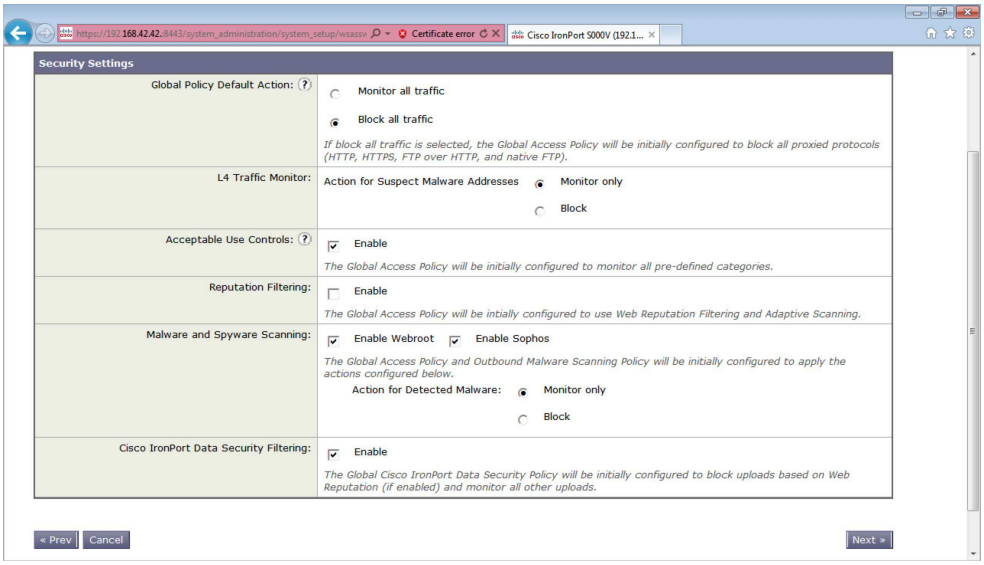


Configure the administrator password and email address:



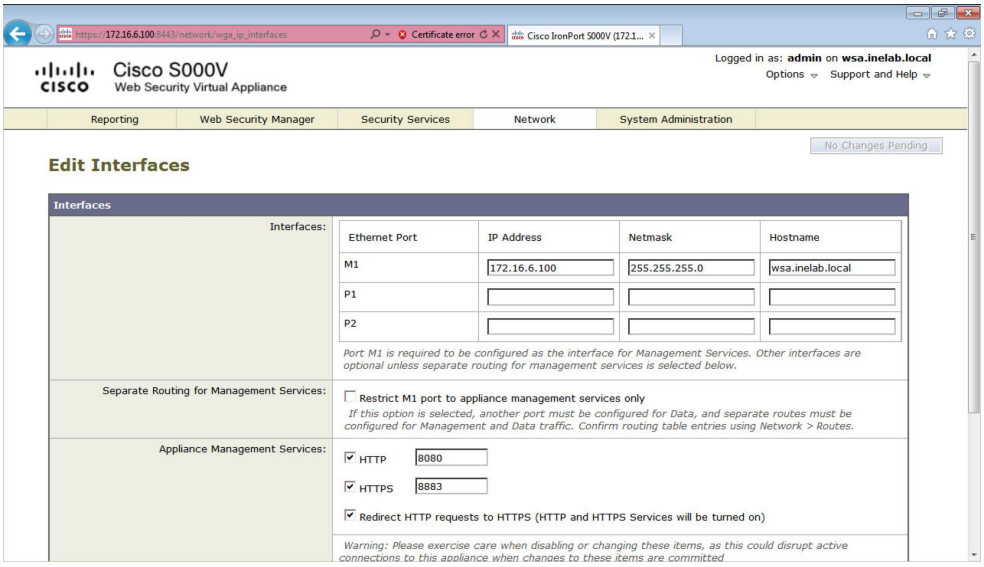
Block all protocols for the **Global Policy** and disable WBRS:

https://t.me/learningnets



All other settings are left at their default values, so screens are missing from the complete **System Setup Wizard**.

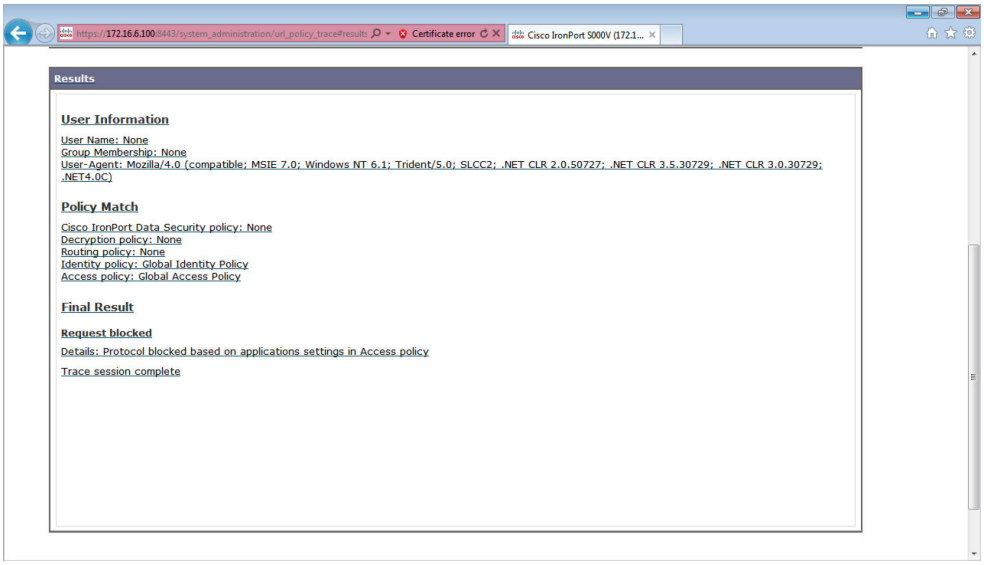
Navigate to **Network -> Interfaces** and change the default HTTPS management port from 8443 to 8883:



Task 2.4 Verification

Use Internet Explorer to manage the WSA. Using the **Policy Trace** tool from **System Administration**, simulate a connection to an IPv4 address; the request will be blocked based on the configured settings for the **Global Policy**:

https://t.me/learningnets



Task 2.5 Solution

R4:

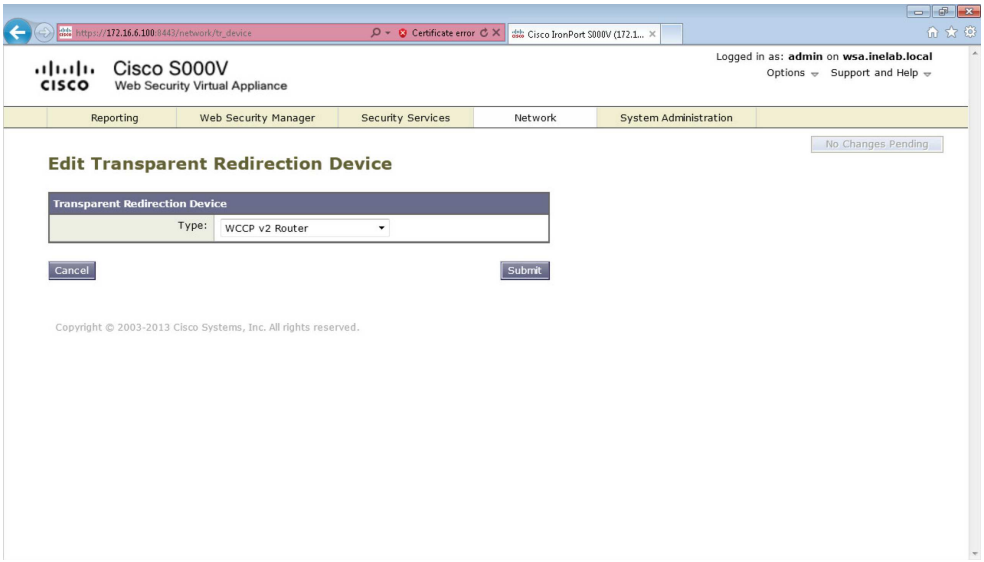
```
ip access-list extended SELF_ZONE_INSPECT_ACL
 permit udp host 172.16.6.100 host 155.1.15.4 eq 2048
!
ip access-list extended REDIRECTED_TRAFFIC
 permit tcp 155.1.99.0 0.0.0.255 any eq 80
 permit tcp 155.1.99.0 0.0.0.255 any eq 443
 permit tcp 155.1.99.0 0.0.0.255 any eq 4443
!
ip access-list standard WSA_GROUP
 permit host 172.16.6.100
!
ip wccp 95 redirect-list REDIRECTED_TRAFFIC group-list WSA_GROUP
!
interface FastEthernet0/1.48
 ip wccp 95 redirect out
```

ASA1:

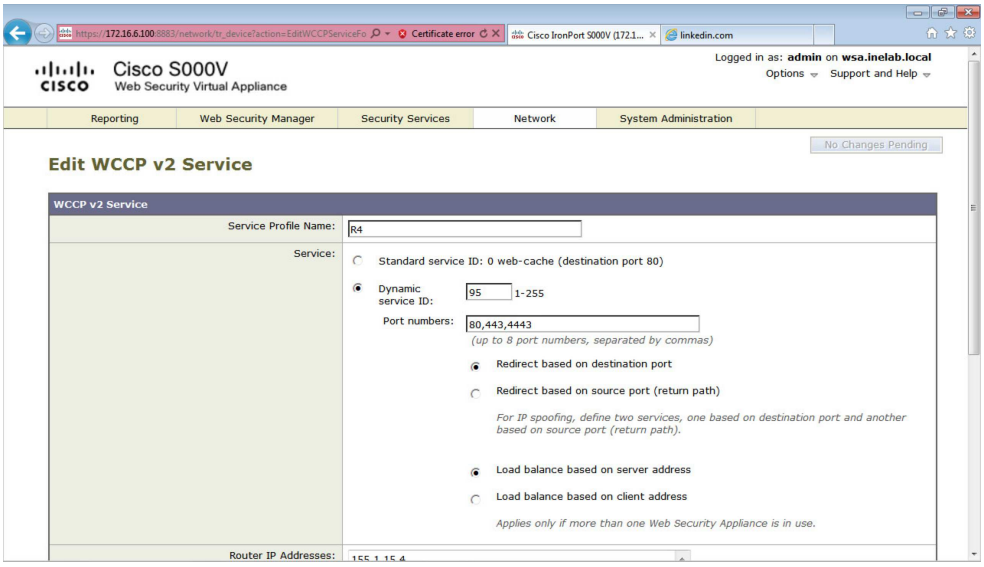
```
access-list DMZ_IN permit gre host 150.1.4.4 host 172.16.6.100
```

Browse to **Network -> Transparent Redirection** and select **WCCP v2 Router**:

https://t.me/learningnets

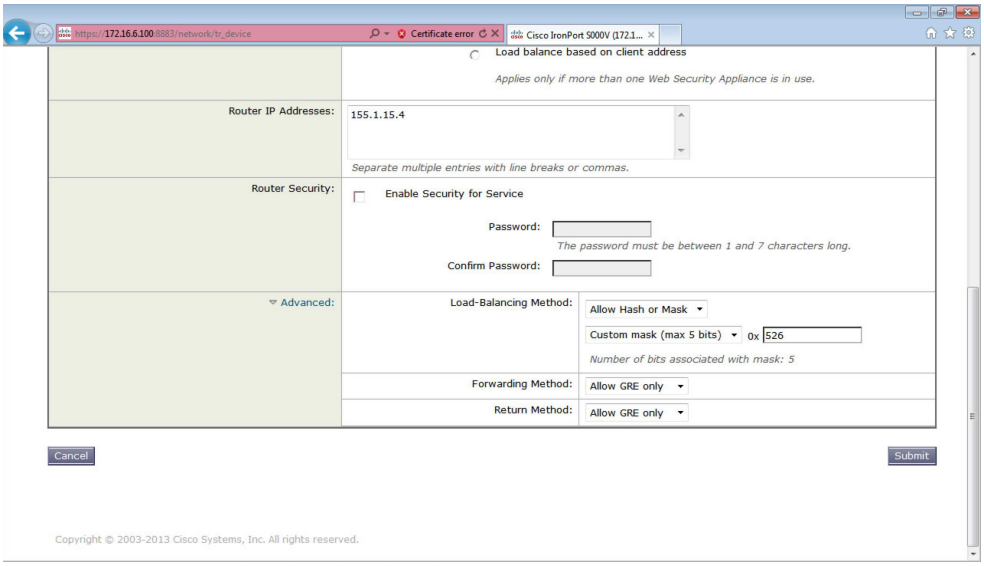


Click **Add Service**, configure the same service-id as on the router, and enable it only for HTTP and HTTPS on both 443 and 4443 ports:



Enable the service for GRE; otherwise WSA will try L2, fail, and not negotiate GRE:

https://t.me/learningnets



Task 2.5 Verification

Verify that WCCP service is functional and the requested output is being matched:

https://t.me/learningnets

```
R4#show ip wccp 95

Global WCCP information:
    Router information:
        Router Identifier:                  150.1.4.4
        Protocol Version:                   2.0

    Service Identifier: 95
        Number of Service Group Clients:    1
        Number of Service Group Routers:    1
        Total Packets s/w Redirected:       0
          Process:                          0
          CEF:                              0
        Service mode:                       Open
        Service Access-list:                -none-
        Total Packets Dropped Closed:       0
        Redirect Access-list:               REDIRECTED_TRAFFIC
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           0
        Group Access-list:                  WSA_GROUP
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total GRE Bypassed Packets Received: 0
!
!R4#show tunnel groups wccp

 WCCP : service group 351 in "Default", ver v2, assgnmnt: mask-value set
   intf: Tunnel0, locally sourced
```

Verify that redirection is performed outbound on R4's VLAN 48 interface:

```
R4#show ip wccp interfaces

WCCP interface configuration: FastEthernet0/1.48
 Output services: 1

        Input services:  0
        Mcast services:  0
        Exclude In:      FALSE
```

Verify that the WCCP UDP control-plane session is present in the firewall state table:

https://t.me/learningnets

```
R4#show policy-firewall session zone-pair UNTRUSTED_TO_SELF


 Zone-pair: UNTRUSTED_TO_SELF
  Service-policy inspect : UNTRUSTED_TO_SELF
    Class-map : INSPECT_UNTRUSTED_TO_SELF(match-any)
      Established Sessions =  1
        Session 4A61B980 (172.16.6.100:2048)=>(155.1.15.4:2048) udp SIS_OPEN
          Created 02:28:37, Last heard 00:00:02
          Bytes sent (initiator:responder) [579256:603104]
    Class-map : PASS_UNTRUSTED_TO_SELF(match-any)
    Class-map : class-default(match-any)
```

Task 2.6 Solution

https://t.me/learningnets

R4:

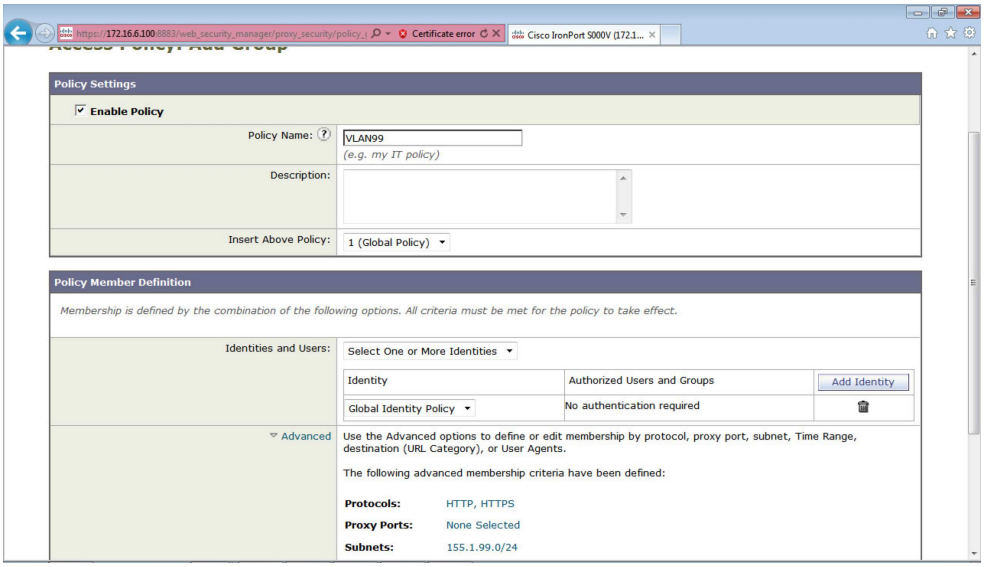
```
ip access-list extended UNTRUSTED_PASS_ACL
 permit tcp host 150.1.1.1 eq 80 155.1.99.0 0.0.0.255
 permit tcp host 150.1.1.1 eq 4443 155.1.99.0 0.0.0.255
!
class-map type inspect match-any PASS_UNTRUSTED_TO_UNTRUSTED
 match access-group name UNTRUSTED_PASS_ACL
!
policy-map type inspect UNTRUSTED_TO_UNTRUSTED
 no class type inspect UNTRUSTED_TO_UNTRUSTED
 class PASS_UNTRUSTED_TO_UNTRUSTED
  pass
 class type inspect UNTRUSTED_TO_UNTRUSTED
  inspect
```

ASA1:

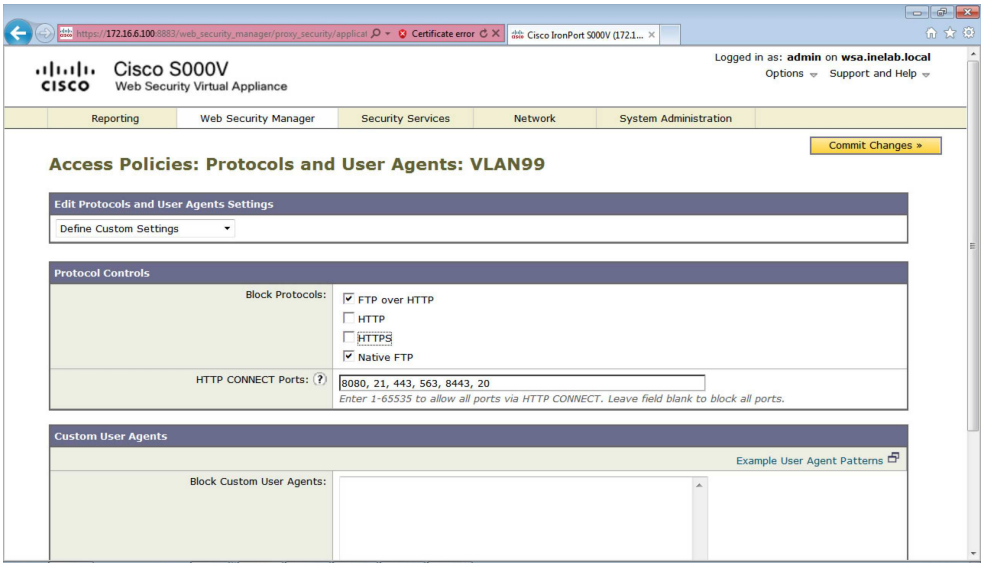
```
access-list DMZ_IN permit tcp 155.1.99.0 255.255.255.0 host 172.16.6.100 eq 3128
!
access-list WCCP_TRAFFIC permit tcp host 150.1.1.1 eq 80 155.1.99.0 255.255.255.0
access-list WCCP_TRAFFIC permit tcp host 150.1.1.1 eq 4443 155.1.99.0 255.255.255.0
!
class-map WCCP_TRAFFIC
 match access-list WCCP_TRAFFIC
!
policy-map global_policy
 class WCCP_TRAFFIC
  set connection advanced-options tcp-state-bypass
```

Navigate to **Web Security Manager -> Access Policies**, click **Add Policy**, and configure it according to the requirements; match on the **Global Identity Policy**, specify the subnet, protocols, and Global Identity Policy:

https://t.me/learningnets

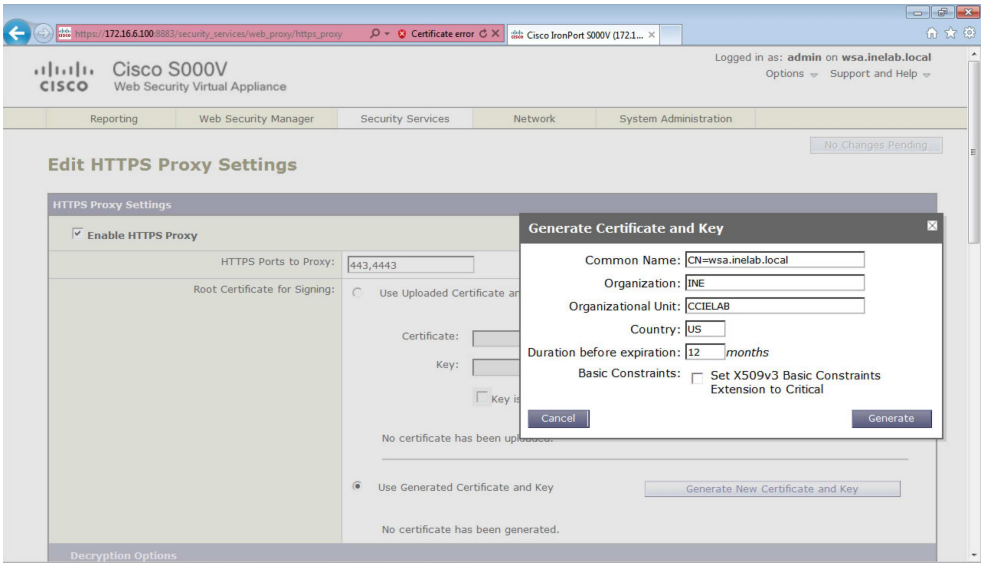


Edit the **Protocols and User Agents** settings for the configured Access Policy, and unblock HTTP/HTTPS access:

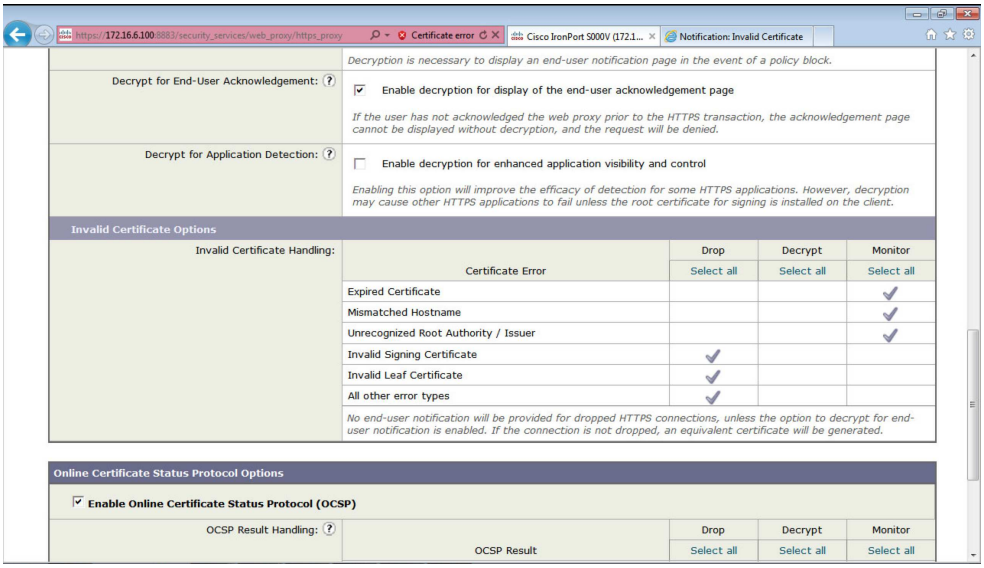


Navigate to **Security Service -> HTTPS Proxy**, click **Enable and Edit Settings**, accept the license agreement, add port 4443 to the proxy port list, and generate the self-signed certificate:

https://t.me/learningnets

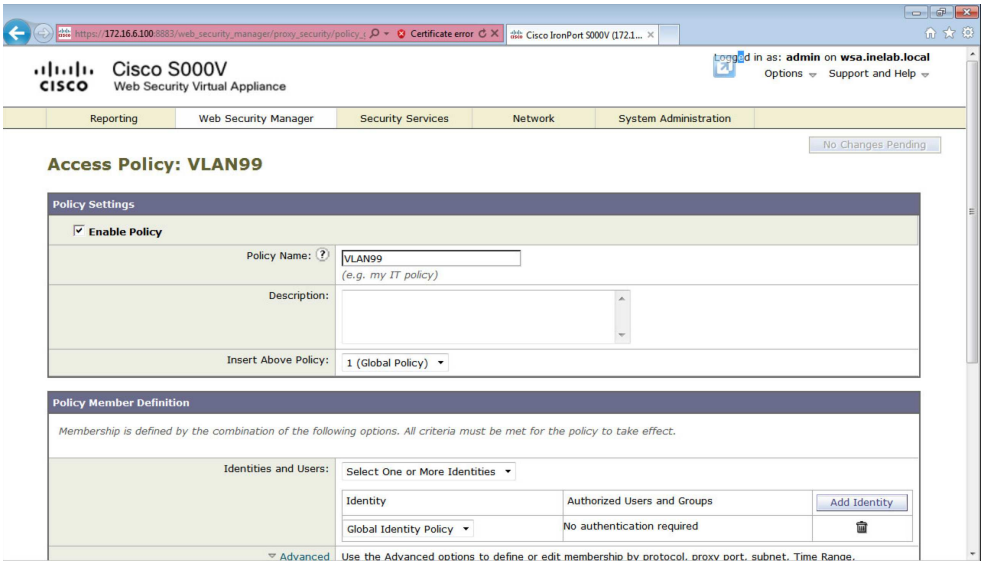


Modify the **Unrecognized Root Authority / Issuer** settings from default of **Drop** to **Monitor** or **Decrypt**:



Due to HTTPS non-decrypted sessions now being controlled by **Decryption Policies**, the configured **Access Policy** has been disabled; activate it again:

https://t.me/learningnets



Task 2.6 Verification

Configure **TEST-PC-B** with an IPv4 address of 155.1.99.50 and use Internet Explorer to access **www.linkedin.com** and **https://www.linkedin.com:4443**. Confirm that the connection is successful and requested output is being matched:

```
R1#show ip http server history


HTTP server history:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes  end-time
      150.1.1.1:4443     172.16.6.100:30428 484         192        11:27:55 04/13
      150.1.1.1:80       172.16.6.100:60186 479         192        11:28:07 04/13
```

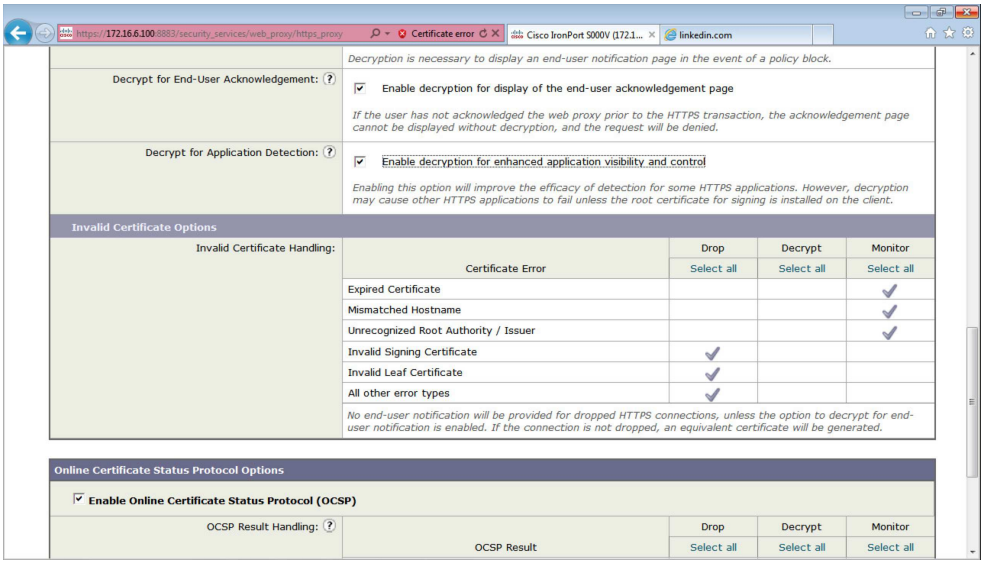
The following log messages should appear in the **accesslogs** log, confirming that both HTTP and HTTPS sessions are proxies by the WSA, and that the HTTPS session was decrypted based on the default action:

https://t.me/learningnets

```
1397400531.230 114 155.1.99.50
TCP_MISS_SSL/200 0 TCP_CONNECT 150.1.1.1:4443 - DIRECT/150.1.1.1 - DECRYPT_ADMIN-DEFAULT_ACTION_7-DefaultGroup-Defau
-NONE-NONE-NONE-DefaultGroup <IW_pnet,-,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_pnet,-,"-","-","Unknown","Unk
1397400536.527 7 155.1.99.50
TCP_MISS_SSL/401 253 GET https://www.linkedin.com:4443/ - DIRECT/150.1.1.1 text/plain DEFAULT_CASE_12-VLAN99-Default
-NONE-NONE-NONE-NONE <IW_pnet,-,0,"-",0,0,0,1,"-",-,-,-,"-",1,-,"-","-",-,-,IW_pnet,-,"-","-","LinkedIn General","Li
1397400548.004 54 155.1.99.50
TCP_MISS/401 253 GET http://www.linkedin.com/ - DIRECT/www.linkedin.com text/plain DEFAULT_CASE_12-VLAN99
-DefaultGroup-NONE-NONE-NONE-DefaultGroup <IW_pnet,-,0,"-",0,0,0,1,"-",-,-,-,"-",1,-,"-","-",-,-,IW_pnet,-,"-","-","
```

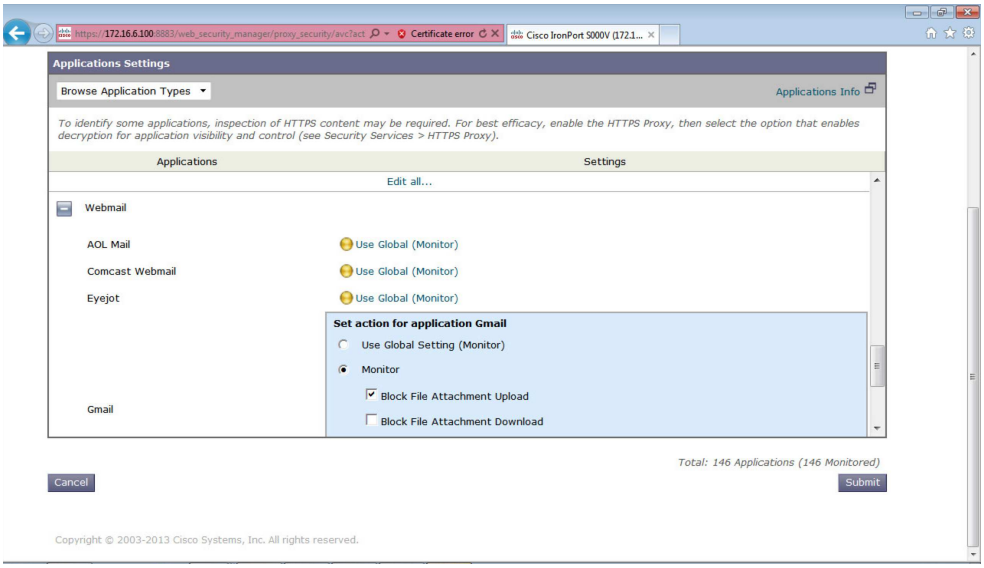
Task 2.7 Solution

Navigate to **Security Service -> HTTPS Proxy**, click **Edit Settings**, and enable decryption for application detection:

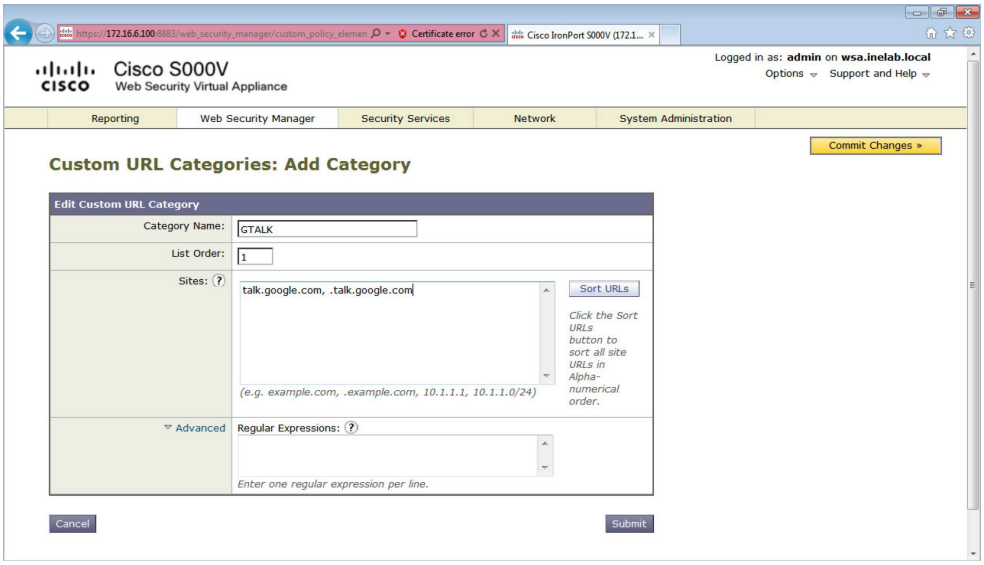


Navigate to **Web Security Manager -> Access Policies** and configure the **Applications** settings for the previously configured access policy; enable **Define Applications Custom Settings** and under the **Webmail** category, select **Block File Attachment Upload**:

https://t.me/learningnets

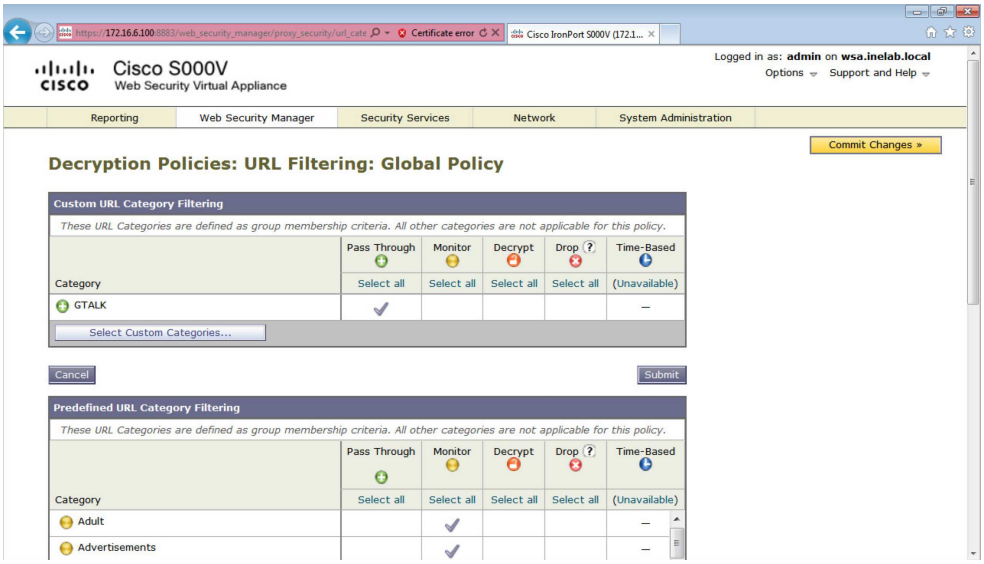


Navigate to **Web Security Manager -> Custm URL Categories**, click **Add Custom Category**, and add **talk.google.com** and **.talk.google.com** to the category.



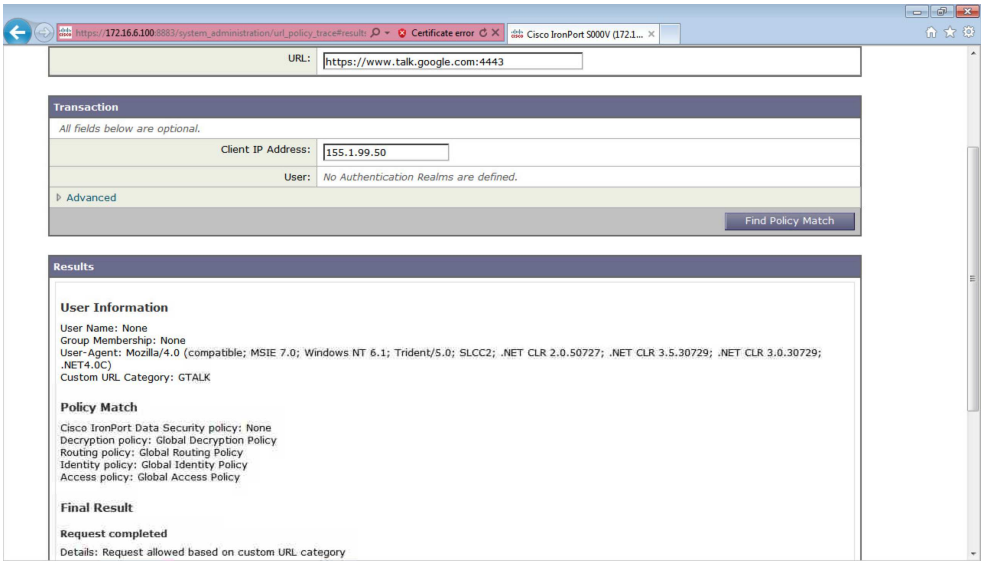
Navigate to **Web Security Manager -> Decryption Policies**, edit the **URL Filtering** settings of the default **Global Policy**, and set the action as **Pass Through** for the previously created URL Category:

https://t.me/learningnets



Task 2.7 Verification

Use the Policy Trace tool to simulate traffic to **www.talk.google.com**; the session should be allowed based on the Custom URL Category settings:



https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 5

CCIE SCv4 Lab 5 Solutions Section 3

1. Task 3.1 Solution
2. Task 3.2 Solution
3. Task 3.3 Solution
4. Task 3.4 Solution
5. Task 3.5 Solution

Task 3.1 Solution

R4:

```
ip http server
crypto key generate rsa general-keys modulus 2048 label VPN_ROOT
!
crypto pki trustpoint VPN_ROOT
 rsakeypair VPN_ROOT
 regenerate
!
crypto pki server VPN_ROOT
 hash sha1
 grant auto rollover ca-cert
 database level names
 lifetime certificate 1095
 lifetime ca-certificate 1095
 database archive pkcs12 password ccielabpassword
 issuer-name CN=R4.inelab.local
 auto-rollover 72
 no shutdown
!
!
ip access-list extended SELF_ZONE_INSPECT_ACL
 permit udp host 150.1.3.3 host 150.1.4.4 eq 123
 permit tcp host 150.1.3.3 host 150.1.4.4 eq 80
```

R3:

https://t.me/learningnets

```
ip http server
crypto key generate rsa general-keys modulus 2048 label VPN_SUBCA
ntp server 150.1.4.4 source loopback0
!
crypto pki trustpoint VPN_SUBCA
 regenerate
 source interface loopback0
 rsakeypair VPN_SUBCA
 enrollment url http://150.1.4.4
 subject-name CN=R3.inelab.local
!
crypto pki server VPN_SUBCA
 mode sub-cs
 hash sha1
 grant auto
 database level names
 lifetime certificate 1095
 lifetime ca-certificate 1095
 database archive pkcs12 password ccielabpassword
 issuer-name CN=R3.inelab.local
 auto-rollover 72
 no shutdown
```

ASA1:

```
access-list OUTSIDE_IN permit udp host 150.1.3.3 host 150.1.4.4 eq 123
access-list OUTSIDE_IN permit tcp host 150.1.3.3 host 150.1.4.4 eq 80
!
access-group OUTSIDE_IN in interface OUTSIDE
```

Task 3.1 Verification

The SUB-CA certificate cannot be automatically granted for security purposes; it must be manually granted. After configuration has been completed on all devices, use command **crypto pki server VPN_ROOT grant all** on R4 for this scope. Verify that both the ROOT-CA and SUB-CA services are enabled:

```
R4#show crypto pki server
Certificate Server VPN_ROOT: Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=R4.inelab.local
    CA cert fingerprint: 16395DD7 E29B186E ECF86AE1 12C24A9C
```

https://t.me/learningnets

```
    Granting mode is: manual
    Last certificate issued serial number (hex): 2
CA certificate expiration timer: 19:13:57 UTC Apr 12 2017
    CRL NextUpdate timer: 01:13:59 UTC Apr 14 2014
    Current primary storage dir: nvram:
Database Level: Names - subject name data written as <serialnum>.cnm
 Auto-Rollover configured, overlap period 72 days
    Autorollover timer: 19:13:57 UTC Jan 30 2017
!
!R3#show crypto pki server

Certificate Server VPN_SUBCA: Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=R3.inelab.local
    CA cert fingerprint: 31133544 EC0959E6 1D7781C9 EC490EC2
    Server configured in subordinate server mode
    Upper CA cert fingerprint: 16395DD7 E29B186E ECF86AE1 12C24A9C  Granting mode is: auto
    Last certificate issued serial number (hex): 1
CA certificate expiration timer: 19:13:57 UTC Apr 12 2017
    CRL NextUpdate timer: 01:25:11 UTC Apr 14 2014
    Current primary storage dir: nvram:
Database Level: Names - subject name data written as <serialnum>.cnm
 Auto-Rollover configured, overlap period 72 days

    Autorollover timer: 19:13:57 UTC Jan 30 2017
```

Verify the ROOT-CA and SUB-CA certificates, and note lifetime, hashing algorithm, and RSA key strength:

```
R4#show crypto pki certificates verbose
 CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=R4.inelab.local
  Subject:
    cn=R4.inelab.local
  Validity Date:  start date: 19:13:57 UTC Apr 13 2014
 end    date: 19:13:57 UTC Apr 12 2017
  Subject Key Info:
    Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit)
```

https://t.me/learningnets

```
Signature Algorithm: SHA1 with RSA Encryption

  Fingerprint MD5: 16395DD7 E29B186E ECF86AE1 12C24A9C
  Fingerprint SHA1: 371E2D82 D5E9F6E6 226BA1EF F724FE93 B80B1A33
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 3E825039 18658999 AA990F20 EB558C9E 68647AA4
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 3E825039 18658999 AA990F20 EB558C9E 68647AA4
    Authority Info Access:
  Associated Trustpoints: VPN_ROOT
!
!R3#show crypto pki certificates verbose
 Certificate (subordinate CA certificate)
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 02
  Certificate Usage: Signature
  Issuer:
    cn=R4.inelab.local
  Subject:
    cn=R3.inelab.local
  Validity Date:  start date: 19:21:48 UTC Apr 13 2014
end   date: 19:13:57 UTC Apr 12 2017
  Subject Key Info:
    Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit)
 Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 31133544 EC0959E6 1D7781C9 EC490EC2
  Fingerprint SHA1: D2243A1A 21AE05EB 5A8662A1 4050FCA5 A916B107
  X509v3 extensions:
    X509v3 Key Usage: 80000000
      Digital Signature
    X509v3 Subject Key ID: A3D576E3 6768CFC9 1AFDA52C C028F50C C892A0B8
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 3E825039 18658999 AA990F20 EB558C9E 68647AA4
    Authority Info Access:
  Associated Trustpoints: VPN_SUBCA
 CA Certificate

  Status: Available
  Version: 3
```

https://t.me/learningnets

```
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=R4.inelab.local
  Subject:
    cn=R4.inelab.local
  Validity Date:
    start date: 19:13:57 UTC Apr 13 2014
    end   date: 19:13:57 UTC Apr 12 2017
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 16395DD7 E29B186E ECF86AE1 12C24A9C
  Fingerprint SHA1: 371E2D82 D5E9F6E6 226BA1EF F724FE93 B80B1A33
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 3E825039 18658999 AA990F20 EB558C9E 68647AA4
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 3E825039 18658999 AA990F20 EB558C9E 68647AA4
    Authority Info Access:
  Associated Trustpoints: VPN_SUBCA
```

Task 3.2 Solution

R3:

```
interface FastEthernet0/1.33
 ip nat inside
!
interface FastEthernet0/0.25
 ip nat outside
!
ip nat inside source static network 155.1.35.0 155.1.33.0 /24
!
crypto pki trustpoint VPN_CLIENT
 subject-name CN=R3.inelab.local
 enrollment url http://150.1.3.3
 ip-address none
 serial-number none
!
```

https://t.me/learningnets

```
crypto pki authenticate VPN_CLIENT
crypto pki enroll VPN_CLIENT
!
ip access-list extended VLAN55_TO_VLAN33
 permit ip 155.1.33.0 0.0.0.255 155.1.55.0 0.0.0.255
!
crypto map VPN local-address loopback0
crypto map VPN 100 ipsec-isakmp
 match address VLAN55_TO_VLAN33
 set peer 150.1.5.5
!
interface FastEthernet0/0.25
 crypto map VPN
```

R5:

```
interface FastEthernet0/1.55
 ip nat inside
!
interface FastEthernet0/0.60
 ip nat outside
!
ip nat inside source static network 155.1.35.0 155.1.55.0 /24
!
crypto pki trustpoint VPN_CLIENT
 subject-name CN=R5.inelab.local
 enrollment url http://150.1.3.3
 ip-address none
 serial-number none
!
crypto pki authenticate VPN_CLIENT
crypto pki enroll VPN_CLIENT
!
ip access-list extended VLAN55_TO_VLAN33
 permit ip 155.1.55.0 0.0.0.255 155.1.33.0 0.0.0.255
!
crypto map VPN local-address loopback0
crypto map VPN 100 ipsec-isakmp
 match address VLAN55_TO_VLAN33
 set peer 150.1.3.3
!
interface FastEthernet0/0.60
 crypto map VPN
```

ASA1:

```
access-list OUTSIDE_IN permit udp host 150.1.3.3 host 150.1.5.5 eq 500
```

https://t.me/learningnets

```
!
policy-map global_policy
 class inspection_default
  inspect ipsec-pass-thru
```

Task 3.2 Verification

Verify that both R3 and R5 are enrolled in PKI, with R3 being the CA server:

```
R3#show crypto pki certificates VPN_CLIENT
Certificate
 Status: Available
  Certificate Serial Number (hex): 03 Certificate Usage: General Purpose
  Issuer:
    cn=R3.inelab.local
  Subject:
    Name: R3
    hostname=R3
    cn=R3.inelab.local
  Validity Date:
    start date: 19:59:00 UTC Apr 13 2014
    end   date: 19:13:57 UTC Apr 12 2017
  Associated Trustpoints: VPN_CLIENT
  Storage: nvram:R3inelabloca#3.cer
 CA Certificate (subordinate CA certificate)
  Status: Available
  Certificate Serial Number (hex): 02
  Certificate Usage: Signature
  Issuer:
    cn=R4.inelab.local
  Subject:
    cn=R3.inelab.local
  Validity Date:
    start date: 19:21:48 UTC Apr 13 2014
    end   date: 19:13:57 UTC Apr 12 2017
  Associated Trustpoints: VPN_CLIENT VPN_SUBCA
  Storage: nvram:R4inelabloca#2CA.cer
!
!R5#show crypto pki certificates VPN_CLIENT
Certificate
 Status: Available
  Certificate Serial Number (hex): 02 Certificate Usage: General Purpose
  Issuer:
    cn=R3.inelab.local
  Subject:
```

https://t.me/learningnets

```
    Name: R5
    hostname=R5
    cn=R5.inelab.local
  Validity Date:
    start date: 19:54:56 UTC Apr 13 2014
    end   date: 19:13:57 UTC Apr 12 2017
  Associated Trustpoints: VPN_CLIENT
  Storage: nvram:R3inelabloca#2.cer
CA Certificate

  Status: Available
  Certificate Serial Number (hex): 02
  Certificate Usage: Signature
  Issuer:
    cn=R4.inelab.local
  Subject:
    cn=R3.inelab.local
  Validity Date:
    start date: 19:21:48 UTC Apr 13 2014
    end   date: 19:13:57 UTC Apr 12 2017
  Associated Trustpoints: VPN_CLIENT
  Storage: nvram:R4inelabloca#2CA.cer
```

Generate traffic to trigger IKEv1 negotiation:

```
R3#ping 155.1.55.5 source fastEthernet0/1.33

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.55.5, timeout is 2 seconds:
Packet sent with a source address of 155.1.35.3
%CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
%CRYPTO-6-IPSEC_USING_DEFAULT: IPSec is using default transforms
.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 4/5/8 ms
```

Verify that RSA-SIG authentication has been negotiated:

```
R3#show crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
```

https://t.me/learningnets

```
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
1003  150.1.3.3       150.1.5.5                ACTIVE aes  sha  rsig 5  23:48:34

       Engine-id:Conn-id =  SW:3

IPv6 Crypto ISAKMP SA
```

Verify that packets flow bidirectionally through the IPsec tunnel:

```
R3#show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: FastEthernet0/0.25
Uptime: 00:12:14 Session status: UP-ACTIVE

Peer: 150.1.5.5 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: R5
      Desc: (none)
  IKEv1 SA: local 150.1.3.3/500 remote 150.1.5.5/500 Active
         Capabilities:(none) connid:1003 lifetime:23:47:44
  IPSEC FLOW: permit ip 155.1.33.0/255.255.255.0 155.1.55.0/255.255.255.0
       Active SAs: 2, origin: crypto map Inbound:  #pkts dec'ed 9 drop 0 life (KB/Sec) 4439342/2865
Outbound: #pkts enc'ed 9 drop 1 life (KB/Sec) 4439342/2865
```

Task 3.3 Solution

```
R4:

aaa new-model
aaa authentication login EZVPN_CLIENT local
aaa authorization network EZVPN_CLIENT local
!
username EZVPN_USER password EZVPN_PASSWORD
!
crypto isakmp policy 200
```

https://t.me/learningnets

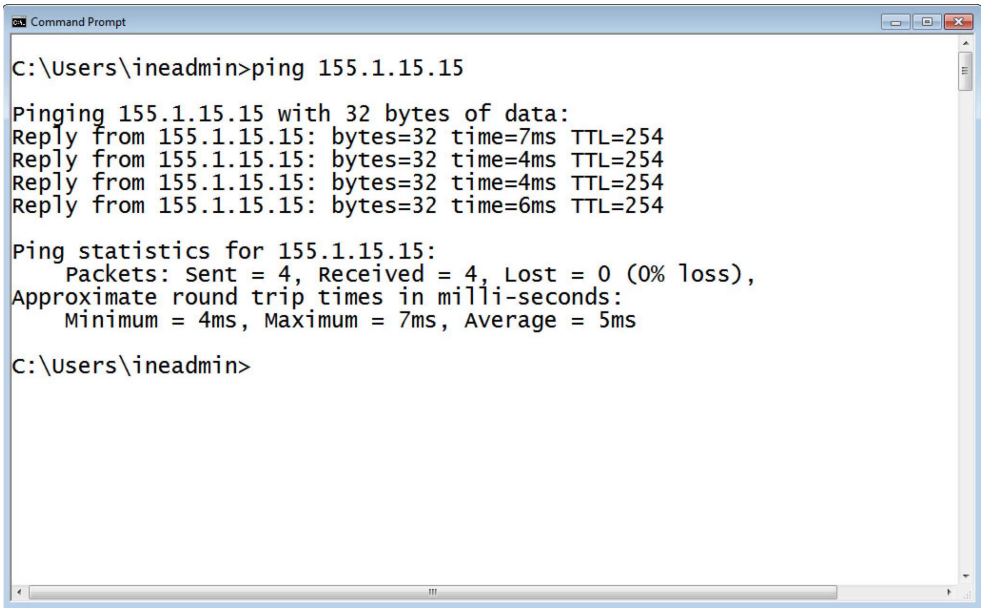
```
 authentication pre-share
 encryption aes
 hash sha
 group 2
!
ip local pool EZVPN_POOL 155.1.130.1 155.1.130.254
crypto isakmp client configuration address-pool local EZVPN_POOL
!
ip access-list extended EZVPN_TUNNEL
 permit ip 155.1.15.0 0.0.0.255 any
!
crypto isakmp client configuration group EZVPN_CLIENT
 key cisco
 pool EZVPN_POOL
 acl EZVPN_TUNNEL
!
crypto isakmp profile EZVPN_ISAKMP
 match identity group EZVPN_CLIENT
 client authentication list EZVPN_CLIENT
 isakmp authorization list EZVPN_CLIENT
 client configuration address respond
 client configuration group EZVPN_CLIENT
 virtual-template 1
!
crypto ipsec transform-set AES_SHA esp-aes esp-sha-hmac
!
crypto ipsec profile EZVPN_IPSEC
 set isakmp-profile EZVPN_ISAKMP
 set transform-set AES_SHA
!
interface Virtual-Template1 type tunnel
 ip nat inside
 ip unnumbered Loopback0
 zone-member security UNTRUSTED
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile EZVPN_IPSEC
!
ip access-list extended NAT_EZVPN
 permit ip 155.1.130.0 0.0.0.255 155.1.15.0 0.0.0.255
!
ip access-list extended SELF_ZONE_INSPECT_ACL
 permit udp 155.1.99.0 0.0.0.255 host 150.1.4.4 eq 500
!
ip access-list extended SELF_ZONE_PASS_ACL
 permit esp 155.1.99.0 0.0.0.255 host 150.1.4.4
!
```

https://t.me/learningnets

```
ip nat inside source list NAT_EZVPN interface FastEthernet0/0.15 overload
```

Task 3.3 Verification

On **TEST-PC-B**, configure the VPN client with required settings, initiate connection and authenticate, and verify that requested output is being matched:



Verify that VPN client traffic through the tunnel generated entries in the firewall state table and that NAT was triggered:

```
R4#show policy-firewall session zone-pair UNTRUSTED_TO_UNTRUSTED
 Zone-pair: UNTRUSTED_TO_UNTRUSTED
  Service-policy inspect : UNTRUSTED_TO_UNTRUSTED
    Class-map : PASS_UNTRUSTED_TO_UNTRUSTED(match-any)
    Class-map : UNTRUSTED_TO_UNTRUSTED(match-any) Established Sessions =  1
 Session 49DF0B80 (155.1.130.2:8)=>(155.1.15.15:0) icmp SIS_OPEN
          Created 00:00:02, Last heard 00:00:00
          ECHO request
          Bytes sent (initiator:responder) [96:96]
    Class-map : class-default(match-any)
!
!R4#show ip nat translations icmp

Pro Inside global      Inside local       Outside local      Outside global
icmp 155.1.15.4:1      155.1.130.2:1      155.1.15.15:1      155.1.15.15:1
```

https://t.me/learningnets

Verify that both IKEv1 and IPsec tunnels are functional and that packets flow bidirectionally through the IPsec tunnel:

```
R4#show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Virtual-Access1
Username: EZVPN_USER
Profile: EZVPN_ISAKMP
Group: EZVPN_CLIENT
Assigned address: 155.1.130.2
Uptime: 00:10:42 Session status: UP-ACTIVE
Peer: 155.1.99.50 port 60375 fvrf: (none) ivrf: (none)
      Phase1_id: EZVPN_CLIENT
      Desc: (none)
  IKEv1 SA: local 150.1.4.4/500 remote 155.1.99.50/60375 Active
          Capabilities:CX connid:4002 lifetime:23:49:10
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 155.1.130.2
        Active SAs: 2, origin: crypto map Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4482551/2957
Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4482551/2957
```

Verify the negotiated algorithms for both IKEv1 and IPsec tunnels:

```
R4#show crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
4002  150.1.4.4       155.1.99.50              ACTIVE aes  sha       2  23:43:11 CX

       Engine-id:Conn-id =  AIM-VPN/EPII-PLUS:2

IPv6 Crypto ISAKMP SA
```

https://t.me/learningnets

```
!
!R4#show crypto ipsec sa peer 155.1.99.50 | i transform
 transform: esp-aes esp-sha-hmac ,
 transform: esp-aes esp-sha-hmac ,
```

Task 3.4 Solution

```
R1:
interface Tunnel124
 tunnel key 124

R2:
interface Tunnel124
 tunnel key 124

R3:
interface Tunnel345
 tunnel key 345

R5:
interface Tunnel345
 tunnel key 345

R4:
interface Tunnel124
 tunnel key 124
 tunnel source Loopback0
 tunnel protection ipsec profile DMVPN shared
!
interface Tunnel345
 tunnel source Loopback0
 tunnel key 345
 tunnel protection ipsec profile DMVPN shared
!
ip access-list extended SELF_ZONE_INSPECT_ACL
 permit udp host 150.1.1.1 host 150.1.4.4 eq 500
 permit udp host 150.1.2.2 host 150.1.4.4 eq 500
 permit udp host 150.1.3.3 host 150.1.4.4 eq 500
 permit udp host 150.1.5.5 host 150.1.4.4 eq 500
!
ip access-list extended SELF_ZONE_PASS_ACL
 permit esp host 150.1.1.1 host 150.1.4.4
 permit esp host 150.1.2.2 host 150.1.4.4
```

https://t.me/learningnets

```
 permit esp host 150.1.3.3 host 150.1.4.4
 permit esp host 150.1.5.5 host 150.1.4.4
 permit gre host 150.1.1.1 host 150.1.4.4
 permit gre host 150.1.2.2 host 150.1.4.4
 permit gre host 150.1.3.3 host 150.1.4.4
 permit gre host 150.1.5.5 host 150.1.4.4
!
ip access-list extended UNTRUSTED_PASS_ACL
 permit esp host 150.1.1.1 host 150.1.2.2
 permit esp host 150.1.2.2 host 150.1.1.1
```

ASA1:

```
access-list OUTSIDE_IN permit udp host 150.1.2.2 host 150.1.4.4 eq 500
access-list OUTSIDE_IN permit udp host 150.1.2.2 host 150.1.1.1 eq 500
access-list OUTSIDE_IN permit udp host 150.1.3.3 host 150.1.4.4 eq 500
access-list OUTSIDE_IN permit udp host 150.1.3.3 host 150.1.5.5 eq 500
!
access-list DMZ_IN permit udp host 150.1.1.1 host 150.1.2.2 eq 500
```

Task 3.4 Verification

Verify that EIGRP neighbors are UP on both DMPVN clouds, a confirmation for hub-to-spoke IPsec tunnel functionality:

```
R4#show ip eigrp neighbors

EIGRP-IPv4 Neighbors for AS(124)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   31.31.31.1              Tu124             12 00:18:05   12  1428  0  17
1   31.31.31.2              Tu124             11 00:18:29    7  1428  0  16
EIGRP-IPv4 Neighbors for AS(345)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   41.41.41.5              Tu345             12 00:16:06    7  1434  0  11
1   41.41.41.3              Tu345             10 00:16:14    6  1434  0  9
```

Verify that spokes from each DMVPN cloud learn the remote spoke prefix through EIGRP:

```
R1#show ip route eigrp 124
```

https://t.me/learningnets

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
D   %    2.2.2.2 [90/28288000] via 31.31.31.4, 00:20:06, Tunnel124
!
!R2#show ip route eigrp 124
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
D   %    1.1.1.1 [90/28288000] via 31.31.31.4, 00:20:16, Tunnel124
!
!R3#show ip route eigrp 124

R3#show ip route eigrp 345
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 155.1.25.15 to network 0.0.0.0

      5.0.0.0/32 is subnetted, 1 subnets
D        5.5.5.5 [90/28288000] via 41.41.41.4, 00:18:34, Tunnel345
```

https://t.me/learningnets

```
!
!R5#show ip route eigrp 345
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      3.0.0.0/32 is subnetted, 1 subnets
D        3.3.3.3 [90/28288000] via 41.41.41.4, 00:18:46, Tunnel345
```

Verify that the requested output is being matched, confirming that spoke-to-spoke tunnel was established:

```
R1#ping 2.2.2.2 source loopback1 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 4/7/20 ms
!
!R1#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel124, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     2       150.1.2.2      31.31.31.2    UP 00:00:36   DT2
                            31.31.31.2    UP 00:00:36     D
     1       150.1.4.4      31.31.31.4    UP 00:00:55     S
!
```

https://t.me/learningnets

```
!R3#ping 5.5.5.5 source loopback1 repeat 10


Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 3.3.3.3
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 8/19/40 ms
!
!R3#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel345, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     2       150.1.5.5      41.41.41.5   IKE 00:00:16     D
                            41.41.41.5   IKE 00:00:16     D
     1       150.1.4.4      41.41.41.4    UP 00:00:30     S
```

Task 3.5 Solution

```
R1:
ip access-list extended RED_EXCEPTION
 deny ip host 150.1.1.1 host 150.1.1.14
!
ip access-list extended GREEN_EXCEPTION
 deny ip host 150.11.1.1 host 150.11.1.14
!
crypto isakmp profile GETVPN_ISAKMP
 keyring DMVPN_KEYRING
 match identity address 150.1.4.4 MGMT
!
crypto gdoi group VRF_RED_GROUP
 identity number 11
 server address ipv4 150.1.4.4
 client registration interface gigabitEthernet0/0
```

https://t.me/learningnets

```
!
crypto gdoi group VRF_GREEN_GROUP
 identity number 33
 server address ipv4 150.1.4.4
 client registration interface gigabitEthernet0/0
!
crypto map VRF_RED_MAP isakmp-profile GETVPN_ISAKMP
crypto map VRF_RED_MAP 100 gdoi
 set group VRF_RED_GROUP
 match address RED_EXCEPTION
!
crypto map VRF_GREEN_MAP isakmp-profile GETVPN_ISAKMP
crypto map VRF_GREEN_MAP 100 gdoi
 set group VRF_GREEN_GROUP
 match address GREEN_EXCEPTION
!
interface GigabitEthernet0/1.11
  crypto map VRF_RED_MAP
!
interface GigabitEthernet0/1.22
  crypto map VRF_GREEN_MAP
```

R2:

```
ip access-list extended RED_EXCEPTION
 deny ip host 150.1.2.1 host 150.1.2.14
!
ip access-list extended GREEN_EXCEPTION
 deny ip host 150.11.2.1 host 150.11.2.14
!
!
crypto isakmp profile GETVPN_ISAKMP
 keyring DMVPN_KEYRING
 match identity address 150.1.4.4 MGMT
!
crypto gdoi group VRF_RED_GROUP
 identity number 11
 server address ipv4 150.1.4.4
 client registration interface gigabitEthernet0/0
!
crypto gdoi group VRF_GREEN_GROUP
 identity number 33
 server address ipv4 150.1.4.4
 client registration interface gigabitEthernet0/0
!
crypto map VRF_RED_MAP isakmp-profile GETVPN_ISAKMP
crypto map VRF_RED_MAP 100 gdoi
```

https://t.me/learningnets

```
 set group VRF_RED_GROUP
 match address RED_EXCEPTION
!
crypto map VRF_GREEN_MAP isakmp-profile GETVPN_ISAKMP
crypto map VRF_GREEN_MAP 100 gdoi
 set group VRF_GREEN_GROUP
 match address GREEN_EXCEPTION
!
interface GigabitEthernet0/1.33
  crypto map VRF_RED_MAP
!
interface GigabitEthernet0/1.44
  crypto map VRF_GREEN_MAP
```

R4:

```
ip access-list extended SELF_ZONE_INSPECT_ACL
 permit udp host 155.1.10.1 host 150.1.4.4 eq 848
 permit udp host 155.1.20.2 host 150.1.4.4 eq 848
```

ASA1:

```
access-list OUTSIDE_IN permit udp host 155.1.20.2 host 150.1.4.4 eq 848
```

Task 3.5 Verification

Verify that R1 and R2 have registered with the KS for both groups, each group being mapped to a VRF on the GMs:

```
R4#show crypto gdoi ks members


Group Member Information :

Number of rekeys sent for group VRF_RED_GROUP : 0
Group Member ID     : 155.1.10.1
Group ID            : 11
Group Name          : VRF_RED_GROUP
Key Server ID       : 150.1.4.4
 Rekeys sent        : 0
 Rekeys retries     : 0
 Rekey Acks Rcvd    : 0
 Rekey Acks missed  : 0

 Sent seq num : 0       0       0       0
```

https://t.me/learningnets

```
Rcvd seq num :  0       0       0       0
Group Member ID     : 155.1.20.2
Group ID            : 11
Group Name          : VRF_RED_GROUP
Key Server ID       : 150.1.4.4
 Rekeys sent        : 0
 Rekeys retries     : 0
 Rekey Acks Rcvd    : 0
 Rekey Acks missed  : 0

 Sent seq num : 0       0       0       0
Rcvd seq num :  0       0       0       0

Number of rekeys sent for group VRF_BLUE_GROUP : 0
Group Member ID     : 155.1.10.1
Group ID            : 33
Group Name          : VRF_BLUE_GROUP
Key Server ID       : 150.1.4.4
 Rekeys sent        : 0
 Rekeys retries     : 0
 Rekey Acks Rcvd    : 0
 Rekey Acks missed  : 0

 Sent seq num : 0       0       0       0
Rcvd seq num :  0       0       0       0
Group Member ID     : 155.1.20.2
Group ID            : 33
Group Name          : VRF_BLUE_GROUP
Key Server ID       : 150.1.4.4

 Rekeys sent        : 0
 Rekeys retries     : 0
 Rekey Acks Rcvd    : 0
 Rekey Acks missed  : 0

 Sent seq num : 0       0       0       0
Rcvd seq num :  0       0       0       0
```

Verify that the requested output is being matched, confirming that ACL policies have been downloaded from the KS:

```
R1#show crypto gdoi ipsec sa

SA created for group VRF_RED_GROUP:
  GigabitEthernet0/1.11:
```

https://t.me/learningnets

```
    protocol = ip
      local ident  = 150.1.0.0/16, port = 0
      remote ident = 150.1.0.0/16, port = 0
      direction: Both, replay: Disabled

SA created for group VRF_GREEN_GROUP:
  GigabitEthernet0/1.22:
    protocol = ip
      local ident  = 150.11.0.0/16, port = 0
      remote ident = 150.11.0.0/16, port = 0
      direction: Both, replay: Disabled
!
!R2#show crypto gdoi ipsec sa


SA created for group VRF_RED_GROUP:
  GigabitEthernet0/1.33:
    protocol = ip
      local ident  = 150.1.0.0/16, port = 0
      remote ident = 150.1.0.0/16, port = 0
      direction: Both, replay: Disabled

SA created for group VRF_GREEN_GROUP:
  GigabitEthernet0/1.44:
    protocol = ip
      local ident  = 150.11.0.0/16, port = 0
      remote ident = 150.11.0.0/16, port = 0
      direction: Both, replay: Disabled
```

Verify that a local ACL exception has been configured to allow unencrypted communication between routers and the switch:

```
R1#show crypto gdoi gm acl
 Group Name: VRF_RED_GROUP
 ACL Downloaded From KS 150.1.4.4:
   access-list  permit ip 150.1.0.0 0.0.255.255 150.1.0.0 0.0.255.255 ACL Configured Locally:

  Map Name: VRF_RED_MAP access-list RED_EXCEPTION deny ip host 150.1.1.1 host 150.1.1.14
Group Name: VRF_GREEN_GROUP
 ACL Downloaded From KS 150.1.4.4:
   access-list  permit ip 150.11.0.0 0.0.255.255 150.11.0.0 0.0.255.255 ACL Configured Locally:
  Map Name: VRF_GREEN_MAP access-list GREEN_EXCEPTION deny ip host 150.11.1.1 host 150.11.1.14
!
!R2#show crypto gdoi gm acl
```

https://t.me/learningnets

```
Group Name: VRF_RED_GROUP
 ACL Downloaded From KS 150.1.4.4:
   access-list  permit ip 150.1.0.0 0.0.255.255 150.1.0.0 0.0.255.255 ACL Configured Locally:

  Map Name: VRF_RED_MAP access-list RED_EXCEPTION deny ip host 150.1.2.1 host 150.1.2.14

Group Name: VRF_GREEN_GROUP
 ACL Downloaded From KS 150.1.4.4:
   access-list  permit ip 150.11.0.0 0.0.255.255 150.11.0.0 0.0.255.255 ACL Configured Locally:
  Map Name: VRF_GREEN_MAP access-list GREEN_EXCEPTION deny ip host 150.11.2.1 host 150.11.2.14
```

Verify that the requested output is being matched, confirming that a local ACL is active and used by the routers:

```
R1#ping vrf RED 150.1.1.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!R1#ping vrf RED 150.1.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!R1#ping vrf GREEN 150.11.1.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.11.1.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!
!R1#ping vrf GREEN 150.11.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.11.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Verify that packets have been encrypted/decrypted for both VRF **RED** and **GREEN**:

```
R1#show crypto ipsec sa vrf RED | i pkts
 #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
```

https://t.me/learningnets

```
 #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
!
!R1#show crypto ipsec sa vrf GREEN | i pkts
 #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
 #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
!
!R2#show crypto ipsec sa vrf RED | i pkts
   #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
 #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
!
!R2#show crypto ipsec sa vrf GREEN | i pkts
 #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
 #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 5

CCIE SCv4 Lab 5 Solutions Section 4

1. Task 4.1 Solution
2. Task 4.2 Solution
3. Task 4.3 Solution
4. Task 4.4 Solution
5. Task 4.5 Solution

Task 4.1 Solution

https://t.me/learningnets

ASA1:

```
ldap attribute-map AUTHENTICATION
 map-name department Privilege-Level
 map-value department CCIELAB 11
!
aaa-server LDAP protocol ldap
aaa-server LDAP (DMZ) host 155.1.15.100
 ldap-base-dn DC=inelab, DC=local
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password 1qaz@WSX
 ldap-login-dn CN=ldapuser,CN=Users,DC=inelab,DC=local
 server-type microsoft
 ldap-attribute-map AUTHENTICATION
!
aaa authentication telnet console LDAP
aaa authentication enable console LDAP
aaa authorization command LOCAL
!
privilege show level 11 mode exec command nameif
privilege show level 11 mode exec command route
!
telnet 150.1.5.5 255.255.255.255 INSIDE
```

Task 4.1 Verification

Verify that telnet service is enabled on ASA **INSIDE** interface, but sessions are not allowed unless source IP address os R5's Loopback0:

https://t.me/learningnets

```
ASA12/act# show asp  table socket



Protocol  Socket    Local Address               Foreign Address         State
TCP       000203ff  172.16.6.1:23               0.0.0.0:*               LISTEN

!
!R5#telnet 172.16.6.1

Trying 172.16.6.1 ... % Connection timed out; remote host not responding
```

Authenticate with **USER3** and verify access to requested commands:

```
R5#telnet 172.16.6.1 /source-interface Loopback0
Trying 172.16.6.1 ... Open



User Access Verification

Username: USER3
Password: ********
Type help or '?' for a list of available commands.ASA12/act> show curpriv
Username : USER3
Current privilege level : 1
Current Mode/s : P_UNPRASA12/act> enable
Password: ********ASA12/act# show curpriv
Username : USER3
Current privilege level : 11
Current Mode/s : P_PRIVASA12/act# show nameif
Interface                Name                    Security
Redundant1               DMZ                      50
Redundant1.25            OUTSIDE                  10
Redundant1.60            INSIDE                   90ASA12/act# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

https://t.me/learningnets

```
Gateway of last resort is not set

C    155.1.202.0 255.255.255.0 is directly connected, FAILOVER
C    155.1.25.0 255.255.255.0 is directly connected, OUTSIDE
O    155.1.20.0 255.255.255.0 [110/12] via 155.1.25.3, 13:32:21, OUTSIDE
O    155.1.10.0 255.255.255.0 [110/12] via 155.1.15.4, 11:57:23, DMZ
C    155.1.15.0 255.255.255.0 is directly connected, DMZ
O    155.1.0.0 255.255.0.0 is a summary, 11:57:23
O    155.1.48.0 255.255.255.0 [110/11] via 155.1.15.4, 11:57:23, DMZ
O    155.1.43.0 255.255.255.0 [110/11] via 155.1.15.4, 11:57:23, DMZ
O    155.1.34.0 255.255.255.0 [110/12] via 155.1.25.3, 13:32:21, OUTSIDE
O    155.1.39.0 255.255.255.0 [110/11] via 155.1.25.3, 13:32:21, OUTSIDE
O    155.1.70.0 255.255.255.0 [110/12] via 155.1.15.4, 11:57:23, DMZ
O    155.1.99.0 255.255.255.0 [110/12] via 155.1.15.4, 11:57:23, DMZ
O    172.16.10.0 255.255.255.0 [110/11] via 155.1.15.4, 11:57:23, DMZ
D    172.16.5.0 255.255.255.0 [90/28416] via 172.16.6.5, 48:14:09, INSIDE
ASA12/act# show interface ip brief
                  ^
ERROR: % Invalid input detected at '^' marker.ERROR: Command authorization failed
ASA12/act# configure terminal
             ^
ERROR: % Invalid input detected at '^' marker.ERROR: Command authorization failed
```

Verify the communication with the LDAP server:

https://t.me/learningnets

```
ASA12/act# show aaa-server LDAP

Server Group:    LDAP
Server Protocol: ldap
Server Address:  155.1.15.100
Server port:     0Server status:   ACTIVE, Last transaction at unknown

Number of pending requests              0
Average round trip time                 0msNumber of authentication requests       12

Number of authorization requests        0
Number of accounting requests           0
Number of retransmissions               0Number of accepts                         11

Number of rejects                       0
Number of challenges                    0
Number of malformed responses           0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
```

Task 4.2 Solution

```
R1:
aaa new-model
!
tacacs server TACACS
 address ipv4 155.1.34.110
 key cisco
 single-connection
!
aaa group server tacacs+ ACS_TACACS
 server name TACACS
 ip tacacs source-interface Loopback0
 ip vrf forwarding MGMT
!
aaa authentication login VTY group ACS_TACACS
aaa authentication enable default group ACS_TACACS
aaa authorization commands 15 VTY group ACS_TACACS
!
aaa authorization config-commands
aaa authorization exec VTY group ACS_TACACS
```

https://t.me/learningnets

```
aaa accounting commands 15 VTY start-stop group ACS_TACACS
!
line console 0
 privilege legel 15
!
line vty 0 14
 login authentication VTY
 authorization exec VTY
 authorization commands 15 VTY
 accounting commands 15 VTY
```

ASA1:

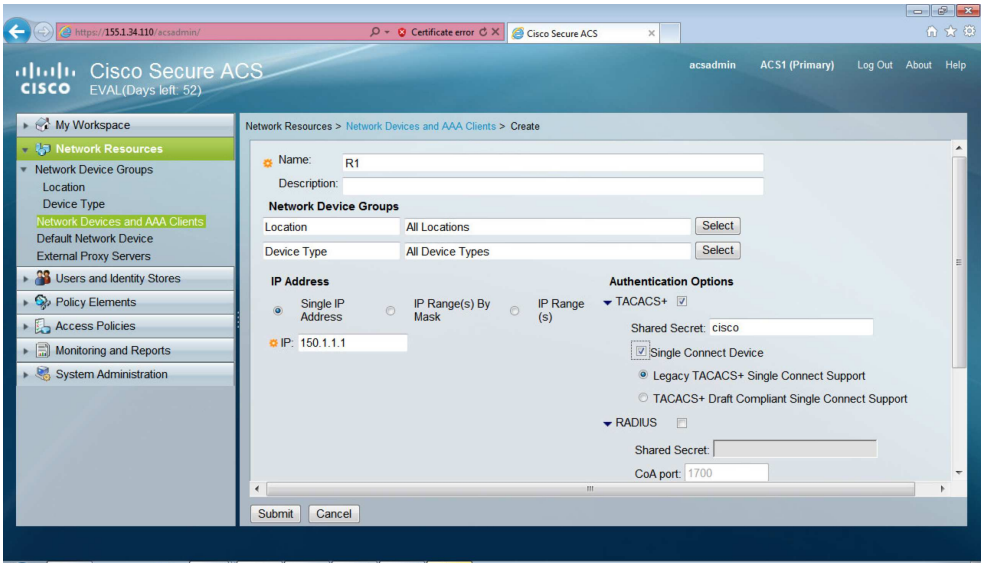
```
access-list DMZ_IN permit tcp host 150.1.1.1 host 155.1.34.110 eq 49
access-list DMZ_IN permit tcp 155.1.99.0 255.255.255.0 host 155.1.34.110 eq 443
```

ASA3 ACS Context:

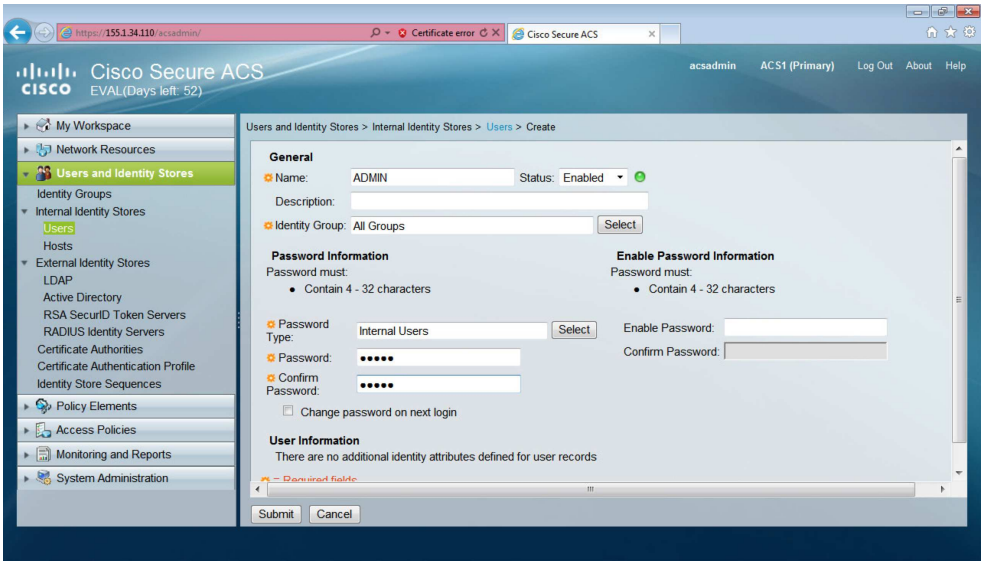
```
route OUTSIDE 150.1.1.1 255.255.255.255 155.1.34.10
route OUTSIDE 155.1.99.0 255.255.255.0 155.1.34.10
!
object network ACS_REAL
 host 172.16.1.100
 nat (INSIDE,OUTSIDE) static 155.1.34.110
!
access-list OUTSIDE_IN permit tcp host 150.1.1.1 host 172.16.1.100 eq 49
access-list OUTSIDE_IN permit tcp 155.1.99.0 255.255.255.0 host 172.16.1.100 eq 443
!
access-group OUTSIDE_IN in interface OUTSIDE
```

From **TEST-PC-B**, use Internet Explorer to browse to ACS and navigate to **Network Resources -> Network Devices and AAA Clients**; click **Create** to add R1 as NAD client for TACACS, and enable **Single Connect Device**:

https://t.me/learningnets

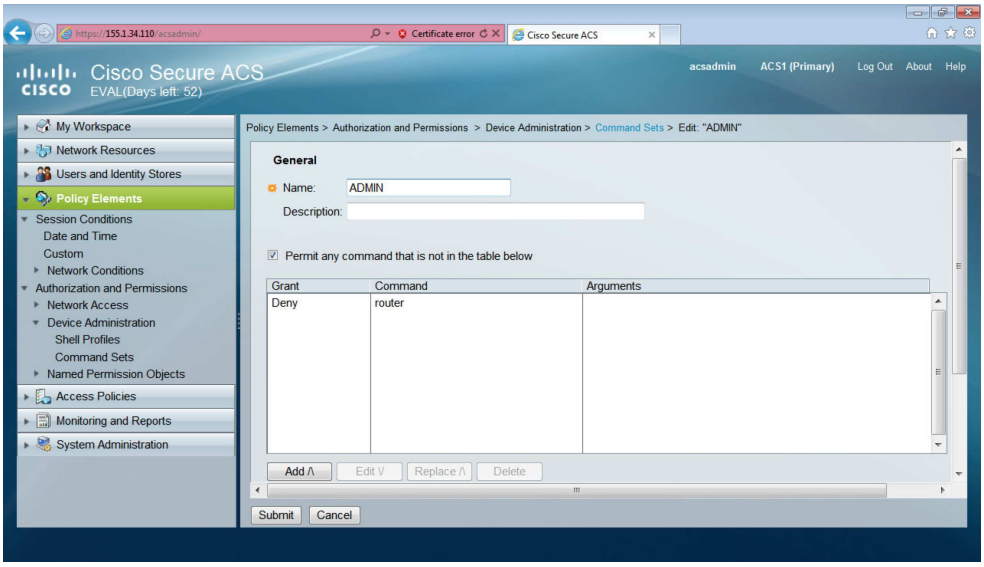


Navigate to **Users and Identity Stores- > Internal Identity Stores -> Users** and click **Create** to add **ADMIN** user to ACS database:

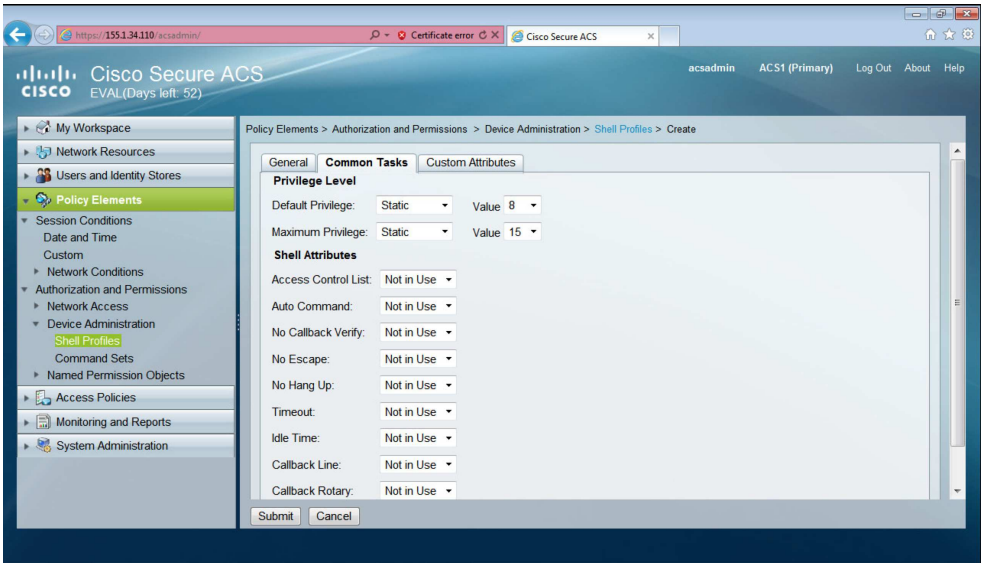


Navigate to **Policy Elements -> Authorization and Permissions -> Device Administration -> Command Sets** and click **Create**; allow access to all unspecified commands but restrict access to configuring routing protocols:

https://t.me/learningnets

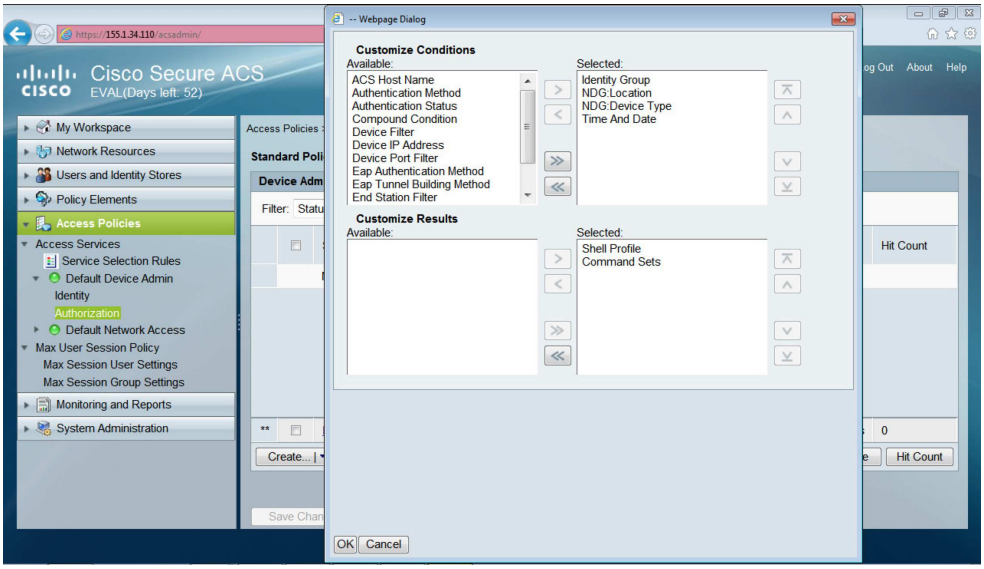


Navigate to **Policy Elements -> Authorization and Permissions -> Device Administration -> Shell Profiles** and click **Create** to assign the default and maximum privilege-level:

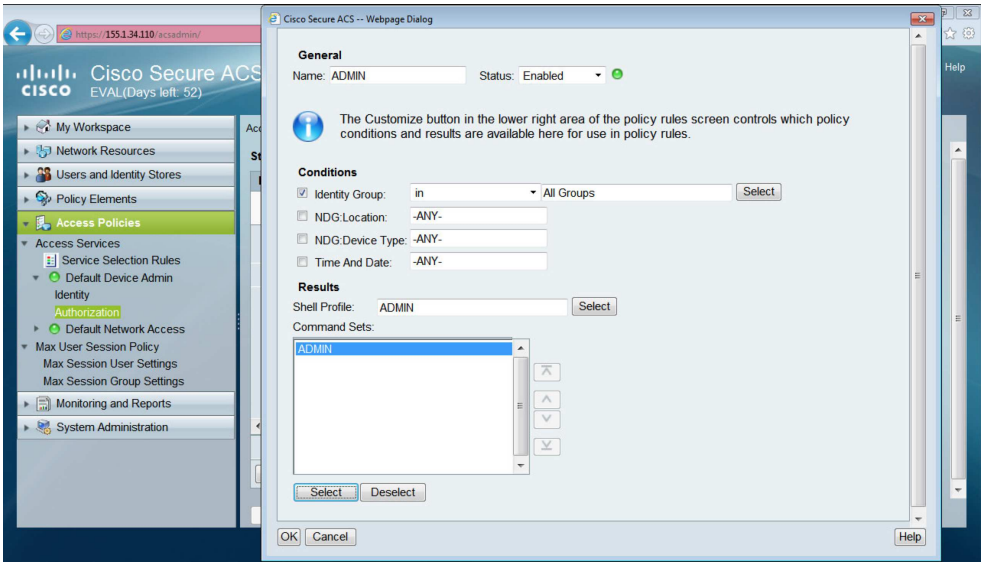


Navigate to **Access Policies -> Default Device Admin -> Authorization** and click **Customize** to add the command set as authorization result:

https://t.me/learningnets



Navigate to **Access Policies -> Default Device Admin -> Authorization** and click **Create** to add the authorization rule:



Task 4.2 Verification

Verify basic authentication from the console of R1:

```
R1#test aaa group ACS_TACACS ADMIN CISCO legacy

Attempting authentication test to server-group ACS_TACACS using tacacs+
User was successfully authenticated.
```

Initiate a telnet session to R1, verify default assigned privilege-level and maximum allowed privilege-level, and verify that the user has access to all commands except

https://t.me/learningnets

routing protocols:

```
SW1#telnet 150.1.1.1
Trying 150.1.1.1 ... Open
username: ADMIN
password:
R1#show privilege
Current privilege level is 8
R1#enable
password: R1#show privilege
Current privilege level is 15
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.R1(config)#interface Loopback0
R1(config-if)#exit
R1(config)#router rip
Command authorization failed.
R1(config)#router ospf 100
Command authorization failed.
R1(config)#router eigrp 100
Command authorization failed.
R1(config)#router bgp 100
Command authorization failed.
```

Task 4.3 Solution

```
R4:
aaa new-model
!
aaa group server radius ACS_RADIUS
 server-private 155.1.34.110 key cisco
 ip radius source-interface Loopback0
!
aaa authentication login default group ACS_RADIUS
aaa authentication login CONSOLE none
aaa authentication enable default group ACS_RADIUS
!
aaa authorization exec VTY group ACS_RADIUS
aaa accounting exec VTY start-stop group ACS_RADIUS
!
line con 0
 privilege level 15
 login authentication CONSOLE
```

https://t.me/learningnets

```
!
line vty 0 14
 authorization exec VTY
 accounting exec VTY
!
ip access-list extended SELF_ZONE_PASS_ACL
 permit udp host 155.1.34.110 eq 1645 host 150.1.4.4
 permit udp host 155.1.34.110 eq 1646 host 150.1.4.4
 permit udp host 155.1.34.110 eq 1812 host 150.1.4.4
 permit udp host 155.1.34.110 eq 1813 host 150.1.4.4
```

ASA1:

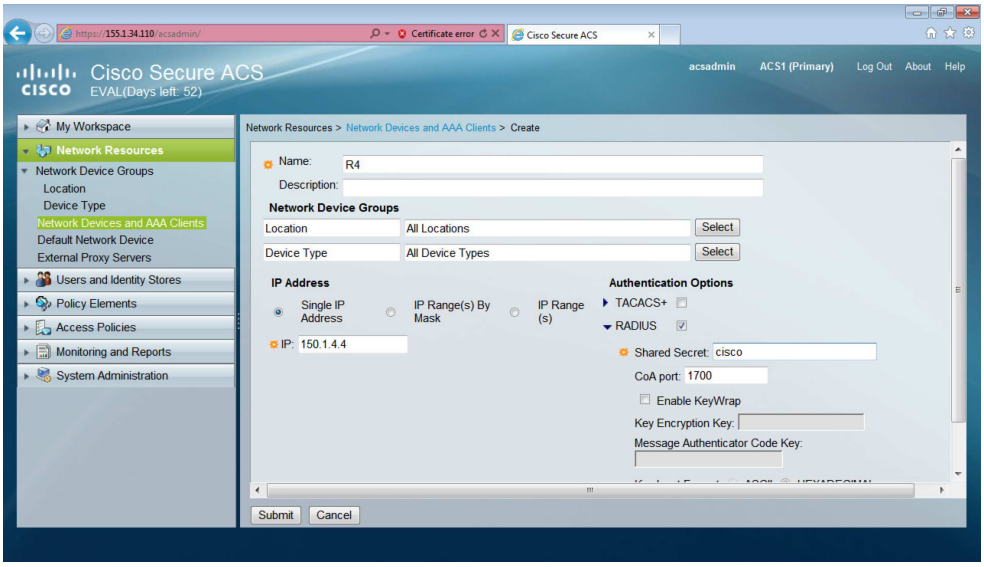
```
access-list DMZ_IN permit udp host 150.1.4.4 host 155.1.34.110 eq 1645
access-list DMZ_IN permit udp host 150.1.4.4 host 155.1.34.110 eq 1646
access-list DMZ_IN permit udp host 150.1.4.4 host 155.1.34.110 eq 1812
access-list DMZ_IN permit udp host 150.1.4.4 host 155.1.34.110 eq 1813
```

ASA3 ACS Context:

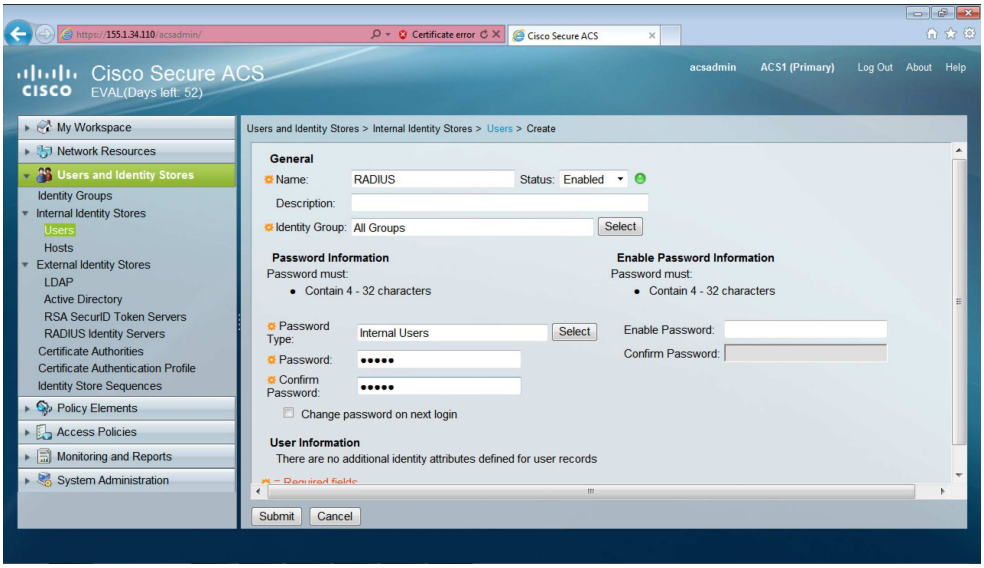
```
route OUTSIDE 150.1.4.4 255.255.255.255 155.1.34.10
!
access-list OUTSIDE_IN permit udp host 150.1.4.4 host 172.16.1.100 eq 1645
access-list OUTSIDE_IN permit udp host 150.1.4.4 host 172.16.1.100 eq 1646
access-list OUTSIDE_IN permit udp host 150.1.4.4 host 172.16.1.100 eq 1812
access-list OUTSIDE_IN permit udp host 150.1.4.4 host 172.16.1.100 eq 1813
```

From **TEST-PC-B**, use Internet Explorer to browse to ACS and navigate to **Network Resources -> Network Devices and AAA Clients**; click **Create** to add R4 as NAD client for RADIUS:

https://t.me/learningnets

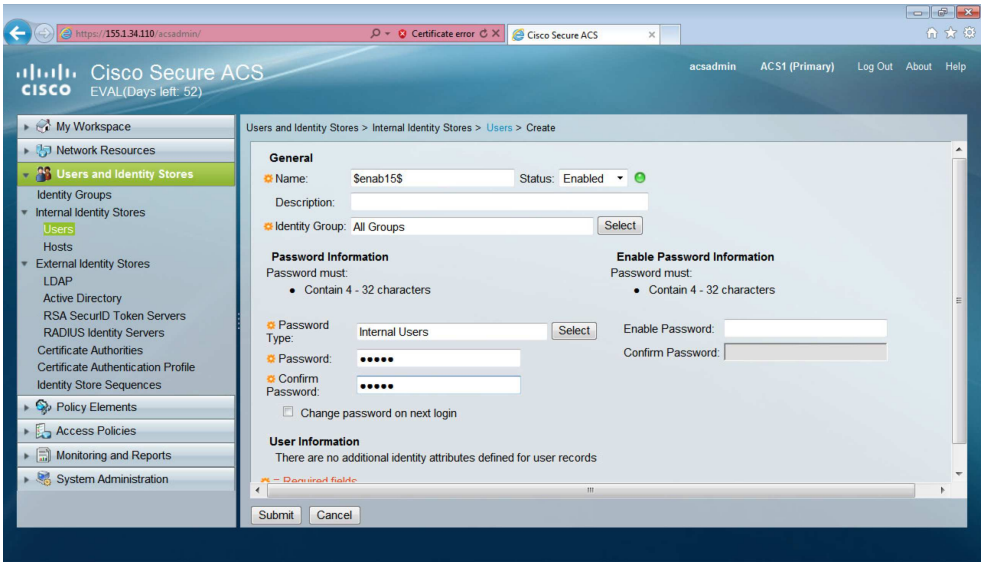


Navigate to **Users and Identity Stores- > Internal Identity Stores -> Users** and click **Create** to add **RADIUS** user to ACS database:

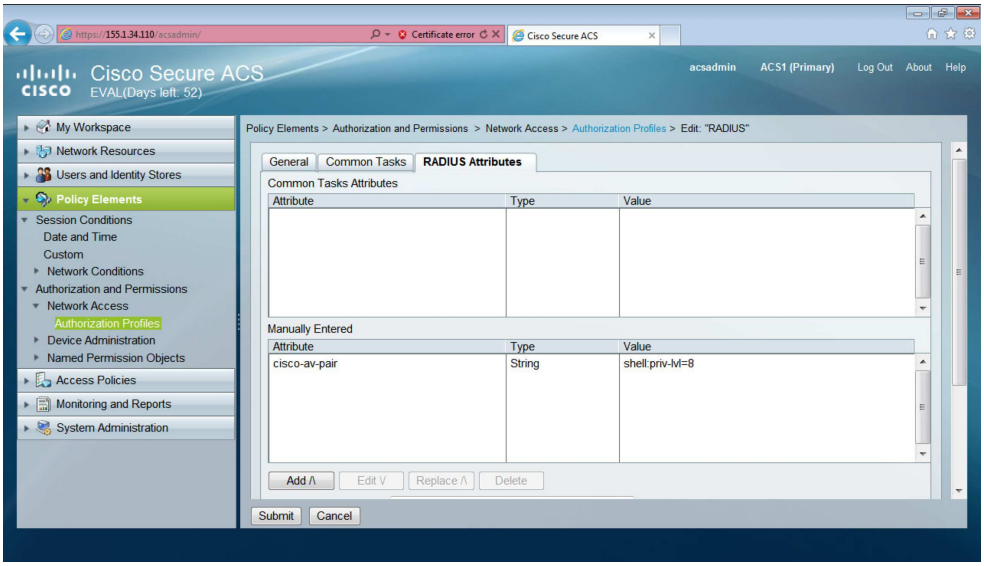


Navigate to **Users and Identity Stores- > Internal Identity Stores -> Users** and click **Create** to add **$enab15$** user to ACS database:

https://t.me/learningnets

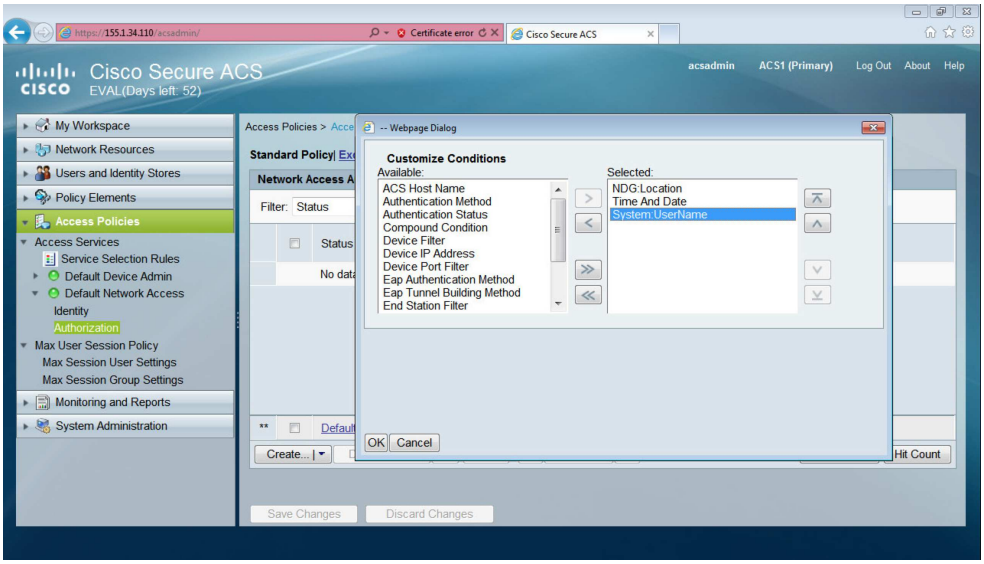


Navigate to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click **Create** to configure privilege-level assignment:

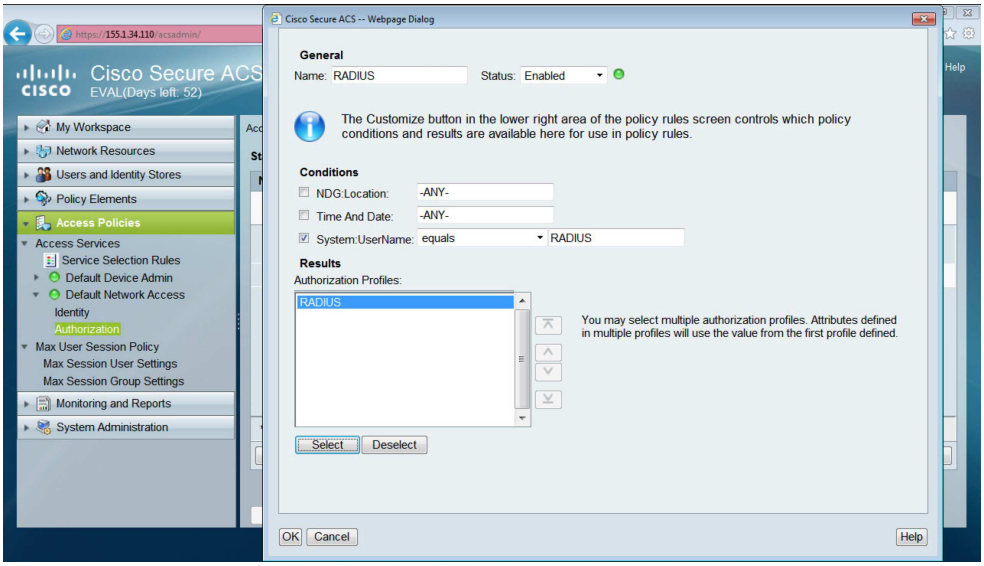


Navigate to **Access Policies -> Default Network Access -> Authorization** and click **Customize** to add the username as condition:

https://t.me/learningnets



Navigate to **Access Policies -> Default Network Access -> Authorization**, click **Add**, and configure the authorization rule for **RADIUS** user:



Task 4.3 Verification

Verify basic authentication from the console of R4:

```
R4#test aaa group ACS_RADIUS RADIUS CISCO legacy

Attempting authentication test to server-group ACS_RADIUS using radius
User was successfully authenticated.
```

https://t.me/learningnets

Initiate a telnet session to R4, and verify default assigned privilege-level and maximum allowed privilege-level:

```
SW3#telnet 155.1.43.4
Trying 155.1.43.4 ... Open



User Access Verification

Username: RADIUS
Password:
R4#show privilege
Current privilege level is 8
R4#enable
Password: R4#show privilege
Current privilege level is 15
```

Verify ACL matches for RADIUS communication, confirming that authentication and accounting session are established with the ACS server:

```
R4#show ip access-lists SELF_ZONE_PASS_ACL
Extended IP access list SELF_ZONE_PASS_ACL
    10 permit ospf any any (16435 matches)
    20 permit esp 155.1.99.0 0.0.0.255 host 150.1.4.4 (28 matches)
    30 permit esp host 150.1.1.1 host 150.1.4.4 (10564 matches)
    40 permit esp host 150.1.2.2 host 150.1.4.4 (10443 matches)
    50 permit gre host 150.1.1.1 host 150.1.4.4 (10485 matches)
    60 permit gre host 150.1.2.2 host 150.1.4.4 (10382 matches)
    70 permit esp host 150.1.3.3 host 150.1.4.4 (9948 matches)
    80 permit esp host 150.1.5.5 host 150.1.4.4 (10057 matches)
    90 permit gre host 150.1.3.3 host 150.1.4.4 (9948 matches)
    100 permit gre host 150.1.5.5 host 150.1.4.4 (10057 matches)
110 permit udp host 155.1.34.110 eq 1645 host 150.1.4.4 (4 matches)
    120 permit udp host 155.1.34.110 eq 1812 host 150.1.4.4
130 permit udp host 155.1.34.110 eq 1646 host 150.1.4.4 (2 matches)

    140 permit udp host 155.1.34.110 eq 1813 host 150.1.4.4
```

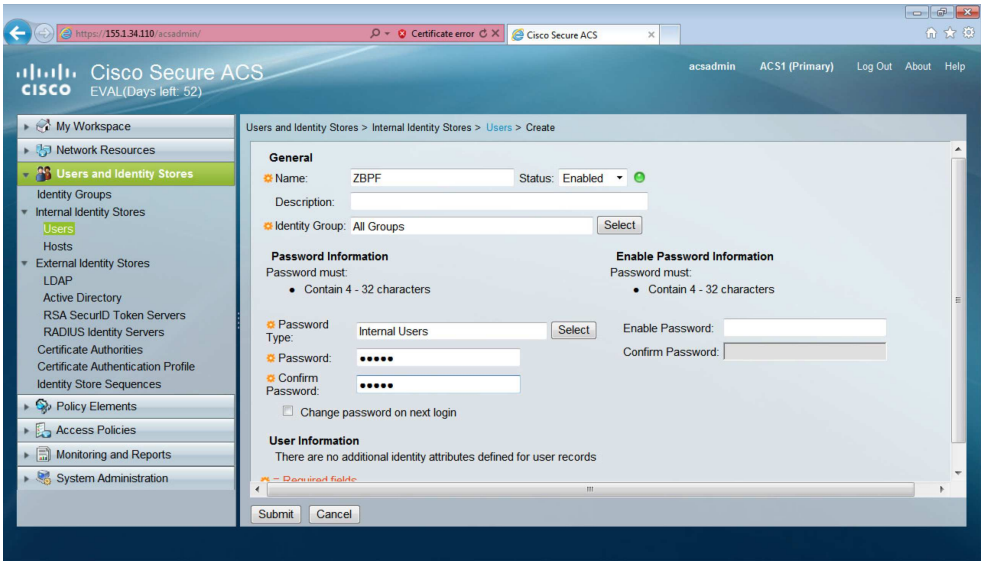
Task 4.4 Solution

https://t.me/learningnets

R4:

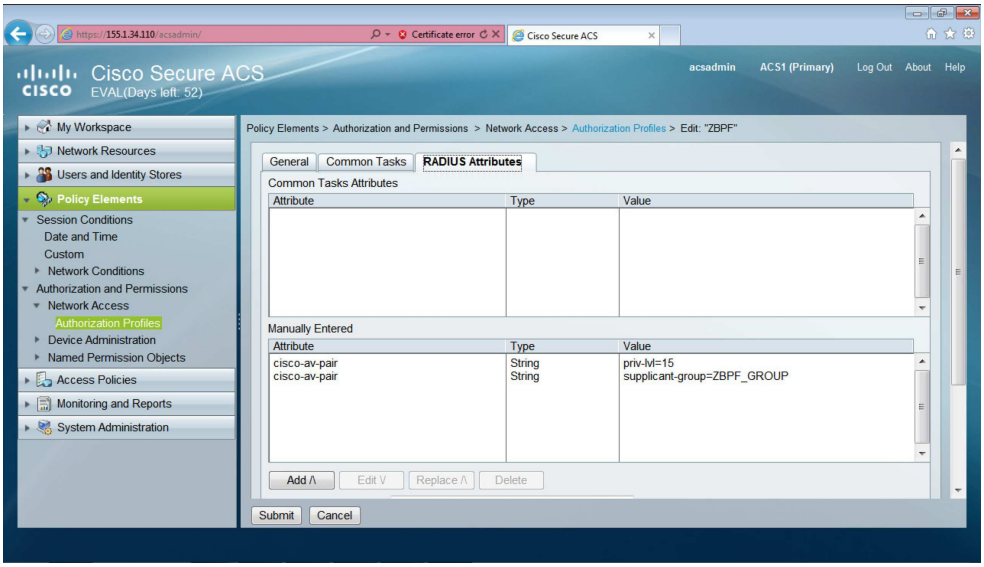
```
aaa authorization auth-proxy default group ACS_RADIUS
ip admission name ACS_AUTHENTICATION proxy telnet
!
interface FastEthernet0/0.41
 ip admission ACS_AUTHENTICATION
!
class-map type inspect match-any ZBPF_AUTHENTICATION
 match user-group ZBPF_GROUP
!
class-map type inspect match-all AUTHENTICATED_TRUSTED_TO_UNTRUSTED
 match class-map TRUSTED_TO_UNTRUSTED
 match class-map ZBPF_AUTHENTICATION
!
policy-map type inspect TRUSTED_TO_UNTRUSTED
 no class type inspect TRUSTED_TO_UNTRUSTED
 class type inspect AUTHENTICATED_TRUSTED_TO_UNTRUSTED
  inspect
```

Navigate to **Users and Identity Stores- > Internal Identity Stores -> Users** and click **Create** to add **ZBPF** user to ACS database:

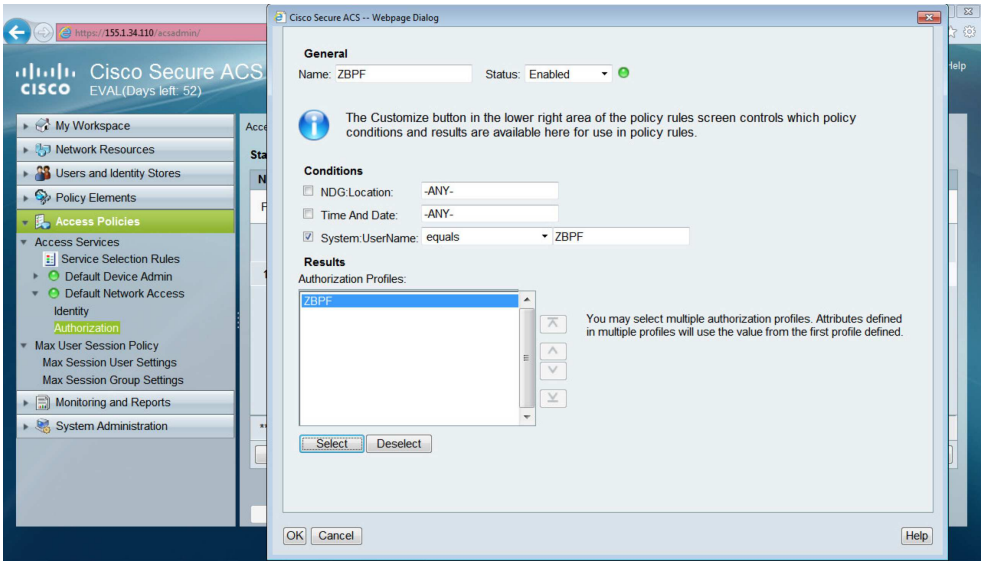


Navigate to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click **Create** to configure privilege-level assignment and supplicant-group:

https://t.me/learningnets



Navigate to **Access Policies -> Default Network Access -> Authorization**, click **Add**, and configure the authorization rule for **ZBPF** user:



Task 4.4 Verification

Verify basic authentication from the console of R4:

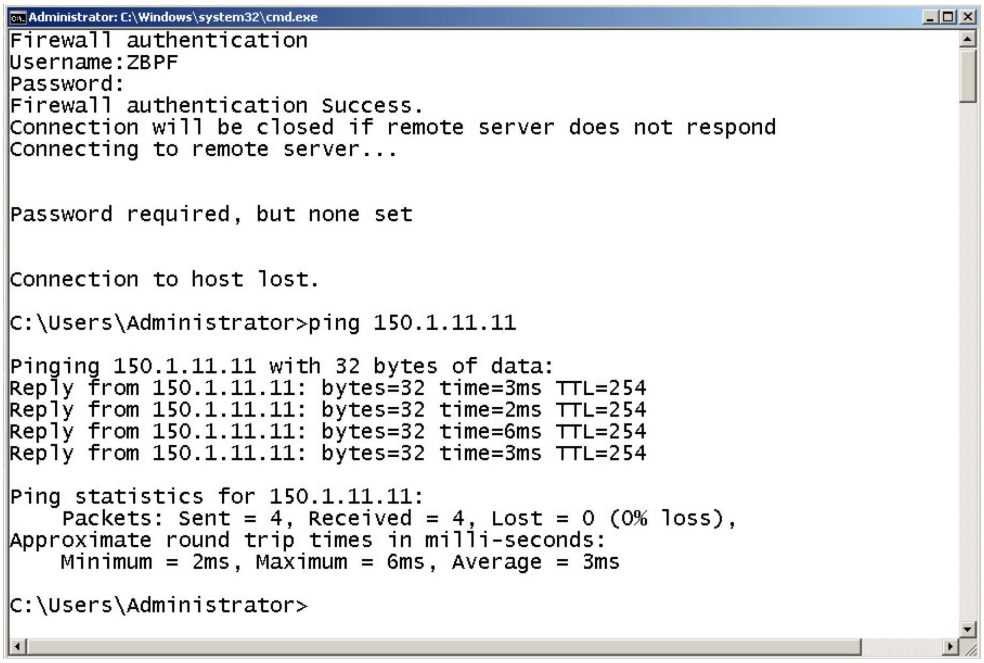
```
R4#test aaa group ACS_RADIUS ZBPF CISCO legacy

Attempting authentication test to server-group ACS_RADIUS using radius
User was successfully authenticated.
```

From **TEST-SRV-A**, initiate a telnet session to the **UNTRUSTED** zone, such as to SW3. R4 will prompt for authentication; test that traffic is allowed after successful

https://t.me/learningnets

authentication:



Verify authentication result on the router, and check the assigned authorization received from RADIUS:

https://t.me/learningnets

```
R4#show ip auth-proxy cache username ZBPF

Authentication Proxy Cache
 User Name                : ZBPF
Client IP                 : 172.16.10.100

Client Port               : 51695
Timeout                   : 60
Time  Remaining           : 59
Connection state          : ESTAB

EPM information : AuthproxyAdmission feature       : Authproxy

AAA Policies              :Supplicant-Group        : ZBPF_GROUP


EOU information
--------------------------------------------------------------------------
Address         Interface              AuthType   Posture-Token Age(min)
--------------------------------------------------------------------------


EPM information : EOU
!
!R4#show epm session ip 172.16.10.100

Admission feature         : Authproxy
AAA Policies              :Supplicant-Group        : ZBPF_GROUP
```

Verify that requested output is being matched:

```
R4#show user-group

Usergroup : ZBPF_GROUP
--------------------------------------------------------------------------
User Name       Type     Interface              Learn         Age (min)
--------------------------------------------------------------------------
172.16.10.100   IPv4     FastEthernet0/0.41     Dynamic          4
```

https://t.me/learningnets

Task 4.5 Solution

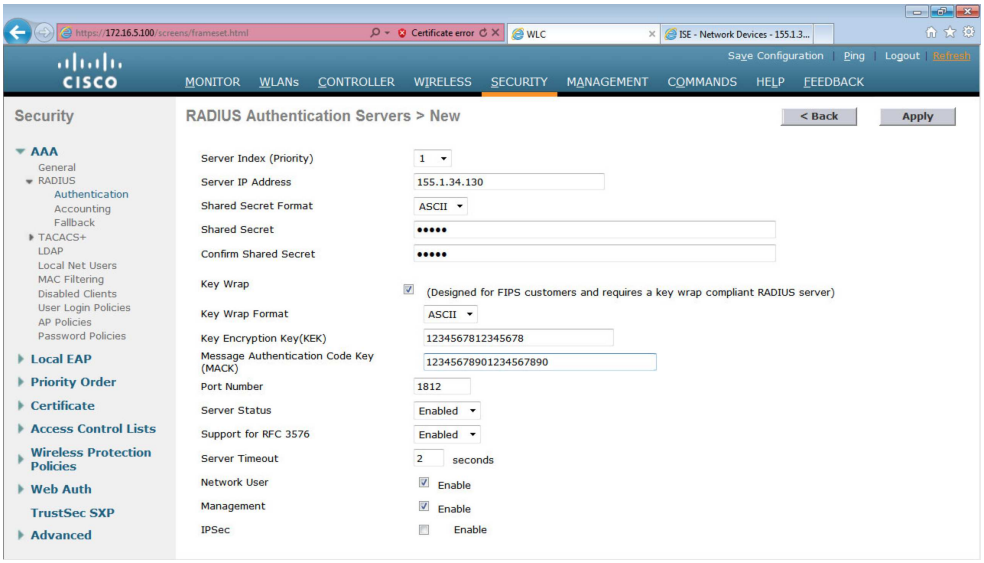
```
ASA1:
access-list DMZ_IN permit tcp 155.1.99.0 255.255.255.0 host 155.1.34.130 eq 443
access-list DMZ_IN permit tcp 155.1.99.0 255.255.255.0 host 172.16.5.100 eq 443
access-list DMZ_IN permit udp 155.1.70.0 255.255.255.0 host 172.16.5.100 eq 5246
access-list DMZ_IN permit udp 155.1.70.0 255.255.255.0 host 172.16.5.100 eq 5247

ASA3 ISE Context:

route OUTSIDE 172.16.5.100 255.255.255.255 155.1.34.10
route OUTSIDE 155.1.99.0 255.255.255.0 155.1.34.10
!
object network ISE_REAL
 host 172.16.3.100
 nat (INSIDE,OUTSIDE) static 155.1.34.130
!
access-list OUTSIDE_IN permit udp host 172.16.5.100 host 172.16.3.100 eq 1645
access-list OUTSIDE_IN permit udp host 172.16.5.100 host 172.16.3.100 eq 1812
access-list OUTSIDE_IN permit tcp 155.1.99.0 255.255.255.0 host 172.16.3.100 eq 443
!
access-group OUTSIDE_IN in interface OUTSIDE
```

From **TEST-PC-B**, use Internet Explorer to browse to WLC and navigate to **Security -> RADIUS -> Authentication**; click **New** and configure ISE as RADIUS server, enable support for **Key Wrap**, and use a random **KEK** key of 16 characters and **MACK** key of 20 characters:

https://t.me/learningnets

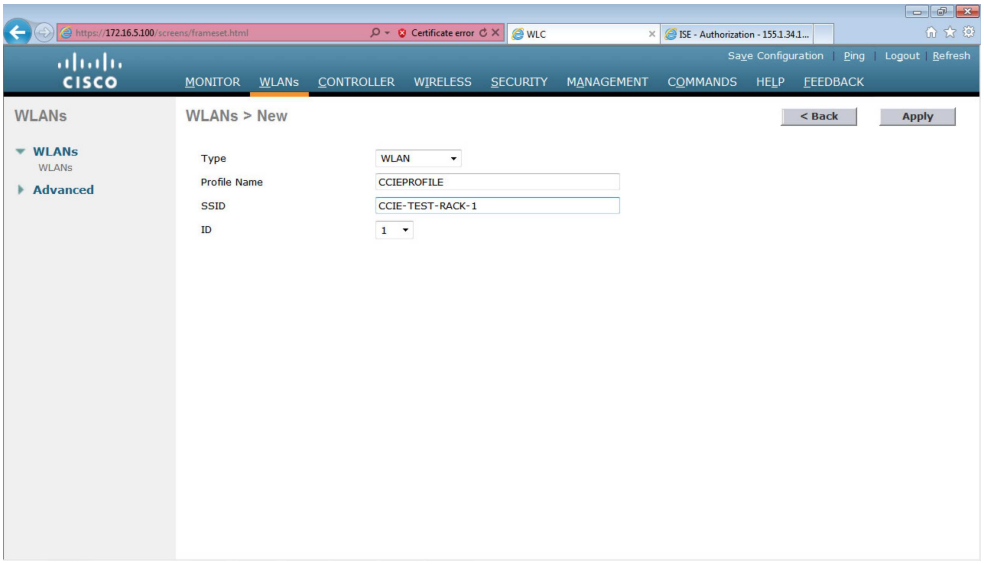


Navigate to **Security -> Access Control Lists -> Access Control Lists** and click **New**; give it the same name as configured in the authorization profile from ISE, and add a single rule to allow all IP traffic:

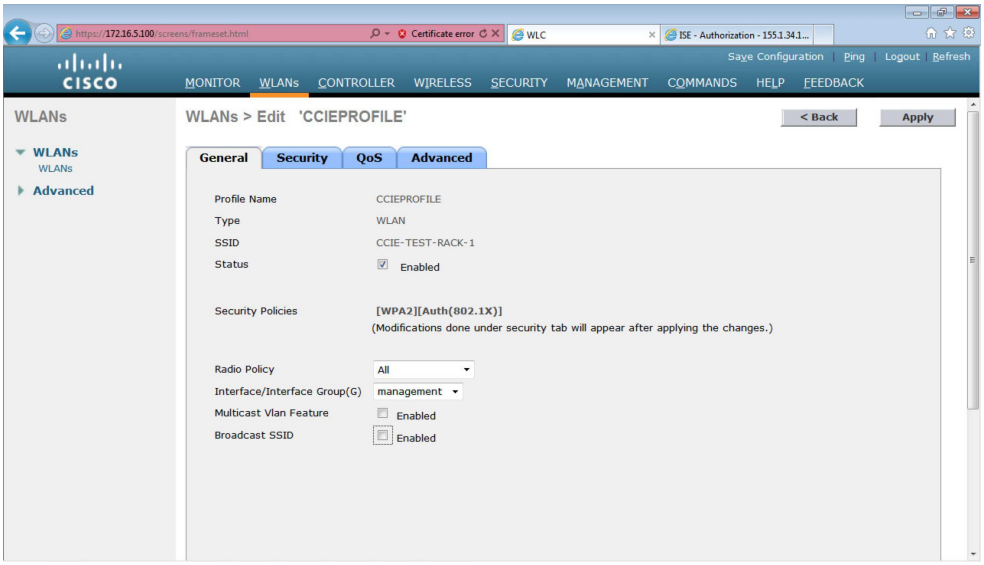


Navigate to **WLANs**, select **Create New**, and click **Go**; configure the SSID according to the task requirements:

https://t.me/learningnets

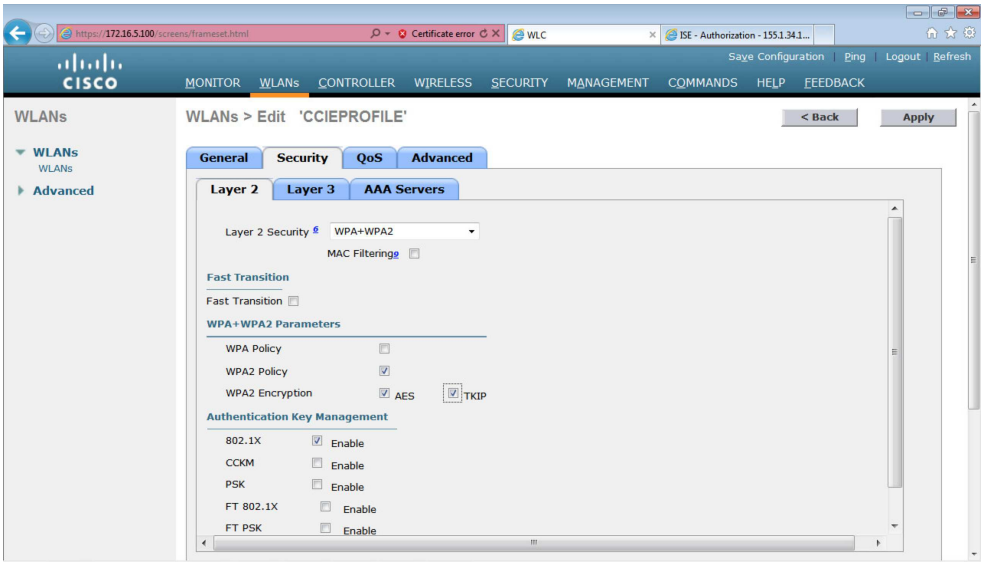


Enable the SSID and disable broadcasting in the **General** section:

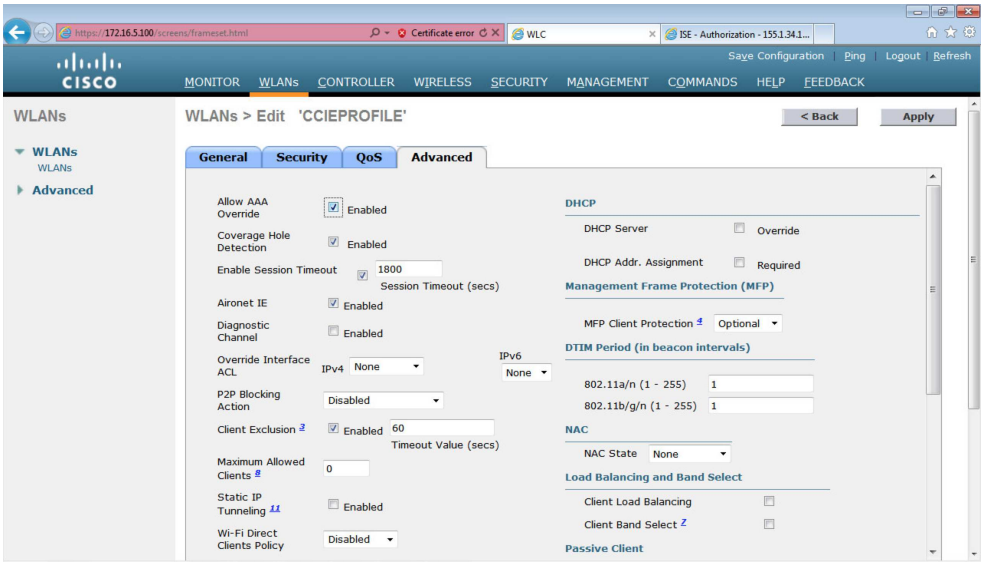


Enable AES and TKIP for WPA2 in the **Security -> Layer2** section:

https://t.me/learningnets

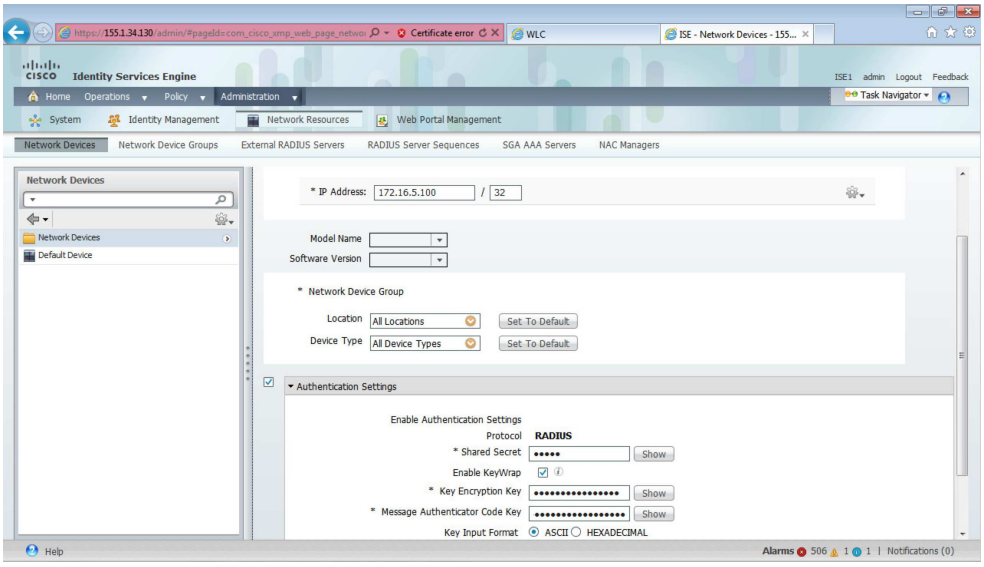


Enable **Allow AAA Override** in the **Advanced** section so that the authorization ACL received from ISE can be applied:

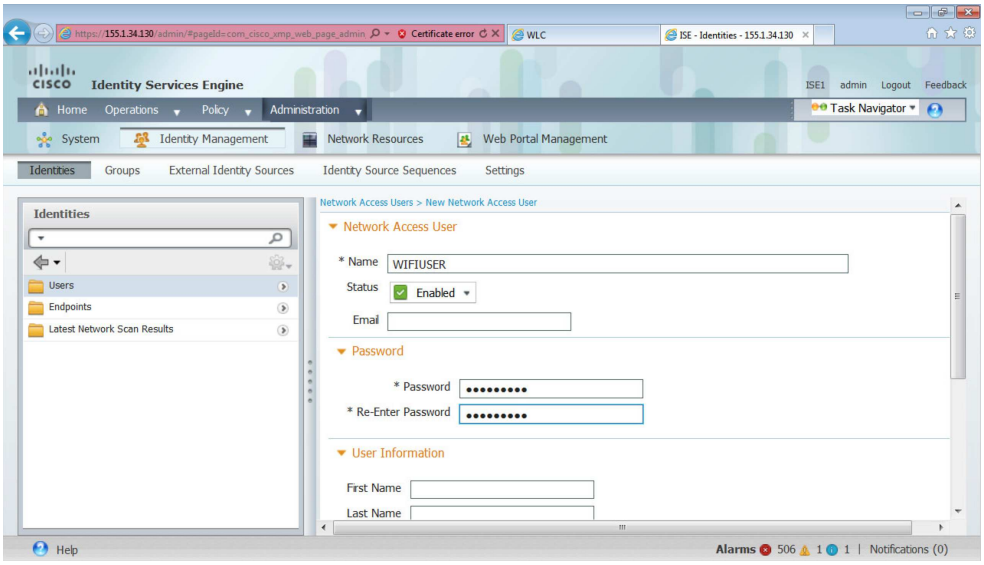


From **TEST-PC-B**, use Internet Explorer to navigate to ISE, **Administration -> Network Resources -> Network Devices**, and click **Add** to add WLC as a NAD client; enable support for **Key Wrap** and use the same keys as configured on WLC:

https://t.me/learningnets

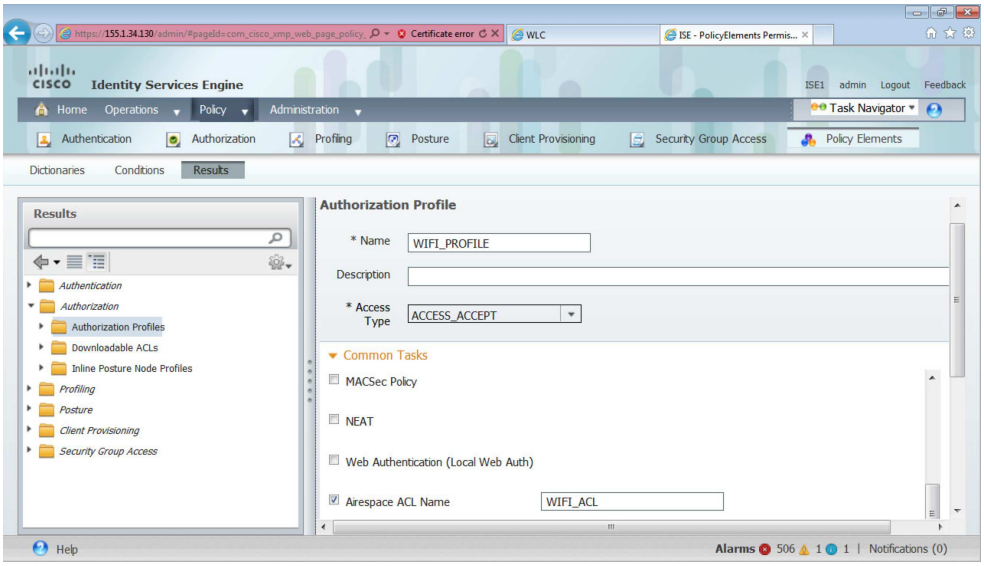


Navigate to **Administration -> Identity Management -> Identities -> Users** and click **Add** to configure the required username/password pair:

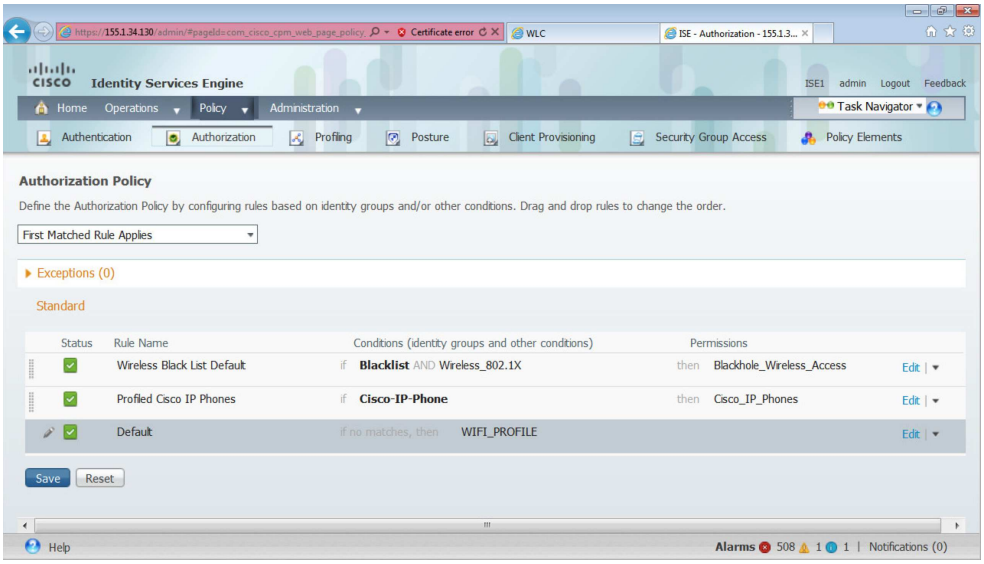


Navigate to **Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles** and configure a profile to assign the ACL name configured on WLC:

https://t.me/learningnets



Navigate to **Policy -> Authorization** and modify the default rule by assigning the previously configured authorization profile:



Task 4.5 Verification

Verify that LAP successfully joined the WLC:

https://t.me/learningnets

```
(Cisco Controller) >show ap summary


Number of APs.................................. 1

Global AP User Name............................ Not Configured
Global AP Dot1x User Name...................... LAPUSER

AP Name             Slots  AP Model              Ethernet MAC       Location          Port  Country  Priority
------------------  -----  --------------------  -----------------  ----------------  ----  -------  --------
RACK1-AP             2     AIR-LAP1262N-A-K9     00:06:f6:3b:9a:da  default location  1       US       1
```

Verify the WLAN basic configuration settings:

```
(Cisco Controller) >show wlan summary


Number of WLANs................................ 1

WLAN ID  WLAN Profile Name / SSID               Status    Interface Name
-------  -----------------------------------  --------  --------------------
1        CCIEPROFILE / CCIE-TEST-RACK-1         Enabled   management
```

Verify that the RADIUS server has been configured for authentication:

```
(Cisco Controller) >show radius summary


Vendor Id Backward Compatibility.................. Disabled
Call Station Id Case............................. lower
Call Station Id Type............................. Mac Address
Aggressive Failover.............................. Enabled
Keywrap.......................................... Disabled
Fallback Test:
    Test Mode.................................... Off
    Probe User Name.............................. cisco-probe
    Interval (in seconds)........................ 300
MAC Delimiter for Authentication Messages........ hyphen
MAC Delimiter for Accounting Messages............ hyphen
Authentication Servers
```

https://t.me/learningnets

```
Idx  Type  Server Address    Port    State     Tout  MgmtTout  RFC3576  IPSec - AuthMode/Phase1/Group/Lifetime/Auth/
---  ----  ----------------  ------  --------  ----  --------  -------  ----------------------------------------
1    NM    155.1.34.130      1812    Enabled   2     2         Enabled   Disabled - none/unknown/group-0/0 none/none


Accounting Servers

Idx  Type  Server Address    Port    State     Tout  MgmtTout  RFC3576  IPSec - AuthMode/Phase1/Group/Lifetime/Auth/

---  ----  ----------------  ------  --------  ----  --------  -------  ----------------------------------------
```

Configure the **WiFi-TEST-PC** with the native 802.1x Windows supplicant for PEAP(EAP-MSCHAPv2) user authentication, disable **Validate Server Certificate**, and do not use Windows credentials for the session. Connect to the WiFi network. You should be prompted for authentication; use the credentials configured on ISE server. Verify that WiFi client is associated and authenticated, and that it has been assigned an IPv4 address from R5, which is the DHCP server:

```
(Cisco Controller) >show client  summary


Number of Clients.............................. 1

MAC Address       AP Name           Status        WLAN/RLAN      Auth Protocol         Port Wired
----------------- ----------------- ------------- -------------- ---- ---------------- ---- -----
ac:f1:df:13:bd:8f RACK1-AP          Associated    1              Yes  802.11n(2.4 GHz) 1    N/A
!
!R5#show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
172.16.5.2          01ac.f1df.13bd.8f       Apr 15 2014 01:39 PM    Automatic
```

Verify that the ACL has been applied to the user's authorization:

```
(Cisco Controller) >show client detail ac:f1:df:13:bd:8f
Client MAC Address............................. ac:f1:df:13:bd:8f
Client Username ............................... WIFIUSER
AP MAC Address................................. f0:29:29:04:21:f0
AP Name.......................................... RACK1-AP
          Client State..................................... Associated
```

https://t.me/learningnets

```
Client NAC OOB State.............................. Access
Wireless LAN Id................................... 1
802.11u........................................... Not Supported
BSSID............................................. f0:29:29:04:21:f0
Connected For .................................... 1017 secs
Channel........................................... 11
IP Address........................................ 172.16.5.2
IPv6 Address...................................... fe80::3c16:4073:f3a4:c679
Association Id.................................... 1
Authentication Algorithm.......................... Open System
Reason Code....................................... 1
Status Code....................................... 0
Client CCX version................................ 5
Client E2E version................................ No E2E support
Diagnostics Capability............................ Supported
S69 Capability.................................... Not Supported
Re-Authentication Timeout......................... 780

--More-- or (q)uit
QoS Level......................................... Silver
802.1P Priority Tag............................... disabled
CTS Security Group Tag............................ Not Applicable
KTS CAC Capability................................ No
WMM Support....................................... Enabled
  APSD ACs.....................................  BK  BE  VI  VO
Power Save........................................ OFF
Current Rate...................................... m0
Supported Rates................................... 1.0,2.0,5.5,11.0,6.0,9.0,
    ..............................................12.0,18.0,24.0,36.0,48.0,
    ..............................................54.0
Mobility State.................................... Local
Mobility Move Count............................... 0
Security Policy Completed......................... Yes
Policy Manager State.............................. RUN
Policy Manager Rule Created....................... Yes
Audit Session ID.................................. ac10056400000001534b4fa9
IPv4 ACL Name..................................... WIFI_ACL
IPv4 ACL Applied Status........................... Yes
IPv6 ACL Name..................................... none
IPv6 ACL Applied Status........................... Unavailable
Policy Type....................................... WPA2
Authentication Key Management..................... 802.1x
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 5

CCIE SCv4 Lab 5 Solutions Section 5

1. Task 5.1 Solution
2. Task 5.2 Solution
3. Task 5.3 Solution
4. Task 5.4 Solution
5. Task 5.5 Solution

Task 5.1 Solution

```
R3:
snmp-server host 172.16.6.55 CISCO
snmp-server source-interface traps loopback0
snmp-server ifindex persist
!
rmon event 1 log trap CISCO description "VLAN33 Interface Congested" owner CISCO
rmon event 2 log trap CISCO description "VLAN33 Interface UnCongested" owner CISCO
!
rmon alarm 1 ifEntry.11.1 60 delta rising-threshold 100 1 falling-threshold 50 2 owner CISCO

ASA1:

access-list OUTSIDE_IN permit udp host 150.1.3.3 host 172.16.6.55 eq snmptrap
```

Task 5.1 Verification

Verify the RMON configuration:

```
R3#show rmon alarms
 Alarm 1 is active, owned by CISCO
Monitors ifInUcastPkts.1 every 60 second(s)
 Taking delta samples, last value was 67
 Rising threshold is 100, assigned to event 1
 Falling threshold is 50, assigned to event 2
```

https://t.me/learningnets

```
 On startup enable rising or falling alarm
!
!R3#show rmon events
 Event 1 is active, owned by CISCO
 Description is VLAN33 Interface Congested Event firing causes log and trap to community CISCO,
 last event fired at  0y0w0d,00:00:00,
 Current uptime       0y0w0d,21:12:54 Event 2 is active, owned by CISCO
 Description is VLAN33 Interface UnCongested Event firing causes log and trap to community CISCO,

 last event fired at  0y0w0d,00:00:00,
 Current uptime       0y0w0d,21:12:54
```

Task 5.2 Solution

```
R3:
ip options drop

ASA1:

access-list IP_OPTIONS_ACL permit ip 172.16.5.0 255.255.255.0 155.1.70.0 255.255.255.0
access-list IP_OPTIONS_ACL permit ip 155.1.70.0 255.255.255.0 172.16.5.0 255.255.255.0
!
class-map IP_OPTIONS_CLASS
 match access-list IP_OPTIONS_ACL
!
policy-map type inspect ip-options IP_OPTIONS_POLICY
 parameters
  eool action clear
  nop action clear
  router-alert action clear
!
policy-map global_policy
 class IP_OPTIONS_CLASS
  inspect ip-options IP_OPTIONS_POLICY
```

Task 5.2 Verification

Verify the ASA configuration:

```
ASA12/act# show service-policy inspect ip-options
```

https://t.me/learningnets

```
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: ip-options _default_ip_options_map, packet 0, drop 0, reset-drop 0
        Router Alert:  allow 0, clear 0 Class-map: IP_OPTIONS_CLASS
      Inspect: ip-options IP_OPTIONS_POLICY, packet 0, drop 0, reset-drop 0
 EOOL:           allow 0, clear 0
 NOP:            allow 0, clear 0
 Router Alert:   allow 0, clear 0
```

Task 5.3 Solution

```
R3:

spd extended-headroom 150
spd headroom 120
ip spd mode aggressive
ip spd queue threshold minimum 75 maximum 150
!
interface FastEthernet0/1
 hold-queue 150 in
```

Task 5.3 Verification

Verify the SPD configuration and hold-queue for VLAN 33 interface:

```
R3#show ip spd
Current mode: normal. Queue min/max thresholds: 75/150, Headroom: 120, Extended Headroom: 150
IP normal queue: 0, priority queue: 0.
SPD special drop mode: aggressively drop bad packets
!
!R3#show interfaces fastEthernet0/1 | i queue
 Input queue: 0/150/0/0 (size/max/drops/flushes); Total output drops: 0

  Output queue: 0/40 (size/max)
```

Task 5.4 Solution

https://t.me/learningnets

```
R3:

ip access-list extended NETFLOW_ACL
 permit ip 155.1.70.0 0.0.0.255 155.1.20.0 0.0.0.255
!
class-map NETFLOW_CLASS
 match access-group name NETFLOW_ACL
!
flow-sampler-map ALL_PACKET
 mode random one-out-of 1
!
flow-sampler-map RANDOM_PACKET
 mode random one-out-of 10
!
policy-map NETFLOW_MAP
 class NETFLOW_CLASS
   netflow-sampler ALL_PACKET
 class class-default
   netflow-sampler RANDOM_PACKET
!
interface FastEthernet0/0.39
 service-policy output NETFLOW_MAP
```

Task 5.4 Verification

Verify the configuration and note statistics:

```
R3#show policy-map interface fastEthernet0/0.39 output

 FastEthernet0/0.39

  Service-policy output: NETFLOW_MAP
 Class-map: NETFLOW_CLASS (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name NETFLOW_ACL netflow-sampler: ALL_PACKET
 Class-map: class-default (match-any)
 92 packets, 9206 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  netflow-sampler: RANDOM_PACKET
```

https://t.me/learningnets

Verify collected statistics; SSH session between IPS and ASA3 is displayed:

```
R3#show ip cache flow

IP packet size distribution (10 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .200 .000 .800 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 8 added
  144 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-other            1      0.0         1    40      0.0       0.0      15.6
IP-other             6      0.0         1   120      0.0       2.9      15.3
Total:               7      0.0         1   111      0.0       2.5      15.3

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0.25      155.1.99.100    Fa0/0.39*     155.1.34.17     06 EBEE 0016     1
```

Task 5.5 Solution

```
R3:

ip access-list extended FRAGMENTS_ACL
 permit ip any any fragment
!
ip access-list extended ICMP_ACL
 permit icmp any any
!
class-map match-any FRAGMENTS_CLASS
```

https://t.me/learningnets

```
 match access-group name FRAGMENTS_ACL
!
class-map match-any ICMP_CLASS
 match access-group name ICMP_ACL
!
class-map type port-filter match-all CLOSED_PORTS_CLASS
 match closed-ports
 match not port tcp 4040
 match not port tcp 5050
!
policy-map type port-filter HOST_PORT_FILTER
 class CLOSED_PORTS_CLASS
  drop
!
policy-map HOST_RATE_LIMIT
 class ICMP_CLASS
  police rate 20 pps burst 5 packets
!
policy-map CEF_EXCEPTION_RATE_LIMIT
 class class-default
  police rate 150 pps burst 30 packets
!
policy-map TRANSIT_RATE_LIMIT
 class FRAGMENTS_CLASS
  police rate 1000000 pps burst 200000 packets
!
control-plane host
 service-policy input HOST_RATE_LIMIT
  service-policy type port-filter input HOST_PORT_FILTER
!
control-plane transit
 service-policy input TRANSIT_RATE_LIMIT
!
control-plane cef-exception
 service-policy input CEF_EXCEPTION_RATE_LIMIT
```

Task 5.5 Verification

Verify the activated control-plane functionalities:

```
R3#show control-plane features
 Total 4 features configured

Control plane host path features :
```

https://t.me/learningnets

```
---------------------------------------------------------
Control-plane Policing activated Apr 14 2014 17:3
TCP/UDP Portfilter activated Apr 14 2014 17:3


---------------------------------------------------------

Control plane transit path features :

---------------------------------------------------------
Control-plane Policing activated Apr 14 2014 17:3

---------------------------------------------------------

Control plane cef-exception path features :

---------------------------------------------------------
Control-plane Policing activated Apr 14 2014 17:3


---------------------------------------------------------
```

Verify the packet counters to see if there is an increasing number of dropped packets:

```
R3#show control-plane counters

Feature Path             Packets processed/dropped/errors
Aggregate                   57134/0/0
Host                        16280/0/0
Transit                        55/0/0
Cef-exception               40838/0/0
```

Verify the configuration:

```
R3#show policy-map control-plane host

 Control Plane Host

  Service-policy input: HOST_RATE_LIMIT
 Class-map: ICMP_CLASS (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name ICMP_ACL
        0 packets, 0 bytes
```

https://t.me/learningnets

```
        5 minute rate 0 bps police:
rate 20 pps, burst 5 packets
        conformed 0 packets; actions:
          transmit
        exceeded 0 packets; actions:
          drop
        conformed 0 pps, exceed 0 pps

    Class-map: class-default (match-any)
      36 packets, 2228 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
!
!R3#show policy-map control-plane cef-exception

 Control Plane Cef-exception

  Service-policy input: CEF_EXCEPTION_RATE_LIMIT
 Class-map: class-default (match-any)
      135 packets, 12888 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  police:
rate 150 pps, burst 30 packets
        conformed 135 packets; actions:
          transmit
        exceeded 0 packets; actions:
          drop
        conformed 0 pps, exceed 0 pps
!
!R3#show policy-map control-plane transit

 Control Plane Transit

  Service-policy input: TRANSIT_RATE_LIMIT
 Class-map: FRAGMENTS_CLASS (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name FRAGMENTS_ACL
        0 packets, 0 bytes
        5 minute rate 0 bps police:
rate 1000000 pps, burst 200000 packets

        conformed 0 packets; actions:
          transmit
        exceeded 0 packets; actions:
          drop
```

https://t.me/learningnets

```
      conformed 0 pps, exceed 0 pps

  Class-map: class-default (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 5

CCIE SCv4 Lab 5 Solutions Section 6

1. Task 6.1 Solution
2. Task 6.2 Solution
3. Task 6.3 Solution
4. Task 6.4 Solution
5. Task 6.5 Solution

Task 6.1 Solution

```
ASA1:
ip verify reverse-path interface DMZ
ip verify reverse-path interface OUTSIDE
ip verify reverse-path interface INSIDE

ASA3 ACS Context:
ip verify reverse-path interface OUTSIDE
ip verify reverse-path interface INSIDE

ASA3 ISE Context:

ip verify reverse-path interface OUTSIDE
ip verify reverse-path interface INSIDE
```

Task 6.1 Verification

Verify unicast RPF statistics:

```
ASA12/act# show ip verify statistics

interface DMZ: 0 unicast rpf drops
interface OUTSIDE: 0 unicast rpf drops
interface INSIDE: 0 unicast rpf drops
!
!ASA34/pri/ISE/act# show ip verify statistics
```

https://t.me/learningnets

```
interface OUTSIDE: 0 unicast rpf drops
interface INSIDE: 0 unicast rpf drops
!
!ASA34/sec/ACS/act# show ip verify statistics

interface OUTSIDE: 0 unicast rpf drops
interface INSIDE: 0 unicast rpf drops
```

Simulate a session with spoofed source, and verify that the firewall drops it:

```
ASA12/act# packet-tracer input INSIDE tcp 150.1.4.4 2000 150.1.11.11 23 detailed

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xabb52c00, priority=1, domain=permit, deny=false
        hits=144496, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0100.0000.0000

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   150.1.11.11     255.255.255.255 DMZ

Phase: 3
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   150.1.4.4       255.255.255.255 DMZ

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
```

https://t.me/learningnets

```
output-interface: DMZ
output-status: up
output-line-status: upAction: drop
Drop-reason: (rpf-violated) Reverse-path verify failed
```

Task 6.2 Solution

```
SW1:

arp access-list DAI_VLAN10
 permit ip host 155.1.10.1 mac host d48c.b5da.d548 log
!
ip arp inspection filter DAI_VLAN10 vlan 10 static
!
ip arp inspection vlan 10
ip arp inspection vlan 10 logging acl-match matchlog
ip arp inspection validate src-mac dst-mac
```

Task 6.2 Verification

Verify the MAC address of R1's Gi0/0 interface; this may differ based on your rack assignment:

```
SW1#show ip arp 155.1.10.1
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  155.1.10.1             130   d48c.b5da.d548  ARPA   Vlan10
```

Verify the DAI configuration:

```
SW1#show ip arp inspection vlan 10
 Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
10      Enabled           Active      DAI_VLAN10         Yes

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
```

https://t.me/learningnets

```
10      Acl-Match         Deny                Off
```

Clear the ARP entry on SW1's table to trigger the log message being displayed:

```
SW1#clear ip arp 155.1.10.1
%SW_DAI-6-ACL_PERMIT: 1 ARPs (Res) on Fa1/0/1, vlan 10.([d48c.b5da.d548/155.1.10.1/001b.d58b.21c1/155.1.10.9/19:35:1
```

Verify that SW1 maintains IP connectivity with R1, confirming that ARP is functional:

```
SW1#ping 155.1.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.10.1, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
```

Verify that the switchport interface to R1 is untrusted, and therefore ARP packets are inspected:

```
SW1#show ip arp inspection interfaces fastEthernet1/0/1

 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
Fa1/0/1           Untrusted               15                 1
```

Task 6.3 Solution

https://t.me/learningnets

```
R5:

access-list 100 permit tcp any 172.16.5.0 0.0.0.255
!
ip tcp intercept list 100
ip tcp intercept watch-timeout 15
ip tcp intercept max-incomplete low 1200 high 1500
ip tcp intercept mode watch
ip tcp intercept drop-mode random
```

Task 6.3 Verification

Verify that R5 watches connections for hosts in VLAN 50:

```
R5#show tcp intercept statistics
 Watching new connections using access-list 100

0 incomplete, 0 established connections (total 0)
0 connection requests per minute
```

Task 6.4 Solution

```
SW1:

mac access-list extended PERMIT_ARP
 permit any any 0x806 0x0
!
ip access-list extended PERMIT_IP
 permit ip host 172.16.10.100 any
!
interface FastEthernet1/0/4
 mac access-group PERMIT_ARP in
 ip access-group PERMIT_IP in
```

Task 6.4 Verification

Verify the filtering configuration:

```
SW1#show mac access-group interface fastEthernet1/0/4
```

https://t.me/learningnets

```
Interface FastEthernet1/0/4: Inbound access-list is PERMIT_ARP
   Outbound access-list is not set
!
!SW1#show ip interface fastEthernet1/0/4
FastEthernet1/0/4 is up, line protocol is up Inbound  access list is PERMIT_IP
```

On R4, clear the ARP entry for **TEST-SRV-A** and verify that IP connectivity is maintained, confirming that ARP is still functional:

```
R4#clear ip arp 172.16.10.100
R4#ping 172.16.10.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.100, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
```

Task 6.5 Solution

```
ASA3 ACS Context:
icmp deny any echo OUTSIDE
icmp permit any OUTSIDE

ASA3 ISE Context:

icmp deny any echo OUTSIDE
icmp permit any OUTSIDE
```

Task 6.5 Verification

Verify that ICMP Echo traffic destined to itself is dropped by the ASA on its **OUTSIDE** interface, but ICMP Echo-Reply is allowed:

```
SW2#ping 155.1.34.17

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.34.17, timeout is 2 seconds:.....
Success rate is 0 percent (0/5)
!
!SW2#ping 155.1.34.18
```

https://t.me/learningnets

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.34.18, timeout is 2 seconds:.....
Success rate is 0 percent (0/5)
!
!ASA34/pri/ISE/act# ping 155.1.34.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.34.10, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
!
!ASA34/sec/ACS/act# ping 155.1.34.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.34.10, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 4

CCIE SCv4 Lab 4 Introduction

Lab Guidelines

The following scenarios are practice labs designed to test your readiness for the Cisco Systems CCIE Security Lab Exam. However, remember that in addition to being designed as a simulation of the actual CCIE lab exam, these practice labs should be used as a learning tool. Instead of rushing through the labs to complete all the configuration steps, take the time to research the networking technology and gain a deeper understanding of the principles behind its operation. For each lab of the CCIE Security Practice Labs Workbook, follow these guidelines:

- Read the entire lab exam before starting the configuration, and correlate tasks within a section to get a complete overview of the lab objectives.
- There are dependencies between tasks of the same section and between tasks from different sections. Carefully read throughout the lab to identify and make notes of it
- The lab consists of six sections that don't necessarily need to be completed in the presented order. However some tasks must be completed before others (such as initialization of ASA firewalls).
- All sections total 100 points, and you must earn a minimum of 80 points to receive a passing grade. To earn the points assigned to each task, you must fulfill all requirements and conform to all restrictions.
- No partial credit is awarded. You will earn all points or zero points for each task; if multiple solutions are available for a task, choose the one that technically best meets the requirements.
- Some tasks present a set of requirements for implementing a technology, and some tasks present outputs to be matched.
- Labs include both configuration and troubleshooting tasks; the number of faults relevant to each troubleshooting task may or not be specified.
- Before starting the exam, verify that all equipment is functional, powered up and that you can access it at the console.
- Routers and switches are preconfigured, do not change it unless specifically allowed

https://t.me/learningnets

by the task. On troubleshooting tickets, you may change any of the initial configurations.

- IPv4/IPv6 static and default routes are allowed to complete any task, but only if this is the only available option, and unless otherwise stated in any task.
- Make sure you do not to lock yourself out of any device, because password recovery or device reset is not available in the lab.
- At the end of the exam, ensure that all devices are accessible at the console by using preconfigured credentials or the ones from specific task requirements.
- For IPv4/IPv6 addressing configuration, the following variables will be used as a reference:
  - **X** is the rack number; the value for **Rack1** will be **1**.
  - **Y** is the device number, with routers ranging from one (1) to seven (7), switches from nine (9) to fourteen (14), and ASA firewalls from fifteen (15) to eighteen (18); the value for **Router1** will be **1**, **Switch1** will be **9**, and **ASA1** will be **15**.

All routers and switches are accessible at the console without requiring any authentication; do not change this. To access other devices within the lab, use the following tables as a reference:

Device	Username	Password
TESTPC-A	ineadmin	ciscoccie
TESTSRV-A	Administrator	Cisco1234
TESTPC-B	ineadmin	ciscoccie
TESTSRV-B	Administrator	Cisco1234
TESTPC-WIFI	ineadmin	ciscoccie

Device	Username	Password
WSA CLI&GUI	admin	default1A

https://t.me/learningnets

Device	Username	Password
ACS1 CLI	admin	default1A
ACS1 GUI	acsadmin	default1A
ACS2 CLI	admin	default1A
ACS2 GUI	acsadmin	default1A
ISE1 CLI&GUI	admin	default1A
ISE2 CLI&GUI	admin	default1A
WLC CLI&GUI	admin	default1A
LAP CLI	cisco	Cisco
IPS CLI&GUI	cisco	ciscoips4240

Lab Instructions

Before you begin, make sure that the initial configuration scripts for each lab have been applied. If you have any questions related to the scenario solutions, visit our CCIE support forum at http://IEOC.com. Refer to the attached physical and logical diagrams on each lab for interface and protocol assignments; you may access these by clicking the **Resources** button in the upper-right corner. Upon lab completion, end-to-end IPv4/IPv6 connectivity is not a requirement unless specifically asked for, but you are required to meet task requirements and restrictions.

Lab Restrictions

Each lab scenario contains explicit general restrictions that you must conform to while configuring the lab. These restrictions are defined in the introductory section for each scenario. Examples of such restrictions include, but are not limited to, not adding additional IP addressing, not changing the default authentication methods,

https://t.me/learningnets

etc. There may also be certain restrictions for particular tasks within a lab scenario. Examples of these restrictions include, but are not limited to, not issuing a particular configuration command, not using the legacy configuration for a technology, etc.

TIP

You may do whatever is necessary to complete a task unless the general requirements for the lab scenario or the specific requirements for the task explicitly prohibit you from doing so. This may include using static routing, NAT statements, ACL exceptions, IPsec/GRE tunneling, etc.

Difficulty Rating

Each lab scenario has been assigned a difficulty rating. Ratings are on a scale of one (1) to ten (10), with 10 being the most difficult. Labs are designed to be more technically challenging than the actual CCIE Security Lab Exam. Do not be discouraged if you score low or do not understand a particular set of technologies. If you are having trouble with a certain area, do not hesitate to read the explanation contained within the solutions guide and study the respective technology using the Technologies Workbook or the Advanced Technologies video course. Remember that these labs are designed to teach you required skills for implementing and troubleshooting a complex network with several technologies mixed together, just as much as they are intended to test your current technical knowledge.

Point Values

As in the actual CCIE Lab exam, each task within a lab is assigned a specific point value. Points are awarded only if the presented solution meets all the given requirements and does not violate any restrictions. No partial credit is awarded for any task. A minimum score of 80 points is required to pass a particular scenario. Some tasks have multiple solutions; as long as the presented solution meets the given requirements, points will be awarded for that task. However, certain solutions may negatively affect previous or future tasks. Make sure that you carefully read all presented requirements and try your best to come up with a technically appropriate solution.

TIP

https://t.me/learningnets

Points will never be awarded for a task in which you have violated the requirements. However, remember the relative point value of the task in question as compared to future tasks. If you cannot find an appropriate solution for a particular task, it is advisable to solve the task by whatever means necessary to complete the future tasks that depend on it.

Loading Initial Config

Each lab contains a set of initial configuration scripts for routers and switches. These configuration scripts include basic Layer 2 and Layer 3 routing connectivity (as well as possible more advanced functionalities for troubleshooting tickets), and must be loaded on your rack before beginning the configuration of the scenario. These are available to be loaded from the Rack Rental Control Panel, or if you are using your own rack, they are attached to each individual lab and available for download. Initial configurations and physical and logical diagrams of each lab are attached to this Introduction; you may access these by clicking the **Resources** button in the upper-right corner.

Rack Rentals

INE has designed the CCIE Security Practice Labs Workbook based around the publicly stated hardware specification used in the actual CCIE Lab exam. To eliminate the cost of buying all the equipment used in the workbook, INE offers cost-effective equipment rentals specifically designed to be used with this and other self-paced training product lines. For more information on rack rentals. visit http://INE.com.

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 4

CCIE SCv4 Lab 4 Tasks

1. Perimeter Security and Services
2. Intrusion Prevention and Content Security
3. Confidentiality and Secure Access
4. Identity Management
5. System Hardening and Availability
6. Threat Identification and Mitigation

Difficulty Rating (10 highest): 8

Point Values

The point values for each section are as follows:

Section	Point Value
Perimeter Security and Services	24
Intrusion Prevention and Content Security	18
Confidentiality and Secure Access	18
Identity Management	15
System Hardening and Availability	12

https://t.me/learningnets

Section	Point Value
Threat Identification and Mitigation	13

GOOD LUCK!

TIP

When taking the CCIE lab exam, you will be provided with a few sheets of scratch paper for notes and diagrams. You should create two diagrams at a minimum: one for the logical Layer 2 topology and one for the logical Layer 3 topology. Note that the physical diagram and the logical Layer 2 diagram are not the same.

Although you are provided with the logical Layer 3 diagram in the lab, it will be in electronic format, which means that you cannot add notes to it and may need to switch between windows to see it on the computer. By having your own diagram, you will be able to take notes on it and quickly reference it as you work through the configuration section. Finally, drawing the Layer 2 and Layer 3 topologies will help you become familiar with a complex network toplogy at first sight.

---

1. Perimeter Security and Services

1.1 ASA Routed Mode (3 points)

- Configure ASA3 in routed single mode with a hostname of **ASA34**, using the information from the table:

Interface	Nameif	Security Level	IPv4 Address
Gi0/0.75	VLAN75	50	180.1.75.Y/24
Gi0/0.74	VLAN74	70	180.1.74.Y/24

https://t.me/learningnets

Interface	Nameif	Security Level	IPv4 Address
Gi0/1	INSIDE	100	180.1.55.Y/24

- Configure it for OSPF in area 0 and EIGRP in AS 400 according to the diagram.
- Perform mutual redistribution between OSPF and EIGRP routing domains.
- ASA3 should have an OSPF and EIGRP router ID of **34.34.34.34**.

1.2 ASA Active-Standby Failover (3 points)

- Configure ASA3 and ASA4 for stateful failover, matching the following output from ASA3:

https://t.me/learningnets

```
ASA34/pri/act(config)# show failover

    Failover On
    Failover unit Primary
    Failover LAN Interface: FAILOVER GigabitEthernet0/2 (up)
    Unit Poll frequency 1 seconds, holdtime 15 seconds
    Interface Poll frequency 1 seconds, holdtime 5 seconds
    Interface Policy 1
    Monitored Interfaces 3 of 114 maximum
    Version: Ours 8.6(1)10, Mate 8.6(1)10
    Last Failover at: 07:50:08 UTC Apr 7 2014
            This host: Primary - Active
                    Active time: 330 (sec)
                    slot 0: ASA5515 hw/sw rev (1.0/8.6(1)10) status (Up Sys)
                      Interface VLAN74 (180.1.74.17): Normal (Monitored)
                      Interface VLAN75 (180.1.75.17): Normal (Monitored)
                      Interface INSIDE (180.1.55.17): Normal (Monitored)
                    slot 1: IPS5515 hw/sw rev (N/A/) status (Unresponsive/Up)
            Other host: Secondary - Standby Ready
                    Active time: 0 (sec)
                    slot 0: ASA5515 hw/sw rev (1.0/8.6(1)10) status (Up Sys)
                      Interface VLAN74 (180.1.74.18): Normal (Monitored)
                      Interface VLAN75 (180.1.75.18): Normal (Monitored)
                      Interface INSIDE (180.1.55.18): Normal (Monitored)
                    slot 1: IPS5515 hw/sw rev (N/A/) status (Unresponsive/Up)

    Stateful Failover Logical Update Statistics
            Link : FAILOVER GigabitEthernet0/2 (up)
```

- Use VLAN 100 for failover with IPv4 addressing in the format of 180.1.100.Y/24.

1.3 ASA Multiple Context Routed (3 points)

- Configure ASA1 in routed multiple mode with a hostname of **ASA1**, using the information from the table:

Interface	Nameif	Security Level	IPv4 Address	Context Name	Context File
E0/0.95	OUTSIDE	10	180.1.95.Y/24	VLAN95	VLAN95.cfg

https://t.me/learningnets

Interface	Nameif	Security Level	IPv4 Address	Context Name	Context File
E0/0.94	OUTSIDE	10	180.1.94.Y/24	VLAN94	VLAN94.cfg
E0/1	INSIDE	90	180.1.99.15/24	VLAN95	VLAN95.cfg
E0/1	INSIDE	90	180.1.99.16/24	VLAN94	VLAN94.cfg

- Configure the prompt to include the context name.
- Configure static routing as follows:
  - in context **VLAN95**, a default route through SW5 and a route for VLAN 88 subnet through R1.
  - in context **VLAN94**, a default route through ASA2 and a route for VLAN 88 subnet through R2.

1.4 ASA Routed Mode (3 points)

- Configure ASA2 in routed single mode with a hostname of **ASA2**, using the information from the table:

Interface	Nameif	Security Level	IPv4 Address
E0/1.74	DMZ	50	180.1.74.Y/24
E0/1.94	INSIDE	10	180.1.94.Y/24
E0/0	OUTSIDE	90	180.1.46.Y/24

https://t.me/learningnets

- Configure it for OSPF in area 0 and area 22 according to the diagram.
- ASA3 should advertise a single default route into area 22.
- Additionally, ASA3 should filter all area 22 prefixes from being advertised into area 0.

1.5 ASA OSPF Default Route (2 points)

- Configure ASA2 to originate a default route into OSPF only if it has ICMP connectivity with ASA1 on VLAN 94.
- Use an ID number of **10** where required.

1.6 ASA Network Address Translation (2 points)

- Configure twice NAT on ASA3 to achieve the following:
  - Translate VLAN 21 and VLAN 22 into ASA3's interface IP address on both **VLAN74** and **VLAN75**.
  - Translate R5's Loopback0 address into ASA3's **VLAN75** interface, unless the destination is SW5's Loopback0.

1.7 IOS CBAC (2 points)

- Configure CBAC on R1 with the following requirements:
  - inspect all TCP, UDP, and ICMP traffic inbound on its VLAN 88 interface.
  - use a hash table size of 4096 and log firewall dropped packets.
  - for SMTP traffic, 10 MB should be the maximum number of bytes that can be transferred in a single session.

- A new server has been installed in VLAN 45 with an IPv4 address of 180.1.45.44, running a TCP application on port 777.
  - Activate inspection for this traffic with an idle timeout of 10 minutes, and limit the inspections to a total of 20000 established firewall sessions.

1.8 IOS CBAC High Availability (3 points)

- Configure R1 and R2 for CBAC stateful traffic inspection and failover.
- R1 and R2 should synchronize the session states, with R1 as the preferred forwarder at all times.
- Ensure that configuration is synchronized between routers and match the following

https://t.me/learningnets

output:

```
R1#show redundancy inter-device

    Redundancy inter-device state: RF_INTERDEV_STATE_ACT
      Scheme: Standby
          Groupname: CBAC_HA Group State: Active
      Peer present: RF_INTERDEV_PEER_COMM
      Security:
          Type:         IPSec
          Profile name: default
          State:        Up
```

- Match the following output:

```
R1#show standby

    GigabitEthernet0/1 - Group 0
      State is Active
        2 state changes, last state change 00:17:56
      Virtual IP address is 172.16.6.1
      Active virtual MAC address is 0000.0c07.ac00
        Local virtual MAC address is 0000.0c07.ac00 (v1 default)
      Hello time 3 sec, hold time 10 sec
        Next hello sent in 1.952 secs
      Preemption enabled
      Active router is local
      Standby router is 172.16.6.22, priority 100 (expires in 10.864 sec)
      Priority 150 (configured 150)
      Group name is "CBAC_HA" (cfgd)
```

1.9 ASA Routing Troubleshooting (3 points)

- Because of asymmetric routing, traffic flows are not functioning properly and packet drops occur.
- Fix the network configuration to match the following outputs:

```
SW5#telnet 180.1.99.1 /source-interface Loopback0
    Trying 180.1.99.1 ... Open
    R1>
```

https://t.me/learningnets

```
!
!SW5#telnet 180.1.99.2 /source-interface Loopback0

Trying 180.1.99.2 ... Open
R2>
```

- Do not use TCP state bypass as a solution.
- No static/dynamic routing changes are allowed for this task.

2. Intrusion Prevention and Content Security

2.1 IPS Initialization (3 points)

- Initialize the IPS using the information from the table:

Variables	Values
Hostname	IPS4240
IPv4 Address	172.16.6.99/24
Default Gateway	172.16.6.1
Telnet	Disabled
Management Access	172.16.6.0/24
Management Type	HTTPS Port 443

- IPS should gather memory usage statistics and rate it to **yellow** when reaching 30% free memory and **red** when reaching 10% free memory.
- Configure IPS for authenticated NTP using a string of **ipskey** and a key-id of **1**.
  - use R1 for this scope.

https://t.me/learningnets

2.2 IPS Inline Interface-Pair (4 points)

- Configure the IPS inline on VLAN 34 and VLAN 46 according to the diagram; traffic in VLAN 34 should be received untagged.
- Ensure that signature changes can be done independently for traffic in the two VLANs.
- For testing purposes, enable the ICMP Echo Request signature on vs0 and match the output:

https://t.me/learningnets

```
R4#ping 180.1.34.3 repeat 1


    Type escape sequence to abort.
    Sending 1, 100-byte ICMP Echos to 180.1.34.3, timeout is 2 seconds:
    !
    Success rate is 100 percent (1/1), round-trip min/avg/max = 4/4/4 ms
    !
    !sensor# show events


    evIdsAlert: eventId=1395322617431000225 severity=informational vendor=Cisco
      originator:
        hostId: IPS4240
        appName: sensorApp
        appInstanceId: 1202
      time: 2014/04/07 19:50:07 2014/04/07 19:50:07 UTC
      signature: description=ICMP Echo Request id=2004 created=20001127 type=other version=S666
        subsigId: 0
        sigDetails: ICMP Echo Request
      interfaceGroup: vs0
      vlan: 34
      participants:
        attacker:
          addr: locality=OUT 180.1.34.4
        target:
          addr: locality=OUT 180.1.34.3
          os: idSource=unknown relevance=relevant type=unknown
      riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
      threatRatingValue: 35
      interface: ge0_2
      protocol: icmp
```

- For testing purposes, enable the ICMP Echo Request signature on vs1 and match the output:

```
ASA2# ping 180.1.46.6 repeat 1
    Type escape sequence to abort.
    Sending 1, 100-byte ICMP Echos to 180.1.46.6, timeout is 2 seconds:
    !
    Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms
    !
```

https://t.me/learningnets

```
! sensor# show events


evIdsAlert: eventId=1395322617431000226 severity=informational vendor=Cisco
  originator:
    hostId: IPS4240
    appName: sensorApp
    appInstanceId: 1202
  time: 2014/04/07 19:51:35 2014/04/07 19:51:35 UTC
  signature: description=ICMP Echo Request id=2004 created=20001127 type=other version=S666
    subsigId: 0
    sigDetails: ICMP Echo Request
  interfaceGroup: vs1
  vlan: 46
  participants:
    attacker:
      addr: locality=OUT 180.1.46.16
    target:
      addr: locality=OUT 180.1.46.6
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
  threatRatingValue: 35
  interface: ge0_2
  protocol: icmp
```

2.3 IPS Custom Signature (3 points)

- Configure a custom signature for VLAN 34 traffic with the following requirements:
  - match on RADIUS authentication requests, both legacy and new ports.
  - produce alert and send SNMP trap to 172.16.6.50 using community of **ipstraps**.
  - fire signature if three RADIUS packets for same victim are detected in 60 seconds.

2.4 WSA Initialization (2 points)

- Initialize the WSA using the information from the table:

Variables	Values
Hostname	wsa.inelab.local

https://t.me/learningnets

Variables	Values
DNS Server	150.1.4.4
NTP Server	150.1.4.4
Proxy Ports	M1 and P1
M1 IPv4 Address	172.16.6.100/24
M1 Default Gateway	172.16.6.1
Admin Password	default1A
Email Address	ccielab@inelab.local
Senderbase Participation	Minimum
Global Policy Action	Block
Global Policy WBRS	Disabled

- Assign **TEST-PC-B** a IPv4 address from VLAN 88 for this scope.

2.5 WSA WCCP Integration (3 points)

- Configure both ASA1 contexts to redirect all HTTP traffic received inbound on its **INSIDE** interface to WSA:
  - Use the M1 port of the WSA for this scope.

- Secure the communication between WCCP clients and the WCCP server with the string **wccpasa** and match the output:

https://t.me/learningnets

```
ASA1/VLAN95# show wccp


    Global WCCP information:
        Router information:
            Router Identifier:                  180.1.99.15
            Protocol Version:                   2.0

        Service Identifier: 94
            Number of Cache Engines:            1
            Number of routers:                  2
            Total Packets Redirected:           0
            Redirect access-list:               REDIRECTED_TRAFFIC
            Total Connections Denied Redirect:  0
            Total Packets Unassigned:           0
            Group access-list:                  WSA_GROUP
            Total Messages Denied to Group:     0
            Total Authentication failures:      0
            Total Bypassed Packets Received:    0

ASA1/VLAN94# show wccp


    Global WCCP information:
        Router information:
            Router Identifier:                  180.1.99.16
            Protocol Version:                   2.0

        Service Identifier: 94
            Number of Cache Engines:            1
            Number of routers:                  2
            Total Packets Redirected:           0
            Redirect access-list:               REDIRECTED_TRAFFIC
            Total Connections Denied Redirect:  0
            Total Packets Unassigned:           0
            Group access-list:                  WSA_GROUP
            Total Messages Denied to Group:     0
            Total Authentication failures:      0
            Total Bypassed Packets Received:    0
```

2.6 WSA Traffic Policies (3 points)

- Configure WSA with an access policy as follows:

https://t.me/learningnets

- it matches on non-user configured identities.
- it is valid only for clients in subnet 172.16.6.0/24.
- it is not active on weekend days.

- R4 has been preconfigured as a DNS server. Configure **TEST-PC-B** with a DNS server of 150.1.4.4.
- Match the output when accessing **www.google.com** from **TEST-PC-B**:

```
SW5#show ip http server history


    HTTP server history:
    local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes  end-time
        150.1.13.13:80       172.16.6.100:62934 477        192        07:51:05 03/02
```

- Considering that **TEST-PC-B** has an IPv4 address of **172.16.6.50**, match the output when accessing **www.yahoo.com**.

```
R4#show ip http server history


    HTTP server history:
    local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes  end-time
          150.1.4.4:80        172.16.6.50:18793 0          0          11:51:21 04/08
```

3. Confidentiality and Secure Access

3.1 VRF Aware DMVPN Phase3 (5 points)

- Configure a DMVPN Phase3 cloud with R1 and R2 as hubs, and R3 and R6 as spokes:
  - use 3DES, MD5, DH group 2, and PSK authentication for IKEv1 Phase1.
  - use 3DES and MD5 for IKEv1 Phase2 and EIGRP in ASA 1236 to advertise VLAN 3, VLAN 6, and VLAN 88.
  - on tunnel interface, use IPv4 addressing in the format 1X.1X.1X.Y/24.
  - do not explicitly allow ESP traffic on ASA1, ASA2, or ASA3/ASA4 failover

https://t.me/learningnets

pair.

- Match the following output on R3:

```
R3#show dmvpn detail

    Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
            N - NATed, L - Local, X - No Socket
            # Ent --> Number of NHRP entries with same NBMA peer
            NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
            UpDn Time --> Up or Down Time for a Tunnel
    ============================================================================

    Interface Tunnel1236 is up/up, Addr. is 11.11.11.3, VRF ""
       Tunnel Src./Dest. addr: 150.1.3.3/MGRE, Tunnel VRF "LAB4"
       Protocol/Transport: "multi-GRE/IP", Protect "DMVPN_PROFILE"
       Interface State Control: Disabled

    IPv4 NHS:
    11.11.11.1  RE NBMA Address: 150.1.1.1 priority = 10 cluster = 1
    11.11.11.2  W NBMA Address: 150.1.2.2 priority = 20 cluster = 1
    Type:Spoke, Total NBMA Peers (v4/v6): 4

    # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
    ----- --------------- --------------- ----- -------- ----- -----------------
        1      150.1.1.1      11.11.11.1    UP 00:16:43    S      11.11.11.1/32

        1      150.1.2.2      11.11.11.2  NHRP 00:16:43   SX      11.11.11.2/32

        2      150.1.6.6      11.11.11.6    UP 00:16:20    D      11.11.11.6/32
        0      150.1.6.6      11.11.11.6    UP 00:16:20    D      172.16.5.0/24

        1      150.1.3.3      11.11.11.3    UP 00:16:20  DLX       180.1.3.0/24
```

- Match the following output on R6:

```
R6#show dmvpn detail

    Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
            N - NATed, L - Local, X - No Socket
            # Ent --> Number of NHRP entries with same NBMA peer
            NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
```

https://t.me/learningnets

```
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel1236 is up/up, Addr. is 11.11.11.6, VRF ""
   Tunnel Src./Dest. addr: 150.1.6.6/MGRE, Tunnel VRF "LAB4"
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN_PROFILE"
   Interface State Control: Enabled

IPv4 NHS:
11.11.11.1  RE NBMA Address: 150.1.1.1 priority = 10 cluster = 1
11.11.11.2  W NBMA Address: 150.1.2.2 priority = 20 cluster = 1
Type:Spoke, Total NBMA Peers (v4/v6): 4

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      150.1.1.1      11.11.11.1    UP 00:16:55    S      11.11.11.1/32

    1      150.1.2.2      11.11.11.2  NHRP 00:16:56   SX      11.11.11.2/32

    2      150.1.3.3      11.11.11.3    UP 00:16:40    D      11.11.11.3/32
    0      150.1.3.3      11.11.11.3    UP 00:16:40    D       180.1.3.0/24

    1      150.1.6.6      11.11.11.6    UP 00:16:40  DLX      172.16.5.0/24
```

3.2 IPsec High Availability (3 points)

- Configure an IPsec tunnel between R1, R2, and R5:
  - use 3DES, MD5, DH group 2, and PSK authentication.
  - on tunnel interface, use IPv4 addressing in the format 2X.2X.2X.Y/24.
  - R1 and R2 should be IKEv1 responders only.
  - do not explicitly allow ESP traffic on ASA1 or ASA3/ASA4 failover pair.

- Match the following output on R1:

```
R1#show crypto session remote 180.1.55.5

    Crypto session current status

    Interface: Tunnel125
    Profile: SVTI_ISAKMP
    Session status: UP-ACTIVE
    Peer: 180.1.55.5 port 500
```

https://t.me/learningnets

```
      IKEv1 SA: local 172.16.6.1/500 remote 180.1.55.5/500 Active
      IPSEC FLOW: permit 47 host 172.16.6.1 host 180.1.55.5
            Active SAs: 2, origin: crypto map
```

- Match the following output on R2:

```
R2#show crypto session remote 180.1.55.5

    Crypto session current status

    Interface: Tunnel125
    Profile: SVTI_ISAKMP
    Session status: UP-STANDBY
    Peer: 180.1.55.5 port 500
      IKEv1 SA: local 172.16.6.1/500 remote 180.1.55.5/500 Active
      IPSEC FLOW: permit 47 host 172.16.6.1 host 180.1.55.5
            Active SAs: 2, origin: crypto map
```

3.3 IPsec Troubleshooting (3 points)

- An IPsec tunnel has been preconfigured between R4 and R5.
- Fix the configuration to match the following outputs:

https://t.me/learningnets

```
R4#show crypto session remote 180.1.55.5

    Crypto session current status

    Interface: FastEthernet0/0
    Session status: UP-ACTIVE
    Peer: 180.1.55.5 port 500
      IKEv1 SA: local 180.1.45.4/500 remote 180.1.55.5/500 Active
      IPSEC FLOW: permit ip host 150.1.4.4 host 150.1.5.5
            Active SAs: 2, origin: crypto map

R4#ping 150.1.5.5 source loopback0


    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 150.1.5.5, timeout is 2 seconds:
    Packet sent with a source address of 150.1.4.4
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

3.4 ASA EzVPN Server (4 points)

- Configure ASA4 as EzVPN server:
  - allocate IPv4 addresses from subnet 180.1.200.0/24 and use **cisco** as the PSK.
  - tunnel only traffic to VLAN 21 and VLAN 22 subnets.
  - filter traffic to allow only ICMP Echo and HTTPS access through the tunnel.
  - your configuration should ensure that all users from VLAN 88 can connect.

- Without configuring the user **EZVPN_SERVER** on the ASA, match the following output for a connected client:

```
ASA34/pri/act# show vpn-sessiondb detail ra-ikev1-ipsec


    Session Type: IKEv1 IPsec Detailed

    Username     : EZVPN_SERVER           Index        : 3
    Assigned IP  : 180.1.200.1            Public IP    : 172.16.6.50
    Protocol     : IKEv1 IPsec
```

https://t.me/learningnets

```
License      : Other VPN
Encryption   : 3DES                  Hashing      : MD5
Bytes Tx     : 660                   Bytes Rx     : 900
Pkts Tx      : 11                    Pkts Rx      : 15
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy         Tunnel Group : EZVPN_SERVER
Login Time   : 18:02:48 UTC Tue Apr 8 2014
Duration     : 0h:19m:18s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 3.1
  UDP Src Port : 57001                 UDP Dst Port : 500
  IKE Neg Mode : Aggressive            Auth Mode    : preSharedKeys
  Encryption   : 3DES                  Hashing      : MD5
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 85242 Seconds
  D/H Group    : 2
  Filter Name  :
  Client OS    : WinNT                 Client OS Ver: 5.0.07.0410

IPsec:
  Tunnel ID    : 3.2
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 180.1.200.1/255.255.255.255/0/0
  Encryption   : 3DES                  Hashing      : MD5
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 27641 Seconds
  Idle Time Out: 30 Minutes            Idle TO Left : 16 Minutes
  Bytes Tx     : 660                   Bytes Rx     : 900
  Pkts Tx      : 11                    Pkts Rx      : 15

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 1159 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

https://t.me/learningnets

3.5 WLC Control-Plane Security (3 points)

- LAP should join the WLC through the spoke-to-spoke tunnel from the DMVPN section.
- Enhance the WiFi infrastructure security as follows:
  - mark the LAP from your rack as friendly.
  - enable infrastructure MFP.
  - authorize the LAP against the local WLC database.

4. Identity Management

4.1 IOS RADIUS Authentication (3 points)

- Configure R4 to authenticate telnet sessions against the ACS server using RADIUS; source packets from Loopback0 interface.
- Use **cisco** for any required password or key.
- User **RESTRICTED** with a password of **restricted** should have the following permissions:
  - run the **show privilege** command.
  - advertise prefixes into OSPF using the **network** command.
  - run the **show ip interface brief** command.
  - configure IP addressing for Loopback0 interface.
  - save the configuration using the **write memory** command.

- User **UNRESTRICTED** with a password of **unrestricted** should have full access.
- If the ACS server is not reachable, the same permissions should apply for both users.
- Do not use TACACS+ or any commands with the **privilege** keyword for this task.
- The ACS server is managed through the IPsec tunnel on ASA3.

4.2 ASA Local Command Authorization (3 points)

- Configure ASA3 to allow telnet traffic from VLAN 55 subnet and authenticate sessions using the local user database.
- Using the default enable authentication method, configure ASA3 to:
  - allow user **PRIV4** access to any **show crypto** type of commands at privilege level 4.

https://t.me/learningnets

- allow user **PRIV6** access to configure nameifs and security-levels and assign IP addresses to interfaces at privilege level 6.
- use **cisco** for any required passwords.

4.3 ASA Cut-Through Proxy (3 points)

- Configure ASA3 to require user authentication before traffic is allowed inbound on its **INSIDE** interface:
  - use RADIUS server from ACS for this scope with a key of **cisco**.
  - after user is authenticated, authorize it for all IP traffic.
  - test with the username/password pair of **asauser/asapass** through telnet on **180.1.55.100**.

- Match the following output if authenticating from R5:

```
ASA34/pri/act# show uauth

                          Current    Most Seen
    Authenticated Users       1          1
    Authen In Progress        0          1
    user 'asauser' at 180.1.55.5, authenticated
       access-list AUTHORIZATION (*)
       absolute   timeout: 0:05:00
       inactivity timeout: 0:00:00
```

- ACS server is managed through the IPsec tunnel on ASA3.

4.4 LAP 802.1x Authentication (3 points)

- Configure SW5 to authenticate the LAP via 802.1x using ISE server with a source of Loopback0:
  - use a RADIUS key of **Cisco123**.
  - authenticate via the username/password pair of **LAPUSER/Cisco123**.
  - configure the switch port to allow the LAP to work in flexconnect mode for locally switched WLANs.
  - authorize LAP in VLAN 3 in case of server/authentication failure, or if EAP supplicant is not active.

https://t.me/learningnets

- Match the following output:

```
SW5#show authentication sessions interface fastEthernet1/0/11

                Interface:  FastEthernet1/0/11
              MAC Address:  0006.f63b.9ada
               IP Address:  180.1.3.51
                User-Name:  LAPUSER
                   Status:  Authz Success
                   Domain:  DATA
```

- ISE server is managed through the IPsec tunnel on ASA3.

4.5 IPS Radius Authentication (3 points)

- Use ACS to authenticate non-console sessions to the IPS; if the ACS server is unreachable, use local database.
  - use a RADIUS key of **ciscoips**.
  - configure username/password pair of **ipsadmin/ipspass** for this scope.
  - without using the RADIUS VSA attributes, ensure that the user has administrator access to the IPS.

5. System Hardening and Availability

5.1 IOS Login Hardening (3 points)

- Configure R3 with the following login policies:
  - after three unsuccessful attempts in 60 seconds, block all further attempts for 600 seconds.
  - ensure that sessions sourced from the subnet 180.1.99.0/24 are exempted from this requirement.
  - log a message at every fifth unsuccessful login attempt.
  - enforce a delay of 3 seconds between successive login attempts.

5.2 IOS System Logging (2 points)

- Configure R3 with the following logging policy:

https://t.me/learningnets

- use informational level on console and buffer.
- send reliable debug level messages to host 180.1.55.66.
- filter OSPF adjacency messages from being displayed, use the string **Neighbor Down** for this.

5.3 IOS TFTP Server (1 points)

- Configure R4 as a TFTP server for its flash IOS image of **c2800nm-adventerprisek9-mz.151-3.T2.bin**.
- Allow only clients from Loopback0 range of 150.1.0.0/16 to download the image.
- TFTP sessions initiated by R4 should use its Loopback0 interface.

5.4 HSRP Authentication (1 points)

- Authenticate HSRP between R1 and R2 using the most secure method and a string of **hsrpkey**.

5.5 IPv6 OSPF Troubleshooting (2 points)

- R1 and R2 have been preconfigured for OSPFv3 on VLAN 99.
- Secure the process to match the output:

```
R2#show ipv6 ospf interface gigabitEthernet0/0

    GigabitEthernet0/0 is up, line protocol is up
      Link Local Address FE80::2, Interface ID 3
      Area 0, Process ID 1, Instance ID 0, Router ID 150.1.2.2
      Network Type BROADCAST, Cost: 1
      AES-CBC-256 encryption MD5 auth SPI 1000, secure socket UP (errors: 0)
```

5.6 IOS Control-Plane Security (3 points)

https://t.me/learningnets

- Configure R4 to limit all telnet and http traffic destined to itself to 16 Kbps, unless sourced from Loopback0 subnet of 150.1.0.0/16.
- Allow only http and telnet sessions for management, if received inbound on Fa0/0 interface.
- Do not configure any interface-level ACL configurations for this task.

6. Threat Identification and Mitigation

6.1 ASA Fragments Attack (1 points)

- Configure the ASA2 to drop any non-initial fragments through the firewalls.
- Do not use the keyword **fragment** in any access-list as part of this task.

6.2 ASA Control-Plane Attack (2 points)

- A DDoS attack has been detected against ASA3, with malformed ESP and IKE packets.
- Configure ASA3 to drop all IKE/IPsec VPN packets destined to itself unless sourced from VLAN 88.
  - the policy should apply only for VLAN 75 interface.

6.3 IP Spoofing Attack (2 points)

- WiFi clients are generating DoS attacks with spoofed IPv4 sources.
- Configure R6 to perform RFC 1918 filtering inbound on its VLAN 6 interface.
- A log message should be generated for each dropped packet.
- Ensure that a log message closely matches the output:

```
%SEC-6-IPACCESSLOGP: list RFC1918_ACL denied udp 10.10.10.10(0) -> 180.1.34.3(0), 1 packet  [RFC1918_FILTER]
```

6.4 ASA System Logging (3 points)

- Configure ASA2 to generate timestamped logging messages:
  - collect the debugging messages in the system memory buffer, use a size of 65536 bytes.
  - save the memory buffer contents when it wraps to the FTP server

https://t.me/learningnets

180.1.46.99 using the username **asalogging** and the password **asapassword**.
    - send an email from **asa2firewall@inelab.local** to **admin@inelab.local** each time the SLA state changes.
    - consider the SMTP servers to be 180.1.46.99 and 180.1.46.100.

6.5 ASA Application Control (3 points)

- Configure ASA2 to silently drop messenger traffic.
- As an exception, allow it between VLAN 34 and VLAN 46.

6.6 ASA Application Control (2 points)

- A CAM table overflow attack has been detected in VLAN 88:
    - attack is causing switches to no longer learn valid MAC addresses and thus perform unknown unicast flooding for all VLANs.
    - configure the switching infrastructure to stop learning MAC addresses for VLAN 88.

- One of the attackers has been identified with the MAC address of **0034.aa12.f0a1**; configure switches to silently drop this traffic.

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 4

CCIE SCv4 Lab 4 Solutions Section 1

1. Task 1.1 Solution
2. Task 1.2 Solution
3. Task 1.3 Solution
4. Task 1.4 Solution
5. Task 1.5 Solution
6. Task 1.6 Solution
7. Task 1.7 Solution
8. Task 1.8 Solution
9. Task 1.9 Solution

Task 1.1 Solution

SW1:

```
interface FastEthernet1/0/17
 switchport mode access
 switchport access vlan 55
 no shutdown
```

SW2:

```
interface FastEthernet1/0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 74,75
 no shutdown
```

ASA3:

```
hostname ASA34
!
interface GigabitEthernet0/0
 no shutdown
!
interface GigabitEthernet0/0.74
```

https://t.me/learningnets

```
 vlan 74
 ip address 180.1.74.17 255.255.255.0
 nameif VLAN74
 security-level 70
!
interface GigabitEthernet0/0.75
 vlan 75
 ip address 180.1.75.17 255.255.255.0
 nameif VLAN75
 security-level 50
!
interface GigabitEthernet0/1
 nameif INSIDE
 ip address 180.1.55.17 255.255.255.0
 no shutdown
!
router eigrp 400
 no auto-summary
 eigrp router-id 34.34.34.34
 network 180.1.55.0 255.255.255.0
 redistribute ospf 400 metric 100000 100 255 1 1500
!
router ospf 400
 router-id 34.34.34.34
 network 180.1.75.0 255.255.255.0 area 0
 network 180.1.74.0 255.255.255.0 area 0
 redistribute eigrp 400 subnets
```

Task 1.1 Verification

Verify switch port level configuration:

```
SW1#show interfaces FastEthernet1/0/17 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/17    off              negotiate      not-trunking  1

Port        Vlans allowed on trunk
Fa1/0/17    55

Port        Vlans allowed and active in management domain
Fa1/0/17    55

Port        Vlans in spanning tree forwarding state and not pruned Fa1/0/17    55
```

https://t.me/learningnets

```
!
!SW2#show interfaces FastEthernet1/0/16 trunk


Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/16    on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa1/0/16    74-75

Port        Vlans allowed and active in management domain
Fa1/0/16    74-75

Port        Vlans in spanning tree forwarding state and not pruned Fa1/0/16    74-75
```

Verify interface nameif, security-level, and IPv4 addressing:

```
ASA34# show nameif
 Interface                Name                    Security
 GigabitEthernet0/0.74    VLAN74                   70
 GigabitEthernet0/0.75    VLAN75                   50
 GigabitEthernet0/1       INSIDE                   100
 !
 !
 ASA3# show ip address
 System IP Addresses:
 Interface                Name                IP address      Subnet mask     Method
 GigabitEthernet0/0.74    VLAN74              180.1.74.17     255.255.255.0   manual
 GigabitEthernet0/0.75    VLAN75              180.1.75.17     255.255.255.0   manual
 GigabitEthernet0/1       INSIDE              180.1.55.17     255.255.255.0   manual
 Current IP Addresses:
 Interface                Name                IP address      Subnet mask     Method
 GigabitEthernet0/0.74    VLAN74              180.1.74.17     255.255.255.0   manual
 GigabitEthernet0/0.75    VLAN75              180.1.75.17     255.255.255.0   manual
 GigabitEthernet0/1       INSIDE              180.1.55.17     255.255.255.0   manual
```

Verify that OSPF and EIGRP neighbors are established:

```
ASA34# show ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.13.13       1   FULL/DR         0:00:38     180.1.75.13     VLAN75
```

https://t.me/learningnets

```
!
!ASA34# show eigrp neighbors

EIGRP-IPv4 neighbors for process 400
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   180.1.55.5              Gi0/1            10  00:04:38 1018 5000  0   11
```

Verify that ASA3 performs redistribution between OSPF and EIGRP:

```
R5#show ip route eigrp | i EX
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
D EX     150.1.3.3 [170/53760] via 180.1.55.17, 00:05:13, FastEthernet0/1
D EX     150.1.4.4 [170/53760] via 180.1.55.17, 00:05:13, FastEthernet0/1
D EX     150.1.13.13 [170/53760] via 180.1.55.17, 00:05:13, FastEthernet0/1
D EX     180.1.3.0/24 [170/53760] via 180.1.55.17, 00:05:13, FastEthernet0/1
D EX     180.1.34.0/24 [170/53760] via 180.1.55.17, 00:05:13, FastEthernet0/1
D EX     180.1.45.0/24 [170/53760] via 180.1.55.17, 00:05:13, FastEthernet0/1
D EX     180.1.74.0/24 [170/53760] via 180.1.55.17, 00:05:18, FastEthernet0/1
D EX     180.1.75.0/24 [170/53760] via 180.1.55.17, 00:05:18, FastEthernet0/1
!
!SW5#show ip route ospf | i E2

O E2    172.16.1.0 [110/20] via 180.1.75.17, 00:06:01, Vlan75
O E2    172.16.3.0 [110/20] via 180.1.75.17, 00:06:01, Vlan75
O E2    180.1.53.0 [110/20] via 180.1.75.17, 00:06:01, Vlan75
O E2    180.1.55.0 [110/20] via 180.1.75.17, 00:06:02, Vlan75
O E2    150.1.11.11 [110/20] via 180.1.75.17, 00:06:01, Vlan75
O E2    150.1.5.5 [110/20] via 180.1.75.17, 00:06:01, Vlan75
```

Verify the OSPF and EIGRP router IDs:

```
ASA34/pri/act# show ospf

 Routing Process "ospf 400" with ID 34.34.34.34 and Domain ID 0.0.1.144
 Supports only single TOS(TOS0) routes
 Does not support opaque LSA
 It is an autonomous system boundary router
 Redistributing External Routes from,
    eigrp 400, includes subnets in redistribution
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 7. Checksum Sum 0x 34584
```

https://t.me/learningnets

```
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm executed 8 times
        Area ranges are
        Number of LSA 15. Checksum Sum 0x 83660
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
!
!ASA34/pri/act# show eigrp topology

EIGRP-IPv4 Topology Table for AS(400)/ID(34.34.34.34)


Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 180.1.53.0 255.255.255.0, 1 successors, FD is 28416
        via 180.1.55.5 (28416/28160), GigabitEthernet0/1
```

Task 1.2 Solution

SW1:

```
interface FastEthernet1/0/19
 switchport mode access
 switchport access vlan 55
 no shutdown
```

SW2:

```
vlan 100
!
interface FastEthernet1/0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 74,75
 no shutdown
```

https://t.me/learningnets

```
!
interface range FastEthernet1/0/17 , FastEthernet1/0/19
 switchport mode access
 switchport access vlan 100
 no shutdown
```

ASA3:

```
prompt hostname priority state
!
interface GigabitEthernet0/2
 no shutdown
!
failover lan unit primary
failover lan interface FAILOVER GigabitEthernet0/2
failover link FAILOVER GigabitEthernet0/2
failover polltime interface 1 holdtime 5
failover interface ip FAILOVER 180.1.100.17 255.255.255.0 standby 180.1.100.18
failover
!
monitor-interface VLAN74
monitor-interface VLAN75
monitor-interface INSIDE
!
interface GigabitEthernet0/0.74
 ip address 180.1.74.17 255.255.255.0 standby 180.1.74.18
!
interface GigabitEthernet0/0.75
 ip address 180.1.75.17 255.255.255.0 standby 180.1.75.18
!
interface GigabitEthernet0/1
 ip address 180.1.55.17 255.255.255.0 standby 180.1.55.18
```

ASA4:

```
interface GigabitEthernet0/2
 no shutdown
!
failover lan unit secondary
failover lan interface FAILOVER GigabitEthernet0/2
failover link FAILOVER GigabitEthernet0/2
failover polltime interface 1 holdtime 5
failover interface ip FAILOVER 180.1.100.17 255.255.255.0 standby 180.1.100.18
failover
```

https://t.me/learningnets

Task 1.2 Verification

Verify that the requested output is being matched:

```
ASA34/pri/act(config)# show failover

Failover On
Failover unit Primary
Failover LAN Interface: FAILOVER GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 1 seconds, holdtime 5 seconds
Interface Policy 1
Monitored Interfaces 3 of 114 maximum
Version: Ours 8.6(1)10, Mate 8.6(1)10
Last Failover at: 07:50:08 UTC Apr 7 2014
        This host: Primary - Active
                Active time: 409 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)10) status (Up Sys)
                  Interface VLAN74 (180.1.74.17): Normal (Monitored)
                  Interface VLAN75 (180.1.75.17): Normal (Monitored)
                  Interface INSIDE (180.1.55.17): Normal (Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/) status (Unresponsive/Up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)10) status (Up Sys)
                  Interface VLAN74 (180.1.74.18): Normal (Monitored)
                  Interface VLAN75 (180.1.75.18): Normal (Monitored)
                  Interface INSIDE (180.1.55.18): Normal (Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/) status (Unresponsive/Up)

Stateful Failover Logical Update Statistics
        Link : FAILOVER GigabitEthernet0/2 (up)
```

Verify the IPv4 addressing for the failover interface:

https://t.me/learningnets

```
ASA34/pri/act# show failover interface

        interface FAILOVER GigabitEthernet0/2
                System IP Address: 180.1.100.17 255.255.255.0 My IP Address    : 180.1.100.17
 Other IP Address : 180.1.100.18
```

Verify that switch port failover interfaces are in VLAN 100:

```
SW2#show spanning-tree interface fastEthernet1/0/17

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
VLAN0100            Desg FWD 19        128.19   P2p
!
!SW2#show spanning-tree interface fastEthernet1/0/19

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
VLAN0100            Desg FWD 19        128.21   P2p
```

Task 1.3 Solution

```
SW1:
interface FastEthernet1/0/13
 switchport mode access
 switchport access vlan 99
 no shutdown

SW2:

interface FastEthernet1/0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 94,95
 no shutdown
```

Convert ASA to multiple mode:

https://t.me/learningnets

```
ciscoasa(config)# mode multiple

WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]

ASA1 System Context:
hostname ASA1
prompt hostname context
!
mac-address auto
!
interface Ethernet0/0
 no shutdown
!
interface Ethernet0/0.94
 vlan 94
!
interface Ethernet0/0.95
 vlan 95
!
interface Ethernet0/1
 no shutdown
!
delete /noconfirm disk0:/*.cfg
!
!
context VLAN94
 allocate-interface Ethernet0/0.94
 allocate-interface Ethernet0/1
 config-url disk0:/VLAN94.cfg
!
context VLAN95
 allocate-interface Ethernet0/0.95
 allocate-interface Ethernet0/1
 config-url disk0:/VLAN95.cfg

ASA1 VLAN94 Context:
interface Ethernet0/1
 nameif INSIDE
 security-level 90
 ip address 180.1.99.16 255.255.255.0
!
interface Ethernet0/0.94
 nameif OUTSIDE
```

https://t.me/learningnets

```
 security-level 10
 ip address 180.1.94.15 255.255.255.0
!
route OUTSIDE 0 0 180.1.94.16
route INSIDE 172.16.6.0 255.255.255.0 180.1.99.2

ASA1 VLAN95 Context:

interface Ethernet0/1
 nameif INSIDE
 security-level 90
 ip address 180.1.99.15 255.255.255.0
!
interface Ethernet0/0.95
 nameif OUTSIDE
 security-level 10
 ip address 180.1.95.15 255.255.255.0
!
route OUTSIDE 0 0 180.1.95.13
route INSIDE 172.16.6.0 255.255.255.0 180.1.99.1
```

Task 1.3 Verification

Verify that switches are forwarding the correct VLANs on the ports connected to ASA1:

```
SW1#show spanning-tree interface fastEthernet1/0/13

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
VLAN0099            Desg FWD 19        128.15   P2p
!
!SW2#show spanning-tree interface fastEthernet1/0/12

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
VLAN0094            Desg FWD 19        128.14   P2p
VLAN0095            Desg FWD 19        128.14   P2p
```

Verify interface allocation to each context:

```
ASA1# show context
```

https://t.me/learningnets

```
Context Name      Class      Interfaces           URL
*admin            default                         disk0:/admin.cfg
VLAN94            default    Ethernet0/0.94,Ethernet0/1 disk0:/VLAN94.cfg
 VLAN95           default    Ethernet0/0.95,Ethernet0/1 disk0:/VLAN95.cfg
```

Verify nameif, security level, and IPv4 addressing for each context:

```
ASA1/VLAN94# show nameif
Interface                 Name                    Security
Ethernet0/0.94            OUTSIDE                  10
Ethernet0/1               INSIDE                   90
!
!ASA1/VLAN94# show ip address

System IP Addresses:
Interface                 Name                    IP address      Subnet mask     Method
Ethernet0/0.94            OUTSIDE                 180.1.94.15     255.255.255.0   manual
Ethernet0/1               INSIDE                  180.1.99.16     255.255.255.0   manual
Current IP Addresses:
Interface                 Name                    IP address      Subnet mask     Method
Ethernet0/0.94            OUTSIDE                 180.1.94.15     255.255.255.0   manual
Ethernet0/1               INSIDE                  180.1.99.16     255.255.255.0   manual
!
!ASA1/VLAN95# show nameif
Interface                 Name                    Security
Ethernet0/0.95            OUTSIDE                  10
Ethernet0/1               INSIDE                   90
!
!ASA1/VLAN95# show ip address

System IP Addresses:
Interface                 Name                    IP address      Subnet mask     Method
Ethernet0/0.95            OUTSIDE                 180.1.95.15     255.255.255.0   manual
Ethernet0/1               INSIDE                  180.1.99.15     255.255.255.0   manual
Current IP Addresses:
Interface                 Name                    IP address      Subnet mask     Method
Ethernet0/0.95            OUTSIDE                 180.1.95.15     255.255.255.0   manual
Ethernet0/1               INSIDE                  180.1.99.15     255.255.255.0   manual
```

https://t.me/learningnets

Task 1.4 Solution

SW1:

```
interface FastEthernet1/0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 74,94
 no shutdown
```

SW2:

```
interface FastEthernet1/0/14
 switchport mode access
 switchport access vlan 46
 no shutdown
```

ASA2:

```
hostname ASA2
!
interface Ethernet0/0
 nameif OUTSIDE
 ip address 180.1.46.16 255.255.255.0
 security-level 10
 no shutdown
!
interface Ethernet0/1
 no shutdown
!
interface Ethernet0/1.74
 vlan 74
 nameif DMZ
 ip address 180.1.74.16 255.255.255.0
 security-level 50
!
interface Ethernet0/1.94
 vlan 94
 nameif INSIDE
 ip address 180.1.94.16 255.255.255.0
 security-level 90
!
prefix-list OSPF_FILTER seq 5 deny 0.0.0.0/0 le 32
!
router ospf 22
```

https://t.me/learningnets

```
 network 180.1.46.0 255.255.255.0 area 22
 network 180.1.74.0 255.255.255.0 area 0
 network 180.1.94.0 255.255.255.0 area 0
 area 0 filter-list prefix OSPF_FILTER in
 area 22 stub no-summary
```

Task 1.4 Verification

Verify the switch port level configuration:

```
SW1#show interfaces FastEthernet1/0/15 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/15    on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa1/0/15    74,94

Port        Vlans allowed and active in management domain
Fa1/0/15    74,94

Port        Vlans in spanning tree forwarding state and not pruned Fa1/0/15    74,94
!
!SW2#show interfaces FastEthernet1/0/14 trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/14    off              negotiate      not-trunking  1

Port        Vlans allowed on trunk
Fa1/0/14    46

Port        Vlans allowed and active in management domain
Fa1/0/14    46

Port        Vlans in spanning tree forwarding state and not pruned Fa1/0/14    46
```

Verify the nameif, security-level, and IPv4 addressing:

```
ASA2# show nameif
Interface                Name                    Security
Ethernet0/0              OUTSIDE                  10
```

https://t.me/learningnets

```
Ethernet0/1.74           DMZ                       50
Ethernet0/1.94           INSIDE                    90
!
!ASA2# show ip address

System IP Addresses:
Interface                Name                  IP address      Subnet mask     Method
Ethernet0/0              OUTSIDE               180.1.46.16     255.255.255.0   manual
Ethernet0/1.74           DMZ                   180.1.74.16     255.255.255.0   manual
Ethernet0/1.94           INSIDE                180.1.94.16     255.255.255.0   manual
Current IP Addresses:
Interface                Name                  IP address      Subnet mask     Method
Ethernet0/0              OUTSIDE               180.1.46.16     255.255.255.0   manual
Ethernet0/1.74           DMZ                   180.1.74.16     255.255.255.0   manual
Ethernet0/1.94           INSIDE                180.1.94.16     255.255.255.0   manual
```

Verify that ASA has OSPF neighbors in both area 0 and area 22:

```
ASA2# show ospf neighbor



Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.6.6         1   FULL/BDR        0:00:39     180.1.46.6      OUTSIDE
34.34.34.34       1   FULL/BDR        0:00:32     180.1.74.17     DMZ
```

Verify that area 22 is configured as totally stubby area, so only a default route is injected:

```
ASA2# show ospf | b Area 22
    Area 22
        Number of interfaces in this area is 1 It is a stub area, no summary LSA in this area
 generates stub default route with cost 1
        Area has no authentication
        SPF algorithm executed 22 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x 26b69
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
!
```

https://t.me/learningnets

```
!R6#show ip route vrf LAB4 ospf


Routing Table: LAB4
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 180.1.46.16 to network 0.0.0.0
O*IA  0.0.0.0/0 [110/2] via 180.1.46.16, 00:14:00, FastEthernet0/0
```

Verify that ASA2 filters area 22 prefixes from being advertised into area 0:

```
ASA2# show ospf | b BACKBONE
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 7 times
        Area ranges are Area-filter OSPF_FILTER in
        Number of LSA 10. Checksum Sum 0x 6994b
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
!
!ASA34/pri/act# show ospf database summary adv-router 180.1.94.16


       OSPF Router with ID (34.34.34.34) (Process ID 400)
ASA34/pri/act#
```

Task 1.5 Solution

```
ASA2:
```

https://t.me/learningnets

```
sla monitor 10
 type echo protocol ipIcmpEcho 180.1.94.15 interface INSIDE
sla monitor schedule 10 life forever start-time now
!
track 10 rtr 10 reachability
!
route INSIDE 0.0.0.0 0.0.0.0 180.1.94.15 1 track 10
!
router ospf 22
 default-information originate
```

Task 1.5 Verification

Verify the SLA and track states:

```
ASA2# show sla monitor configuration 10
IP SLA Monitor, Infrastructure Engine-II. Entry number: 10
Owner:
Tag: Type of operation to perform: echo
Target address: 180.1.94.15
Interface: INSIDE
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
!
!ASA2# show sla monitor operational-state

Entry number: 10
Modification time: 08:58:36.416 UTC Mon Apr 7 2014
Number of Octets Used by this Entry: 1480
Number of operations attempted: 47
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
```

https://t.me/learningnets

```
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 09:44:36.417 UTC Mon Apr 7 2014 Latest operation return code: OK
RTT Values:
RTTAvg: 1       RTTMin: 1       RTTMax: 1
NumOfRTT: 1     RTTSum: 1       RTTSum2: 1
!
!ASA2# show track

Track 10
  Response Time Reporter 10 reachability Reachability is Up
  1 change, last change 00:45:59 Latest operation return code: OK
  Latest RTT (millisecs) 1
  Tracked by: STATIC-IP-ROUTING 0
```

Verify that the static route is present in the routing table and being originated in the OSPF database:

```
ASA2# show route INSIDE


Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 180.1.94.15 to network 0.0.0.0

C    180.1.94.0 255.255.255.0 is directly connected, INSIDE
S*   0.0.0.0 0.0.0.0 [1/0] via 180.1.94.15, INSIDE
!
!ASA2# show ospf database external 0.0.0.0


       OSPF Router with ID (180.1.94.16) (Process ID 22)


                Type-5 AS External Link States
```

https://t.me/learningnets

```
  LS age: 1087
  Options: (No TOS-capability, DC)
  LS Type: AS External Link Link State ID: 0.0.0.0 (External Network Number )
Advertising Router: 180.1.94.16
  LS Seq Number: 80000002
  Checksum: 0x5d1b
  Length: 36 Network Mask:0.0.0.0

        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 1
        Forward Address: 0.0.0.0
        External Route Tag: 22
```

Verify that the route is propagated in the OSPF domain:

```
R4#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "ospf 400", distance 110, metric 1, candidate default path
  Tag 22, type extern 2, forward metric 12
  Last update from 180.1.45.13 on FastEthernet0/0, 00:49:23 ago
  Routing Descriptor Blocks: * 180.1.45.13, from 180.1.94.16, 00:49:23 ago, via FastEthernet0/0

      Route metric is 1, traffic share count is 1
      Route tag 22
```

Task 1.6 Solution

ASA3:

```
object-group network REAL_SOURCE
 network-object 172.16.1.0 255.255.255.0
 network-object 172.16.3.0 255.255.255.0
!
nat (INSIDE,VLAN74) source dynamic REAL_SOURCE interface
nat (INSIDE,VLAN75) source dynamic REAL_SOURCE interface
!
!
object network R5_LOOPBACK_REAL
 host 150.1.5.5
!
object network SW5_LOOPBACK_REAL
 host 150.1.13.13
```

https://t.me/learningnets

```
!
nat (INSIDE,VLAN75) source static R5_LOOPBACK_REAL R5_LOOPBACK_REAL destination static SW5_LOOPBACK_REAL SW5_LOOPBAC
nat (INSIDE,VLAN75) source dynamic R5_LOOPBACK_REAL interface
```

Task 1.6 Verification

Verify the exact NAT matches based on source/destination of the traffic:

```
ASA34/pri/act# show nat detail

Manual NAT Policies (Section 1)
1 (INSIDE) to (VLAN74) source dynamic REAL_SOURCE interface
    translate_hits = 46, untranslate_hits = 0
    Source - Origin: 172.16.1.0/24, 172.16.3.0/24, Translated: 180.1.74.17/24
2 (INSIDE) to (VLAN75) source dynamic REAL_SOURCE interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 172.16.1.0/24, 172.16.3.0/24, Translated: 180.1.75.17/24
3 (INSIDE) to (VLAN75) source static R5_LOOPBACK_REAL R5_LOOPBACK_REAL   destination static SW5_LOOPBACK_REAL SW5_LO
    translate_hits = 1, untranslate_hits = 0
    Source - Origin: 150.1.5.5/32, Translated: 150.1.5.5/32
    Destination - Origin: 150.1.13.13/32, Translated: 150.1.13.13/32
4 (INSIDE) to (VLAN75) source dynamic R5_LOOPBACK_REAL interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 150.1.5.5/32, Translated: 180.1.75.17/24
```

Verify traffic initiated from R5's Loopback0 using packet-tracer:

```
ASA34/pri/act# packet-tracer input INSIDE tcp 150.1.5.5 20000 150.1.13.13 23 detailed

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   150.1.13.13     255.255.255.255 VLAN75

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

https://t.me/learningnets

```
 Forward Flow based lookup yields rule:
 in  id=0x7fff2e098d50, priority=0, domain=inspect-ip-options, deny=true
        hits=173, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=INSIDE, output_ifc=any

Phase: 3
Type: FOVER
Subtype: standby-update
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fff2e267bd0, priority=20, domain=lu, deny=false
        hits=6, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=INSIDE, output_ifc=any

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (INSIDE,VLAN75) source static R5_LOOPBACK_REAL R5_LOOPBACK_REAL destination static SW5_LOOPBACK_REAL SW5_LOOPBAC
Additional Information:Static translate 150.1.5.5/20000 to 150.1.5.5/20000
 Forward Flow based lookup yields rule:
 in  id=0x7fff2e289bd0, priority=6, domain=nat, deny=false
        hits=3, user_data=0x7fff2e25c8f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=150.1.5.5, mask=255.255.255.255, port=0
        dst ip/id=150.1.13.13, mask=255.255.255.255, port=0, dscp=0x0
        input_ifc=INSIDE, output_ifc=VLAN75
!
!ASA34/pri/act# packet-tracer input INSIDE tcp 150.1.5.5 20000 150.1.4.4 23 detailed

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   150.1.4.4       255.255.255.255 VLAN75

Phase: 2
Type: IP-OPTIONS
```

https://t.me/learningnets

```
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fff2e098d50, priority=0, domain=inspect-ip-options, deny=true
        hits=174, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=INSIDE, output_ifc=any

Phase: 3
Type: FOVER
Subtype: standby-update
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fff2e267bd0, priority=20, domain=lu, deny=false
        hits=7, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=INSIDE, output_ifc=any

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:nat (INSIDE,VLAN75) source dynamic R5_LOOPBACK_REAL interface
Additional Information:Dynamic translate 150.1.5.5/20000 to 180.1.75.17/54370

 Forward Flow based lookup yields rule:
 in  id=0x7fff2e287bc0, priority=6, domain=nat, deny=false
        hits=1, user_data=0x7fff2e286de0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=150.1.5.5, mask=255.255.255.255, port=0
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=INSIDE, output_ifc=VLAN
```

Task 1.7 Solution

R1:

```
ip inspect name VLAN88_CBAC icmp
ip inspect name VLAN88_CBAC tcp
```

https://t.me/learningnets

```
ip inspect name VLAN88_CBAC udp
ip inspect name VLAN88_CBAC smtp max-data 10000000
!
ip inspect log drop-pkt
ip inspect hashtable-size 4096
!
access-list 2 permit host 180.1.45.44
ip port-map user-1 port tcp 777 list 2
ip inspect name VLAN88_CBAC user-1 timeout 600
ip inspect name VLAN88_CBAC parameter max-sessions 20000
!
ip access-list extended VLAN99_INBOUND
 deny ip any any
!
interface GigabitEthernet0/1
 ip inspect VLAN88_CBAC in
!
interface GigabitEthernet0/0
 ip access-group VLAN99_INBOUND in
```

Task 1.7 Verification

Verify the inspection configuration:

https://t.me/learningnets

```
R1#show ip inspect config
 Dropped packet logging is enabled

Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [unlimited : unlimited] connections
max-incomplete sessions thresholds are [unlimited : unlimited]
max-incomplete tcp connections per host is unlimited. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
tcp reassembly queue length 16; timeout 5 sec; memory-limit 1024 kilo bytes
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name VLAN88_CBAC icmp alert is on audit-trail is off timeout 10
 tcp alert is on audit-trail is off timeout 3600
 udp alert is on audit-trail is off timeout 30
 smtp max-data 10000000 alert is on audit-trail is off timeout 3600
 user-1 alert is on audit-trail is off timeout 600
 session threshold is 20000
```

Verify that CBAC is enabled, as well as ACL in the reverse direction:

```
R1#show ip interface gigabitEthernet 0/1 | i Output
  Output features: Firewall (NAT), Firewall (inspect)
!
!R1#show ip interface gigabitEthernet 0/0 | i Inbound|Output

  Inbound  access list is VLAN99_INBOUND
  Output features: Firewall (NAT), Firewall (inspect)
```

Task 1.8 Solution

```
R1:
interface GigabitEthernet0/1
 standby ip 172.16.6.1
 standby priority 150
 standby preempt
 standby name CBAC_HA
!
ipc zone default
 association 1
```

https://t.me/learningnets

```
  no shutdown
  protocol sctp
  local-port 5000
  local-ip 172.16.6.11
  remote-port 5000
  remote-ip 172.16.6.22
!
crypto isakmp key cbacha address 172.16.6.11
!
redundancy inter-device
 scheme standby CBAC_HA
 security ipsec default
```

R2:

```
interface GigabitEthernet0/1
 standby ip 172.16.6.1
 standby preempt
 standby name CBAC_HA
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
  local-port 5000
  local-ip 172.16.6.22
  remote-port 5000
  remote-ip 172.16.6.11
!
crypto isakmp key cbacha address 172.16.6.11
!
redundancy inter-device
 scheme standby CBAC_HA
 security ipsec default
```

Save the configuration and reload both devices.

```
R1:
interface GigabitEthernet0/1
 ip inspect VLAN88_CBAC in redundancy stateful CBAC_HA
```

R2:

```
ip inspect name VLAN88_CBAC icmp
```

https://t.me/learningnets

```
ip inspect name VLAN88_CBAC tcp
ip inspect name VLAN88_CBAC udp
ip inspect name VLAN88_CBAC smtp max-data 10000000
!
ip inspect log drop-pkt
ip inspect hashtable-size 4096
ip access-list log-update threshold 1
!
access-list 2 permit host 180.1.45.44
ip port-map user-1 port tcp 777 list 2
ip inspect name VLAN88_CBAC user-1 timeout 600
ip inspect name VLAN88_CBAC parameter max-sessions 20000
!
ip access-list extended VLAN99_INBOUND
 deny ip any any log
!
interface GigabitEthernet0/1
 ip inspect VLAN88_CBAC in redundancy stateful CBAC_HA
!
interface GigabitEthernet0/0
 ip access-group VLAN99_INBOUND in
```

Task 1.8 Verification

Verify that the requested output is matched:

```
R1#show redundancy inter-device

Redundancy inter-device state: RF_INTERDEV_STATE_ACT
  Scheme: Standby
      Groupname: CBAC_HA Group State: Active
  Peer present: RF_INTERDEV_PEER_COMM
  Security:
      Type:         IPSec
      Profile name: default
      State:        Up
!
!R1#show standby

GigabitEthernet0/1 - Group 0
  State is Active
    2 state changes, last state change 00:20:02
  Virtual IP address is 172.16.6.1
  Active virtual MAC address is 0000.0c07.ac00
    Local virtual MAC address is 0000.0c07.ac00 (v1 default)
```

https://t.me/learningnets

```
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.432 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.6.22, priority 100 (expires in 9.584 sec)
  Priority 150 (configured 150)
  Group name is "CBAC_HA" (cfgd)
```

Verify that R2 is in standby state with communication being functional:

```
R2#show redundancy inter-device

Redundancy inter-device state: RF_INTERDEV_STATE_STDBY
  Scheme: Standby
      Groupname: CBAC_HA Group State: Standby
  Peer present: RF_INTERDEV_PEER_COMM
  Security:
      Type:         IPSec
      Profile name: default
      State:        Up
```

Confirm that the IKEv1/IPsec tunnel has been established and packets are bidirectionally flowing:

https://t.me/learningnets

```
R1#show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.6.22     172.16.6.11     QM_IDLE           1003 ACTIVE


IPv6 Crypto ISAKMP SA
!
!R1#show crypto ipsec sa peer 172.16.6.22 | i pkts
 #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
 #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6

    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
```

Configure **TEST-PC-B** with IPv4 address in VLAN 88 and a default gateway of **172.16.6.1**; initiate a telnet session to SW5 and verify the session state in both firewall tables:

```
R1#show ip inspect ha sessions detail

Sess_ID    (src_addr:port)=>(dst_addr:port)   proto sess_state   ha_stateEstablished Sessions
2CDC0460 (172.16.6.50:15808)=>(150.1.13.13:00023) tcp   SIS_OPEN     HA_ACTIVE
  Created 00:00:01, Last heard 00:00:01
  Bytes sent (initiator:responder) [21:49]
In  SID 150.1.13.13[23:23]=>172.16.6.50[15808:15808] on ACL VLAN99_INBOUND  (5 matches)
 HA state: HA_ACTIVE
Half-open Sessions
!
!R2#show ip inspect ha sessions detail

Sess_ID    (src_addr:port)=>(dst_addr:port)   proto sess_state   ha_stateEstablished Sessions
2D176E54 (172.16.6.50:15808)=>(150.1.13.13:00023) tcp   SIS_OPEN     HA_STANDBY
  Created 00:00:04, Last heard never
  Bytes sent (initiator:responder) [0:0]
```

https://t.me/learningnets

```
In  SID 150.1.13.13[23:23]=>172.16.6.50[15808:15808] on ACL VLAN99_INBOUND
 HA state: HA_STANDBY
```

Task 1.9 Solution

ASA3:

```
access-list VLAN75_IN extended permit tcp host 150.1.13.13 host 180.1.99.1 eq 23
access-list VLAN75_IN extended permit tcp host 150.1.13.13 host 180.1.99.2 eq 23
!
access-group VLAN75_IN in interface VLAN75
```

ASA2:

```
access-list DMZ_IN extended permit tcp host 150.1.13.13 host 180.1.99.1 eq 23
access-list DMZ_IN extended permit tcp host 150.1.13.13 host 180.1.99.2 eq 23
!
access-group DMZ_IN in interface DMZ
```

ASA1 System Context:

```
failover lan unit primary
failover lan interface FAILOVER Ethernet0/2
failover link FAILOVER Ethernet0/2
failover interface ip FAILOVER 180.1.100.17 255.255.255.0 standby 180.1.100.18
!
failover group 1
failover group 2
failover
```

ASA1 VLAN94 Context:

```
access-list OUTSIDE_IN extended permit tcp host 150.1.13.13 host 180.1.99.1 eq telnet
access-list OUTSIDE_IN extended permit tcp host 150.1.13.13 host 180.1.99.2 eq telnet
!
access-group OUTSIDE_IN in interface OUTSIDE
!
interface Ethernet0/1
 asr-group 1
```

ASA1 VLAN95 Context:

```
interface Ethernet0/1
 asr-group 1
```

SW2:

```
interface FastEthernet1/0/13
 no shutdown
```

https://t.me/learningnets

```
R1:
ip access-list extended VLAN99_INBOUND
 1 permit tcp host 150.1.13.13 host 180.1.99.1 eq 23
!
ip access-list resequence VLAN99_INBOUND 10 10


R2:#B#
ip access-list extended VLAN99_INBOUND
 1 permit tcp host 150.1.13.13 host 180.1.99.2 eq 23
!
ip access-list resequence VLAN99_INBOUND 10 10
```

Task 1.9 Verification

Verify that the requested output is matched, and check the session state in VLAN94 context:

https://t.me/learningnets

```
SW5#telnet 180.1.99.1 /source-interface Loopback0
Trying 180.1.99.1 ... Open
R1>
!
!ASA1/VLAN94# show conn long

1 in use, 2 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
TCP OUTSIDE:150.1.13.13/29456 (150.1.13.13/29456) INSIDE:180.1.99.1/23 (180.1.99.1/23), flags UIOB, idle 1m25s, upti
!
!SW5#telnet 180.1.99.2 /source-interface Loopback0
Trying 180.1.99.2 ... Open
R2>
!
!ASA1/VLAN94# show conn long

1 in use, 2 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
TCP OUTSIDE:150.1.13.13/46707 (150.1.13.13/46707) INSIDE:180.1.99.2/23 (180.1.99.2/23), flags UIOB, idle 11s, uptime
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 4

CCIE SCv4 Lab 4 Solutions Section 2

1. Task 2.1 Solution
2. Task 2.2 Solution
3. Task 2.3 Solution
4. Task 2.4 Solution
5. Task 2.5 Solution
6. Task 2.6 Solution

Task 2.1 Solution

SW3:

```
interface GigabitEthernet1/0/10
 switchport mode access
 switchport access vlan 88
 no shutdown
```

R1:

```
ntp master
ntp trusted-key 1
ntp authentication-key 1 md5 ipskey
```

IPS:

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# host-name IPS4240
sensor(config-hos-net)# host-ip 172.16.6.99/24,172.16.6.1
sensor(config-hos-net)# access-list 172.16.6.0/24
sensor(config-hos-net)# telnet-option disabled
sensor(config-hos-net)# exit
sensor(config-hos)# ntp-option enabled
sensor(config-hos-ena)# ntp-servers 172.16.6.11 key-id 1
sensor(config-hos-ena)# ntp-keys 1 md5-key ipskey
sensor(config-hos-ena)# exit
```

https://t.me/learningnets

```
sensor(config-hos)# exit
Apply Changes?[yes]:
!
!
sensor(config)# service health-monitor
sensor(config-hea)# memory-usage-policy
sensor(config-hea-mem)# enable true
sensor(config-hea-mem)# yellow-threshold 70
sensor(config-hea-mem)# red-threshold 90
sensor(config-hea-mem)# exit
sensor(config-hea)# exit
Apply Changes?[yes]:
```

Task 2.1 Verification

Verify the configured host settings:

```
sensor(config-hos-net)# show settings

   network-settings
   ------------------------------------------------
host-ip: 172.16.6.99/24,172.16.6.1 default: 192.168.1.2/24,192.168.1.1
 host-name: IPS4240 default: sensor
 telnet-option: disabled default: disabled
 access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------ network-address: 172.16.6.0/24

        ------------------------------------------------
```

Verify current sensor health indicators:

```
sensor# show health

Overall Health Status                                 Red
Health Status for Failed Applications                 Green
Health Status for Signature Updates                   Red
Health Status for License Key Expiration              Red
Health Status for Running in Bypass Mode              Green
Health Status for Interfaces Being Down               Green
Health Status for the Inspection Load                 Green
Health Status for the Time Since Last Event Retrieval Red
Health Status for the Number of Missed Packets        Green
Health Status for the Memory Usage                    Yellow
```

https://t.me/learningnets

```
Health Status for Global Correlation                    Green
Health Status for Network Participation                 Not Enabled

Security Status for Virtual Sensor vs0   Green
```

Verify that IPS is NTP synchronized:

```
R1#show clock

18:31:41.825 UTC Mon Apr 7 2014
!
!sensor# show clock detail
 .18:31:43 UTC Mon Apr 07 2014
Time source is NTP
```

Task 2.2 Solution

```
SW1:
interface FastEthernet1/0/21
 switchport trunk allowed vlan remove 46
!
interface FastEthernet1/0/22
 switchport trunk allowed vlan remove 34

SW3:
interface GigabitEthernet1/0/8
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 34
 switchport trunk allowed vlan 34,46
 switchport mode trunk
 no shutdown
!
interface GigabitEthernet1/0/20
  switchport trunk allowed vlan remove 46

SW4:
interface GigabitEthernet1/0/9
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 34
 switchport trunk allowed vlan 34,46
 switchport mode trunk
 no shutdown
```

https://t.me/learningnets

```
!
interface GigabitEthernet1/0/20
  switchport trunk allowed vlan remove 34
```

IPS:

```
sensor(config)# service interface
sensor(config-int)# physical-interfaces gigabitEthernet0/0
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# default-vlan 34
sensor(config-int-phy)# exit
sensor(config-int)# physical-interfaces gigabitEthernet0/2
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# default-vlan 34
sensor(config-int-phy)# exit
sensor(config-int)# exit
Apply Changes?[yes]:
!
!
sensor(config)# service interface
sensor(config-int)# inline-interfaces IPS
sensor(config-int-inl)# interface1 gigabitEthernet0/0
sensor(config-int-inl)# interface2 gigabitEthernet0/2
sensor(config-int-inl)# subinterface-type vlan-group
sensor(config-int-inl-vla)# subinterface 1
sensor(config-int-inl-vla-sub)# vlans unassigned
sensor(config-int-inl-vla-sub)# exit
sensor(config-int-inl-vla)# subinterface 2
sensor(config-int-inl-vla-sub)# vlans range 46
sensor(config-int-inl-vla-sub)# exit
sensor(config-int-inl-vla)# exit
sensor(config-int-inl)# exit
sensor(config-int)# exit
Apply Changes?[yes]:
!
!
sensor# copy signature-definition sig0 sig1
sensor(config)# service analysis-engine
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)# logical-interface IPS subinterface-number 1
sensor(config-ana-vir)# exit
sensor(config-ana)# virtual-sensor vs1
sensor(config-ana-vir)# logical-interface IPS subinterface-number 2
sensor(config-ana-vir)# signature-definition sig1
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
```

https://t.me/learningnets

```
Apply Changes?[yes]:
!
!
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 2000 0
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# enabled true
sensor(config-sig-sig-sta)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes?[yes]:
!
!
sensor(config)# service signature-definition sig1
sensor(config-sig)# signatures 2004 0
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# enabled true
sensor(config-sig-sig-sta)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes?[yes]:
```

Task 2.2 Verification

Verify the trunking NATIVE VLAN configuration on switch ports facing the IPS:

```
SW3#show interfaces gigabitEthernet1/0/8 trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/8     on               802.1q         trunking      34

Port        Vlans allowed on trunk
Gi1/0/8     34,46

Port        Vlans allowed and active in management domain
Gi1/0/8     34,46

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/8     34,46
!
!SW4#show interfaces gigabitEthernet1/0/9 trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/9     on               802.1q         trunking      34
```

https://t.me/learningnets

```
Port        Vlans allowed on trunk
Gi1/0/9     34,46

Port        Vlans allowed and active in management domain
Gi1/0/9     34,46

Port        Vlans in spanning tree forwarding state and not pruned Gi1/0/9      34,46
```

Verify the IPS interface status:

https://t.me/learningnets

```
sensor# show interfaces brief

CC   Interface            Sensing State   Link   Inline Mode                                  Pair Status
GigabitEthernet0/0   Enabled          Up     Paired with interface GigabitEthernet0/2   Up

*    Management0/0        Disabled        Up
     GigabitEthernet0/1   Disabled        Down   Unpaired                                     N/A
GigabitEthernet0/2   Enabled          Up     Paired with interface GigabitEthernet0/0   Up

     GigabitEthernet0/3   Disabled        Down   Unpaired                                     N/A
!
!sensor(config-int-inl)# show settings

   name: IPS
   ------------------------------------------------
      description:  <defaulted> interface1: GigabitEthernet0/0
 interface2: GigabitEthernet0/2
 subinterface-type

      ------------------------------------------------ vlan-group

         ------------------------------------------------
            subinterface (min: 1, max: 255, current: 2)
            ------------------------------------------------ subinterface-number: 1

               ------------------------------------------------
                  description:  <defaulted> vlans

                  ------------------------------------------------ unassigned

                     ------------------------------------------------
                     ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------ subinterface-number: 2

               ------------------------------------------------
                  description:  <defaulted> vlans

                  ------------------------------------------------ range: 46
```

https://t.me/learningnets

Verify that the requested output is being matched for ICMP Echo Request in VLAN 34:

```
R4#ping 180.1.34.3 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 180.1.34.3, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 4/4/4 ms
!
!sensor# show events



evIdsAlert: eventId=1395322617431000231 severity=informational vendor=Cisco
  originator:
    hostId: IPS4240
    appName: sensorApp
    appInstanceId: 1202
  time: 2014/04/07 20:09:49 2014/04/07 20:09:49 UTC
  signature: description=ICMP Echo Request id=2004 created=20001127 type=other version=S666
    subsigId: 0
    sigDetails: ICMP Echo Request
  interfaceGroup: vs0
  vlan: 34
  participants:
    attacker:
      addr: locality=OUT 180.1.34.4
    target:
      addr: locality=OUT 180.1.34.3
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
  threatRatingValue: 35
  interface: ge0_2
  protocol: icmp
```

Verify that the requested output is being matched for ICMP Echo Request in VLAN 46:

```
ASA2#ping 180.1.46.6 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 180.1.46.6, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms
!
```

https://t.me/learningnets

```
!sensor# show events


evIdsAlert: eventId=1395322617431000232 severity=informational vendor=Cisco
  originator:
    hostId: IPS4240
    appName: sensorApp
    appInstanceId: 1202
  time: 2014/04/07 20:10:34 2014/04/07 20:10:34 UTC
  signature: description=ICMP Echo Request id=2004 created=20001127 type=other version=S666
    subsigId: 0
    sigDetails: ICMP Echo Request
  interfaceGroup: vs1
  vlan: 46
  participants:
    attacker:
      addr: locality=OUT 180.1.46.16
    target:
      addr: locality=OUT 180.1.46.6
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
  threatRatingValue: 35
  interface: ge0_2
  protocol: icmp
```

Task 2.3 Solution

IPS:

```
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 60005 0
sensor(config-sig-sig)# engine atomic-ip
sensor(config-sig-sig-ato)# specify-l4-protocol yes
sensor(config-sig-sig-ato-yes)# l4-protocol udp
sensor(config-sig-sig-ato-yes-udp)# specify-dst-port yes
sensor(config-sig-sig-ato-yes-udp-yes)# dst-port 1645,1812
sensor(config-sig-sig-ato-yes-udp-yes)# exit
sensor(config-sig-sig-ato-yes-udp)# exit
sensor(config-sig-sig-ato-yes)# exit
sensor(config-sig-sig-ato)# event-action produce-alert|request-snmp-trap
sensor(config-sig-sig-ato)# exit
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# enabled true
sensor(config-sig-sig-sta)# exit
```

https://t.me/learningnets

```
sensor(config-sig-sig)# event-counter
sensor(config-sig-sig-eve)# event-count-key xxBx
sensor(config-sig-sig-eve)# event-count 3
sensor(config-sig-sig-eve)# specify-alert-interval yes
sensor(config-sig-sig-eve-yes)# alert-interval 60
sensor(config-sig-sig-eve-yes)# exit
sensor(config-sig-sig-eve)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes?[yes]:
!
!
sensor(config)# service notification
sensor(config-not)# enable-notifications true
sensor(config-not)# trap-destinations 172.16.6.50
sensor(config-not-tra)# trap-community-name ipstraps
sensor(config-not-tra)# exit
sensor(config-not)# exit
Apply Changes?[yes]:
Warning: Reboot is required before the configuration change will take effect
Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [yes]:
```

Task 2.3 Verification

For testing, enable AAA on R4 and configure R3 as RADIUS server; test authentication to trigger the signature to fire:

```
R4:
aaa new-model
radius-server host 180.1.34.3 key cisco

R4#test aaa group radius cisco cisco legacy

Attempting authentication test to server-group radius using radius
No authoritative response from any server.
```

Verify the event store on IPS:

```
sensor# show events
```

https://t.me/learningnets

```
evIdsAlert: eventId=1395322617431000249 severity=medium vendor=Cisco alarmTraits=2147516416
  originator:
    hostId: IPS4240
    appName: sensorApp
    appInstanceId: 1202
  time: 2014/04/07 20:26:40 2014/04/07 20:26:40 UTC
  signature: description=My Sig id=60005 created=20000101 type=other version=custom
    subsigId: 0
    sigDetails: My Sig Info
  interfaceGroup: vs0
  vlan: 34
  participants:
    attacker:
      addr: locality=OUT 180.1.34.4
      port: 1645
    target:
      addr: locality=OUT 180.1.34.3
      port: 1645
      os: idSource=unknown relevance=relevant type=unknown actions:
snmpTrapRequested: true

  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 66
  threatRatingValue: 66
  interface: ge0_2
  protocol: udp
```

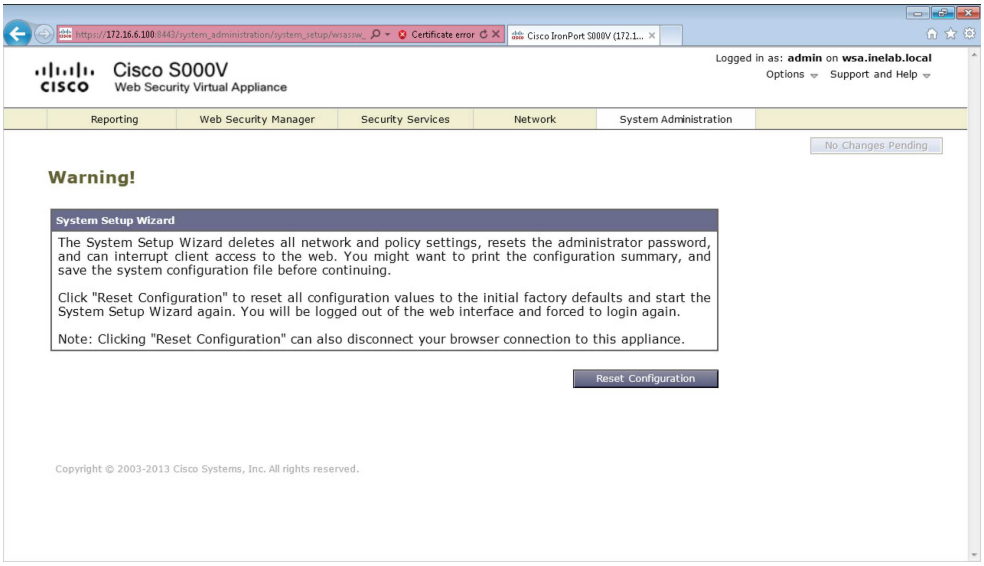
Task 2.4 Solution

```
SW6:

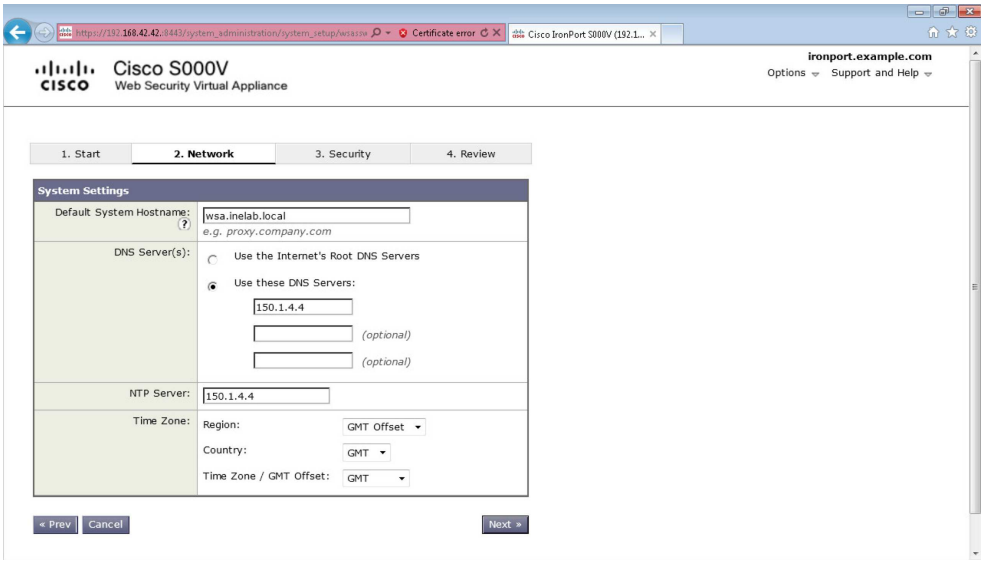
interface FastEthernet1/0/10
 switchport mode access
 switchport access vlan 88
 no shutdown
```

Using Internet Explorer from **TEST-PC-B**, navigate to **https://172.16.6.100:8443**, authenticate and browse to **System Administration -> System Setup Wizard**, and click **Reset Configuration**:

https://t.me/learningnets

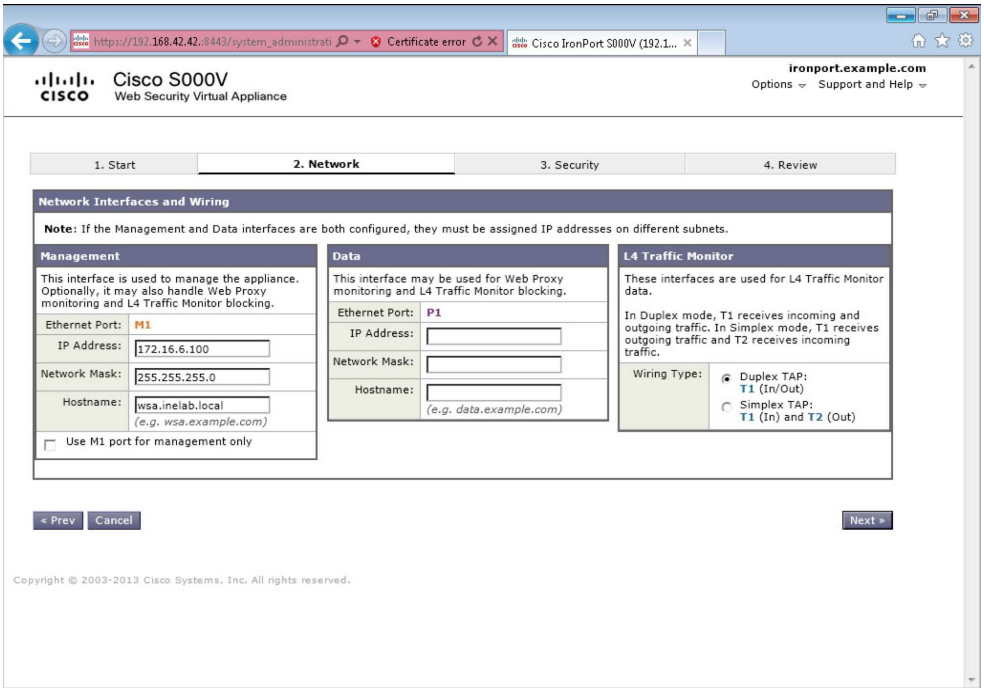


Configure **TEST-PC-B** with IPv4 address from subnet 192.168.42.0/24 , and use Internet Explorer to navigate to **https://192.168.42.42:8443**. Authenticate with the default credentials of **admin/ironport** and browse to **System Administration -> System Setup Wizard**. Configure hostname, DNS, and NTP server:

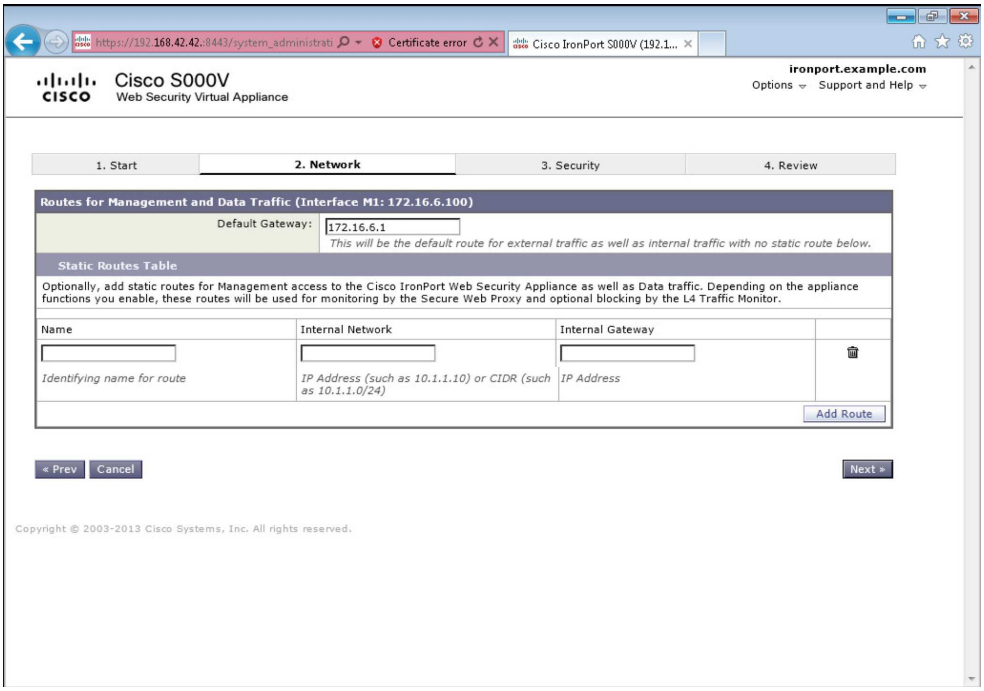


Configure the M1 interface for both proxy and management:

https://t.me/learningnets

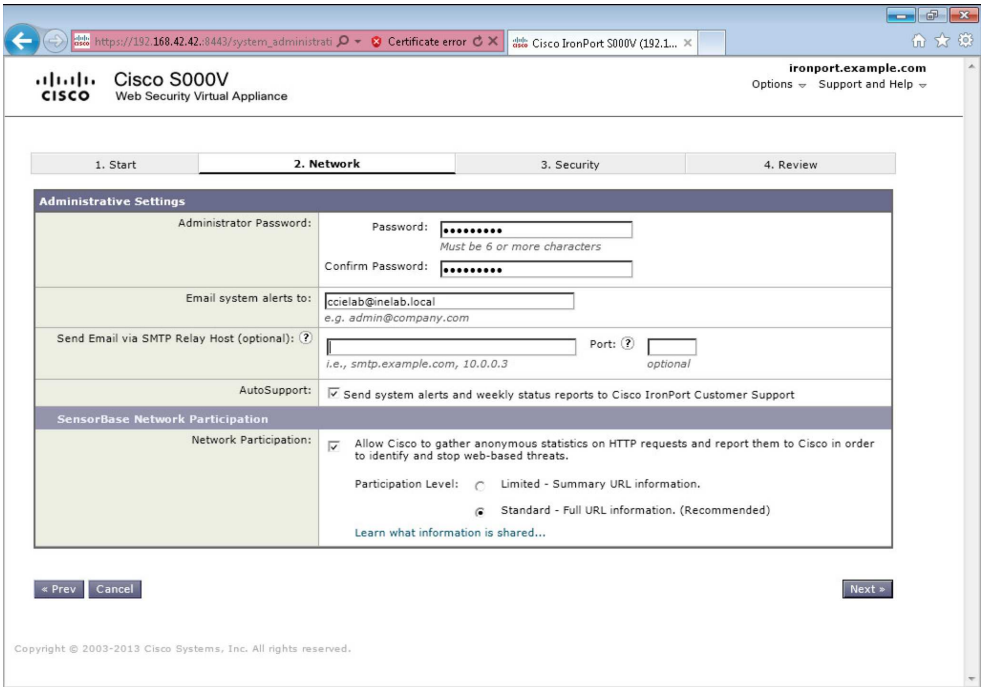


Configure the default gateway for M1 port:

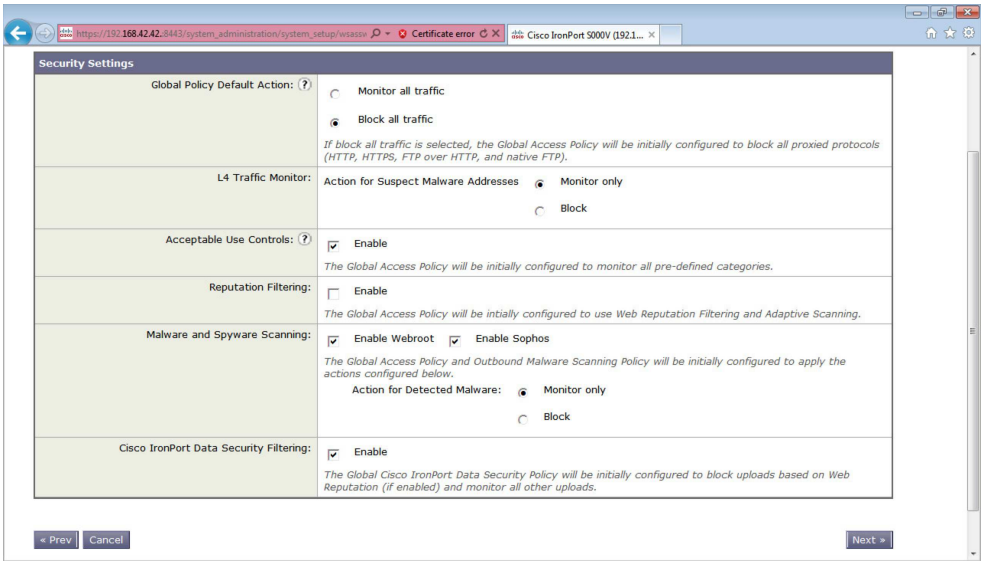


Configure the administrator password and email address:

https://t.me/learningnets



Block all protocols for the **Global Policy** and disable WBRS:

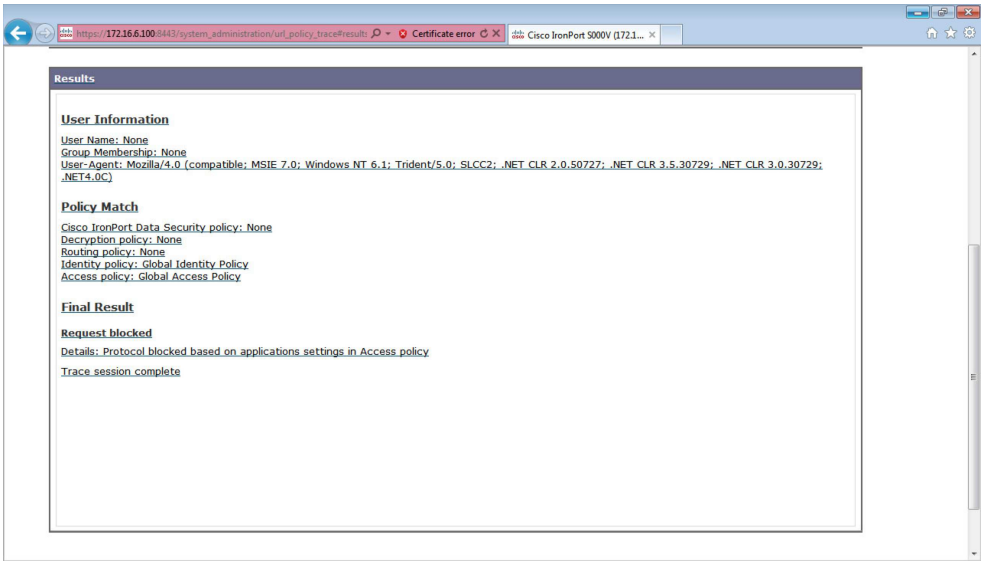


All other settings are left at their default values, so screens are missing from the complete **System Setup Wizard**.

Task 2.4 Verification

Use Internet Explorer to manage the WSA. Using the **Policy Trace** tool from **System Administration**, simulate a connection to an IPv4 address; the request will be blocked based on the configured settings for the **Global Policy**:

https://t.me/learningnets



Task 2.5 Solution

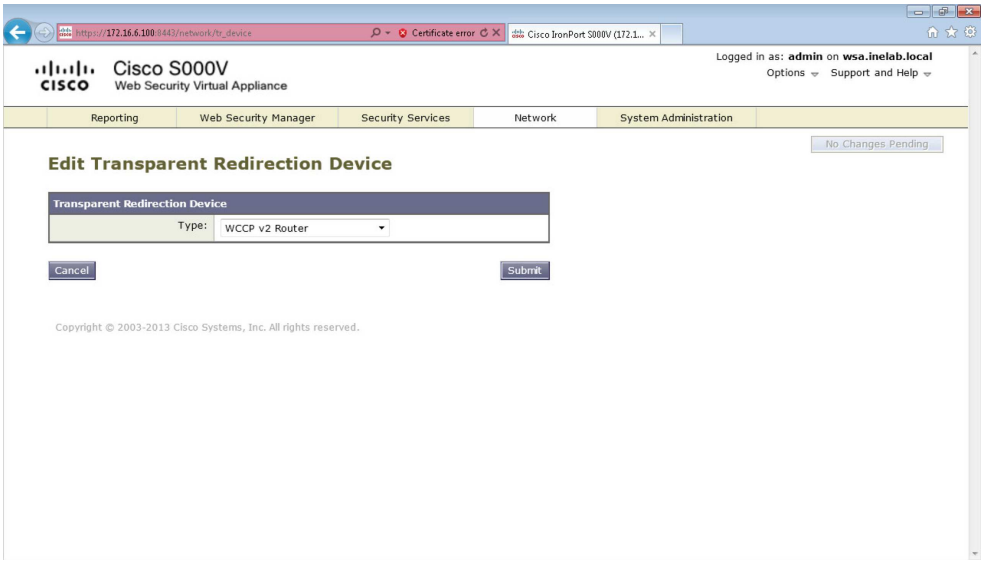
```
ASA1 VLAN94 Context:
route INSIDE 172.16.6.100 255.255.255.255 180.1.99.1
!
access-list REDIRECTED_TRAFFIC permit tcp any any eq 80
access-list WSA_GROUP extended permit ip host 172.16.6.100 any
!
wccp 94 redirect-list REDIRECTED_TRAFFIC group-list WSA_GROUP password wccpasa
wccp interface INSIDE 94 redirect in


ASA1 VLAN95 Context:

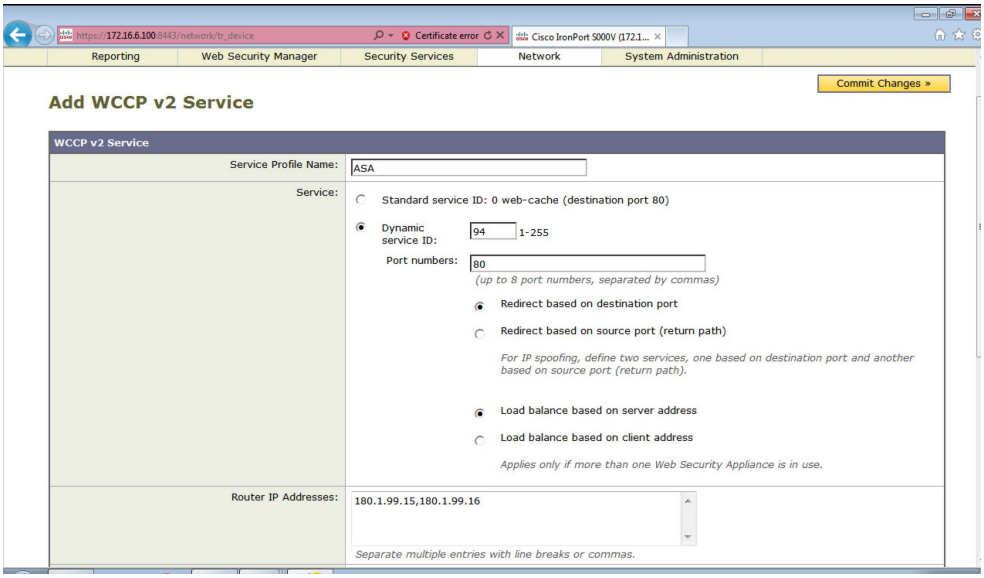
access-list REDIRECTED_TRAFFIC permit tcp any any eq 80
access-list WSA_GROUP extended permit ip host 172.16.6.100 any
!
wccp 94 redirect-list REDIRECTED_TRAFFIC group-list WSA_GROUP password wccpasa
wccp interface INSIDE 94 redirect in
```

Browse to **Network -> Transparent Redirection** and select **WCCP v2 Router**:

https://t.me/learningnets

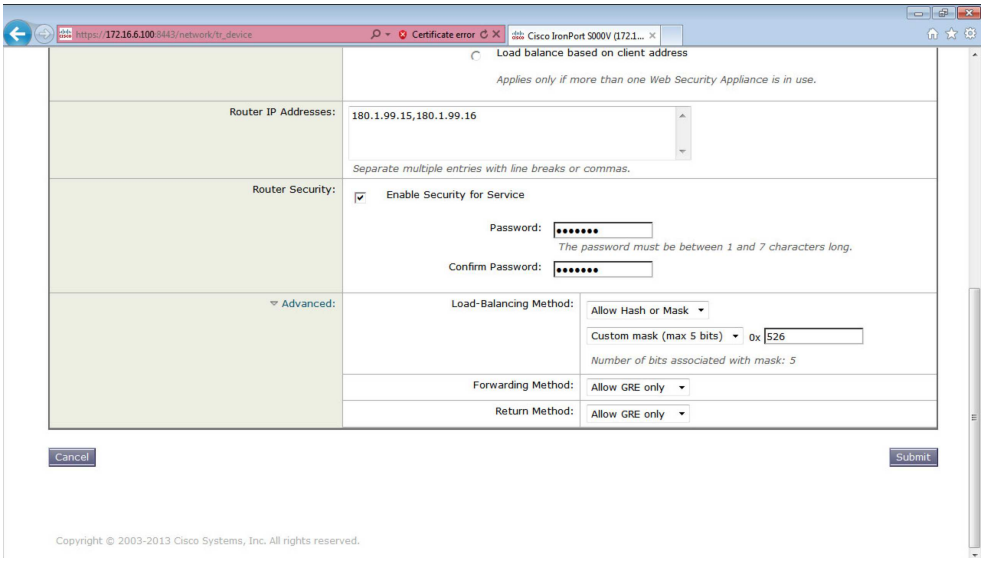


Click **Add Service**, configure the same service-id as on the ASA contexts, and enable it only for HTTP traffic:



Enable the service for GRE; otherwise WSA will try L2, fail, and not negotiate GRE. Also enable authentication:

https://t.me/learningnets



Task 2.5 Verification

Verify that the requested output is matched on both ASA1 contexts:

```
ASA1/VLAN95# show wccp


Global WCCP information:
    Router information:
        Router Identifier:                  180.1.99.15
        Protocol Version:                   2.0

    Service Identifier: 94
        Number of Cache Engines:            1
        Number of routers:                  2
        Total Packets Redirected:           0
        Redirect access-list:               REDIRECTED_TRAFFIC
        Total Connections Denied Redirect:  0
        Total Packets Unassigned:           0
        Group access-list:                  WSA_GROUP
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0
!
!ASA1/VLAN94# show wccp


Global WCCP information:
    Router information:
        Router Identifier:                  180.1.99.16
        Protocol Version:                   2.0
```

https://t.me/learningnets

```
    Service Identifier: 94
        Number of Cache Engines:             1
        Number of routers:                   2
        Total Packets Redirected:            0
        Redirect access-list:                REDIRECTED_TRAFFIC
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   WSA_GROUP
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
```

Verify that the WCCP client and WCCP servers have established communication:

```
ASA1/VLAN94# show wccp 94 detail


WCCP Cache-Engine information:
        Web Cache ID:          172.16.6.100
        Protocol Version:      2.0 State:                  Usable
        Initial Hash Info:     00000000000000000000000000000000
                               00000000000000000000000000000000
        Assigned Hash Info:    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                               FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Hash Allotment:        256 (100.00%)
        Packets Redirected:    0 Connect Time:          00:14:07
!
!ASA1/VLAN95# show wccp 94 detail


WCCP Cache-Engine information:
        Web Cache ID:          172.16.6.100
        Protocol Version:      2.0 State:                  Usable
        Initial Hash Info:     00000000000000000000000000000000
                               00000000000000000000000000000000
        Assigned Hash Info:    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                               FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Hash Allotment:        256 (100.00%)
        Packets Redirected:    0 Connect Time:          00:18:15
```

Verify at the CBAC level that sessions appear in the firewall state table:

https://t.me/learningnets

```
R1#show ip inspect ha sessions detail

Sess_ID    (src_addr:port)=>(dst_addr:port)   proto sess_state   ha_stateEstablished Sessions
2CDBEED0 (172.16.6.100:02048)=>(180.1.99.15:02048) udp   SIS_OPEN     HA_ACTIVE
  Created 00:19:27, Last heard 00:00:08
  Bytes sent (initiator:responder) [17428:18580]
In  SID 180.1.99.15[2048:2048]=>172.16.6.100[2048:2048] on ACL VLAN99_INBOUND  (117 matches)
 HA state: HA_ACTIVE
2CDC0010 (172.16.6.100:02048)=>(180.1.99.16:02048) udp   SIS_OPEN     HA_ACTIVE
  Created 00:19:27, Last heard 00:00:08
  Bytes sent (initiator:responder) [18072:15656]
In  SID 180.1.99.16[2048:2048]=>172.16.6.100[2048:2048] on ACL VLAN99_INBOUND  (99 matches)
 HA state: HA_ACTIVE
!
!R2#show ip inspect ha sessions detail

Sess_ID    (src_addr:port)=>(dst_addr:port)   proto sess_state   ha_stateEstablished Sessions
2D1758C4 (172.16.6.100:02048)=>(180.1.99.15:02048) udp   SIS_OPEN     HA_STANDBY
  Created 00:20:11, Last heard never
  Bytes sent (initiator:responder) [0:0]
In  SID 180.1.99.15[2048:2048]=>172.16.6.100[2048:2048] on ACL VLAN99_INBOUND
 HA state: HA_STANDBY
2D175F3C (172.16.6.100:02048)=>(180.1.99.16:02048) udp   SIS_OPEN     HA_STANDBY
  Created 00:16:32, Last heard never
  Bytes sent (initiator:responder) [0:0]
In  SID 180.1.99.16[2048:2048]=>172.16.6.100[2048:2048] on ACL VLAN99_INBOUND
 HA state: HA_STANDBY
```

Task 2.6 Solution

```
R1:
ip access-list extended VLAN99_INBOUND
 1 permit gre host 180.1.99.15 host 172.16.6.100
 2 permit gre host 180.1.99.16 host 172.16.6.100
!
ip access-list resequence VLAN99_INBOUND 10 10

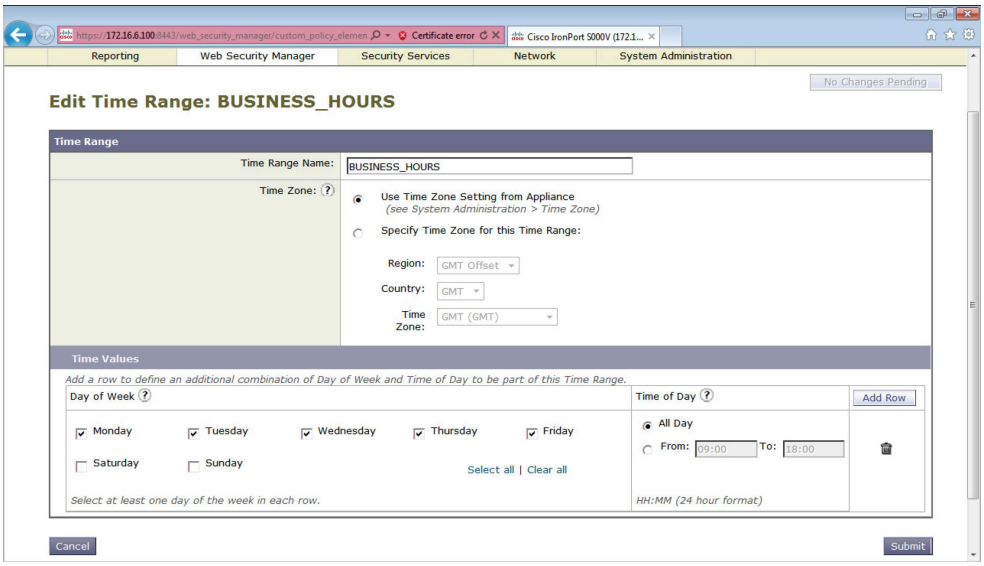
R2:

ip access-list extended VLAN99_INBOUND
 1 permit gre host 180.1.99.15 host 172.16.6.100
 2 permit gre host 180.1.99.16 host 172.16.6.100
!
```

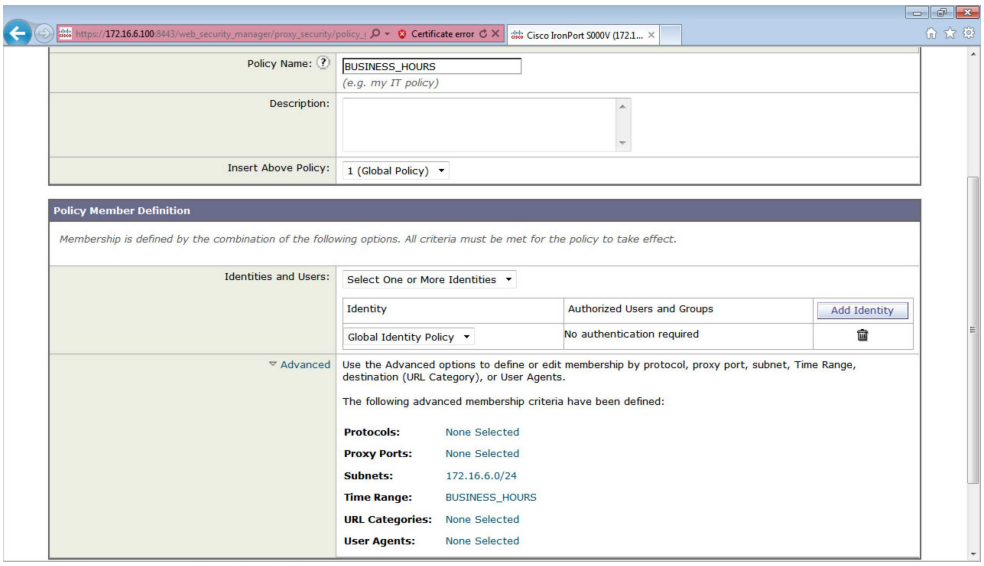
https://t.me/learningnets

```
ip access-list resequence VLAN99_INBOUND 10 10
```

Use Internet Explorer to navigate to **Web Security Manager -> Defined Time Ranges**, click **Add Time Range**, and configure it according to the task requirements:

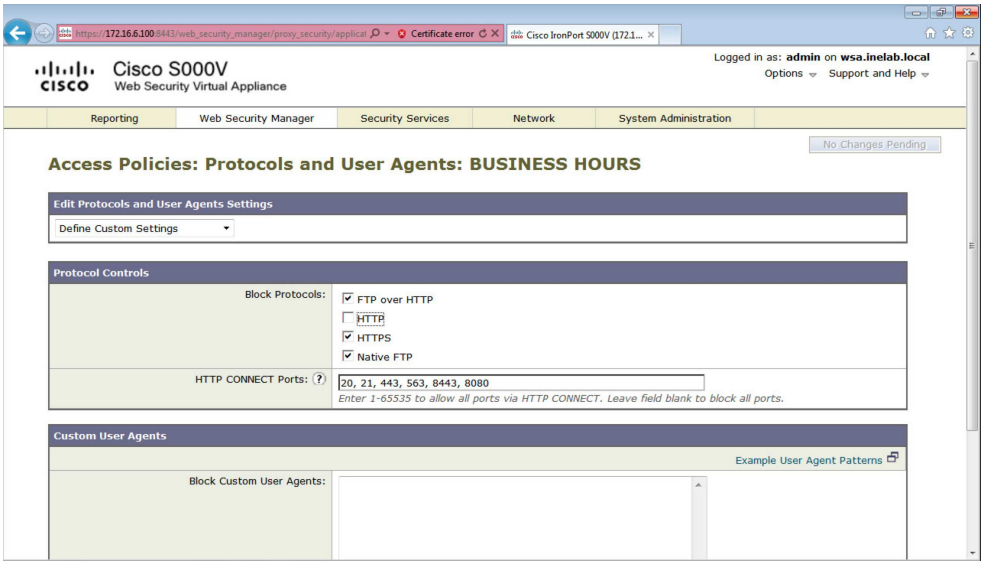


Navigate to **Web Security Manager -> Access Policies**, click **Add Policy**, and configure it according to the requirements; match on the **Global Identity Policy**, and specify the subnet and defined time-range:

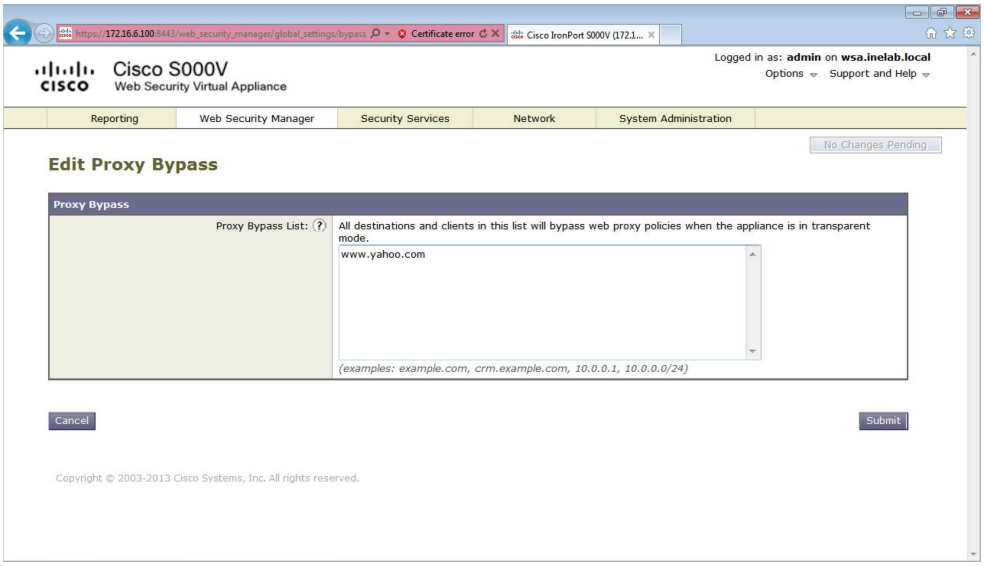


Edit the **Protocols and User Agents** settings for the configured Access Policy, and unblock HTTP access:

https://t.me/learningnets



Navigate to **Web Security Manager -> Bypass Settings -> Edit Proxy Bypass Settings** and add **www.yahoo.com**.



Task 2.6 Verification

Configure **TEST-PC-B** with a IPv4 address of 172.16.6.50 and use Internet Explorer to access **www.yahoo.com**. Because the proxy bypass list is being configured, the following log messages will be visible in WSA **bypasslogs**:

```
Tue Apr  8 12:01:27 2014 Info: Connection from 172.16.6.50:19146 to 150.1.4.4:80 bypassed
Tue Apr  8 12:01:27 2014 Info: Connection from 172.16.6.50:19147 to 150.1.4.4:80 bypassed
```

https://t.me/learningnets

Confirm that the requested output is being matched:

```
SW5#show ip http server history


HTTP server history:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes  end-time
    150.1.13.13:80       172.16.6.100:47341 477        192        08:03:29 03/02
```

Use Internet Explorer to access **www.google.com**. The following log messages will be visible on WSA **accesslogs**, confirming that the session is proxied by WSA:

```
1396959609.553 15
172.16.6.50 TCP_MISS/401 253 GET http://www.google.com/ - DIRECT/www.google.com text/plain DEFAULT_CASE_12-BUSINESS_
-NONE-NONE-NONE-DefaultGroup <IW_srch,-,0,"-",0,0,0,1,"-",-,-,-,"-",1,-,"-","-",-,-,IW_srch,-,"-","-","Google","Sear
```

Confirm that the requested output is being matched:

```
R4#show ip http server history


HTTP server history:
local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes  end-time
      150.1.4.4:80        172.16.6.50:19454 397        192        12:39:12 04/08
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 4

CCIE SCv4 Lab 4 Solutions Section 3

1. Task 3.1 Solution
2. Task 3.2 Solution
3. Task 3.3 Solution
4. Task 3.4 Solution
5. Task 3.5 Solution

Task 3.1 Solution

R1:

```
ip access-list extended VLAN99_INBOUND
 1 permit udp host 150.1.3.3 host 150.1.1.1 eq 500
 2 permit esp host 150.1.3.3 host 150.1.1.1
 3 permit udp host 150.1.6.6 host 150.1.1.1 eq 500
 4 permit esp host 150.1.6.6 host 150.1.1.1
!
ip access-list resequence VLAN99_INBOUND 10 10
!
crypto isakmp policy 200
 authentication pre-share
 encryption 3des
 hash md5
 group 2
!
crypto isakmp key DMVPN address 150.1.3.3
crypto isakmp key DMVPN address 150.1.6.6
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
crypto ipsec profile DMVPN
 set transform-set 3DES_MD5
!
interface Tunnel1236
 ip address 11.11.11.1 255.255.255.0
 tunnel source Loopback0
```

https://t.me/learningnets

```
 tunnel mode gre multipoint
 no ip split-horizon eigrp 1236
 ip nhrp redirect
 ip nhrp network-id 1236
 ip nhrp map multicast dynamic
 tunnel protection ipsec profile DMVPN
!
router eigrp 1236
 no auto-summary
 network 11.11.11.0 0.0.0.255
 network 172.16.6.0 0.0.0.255
```

R2:

```
ip access-list extended VLAN99_INBOUND
 1 permit udp host 150.1.4.4 host 150.1.2.2 eq 500
 2 permit esp host 150.1.4.4 host 150.1.2.2
 3 permit udp host 150.1.6.6 host 150.1.2.2 eq 500
 4 permit esp host 150.1.6.6 host 150.1.2.2
!
ip access-list resequence VLAN99_INBOUND 10 10
!
crypto isakmp policy 200
 authentication pre-share
 encryption 3des
 hash md5
 group 2
!
crypto isakmp key DMVPN address 150.1.3.3
crypto isakmp key DMVPN address 150.1.6.6
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
crypto ipsec profile DMVPN_PROFILE
 set transform-set 3DES_MD5
!
interface Tunnel1236
 ip address 11.11.11.2 255.255.255.0
 tunnel source Loopback0
 tunnel mode gre multipoint
 no ip split-horizon eigrp 1236
 ip nhrp redirect
 ip nhrp network-id 1236
 ip nhrp map multicast dynamic
 tunnel protection ipsec profile DMVPN_PROFILE
!
router eigrp 1236
```

https://t.me/learningnets

```
 no auto-summary
 network 11.11.11.0 0.0.0.255
 network 172.16.6.0 0.0.0.255
```

R3:

```
crypto isakmp policy 200
 authentication pre-share
 encryption 3des
 hash md5
 group 2
!
crypto keyring DMVPN_KEYRING vrf LAB4
 pre-shared-key address 150.1.1.1 key DMVPN
 pre-shared-key address 150.1.2.2 key DMVPN
 pre-shared-key address 150.1.6.6 key DMVPN
!
crypto isakmp profile DMVPN_ISAKMP
 keyring DMVPN_KEYRING
 match identity address 150.1.1.1 255.255.255.255 LAB4
 match identity address 150.1.2.2 255.255.255.255 LAB4
 match identity address 150.1.6.6 255.255.255.255 LAB4
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
crypto ipsec profile DMVPN_PROFILE
 set transform-set 3DES_MD5
 set isakmp-profile DMVPN_ISAKMP
!
interface Tunnel1236
 ip address 11.11.11.3 255.255.255.0
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel vrf LAB4
 if-state nhrp
 ip nhrp shortcut
 ip nhrp network-id 1236
 ip nhrp nhs 11.11.11.1 nbma 150.1.1.1 multicast priority 10 cluster 1
 ip nhrp nhs 11.11.11.2 nbma 150.1.2.2 multicast priority 20 cluster 1
 ip nhrp nhs cluster 1 max-connections 1
 tunnel protection ipsec profile DMVPN_PROFILE
!
router eigrp 1236
 no auto-summary
 network 11.11.11.0 0.0.0.255
 network 180.1.3.0 0.0.0.255
```

https://t.me/learningnets

R6:

```
crypto isakmp policy 200
 authentication pre-share
 encryption 3des
 hash md5
 group 2
!
crypto keyring DMVPN_KEYRING vrf LAB4
 pre-shared-key address 150.1.1.1 key DMVPN
 pre-shared-key address 150.1.2.2 key DMVPN
 pre-shared-key address 150.1.3.3 key DMVPN
!
crypto isakmp profile DMVPN_ISAKMP
 keyring DMVPN_KEYRING
 match identity address 150.1.1.1 255.255.255.255 LAB4
 match identity address 150.1.2.2 255.255.255.255 LAB4
 match identity address 150.1.3.3 255.255.255.255 LAB4
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
crypto ipsec profile DMVPN_PROFILE
 set transform-set 3DES_MD5
 set isakmp-profile DMVPN_ISAKMP
!
interface Tunnel1236
 ip address 11.11.11.6 255.255.255.0
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel vrf LAB4
 if-state nhrp
 ip nhrp shortcut
 ip nhrp network-id 1236
 ip nhrp nhs 11.11.11.1 nbma 150.1.1.1 multicast priority 10 cluster 1
 ip nhrp nhs 11.11.11.2 nbma 150.1.2.2 multicast priority 20 cluster 1
 ip nhrp nhs cluster 1 max-connections 1
 tunnel protection ipsec profile DMVPN_PROFILE
!
router eigrp 1236
 no auto-summary
 network 11.11.11.0 0.0.0.255
 network 172.16.5.0 0.0.0.255
```

ASA1 VLAN94 Context:

```
access-list OUTSIDE_IN permit udp host 150.1.3.3 host 150.1.1.1 eq 500
access-list OUTSIDE_IN permit udp host 150.1.3.3 host 150.1.2.2 eq 500
```

https://t.me/learningnets

```
access-list OUTSIDE_IN permit udp host 150.1.6.6 host 150.1.1.1 eq 500
access-list OUTSIDE_IN permit udp host 150.1.6.6 host 150.1.2.2 eq 500
!
route INSIDE 150.1.1.1 255.255.255.255 180.1.99.1
route INSIDE 150.1.2.2 255.255.255.255 180.1.99.2
!
policy-map global_policy
 class inspection_default
  inspect ipsec-pass-thru
```

ASA1 VLAN95 Context:

```
policy-map global_policy
 class inspection_default
  inspect ipsec-pass-thru
```

ASA2:

```
access-list DMZ_IN permit udp host 150.1.3.3 host 150.1.1.1 eq 500
access-list DMZ_IN permit udp host 150.1.3.3 host 150.1.2.2 eq 500
access-list DMZ_IN permit udp host 150.1.3.3 host 150.1.6.6 eq 500
!
access-list OUTSIDE_IN permit udp host 150.1.6.6 host 150.1.1.1 eq 500
access-list OUTSIDE_IN permit udp host 150.1.6.6 host 150.1.2.2 eq 500
access-list OUTSIDE_IN permit udp host 150.1.6.6 host 150.1.3.3 eq 500
!
access-group OUTSIDE_IN in interface OUTSIDE
!
policy-map global_policy
 class inspection_default
  inspect ipsec-pass-thru
```

ASA3:

```
access-list VLAN75_IN permit udp host 150.1.3.3 host 150.1.1.1 eq 500
access-list VLAN75_IN permit udp host 150.1.3.3 host 150.1.2.2 eq 500
access-list VLAN75_IN permit udp host 150.1.3.3 host 150.1.6.6 eq 500
!
policy-map global_policy
 class inspection_default
  inspect ipsec-pass-thru
```

Task 3.1 Verification

Verify that the requested output is matched, so both spoke-to-hub and spoke-to-spoke tunnels have been negotiated successfully; spoke-to-spoke was automatically

https://t.me/learningnets

triggered by the LAP registering with the WLC:

```
R3#show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface Tunnel1236 is up/up, Addr. is 11.11.11.3, VRF ""
   Tunnel Src./Dest. addr: 150.1.3.3/MGRE, Tunnel VRF "LAB4"
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN_PROFILE"
   Interface State Control: Disabled

IPv4 NHS:
11.11.11.1  RE NBMA Address: 150.1.1.1 priority = 10 cluster = 1
11.11.11.2  W NBMA Address: 150.1.2.2 priority = 20 cluster = 1
Type:Spoke, Total NBMA Peers (v4/v6): 4

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      150.1.1.1      11.11.11.1    UP 00:02:35    S      11.11.11.1/32

    1      150.1.2.2      11.11.11.2  NHRP 01:37:24   SX      11.11.11.2/32

    2      150.1.6.6      11.11.11.6    UP 00:02:00    D      11.11.11.6/32
    0      150.1.6.6      11.11.11.6    UP 00:02:00    D      172.16.5.0/24

    1      150.1.3.3      11.11.11.3    UP 00:02:00  DLX       180.1.3.0/24
!
!R6#show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface Tunnel1236 is up/up, Addr. is 11.11.11.6, VRF ""
   Tunnel Src./Dest. addr: 150.1.6.6/MGRE, Tunnel VRF "LAB4"
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN_PROFILE"
   Interface State Control: Enabled
```

https://t.me/learningnets

```
IPv4 NHS:
11.11.11.1  RE NBMA Address: 150.1.1.1 priority = 10 cluster = 1
11.11.11.2  W NBMA Address: 150.1.2.2 priority = 20 cluster = 1
Type:Spoke, Total NBMA Peers (v4/v6): 4

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      150.1.1.1      11.11.11.1    UP 00:02:45    S      11.11.11.1/32

    1      150.1.2.2      11.11.11.2  NHRP 01:37:34   SX      11.11.11.2/32

    2      150.1.3.3      11.11.11.3    UP 00:02:17    D      11.11.11.3/32
    0      150.1.3.3      11.11.11.3    UP 00:02:17    D       180.1.3.0/24

    1      150.1.6.6      11.11.11.6    UP 00:02:17  DLX      172.16.5.0/24
```

Because of the NHS clustering configuration, NHRP registration was performed only with the hub with the highest priority:

```
R6#show ip eigrp 1236 neighbors

EIGRP-IPv4 Neighbors for AS(1236)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   11.11.11.1              Tu1236            14 03:13:09   10  1434  0  7
!
!R6#show ip route eigrp 1236
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D        172.16.6.0/24 [90/26882560] via 11.11.11.1, 00:04:11, Tunnel1236
      180.1.0.0/24 is subnetted, 1 subnets
D        180.1.3.0 [90/28162560] via 11.11.11.1, 03:12:03, Tunnel1236
!
!R6#show crypto isakmp sa
```

https://t.me/learningnets

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
150.1.1.1       150.1.6.6       QM_IDLE           1013 ACTIVE
150.1.3.3       150.1.6.6       QM_IDLE           1014 ACTIVE

IPv6 Crypto ISAKMP SA
```

Verify the same on the other spoke:

```
R3#show ip eigrp 1236 neighbors

EIGRP-IPv4 Neighbors for AS(1236)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   11.11.11.1              Tu1236            14 00:06:29     4  1434  0  6
!
!R3#show ip route eigrp 1236
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 1 subnets
D        172.16.5.0 [90/28162560] via 11.11.11.1, 00:06:20, Tunnel1236
D        172.16.6.0 [90/26882560] via 11.11.11.1, 00:06:35, Tunnel1236
!
!R3#show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
150.1.3.3       150.1.6.6       QM_IDLE           1009 ACTIVE
150.1.1.1       150.1.3.3       QM_IDLE           1008 ACTIVE


IPv6 Crypto ISAKMP SA
```

Verify that requested algorithms have been used and negotiated, for example on R3:

https://t.me/learningnets

```
R3#show crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
1009  150.1.3.3       150.1.6.6               ACTIVE 3des md5  psk  2  23:50:39
       Engine-id:Conn-id =  SW:9
1008  150.1.3.3       150.1.1.1               ACTIVE 3des md5  psk  2  23:50:03

       Engine-id:Conn-id =  SW:8

IPv6 Crypto ISAKMP SA
!
!R3#show crypto ipsec sa | i transform

        transform: esp-3des esp-md5-hmac ,
        transform: esp-3des esp-md5-hmac ,
        transform: esp-3des esp-md5-hmac ,
        transform: esp-3des esp-md5-hmac ,
```

Verify that ESP is statefully inspected by ASA firewalls, for example on ASA3:

```
ASA34/pri/act# show service-policy inspect ipsec-pass-thru table


Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
Inspect: ipsec-pass-thru _default_ipsec_passthru_map, packet 225, lock fail 0, drop 0, reset-drop 0
```

Verify that packets flow successfully through the IPsec tunnel:

```
R3#ping 11.11.11.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!
```

https://t.me/learningnets

```
!R3#ping 11.11.11.6


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.6, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
!
!R6#ping 11.11.11.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
!
!R6#ping 11.11.11.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.3, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

Task 3.2 Solution

```
ASA1 VLAN95 Context:
access-list OUTSIDE_IN permit udp host 180.1.55.5 host 172.16.6.1 eq 500
!
access-group OUTSIDE_IN in interface OUTSIDE

R1:
ip access-list extended VLAN99_INBOUND
 1 permit udp host 180.1.55.5 host 172.16.6.1 eq 500
 2 permit esp host 180.1.55.5 host 172.16.6.1
!
ip access-list resequence VLAN99_INBOUND 10 10
!
crypto keyring SVTI_KEYRING
 pre-shared-key address 180.1.55.5 255.255.255.255 key SVTI
!
crypto isakmp profile SVTI_ISAKMP
 keyring SVTI_KEYRING
 match identity address 180.1.55.5 255.255.255.255
!
crypto ipsec profile SVTI_PROFILE
 set transform-set 3DES_MD5
 set isakmp-profile SVTI_ISAKMP
```

https://t.me/learningnets

```
 responder-only
 redundancy CBAC_HA stateful
!
interface Tunnel125
 ip address 21.21.21.1 255.255.255.0
 tunnel source 172.16.6.1
 tunnel destination 180.1.55.5
 tunnel mode gre ip
 tunnel protection ipsec profile SVTI_PROFILE
```

R2:

```
ip access-list extended VLAN99_INBOUND
 1 permit udp host 180.1.55.5 host 172.16.6.1 eq 500
 2 permit esp host 180.1.55.5 host 172.16.6.1
!
ip access-list resequence VLAN99_INBOUND 10 10
!
crypto keyring SVTI_KEYRING
 pre-shared-key address 180.1.55.5 255.255.255.255 key SVTI
!
crypto isakmp profile SVTI_ISAKMP
 keyring SVTI_KEYRING
 match identity address 180.1.55.5 255.255.255.255
!
crypto ipsec profile SVTI_PROFILE
 set transform-set 3DES_MD5
 set isakmp-profile SVTI_ISAKMP
 responder-only
 redundancy CBAC_HA stateful
!
interface Tunnel125
 ip address 21.21.21.2 255.255.255.0
 tunnel source 172.16.6.1
 tunnel destination 180.1.55.5
 tunnel mode gre ip
 tunnel protection ipsec profile SVTI_PROFILE
```

R5:

```
crypto isakmp policy 200
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
```

https://t.me/learningnets

```
!
crypto keyring SVTI_KEYRING
 pre-shared-key address 172.16.6.1 255.255.255.255 key SVTI
!
crypto isakmp profile SVTI_ISAKMP
 keyring SVTI_KEYRING
 match identity address 172.16.6.1 255.255.255.255
!
crypto ipsec profile SVTI_PROFILE
 set transform-set 3DES_MD5
 set isakmp-profile SVTI_ISAKMP
!
interface Tunnel125
 ip address 21.21.21.5 255.255.255.0
 tunnel source 180.1.55.5
 tunnel destination 172.16.6.1
 tunnel mode gre ip
 tunnel protection ipsec profile SVTI_PROFILE
```

Task 3.2 Verification

Verify that the requested output is being matched:

https://t.me/learningnets

```
R1#show crypto session remote 180.1.55.5

Crypto session current status

Interface: Tunnel125
Profile: SVTI_ISAKMP
Session status: UP-ACTIVE
Peer: 180.1.55.5 port 500
  IKEv1 SA: local 172.16.6.1/500 remote 180.1.55.5/500 Active
  IPSEC FLOW: permit 47 host 172.16.6.1 host 180.1.55.5
        Active SAs: 2, origin: crypto map
!
!R2#show crypto session remote 180.1.55.5

Crypto session current status

Interface: Tunnel125
Profile: SVTI_ISAKMP
Session status: UP-STANDBY
Peer: 180.1.55.5 port 500
  IKEv1 SA: local 172.16.6.1/500 remote 180.1.55.5/500 Active
  IPSEC FLOW: permit 47 host 172.16.6.1 host 180.1.55.5
        Active SAs: 2, origin: crypto map
```

Verify that High Availability is enabled for the IPsec configuration:

```
R1#show crypto ha
 IKE VIP: 172.16.6.1
  stamp: FF B6 5A C2 CC 93 58 8F 46 83 9F 0D FE 75 68 76 IPSec VIP: 172.16.6.1
!
!R2#show crypto ha
 IKE VIP: 172.16.6.1
  stamp: FF B6 5A C2 CC 93 58 8F 46 83 9F 0D FE 75 68 76 IPSec VIP: 172.16.6.1
```

Verify that packets flow successfully through the IPsec tunnel, and that the required algorithms have been negotiated:

```
R1#ping 21.21.21.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 21.21.21.5, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
!
```

https://t.me/learningnets

```
!R5#ping 21.21.21.1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 21.21.21.1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
!
!R5#show crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
1002  180.1.55.5      172.16.6.1               ACTIVE 3des md5  psk  2  23:57:19

       Engine-id:Conn-id =  SW:2

IPv6 Crypto ISAKMP SA
!
!R5#show crypto ipsec sa peer 172.16.6.1

interface: Tunnel125
    Crypto map tag: Tunnel125-head-0, local addr 180.1.55.5

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (180.1.55.5/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.6.1/255.255.255.255/47/0)
   current_peer 172.16.6.1 port 500
     PERMIT, flags={origin_is_acl,} #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 180.1.55.5, remote crypto endpt.: 172.16.6.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0xA399C2C1(2744763073)
     PFS (Y/N): N, DH group: none
inbound esp sas:
      spi: 0x954590C7(2504364231) transform: esp-3des esp-md5-hmac ,
```

https://t.me/learningnets

```
        in use settings ={Tunnel, }
        conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: Tunnel125-head-0
        sa timing: remaining key lifetime (k/sec): (4527301/3505)
        IV size: 8 bytes
        replay detection support: Y Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:
 outbound esp sas:
      spi: 0xA399C2C1(2744763073) transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: Tunnel125-head-0
        sa timing: remaining key lifetime (k/sec): (4527301/3505)
        IV size: 8 bytes
        replay detection support: Y Status: ACTIVE


     outbound ah sas:

     outbound pcp sas:
```

Task 3.3 Solution

```
ASA3:
access-list VLAN75_IN permit udp host 180.1.45.4 host 180.1.55.5

R4:
crypto isakmp policy 100
 authentication pre-share
!
ip access-list extended LOOPBACK
 permit ip host 150.1.4.4 host 150.1.5.5
 no permit ip host 150.1.5.5 host 150.1.4.4

SW3:

no vlan access-map VACL 10
```

Task 3.3 Verification

Generate interesting traffic and verify that packets flow successfully through the

https://t.me/learningnets

IPsec tunnel:

```
R4#ping 150.1.5.5 source loopback0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.5.5, timeout is 2 seconds:
Packet sent with a source address of 150.1.4.4

%CRYPTO-6-IPSEC_USING_DEFAULT: IPSec is using default transforms.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/4 ms
!
!R4#show crypto ipsec sa peer 180.1.55.5

interface: FastEthernet0/0
    Crypto map tag: VPN, local addr 180.1.45.4

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (150.1.4.4/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (150.1.5.5/255.255.255.255/0/0)
   current_peer 180.1.55.5 port 500
     PERMIT, flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 180.1.45.4, remote crypto endpt.: 180.1.55.5
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x5D9CA1B4(1570546100)
     PFS (Y/N): N, DH group: none
 inbound esp sas:
      spi: 0xF966F646(4184274502)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5, flow_id: AIM-VPN/EPII-PLUS:5, sibling_flags 80000046, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4388478/3577)
        IV size: 16 bytes
        replay detection support: Y Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:
 outbound esp sas:
```

https://t.me/learningnets

```
      spi: 0x5D9CA1B4(1570546100)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 6, flow_id: AIM-VPN/EPII-PLUS:6, sibling_flags 80000046, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4388478/3577)
        IV size: 16 bytes
        replay detection support: Y Status: ACTIVE


     outbound ah sas:

     outbound pcp sas:
```

Task 3.4 Solution

ASA3:

```
crypto ikev1 enable VLAN75
crypto ikev1 policy 100
 authentication pre-share
 encryption 3des
 hash md5
 group 2
!
ip local pool EZVPN_SERVER 180.1.200.1-180.1.200.254
!
access-list SPLIT_TUNNEL standard permit 172.16.1.0 255.255.255.0
access-list SPLIT_TUNNEL standard permit 172.16.3.0 255.255.255.0
!
group-policy DfltGrpPolicy attributes
 address-pools value EZVPN_SERVER
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT_TUNNEL
!
tunnel-group EZVPN_SERVER type remote-access
tunnel-group EZVPN_SERVER general-attributes
 default-group-policy DfltGrpPolicy
!
tunnel-group EZVPN_SERVER ipsec-attributes
 ikev1 pre-shared-key cisco
 ikev1 user-authentication none
!
crypto ipsec ikev1 transform-set 3DES_MD5 esp-3des esp-md5-hmac
crypto dynamic-map DYNAMIC 100 set ikev1 transform-set 3DES_MD5
crypto dynamic-map DYNAMIC 100 set reverse-route
```

https://t.me/learningnets

```
crypto map VPN 100 ipsec-isakmp dynamic DYNAMIC
crypto map VPN interface VLAN75
!
router eigrp 400
 redistribute static metric 100000 100 255 1 1500
!
no sysopt connection permit-vpn
!
access-list VLAN75_IN permit icmp 180.1.200.0 255.255.255.0 172.16.1.0 255.255.255.0 echo
access-list VLAN75_IN permit icmp 180.1.200.0 255.255.255.0 172.16.3.0 255.255.255.0 echo
access-list VLAN75_IN permit tcp 180.1.200.0 255.255.255.0 172.16.1.0 255.255.255.0 eq 443
access-list VLAN75_IN permit tcp 180.1.200.0 255.255.255.0 172.16.3.0 255.255.255.0 eq 443
!
object network EZVPN_NAT
 subnet 180.1.200.0 255.255.255.0
!
nat (INSIDE,VLAN75) 1 source static REAL_SOURCE REAL_SOURCE destination static EZVPN_NAT EZVPN_NAT
```

R1:

```
ip access-list extended VLAN99_INBOUND
 1 permit esp host 180.1.75.17 172.16.6.0 0.0.0.255
!
ip access-list resequence VLAN99_INBOUND 10 10
```

R2:

```
ip access-list extended VLAN99_INBOUND
 1 permit esp host 180.1.75.17 172.16.6.0 0.0.0.255
!
ip access-list resequence VLAN99_INBOUND 10 10
```

Task 3.4 Verification

Configure the VPN client from **TEST-PC-B** and connect to the ASA; there should be no XAUTH. Verify that the requested output is being matched:

```
ASA34/pri/act# show vpn-sessiondb detail ra-ikev1-ipsec


Session Type: IKEv1 IPsec Detailed

Username     : EZVPN_SERVER           Index        : 4
Assigned IP  : 180.1.200.1            Public IP    : 172.16.6.50
Protocol     : IKEv1 IPsec
```

https://t.me/learningnets

```
License      : Other VPN
Encryption   : 3DES                  Hashing      : MD5
Bytes Tx     : 0                     Bytes Rx     : 0
Pkts Tx      : 0                     Pkts Rx      : 0
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy         Tunnel Group : EZVPN_SERVER
Login Time   : 18:37:18 UTC Tue Apr 8 2014
Duration     : 0h:00m:29s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 4.1
  UDP Src Port : 55336                 UDP Dst Port : 500
  IKE Neg Mode : Aggressive            Auth Mode    : preSharedKeys
  Encryption   : 3DES                  Hashing      : MD5
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 86371 Seconds
  D/H Group    : 2
  Filter Name  :
  Client OS    : WinNT                 Client OS Ver: 5.0.07.0410

IPsec:
  Tunnel ID    : 4.2
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 180.1.200.1/255.255.255.255/0/0
  Encryption   : 3DES                  Hashing      : MD5
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 28770 Seconds
  Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
  Bytes Tx     : 0                     Bytes Rx     : 0
  Pkts Tx      : 0                     Pkts Rx      : 0

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 30 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

https://t.me/learningnets

For testing purposes, generate ICMP traffic from **TEST-PC-B** to ACS1 and ISE1, and verify that ACL entries are matched on ASA:

```
ASA34/pri/act#   show access-list VLAN75_IN | i echo

access-list VLAN75_IN line 7 extended permit icmp 180.1.200.0 255.255.255.0 172.16.1.0 255.255.255.0 echo (hitcnt=1)
access-list VLAN75_IN line 8 extended permit icmp 180.1.200.0 255.255.255.0 172.16.3.0 255.255.255.0 echo (hitcnt=1)
```

Verify that packets flow bidirectionally through the IPsec tunnel:

```
ASA34/pri/act# show crypto ipsec sa peer 172.16.6.50
peer address: 172.16.6.50
    Crypto map tag: DYNAMIC, seq num: 100, local addr: 180.1.75.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (180.1.200.1/255.255.255.255/0/0)
      current_peer: 172.16.6.50, username: EZVPN_SERVER
      dynamic allocated peer ip: 180.1.200.1
 #pkts encaps: 8, #pkts encrypt: 8, #pkts digest: 8
 #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8

      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 8, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 180.1.75.17/0, remote crypto endpt.: 172.16.6.50/0
      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: C805F0BF
      current inbound spi : 1BD8F4FC

    inbound esp sas:
      spi: 0x1BD8F4FC (467203324)
         transform: esp-3des esp-md5-hmac no compression
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 16384, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28619
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x000001FF
    outbound esp sas:
```

https://t.me/learningnets

```
      spi: 0xC805F0BF (3355832511)
         transform: esp-3des esp-md5-hmac no compression
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 16384, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28619
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Task 3.5 Solution

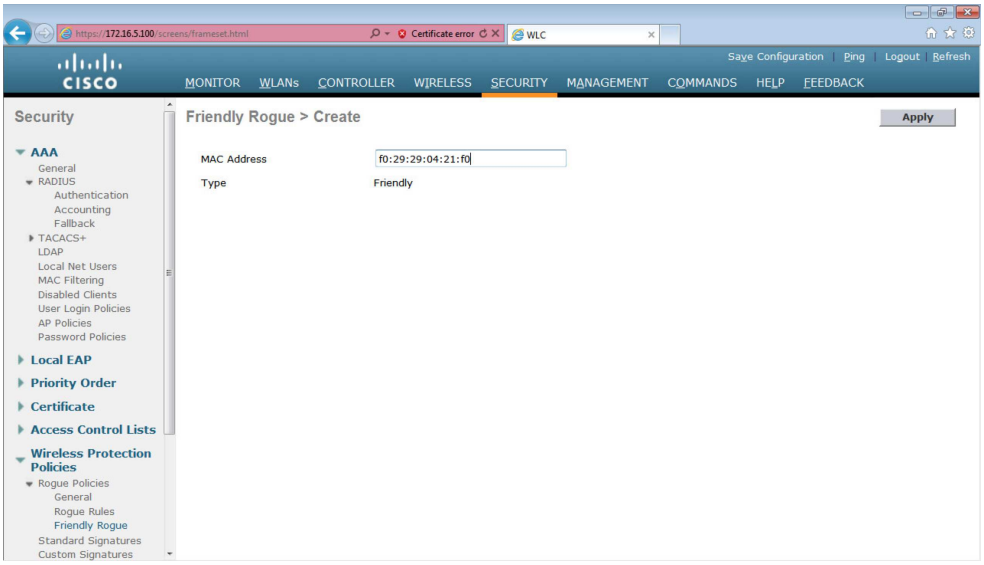
Identify the WIFI MAC address of the LAP from your rack:

```
(Cisco Controller) >show ap join stats summary all


Number of APs.................................................. 1

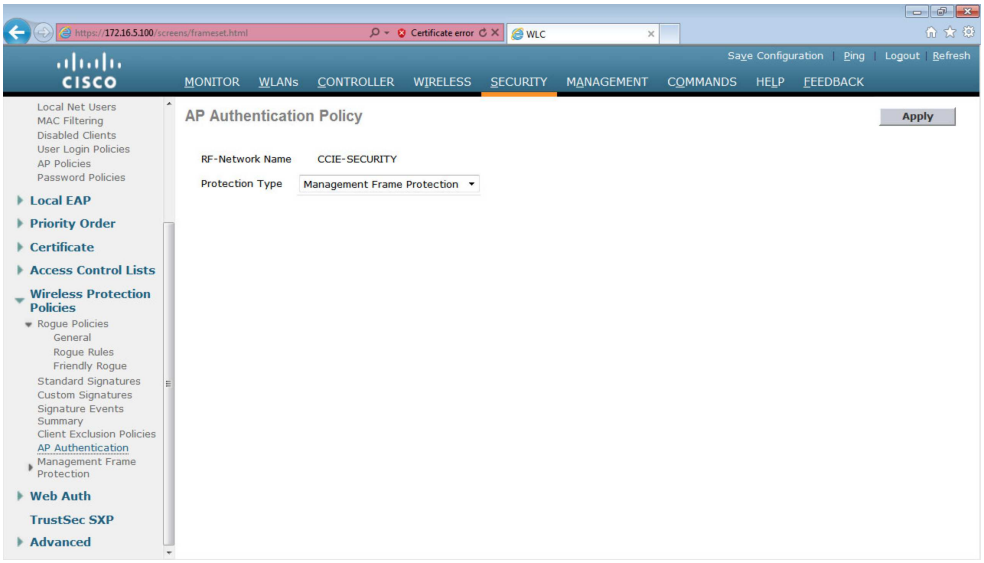
Base Mac              AP EthernetMac       AP Name                IP Address         Status
f0:29:29:04:21:f0
    00:06:f6:3b:9a:da    RACK2-AP               180.1.3.51         Joined
```

Use Internet Explorer to access WLC on **https://172.16.5.100**, navigate to **Security -> Wireless Protection Policies -> Rogue Policies -> Friendly Rogue**, and add the WIFI MAC address:

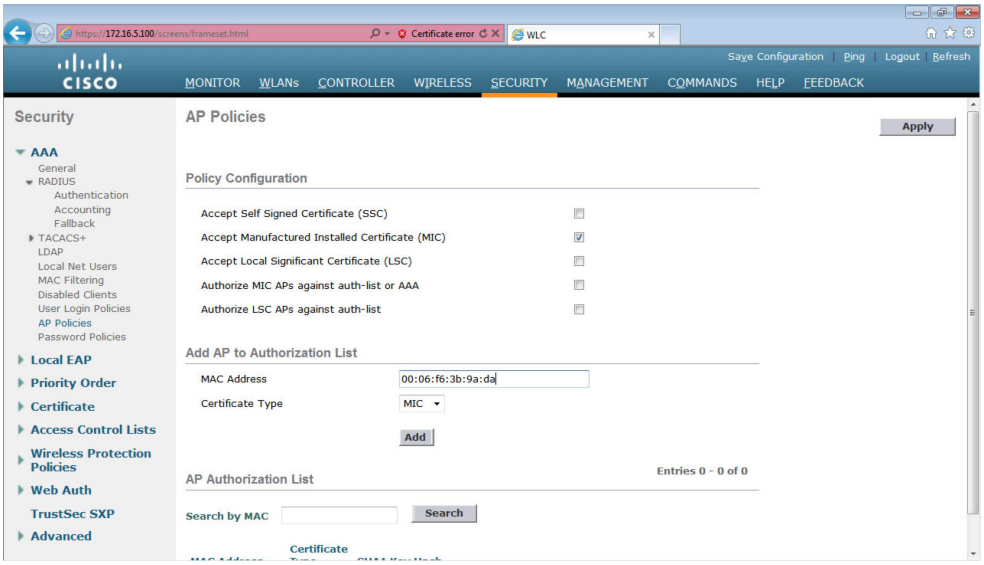


https://t.me/learningnets

Navigate to **Security -> Wireless Protection Policies -> Rogue Policies -> AP Authentication** and enable MFP:

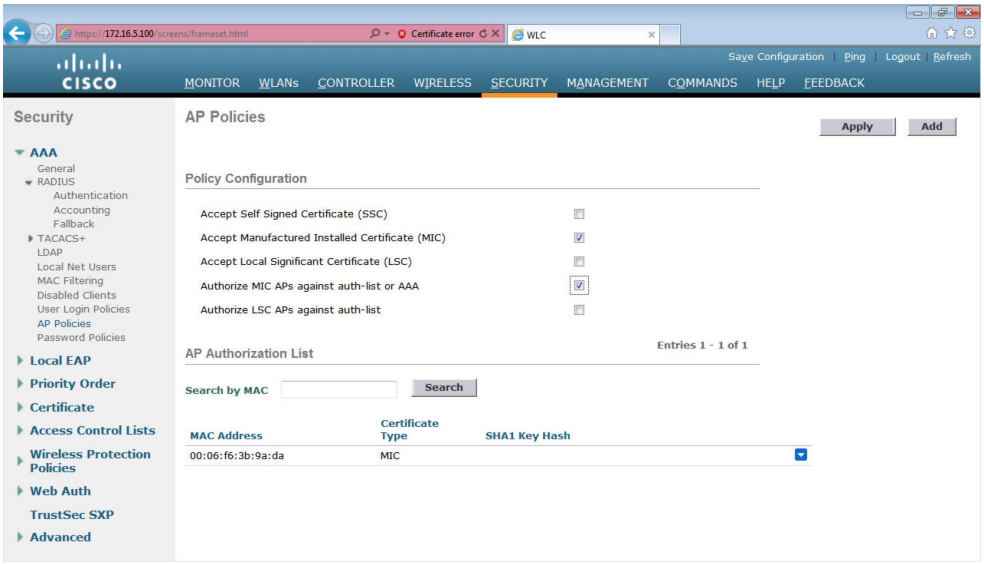


Navigate to **Security -> AAA -> AP Policies**, click **Add**, and configure the Ethernet MAC address of the LAP from your rack:



Navigate to **Security -> AAA -> AP Policies** and enable **Authorize MIC APs against auth-list or AAA**:

https://t.me/learningnets



Task 3.5 Verification

Verify that LAP has been assigned an IPv4 address from R3 and has joined the WLC:

```
R3#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
180.1.3.51          0100.06f6.3b9a.da       Apr 09 2014 05:10 PM    Automatic
!
!(Cisco Controller) >show ap summary


Number of APs.................................. 1

Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model             Ethernet MAC       Location          Port  Country  Priority
------------------  -----  -------------------  -----------------  ----------------  ----  -------  --------
RACK1-AP            2      AIR-LAP1262N-A-K9    00:06:f6:3b:9a:da  default location  1        US       1
```

Verify the friendly rogue rule for the LAP:

```
(Cisco Controller) >show rogue ap friendly summary
```

https://t.me/learningnets

```
Number of APs.................................. 1

MAC Address        State              # APs # Clients Last Heard
-----------------  -----------------  ----- --------- ----------------------
f0:29:29:04:21:f0  Internal           0     0         Not Heard
```

Verify that infrastructure MFP is enabled:

```
(Cisco Controller) >show wps mfp summary

Global Infrastructure MFP state.................. Enabled

Controller Time Source Valid..................... False

                                    WLAN       Client
WLAN ID  WLAN Name                  Status     Protection
-------  -------------------------  ---------  ----------
```

Verify that WLC authorizes the LAP MAC address against the local database:

```
(Cisco Controller) >show auth-list

Authorize MIC APs against AAA ................... enabled
Authorize LSC APs against Auth-List ..... disabled
APs Allowed to Join AP with Manufacturing Installed Certificate.... yes
  AP with Self-Signed Certificate................. no
  AP with Locally Significant Certificate........ no

Mac Addr                  Cert Type    Key Hash
-----------------------   ----------   ----------------------------------------
00:06:f6:3b:9a:da         MIC
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 4

CCIE SCv4 Lab 4 Solutions Section 4

1. Task 4.1 Solution
2. Task 4.2 Solution
3. Task 4.3 Solution
4. Task 4.4 Solution
5. Task 4.5 Solution

Task 4.1 Solution

R4:

```
aaa new-model
!
aaa group server radius ACS_RADIUS
 server-private 172.16.1.100 key cisco
 ip radius source-interface Loopback0
!
aaa authentication login VTY group ACS_RADIUS local
aaa authorization exec VTY group ACS_RADIUS local
!
username RESTRICTED view RESTRICTED password restricted
username UNRESTRICTED view root password restricted
!
line vty 0 15
 login authentication VTY
 authorization exec VTY
!
enable password cisco
!
enable view
!
configure terminal
parser view RESTRICTED
 secret cisco
 commands exec include show privilege
 commands exec include configure terminal
```

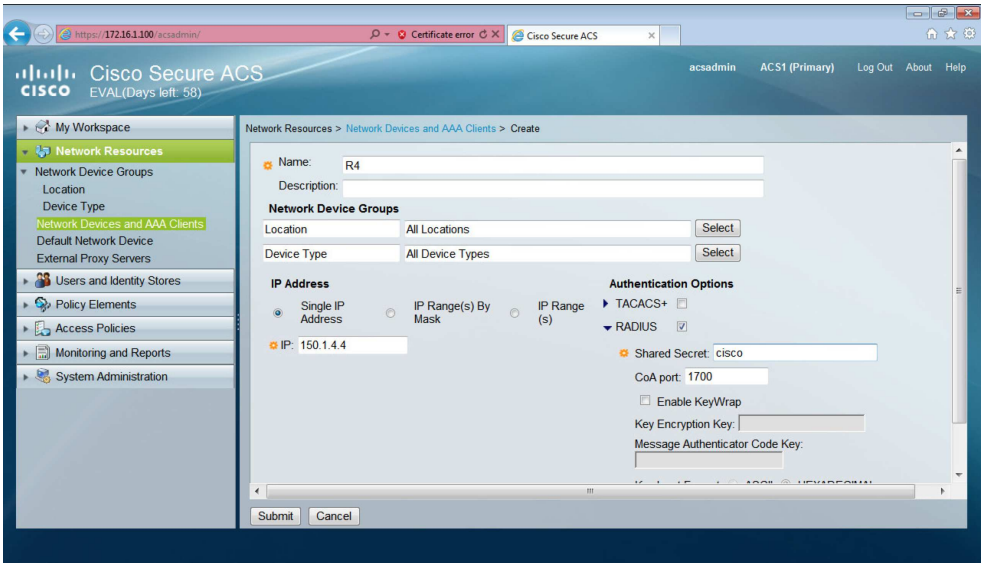
https://t.me/learningnets

```
 commands configure include router
 commands router include network
 commands exec include show ip interface brief
 commands configure include interface loopback0
 commands interface include ip address
 commands exec include write memory
!
no enable password cisco


ASA3:

access-list VLAN75_IN permit udp host 150.1.4.4 host 172.16.1.100 eq 1645
access-list VLAN75_IN permit udp host 150.1.4.4 host 172.16.1.100 eq 1812
!
object network ACS_REAL
 host 172.16.1.100
!
object network R4_REAL
 host 150.1.4.4
!
nat (INSIDE,VLAN75) 1 source static ACS_REAL ACS_REAL destination static R4_REAL R4_REAL
```

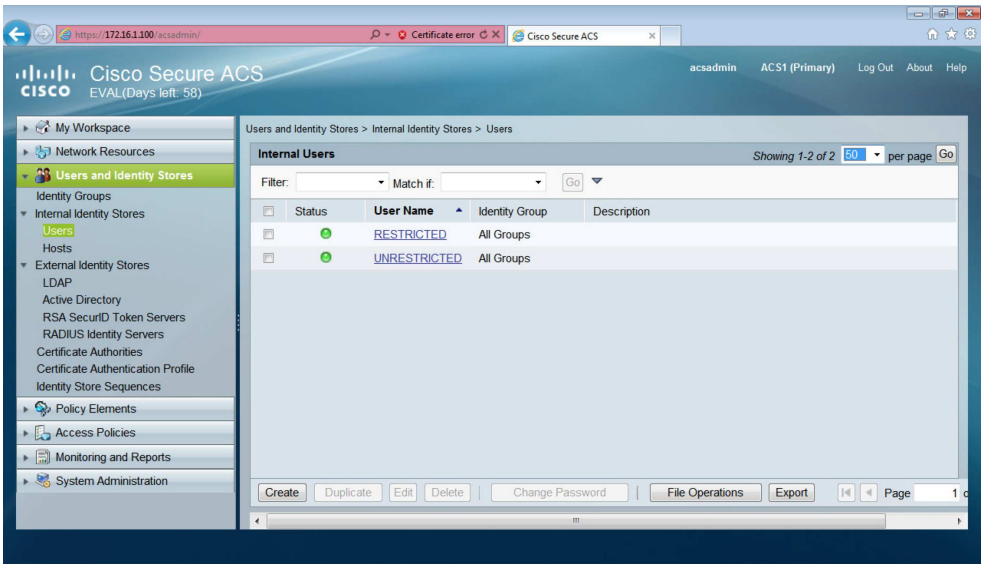
From **TEST-PC-B**, use Internet Explorer to browse to ACS and navigate to **Network Resources -> Network Devices and AAA Clients**; click **Create** to add R4 as NAD client for RADIUS:



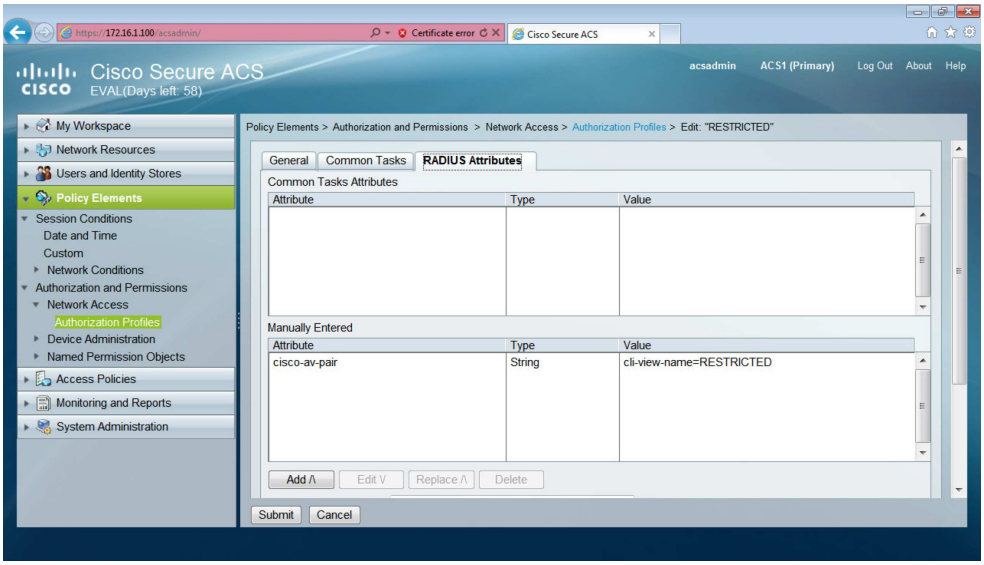
Navigate to **Users and Identity Stores- > Internal Identity Stores -> Users** and click **Create** to add both **RESTRICTED** and **UNRESTRICTED** users to ACS

https://t.me/learningnets

database:

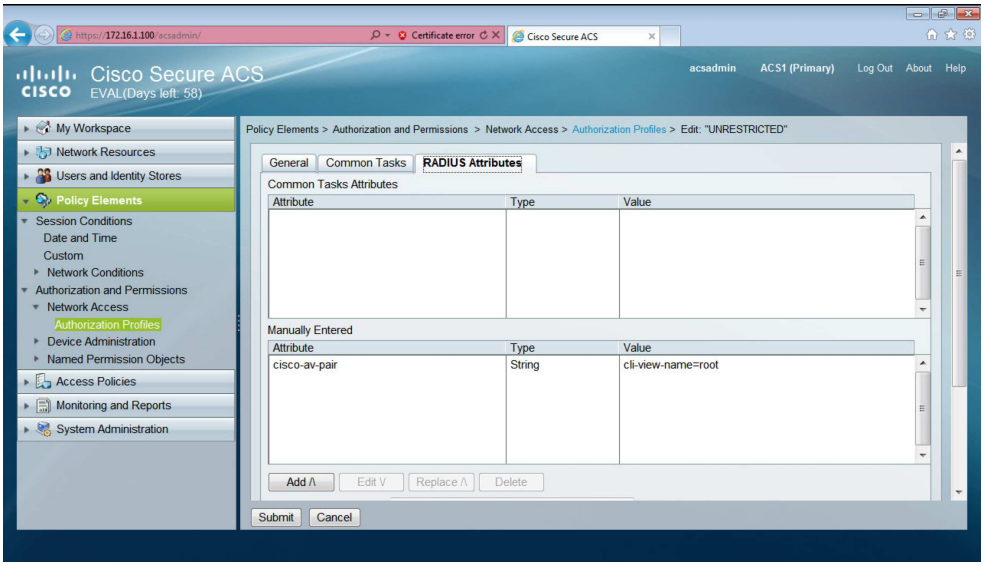


Navigate to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click **Create** to configure view assignment, for example **RESTRICTED** view:

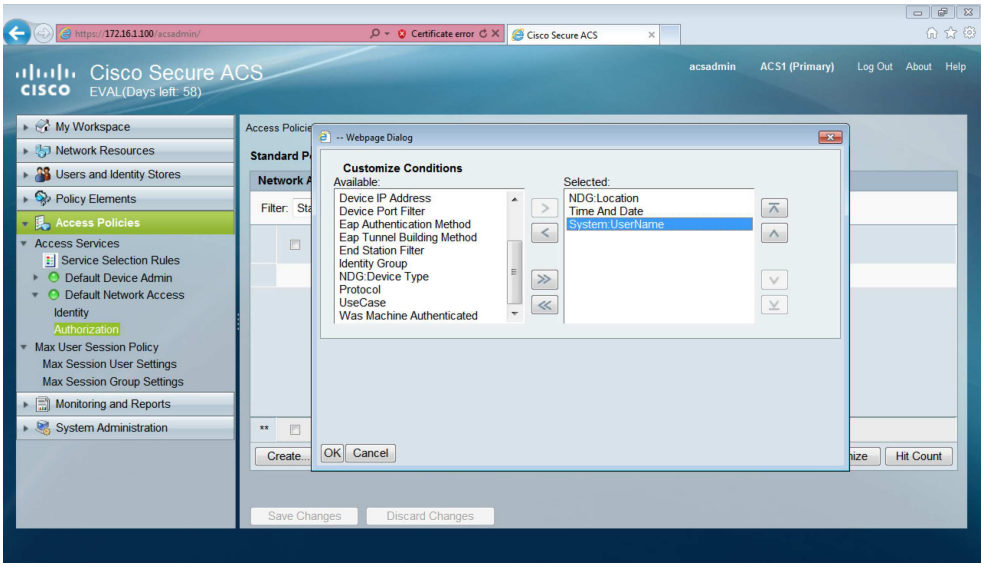


Navigate to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click **Create** to configure view assignment, for example **UNRESTRICTED** view:

https://t.me/learningnets

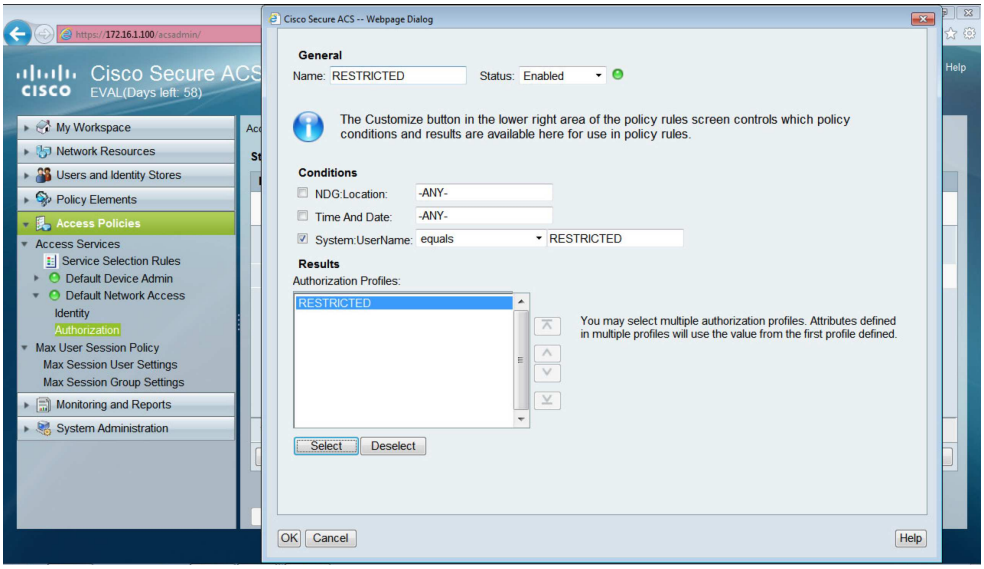


Navigate to **Access Policies -> Default Network Access -> Authorization** and click **Customize** to add the username as condition:

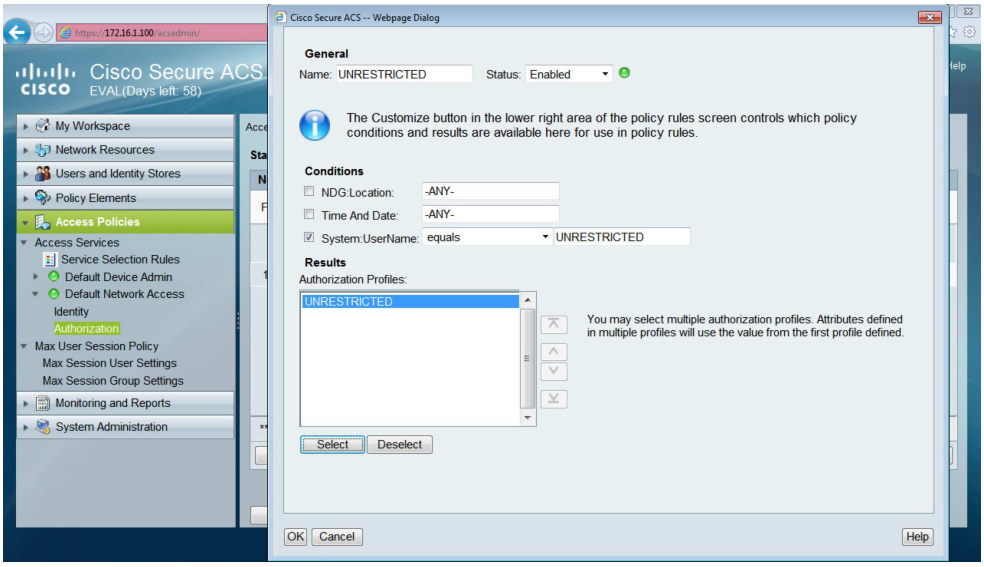


Navigate to **Access Policies -> Default Network Access -> Authorization**, click **Add**, and configure the rule for **RESTRICTED** user:

https://t.me/learningnets



Navigate to **Access Policies -> Default Network Access -> Authorization**, click **Add**, and configure the rule for **UNRESTRICTED** user:



Task 4.1 Verification

Verify basic authentication from R4:

https://t.me/learningnets

```
R4#test aaa group ACS_RADIUS RESTRICTED restricted legacy

Attempting authentication test to server-group ACS_RADIUS using radius
User was successfully authenticated.

!
!R4#test aaa group ACS_RADIUS UNRESTRICTED unrestricted legacy

Attempting authentication test to server-group ACS_RADIUS using radius
User was successfully authenticated.
```

Telnet to R4 and authenticate with the **UNRESTRICTED** user; verify the view assignment and confirm that it has full configuration access:

```
R4#telnet 150.1.4.4
Trying 150.1.4.4 ... Open


User Access Verification

Username: UNRESTRICTED
Password:
R4>show privilege
Currently in View Context with view 'root'
R4>configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.R4(config)>interface FastEthernet0/0
R4(config-if)>
```

Telnet to R4 and authenticate with the **RESTRICTED** user; verify the view assignment and confirm that it has restricted configuration access:

```
R4#telnet 150.1.4.4
Trying 150.1.4.4 ... Open


User Access Verification

Username: RESTRICTED
Password:
R4>show privilege
Currently in View Context with view 'RESTRICTED'
R4>configure terminal
```

https://t.me/learningnets

```
Enter configuration commands, one per line.  End with CNTL/Z.R4(config)>interface FastEthernet0/0

                                ^% Invalid input detected at '^' marker.
R4(config)>interface Loopback0
R4(config-if)>exit
R4(config)>exitR4>show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            180.1.45.4      YES NVRAM  up                    up
FastEthernet0/1            180.1.34.4      YES NVRAM  up                    up
Loopback0                  150.1.4.4       YES NVRAM  up                    up      R4>write memory
Building configuration...
[OK]

R4>
```

Task 4.2 Solution

```
ASA3:

telnet 180.1.55.0 255.255.255.0 INSIDE
!
aaa authentication telnet console LOCAL
aaa authorization command LOCAL
!
username PRIV4 password cisco
username PRIV6 password cisco
enable password cisco level 4
enable password cisco level 6
!
privilege show level 4 command crypto
privilege level 6 command configure
privilege configure level 6 command interface
privilege configure level 6 command nameif
privilege configure level 6 command security-level
privilege configure level 6 command ip
```

Task 4.2 Verification

Telnet from R5 and authenticate with user **PRIV4**; verify available commands:

```
R5#telnet 180.1.55.17
Trying 180.1.55.17 ... Open
```

https://t.me/learningnets

```
User Access Verification

Username: PRIV4
Password: *****
Type help or '?' for a list of available commands.ASA34/pri/act> enable 4
Password: *****ASA34/pri/act# show curpriv
Username : enable_4Current privilege level : 4
Current Mode/s : P_PRIVASA34/pri/act# configure terminal
                 ^
ERROR: % Invalid input detected at '^' marker.ERROR: Command authorization failed
ASA34/pri/act# show crypto isakmp sa

There are no IKEv1 SAs

There are no IKEv2 SAsASA34/pri/act# show int ip brief
                      ^
ERROR: % Invalid input detected at '^' marker.ERROR: Command authorization failed
```

Telnet from R5 and authenticate with user **PRIV6**; verify available commands:

https://t.me/learningnets

```
R5#telnet 180.1.55.17

Trying 180.1.55.17 ... Open


User Access Verification

Username: PRIV6
Password: *****
Type help or '?' for a list of available commands.ASA34/pri/act> enable 6

Password: *****ASA34/pri/act# show curpriv

Username : enable_6Current privilege level : 6

Current Mode/s : P_PRIV
ASA34/pri/act# configure terminalASA34/pri/act(config)# router eigrp 400

                             ^
ERROR: % Invalid input detected at '^' marker.ERROR: Command authorization failed

ASA34/pri/act(config)# interface GigabitEthernet0/1ASA34/pri/act(config-if)# description TEST

                             ^
ERROR: % Invalid input detected at '^' marker.ERROR: Command authorization failed
ASA34/pri/act(config-if)# nameif INSIDE
ASA34/pri/act(config-if)# security-level 100
```

Task 4.3 Solution

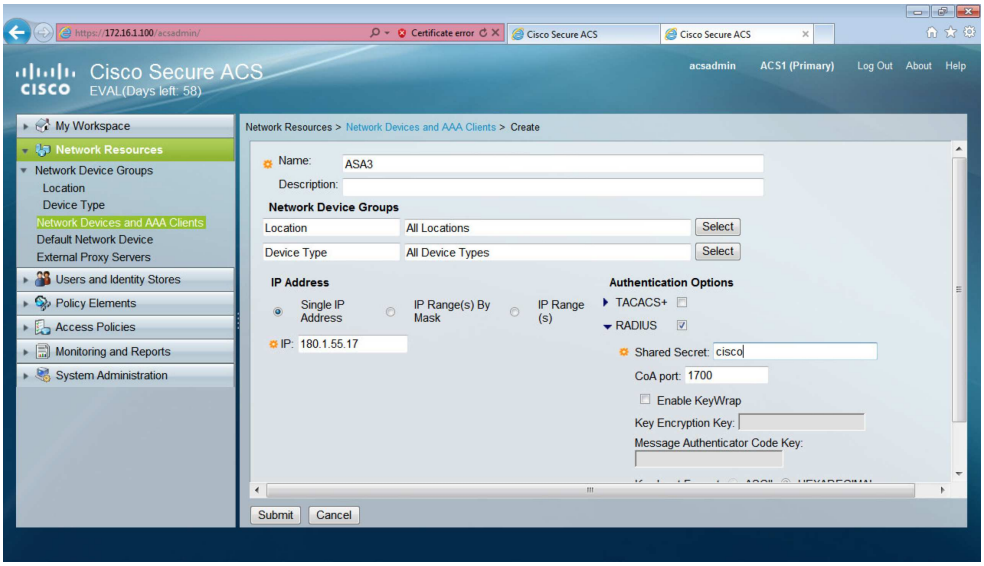
```
ASA3:

aaa-server ACS_RADIUS protocol radius
aaa-server ACS_RADIUS (INSIDE) host 172.16.1.100
 key cisco
!
virtual telnet 180.1.55.100
access-list AUTH_RADIUS permit tcp any host 180.1.55.100 eq 23
aaa authentication match AUTH_RADIUS INSIDE ACS_RADIUS
!
access-list AUTHORIZATION permit ip any any
```

https://t.me/learningnets

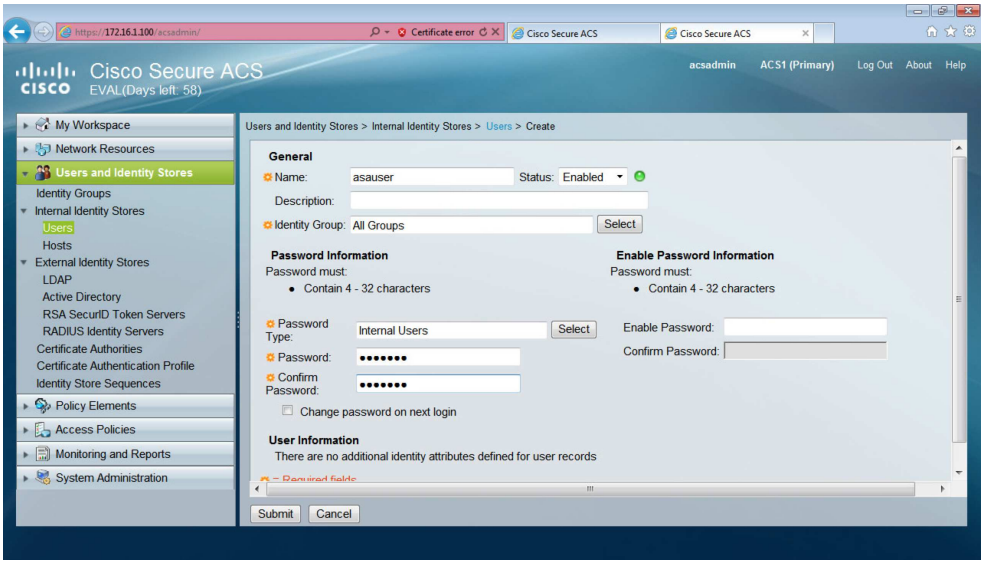
```
!
access-list INSIDE_IN permit udp host 180.1.55.5 host 172.16.6.1 eq 500
access-list INSIDE_IN permit tcp any host 180.1.55.100 eq 23
access-group INSIDE_IN in interface INSIDE per-user-override
!
policy-map global_policy
 class inspection_default
  inspect icmp
```

From **TEST-PC-B**, use Internet Explorer to browse to ACS and navigate to **Network Resources -> Network Devices and AAA Clients**; click **Create** to add ASA3 as NAD client for RADIUS:

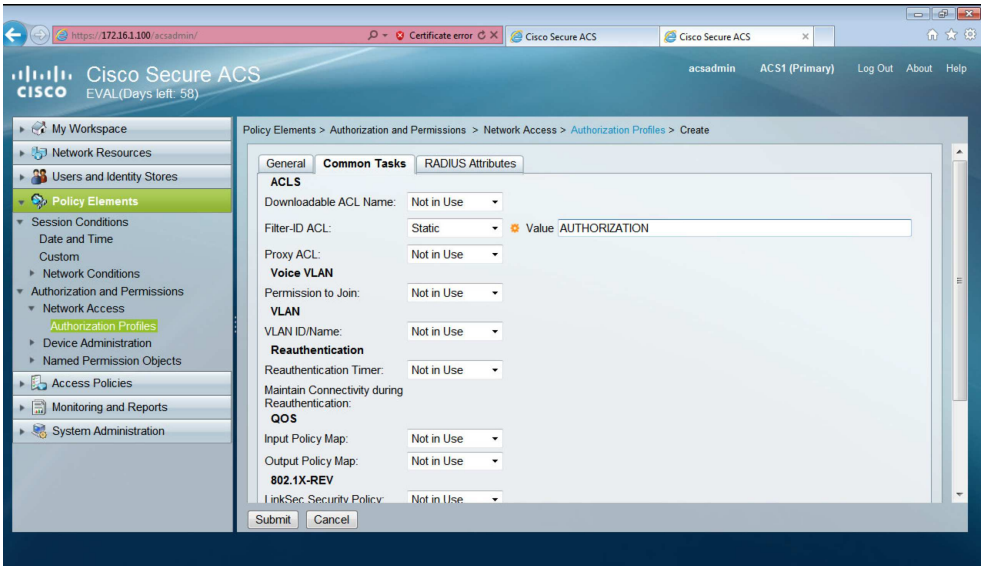


Navigate to **Users and Identity Stores- > Internal Identity Stores -> Users** and click **Create** to add the authenticating username to the ACS database:

https://t.me/learningnets

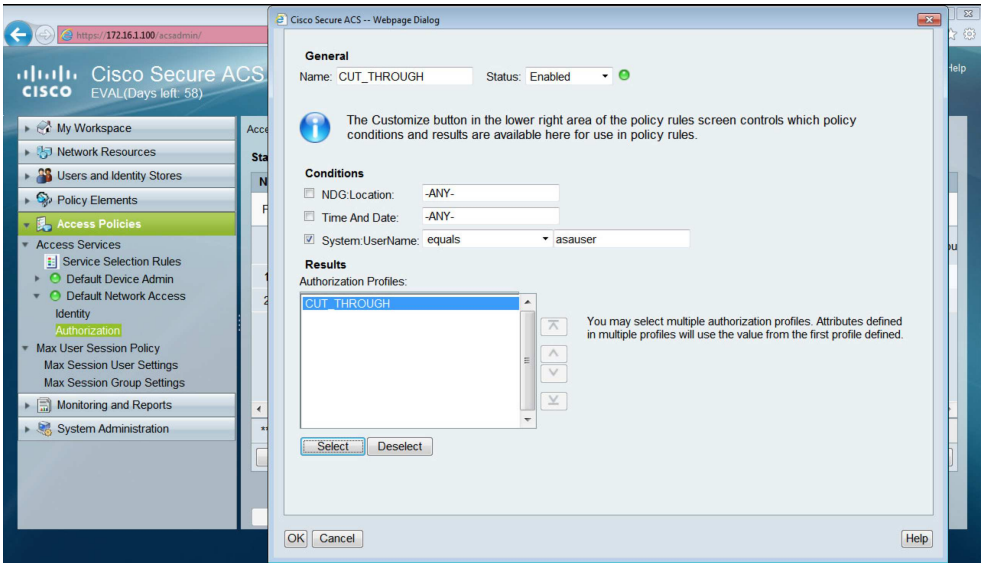


Navigate to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click **Create** to assign the Filter-ID ACL:



Navigate to **Access Policies -> Default Network Access -> Authorization**, click **Add**, and configure the rule for cut-through proxy:

https://t.me/learningnets



Task 4.3 Verification

Test basic authentication from ASA:

```
ASA34/pri/act# test aaa authentication ACS_RADIUS username asauser password asapass

Server IP Address or name: 172.16.1.100
INFO: Attempting Authentication test to IP address <172.16.1.100> (timeout: 12 seconds)
INFO: Authentication Successful
```

Verify that before authentication, outbound traffic is not allowed:

```
R5#telnet 150.1.13.13 80
Trying 150.1.13.13, 80 ... % Connection refused by remote host
```

Authenticate and verify that access is now allowed:

```
R5#telnet 180.1.55.100
Trying 180.1.55.100 ... Open

LOGIN Authentication

Username: asauser

Password:

Authentication Successful
```

https://t.me/learningnets

```
[Connection to 180.1.55.100 closed by foreign host]
!
!R5#telnet 150.1.13.13 80
Trying 150.1.13.13, 80 ... Open
]HTTP/1.1 400 Bad Request
Date: Tue, 02 Mar 1993 21:48:29 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request
[Connection to 150.1.13.13 closed by foreign host]
```

Verify the authenticated user and its received authorization, and that the requested output is matched:

```
ASA34/pri/act# show uauth

                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1user 'asauser' at 180.1.55.5, authenticated
access-list AUTHORIZATION (*)
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
!
!ASA34/pri/act# show access-list  AUTHORIZATION
access-list AUTHORIZATION; 1 elements; name hash: 0xc2ae3e18
access-list AUTHORIZATION line 1 extended permit ip any any (hitcnt=2) 0x6c18a992
```

Task 4.4 Solution

```
SW5:
aaa new-model
!
aaa group server radius ISE_RADIUS
 server-private 172.16.3.100 key Cisco123
 ip radius source-interface Loopback0
!
aaa authentication dot1x default group ISE_RADIUS
dot1x system-auth-control
ip device tracking
```

https://t.me/learningnets

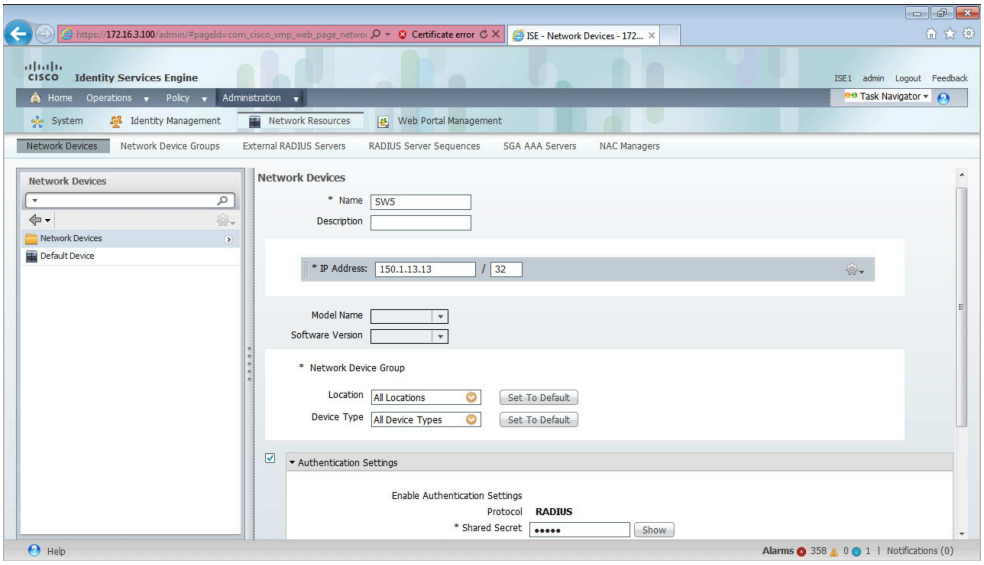
```
!
default interface FastEthernet1/0/11
!
interface FastEthernet1/0/11
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3
 switchport trunk native vlan 3
 switchport mode trunk
 authentication host-mode multi-host
 authentication event fail action authorize vlan 3
 authentication event server dead action authorize vlan 3
 authentication event no-response action authorize vlan 3
 authentication port-control auto
 dot1x pae authenticator
```

ASA3:

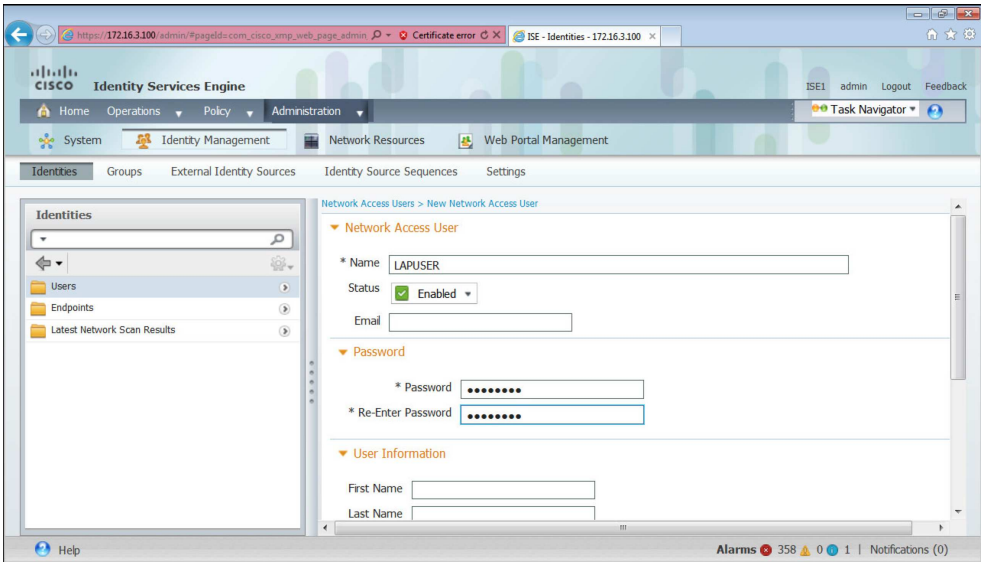
```
access-list VLAN75_IN extended permit udp host 150.1.13.13 host 172.16.3.100 eq radius
access-list VLAN75_IN extended permit udp host 150.1.13.13 host 172.16.3.100 eq 1812
!
!
object network ISE_REAL
 host 172.16.3.100
!
object network SW5_REAL
 host 150.1.13.13
!
nat (INSIDE,VLAN75) 1 source static ISE_REAL ISE_REAL destination static SW5_REAL SW5_REAL
```

From **TEST-PC-B**, use Internet Explorer to navigate to ISE, **Administration -> Network Resources -> Network Devices**, and click **Add** to add SW5 as a NAD client:

https://t.me/learningnets

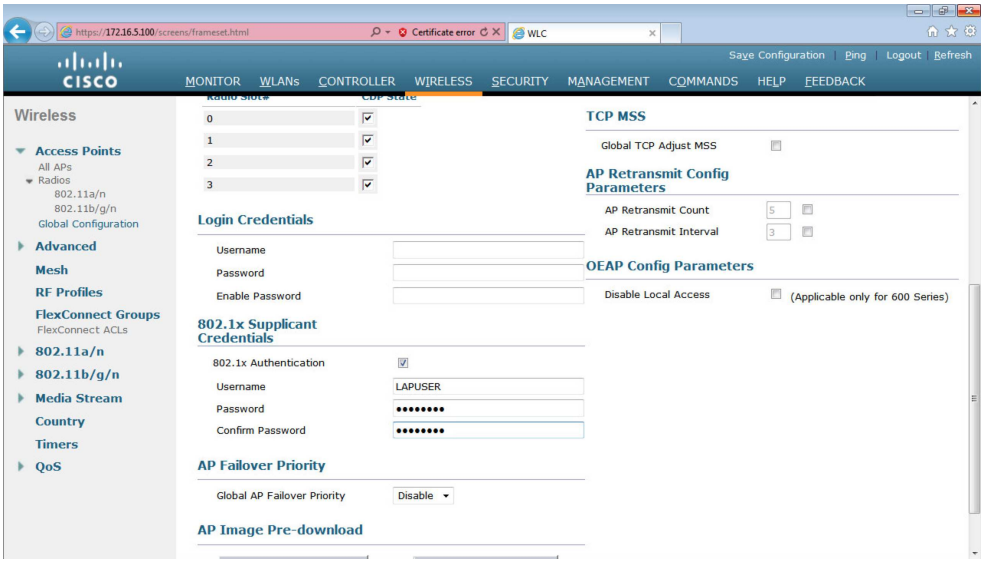


Navigate to **Administration -> Identity Management -> Identities -> Users** and click **Add** to configure the required username/password pair:



From **TEST-PC-B**, use Internet Explorer to navigate to WLC, **Wireless -> Access Points -> Global Configuration** and enable **802.1x Supplicant Credentials**:

https://t.me/learningnets



Task 4.4 Verification

Verify that the requested output is matched; note the host-mode of **multi-host** to accommodate for locally switched WLANs:

```
SW5#show authentication sessions interface fastEthernet1/0/11
            Interface:  FastEthernet1/0/11
          MAC Address:  0006.f63b.9ada
           IP Address:  180.1.3.51
            User-Name:  LAPUSER
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure Oper host mode:  multi-host

     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Group:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  00000000000000080BD70142
      Acct Session ID:  0x00000009
               Handle:  0xB1000008

Runnable methods list:
       Method   State
       dot1x    Authc Success
```

https://t.me/learningnets

Verify that IP connectivity with the LAP is still functional:

```
R3#ping 180.1.3.51

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 180.1.3.51, timeout is 2 seconds:!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 4.5 Solution

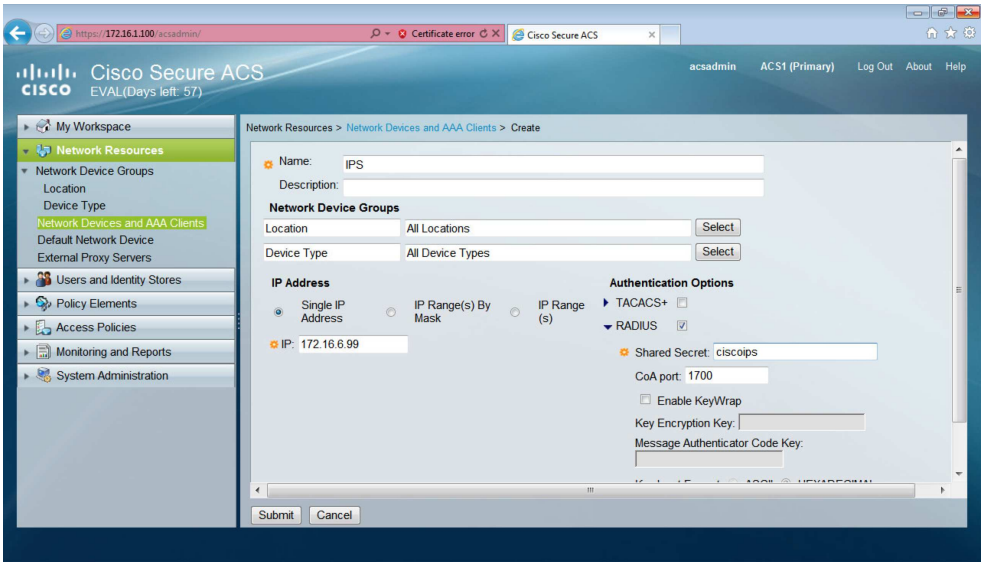
```
IPS:
sensor(config)# service aaa
sensor(config-aaa)# aaa radius
sensor(config-aaa-rad)# default-user-role administrator
sensor(config-aaa-rad)# primary-server
sensor(config-aaa-rad-pri)# server-address 172.16.1.100
sensor(config-aaa-rad-pri)# shared-secret ciscoips
sensor(config-aaa-rad-pri)# exit
sensor(config-aaa-rad)# local-fallback enabled
sensor(config-aaa-rad)# console-authentication local
sensor(config-aaa-rad)# exit
sensor(config-aaa)# exit
Apply Changes?[yes]:

ASA3:

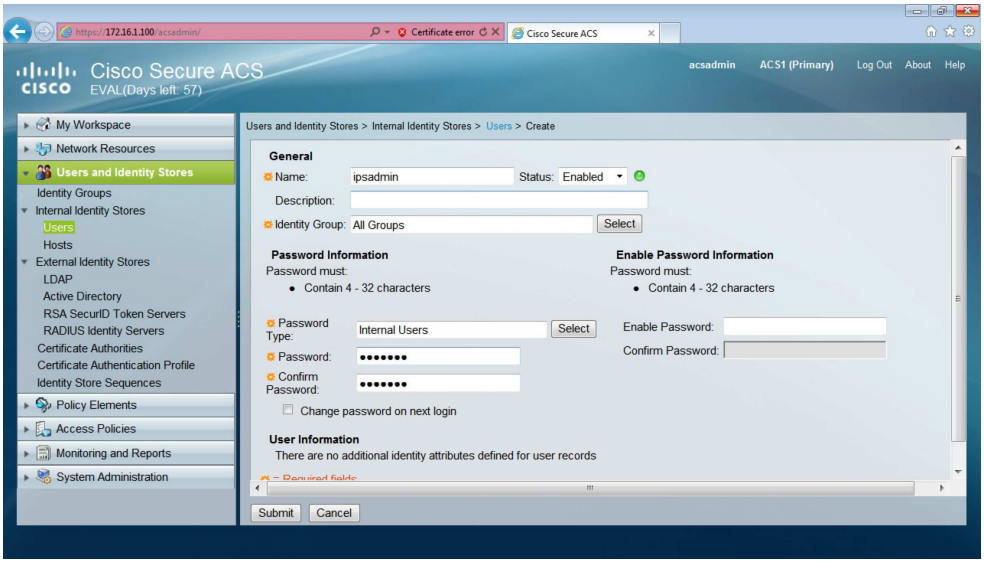
access-list VLAN75_IN extended permit udp host 172.16.6.99 host 172.16.1.100 eq radius
access-list VLAN75_IN extended permit udp host 172.16.6.99 host 172.16.1.100 eq 1812
!
object network IPS_REAL
 host 172.16.6.99
!
nat (INSIDE,VLAN75) 1 source static ACS_REAL ACS_REAL destination static IPS_REAL IPS_REAL
```

From **TEST-PC-B**, use Internet Explorer to browse to ACS and navigate to **Network Resources -> Network Devices and AAA Clients**; click **Create** to add IPS as NAD client for RADIUS:

https://t.me/learningnets



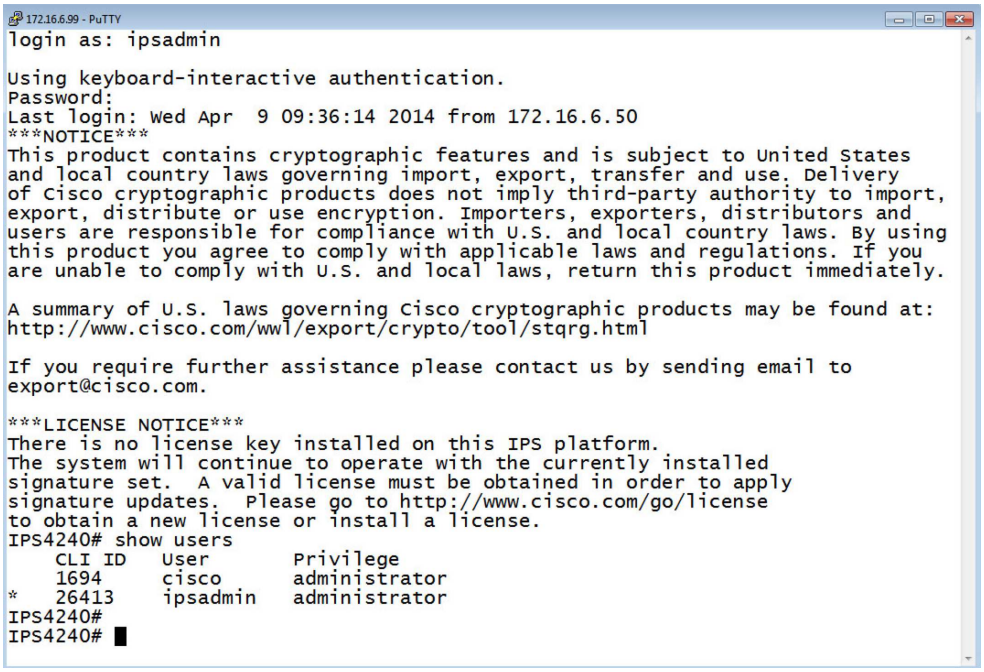
Navigate to **Users and Identity Stores- > Internal Identity Stores -> Users** and click **Create** to add user to ACS database:



Task 4.5 Verification

From **TEST-PC-B**, initiate an SSH session to the IPS; authenticate with RADIUS credentials and verify the locally assigned role:

https://t.me/learningnets



https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 4

CCIE SCv4 Lab 4 Solutions Section 5

1. Task 5.1 Solution
2. Task 5.2 Solution
3. Task 5.3 Solution
4. Task 5.4 Solution
5. Task 5.5 Solution
6. Task 5.6 Solution

Task 5.1 Solution

```
R3:


access-list 10 permit 180.1.99.0 0.0.0.255
!
login block-for 600 attempts 3 within 60
login quiet-mode access-class 10
login on-failure log every 5
login delay 3
!
line vty 0 15
 login local
```

Task 5.1 Verification

Verify the configuration:

```
R3#show login
  A login delay of 3 seconds is applied.
 Quiet-Mode access list 10 is applied.
 Every 5 failed login is logged.


     Router enabled to watch for login Attacks.
If more than 3 login failures occur in 60 seconds or less,
```

https://t.me/learningnets

```
logins will be disabled for 600 seconds.


     Router presently in Normal-Mode.
     Current Watch Window
         Time remaining: 28 seconds.
         Login failures for current window: 0.
     Total login failures: 0.
```

Telnet top R3 and fail 3 authentication attempts in 60 seconds:

```
R4#telnet 180.1.34.3
Trying 180.1.34.3 ... Open


User Access Verification

Username: user1
Password:
% Login invalid

Username: user1
Password:
% Login invalid

Username: user1
Password:
% Login invalid
[Connection to 180.1.34.3 closed by foreign host]
```

Verify that access is denied now:

```
R4#telnet 180.1.34.3
Trying 180.1.34.3 ... % Connection refused by remote host
```

Verify that the router started the quiet-mode period:

```
R3#show login

     A login delay of 3 seconds is applied.
     Quiet-Mode access list 10 is applied.
     Every 5 failed login is logged.
```

https://t.me/learningnets

```
     Router enabled to watch for login Attacks.
     If more than 3 login failures occur in 60 seconds or less,
     logins will be disabled for 600 seconds.
 Router presently in Quiet-Mode.
 Will remain in Quiet-Mode for 557 seconds.
     Restricted logins filtered by applied ACL 10.
!
!R3#show login failures

Total failed logins: 3
Detailed information about last 50 failures

Username        SourceIPAddr    lPort Count TimeStamp
user1           180.1.34.4      23    3     11:47:28 UTC Wed Apr 9 2014
```

The following log message should appear on R3's console:

```
%SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failures is 6 secs, [user: user1] [Source: 180.1.34.4] [loca
```

The following log message will be displayed when the quiet period expires:

```
%SEC_LOGIN-5-QUIET_MODE_OFF: Quiet Mode is OFF, because block period timed out at 11:57:28 UTC Wed Apr 9 2014
```

Task 5.2 Solution

https://t.me/learningnets

R3:

```
logging discriminator OSPF msg-body drops Neighbor Down
!
logging on
logging buffered discriminator OSPF informational
logging console discriminator OSPF informational
logging trap debugging
logging host 180.1.55.66 vrf LAB4 transport tcp discriminator OSPF
```

ASA3:

```
access-list VLAN75_IN extended permit tcp host 180.1.34.3 host 180.1.55.66 eq 601
```

Task 5.2 Verification

Verify the logging configuration:

```
R3#show logging

Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering

Active Message Discriminator:
OSPF      msg-body       drops    Neighbor Down




No Inactive Message Discriminator.

 Console logging: level informational, 175 messages logged, xml disabled,
filtering disabled, discriminator(OSPF),
                     0 messages rate-limited, 3 messages dropped-by-MD
    Monitor logging: level informational, 0 messages logged, xml disabled,
                     filtering disabled
Buffer logging:  level informational, 11 messages logged, xml disabled,
 filtering disabled, discriminator(OSPF),
                     0 messages rate-limited, 3 messages dropped-by-MD
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.
```

https://t.me/learningnets

```
Trap logging: level debugging, 181 message lines logged
        Logging to 180.1.55.66  (LAB4) (tcp port 601, audit disabled,
              link down),
              0 message lines logged,
              0 message lines rate-limited,
              3 message lines dropped-by-MD,
              xml disabled, sequence number disabled filtering enabled, discriminator (OSPF)
```

Clear the OSPF process and note that only neighbor up messages are being logged:

```
R3#clear ip ospf process

Reset ALL OSPF processes? [no]: yes
%OSPF-5-ADJCHG: Process 400, Nbr 150.1.4.4 on FastEthernet0/0 from LOADING to FULL, Loading Done
```

Task 5.3 Solution

```
R4:

access-list 20 permit 150.1.0.0 0.0.255.255
ip tftp source-interface loopback0
!
tftp-server flash:/c2800nm-adventerprisek9-mz.151-3.T2.bin 20
```

Task 5.3 Verification

Verify that the TFTP server restricts access only to sources from 150.1.0.0/16 subnet:

```
SW5#copy tftp: null:
Address or name of remote host [150.1.4.4]?
Source filename [c2800nm-adventerprisek9-mz.151-3.T2.bin]?
Accessing tftp://150.1.4.4/c2800nm-adventerprisek9-mz.151-3.T2.bin...
%Error opening tftp://150.1.4.4/c2800nm-adventerprisek9-mz.151-3.T2.bin (No such file or directory)
!
!R4#copy tftp: null:
Address or name of remote host [150.1.4.4]?
Source filename [c2800nm-adventerprisek9-mz.151-3.T2.bin]?
Accessing tftp://150.1.4.4/c2800nm-adventerprisek9-mz.151-3.T2.bin...
```

https://t.me/learningnets

```
Loading c2800nm-adventerprisek9-mz.151-3.T2.bin from 150.1.4.4 (via Loopback0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 66537232 bytes]
66537232 bytes copied in 395.108 secs (168403 bytes/sec)
```

Task 5.4 Solution

```
R1 & R2:

interface GigabitEthernet0/1
 standby authentication md5 key-string hsrpkey
```

Task 5.4 Verification

Verify that HSRP MD5 authentication is enabled:

```
R1#show standby

GigabitEthernet0/1 - Group 0
  State is Active
    2 state changes, last state change 21:45:15
  Virtual IP address is 172.16.6.1
  Active virtual MAC address is 0000.0c07.ac00
    Local virtual MAC address is 0000.0c07.ac00 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.712 secs Authentication MD5, key-string

  Preemption enabled
  Active router is local
  Standby router is 172.16.6.22, priority 100 (expires in 9.264 sec)
  Priority 150 (configured 150)
  Group name is "CBAC_HA" (cfgd)
```

Task 5.5 Solution

```
R1 & R2:

interface GigabitEthernet0/0
```

https://t.me/learningnets

```
 ipv6 ospf encryption ipsec spi 1000 esp aes-cbc 256 0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDE
```

Task 5.5 Verification

Verify that the requested output is being matched:

```
R2#show ipv6 ospf interface gigabitEthernet0/0

GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::2, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 150.1.2.2
  Network Type BROADCAST, Cost: 1
  AES-CBC-256 encryption MD5 auth SPI 1000, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 150.1.2.2, local address FE80::2
  Backup Designated router (ID) 150.1.1.1, local address FE80::1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Graceful restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 150.1.1.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

Task 5.6 Solution

```
R4:

ip access-list extended COPP_ACL
 deny tcp 150.1.0.0 0.0.255.255 any eq 23
 deny tcp 150.1.0.0 0.0.255.255 any eq 80
 permit tcp any any eq 23
 permit tcp any any eq 80
!
class-map COPP_CLASS
 match access-group name COPP_ACL
!
policy-map COPP_POLICY
 class COPP_CLASS
```

https://t.me/learningnets

```
  police 16000 conform-action transmit exceed-action drop
!
control-plane
 service-policy input COPP_POLICY
!
control-plane host
 management-interface FastEthernet0/0 allow http telnet
```

Task 5.6 Verification

Verify the control-plane enabled features:

```
R4#show control-plane features

Total 2 features configured

Control plane aggregate path features :

-------------------------------------------------------
Control-plane Policing activated Apr 09 2014 17:2

-------------------------------------------------------

Control plane host path features :

-----------------------------------------------------------Management-Interface activated Apr 09 2014 17:2



-------------------------------------------------------
```

Verify that telnet works only through the FastEthernet0/0 interface:

```
R4#show management-interface
 Management interface FastEthernet0/0
        Protocol        Packets processed
            http                 0
          telnet                25
!
!R4#telnet 180.1.34.4
Trying 180.1.34.4 ... % Connection timed out; remote host not responding
!
!R4#telnet 180.1.45.4

Trying 180.1.45.4 ... Open
```

https://t.me/learningnets

```
User Access Verification

Username:
```

Verify that telnet packets matched the policing class, because the source was not in Loopback0 range:

```
R4#show policy-map control-plane input

 Control Plane

  Service-policy input: COPP_POLICY

    Class-map: COPP_CLASS (match-all)
      17 packets, 1029 bytes
      5 minute offered rate 0 bps, drop rate 0 bps Match: access-group name COPP_ACL
police:
cir 16000 bps, bc 1500 bytes
conformed 17 packets, 1029 bytes; actions:
transmit

        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps

    Class-map: class-default (match-any)
      130 packets, 15161 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Source a telnet session from Loopback0 range and verify that packet counters are not modified, and therefore traffic is not policed:

```
SW5#telnet 180.1.45.4 /source-interface loopback0
Trying 180.1.45.4 ... Open


User Access Verification
Username:
!
!R4#show policy-map control-plane input

 Control Plane
```

https://t.me/learningnets

```
  Service-policy input: COPP_POLICY

    Class-map: COPP_CLASS (match-all)
      17 packets, 1029 bytes
      5 minute offered rate 0 bps, drop rate 0 bps Match: access-group name COPP_ACL
police:
cir 16000 bps, bc 1500 bytes
conformed 17 packets, 1029 bytes; actions:
transmit

        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps

    Class-map: class-default (match-any)
      228 packets, 26060 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

https://t.me/learningnets

CCIE Security v4 Practice Labs Workbook - CCIE Security V4 Full-Scale Lab 4

CCIE SCv4 Lab 4 Solutions Section 6

1. Task 6.1 Solution
2. Task 6.2 Solution
3. Task 6.3 Solution
4. Task 6.4 Solution
5. Task 6.5 Solution
6. Task 6.6 Solution

Task 6.1 Solution

```
ASA2:

fragment chain 1 OUTSIDE
fragment chain 1 INSIDE
fragment chain 1 DMZ
```

Task 6.1 Verification

Verify configuration:

```
ASA2# show fragment

Interface: OUTSIDE Size: 200, Chain: 1, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: DMZ Size: 200, Chain: 1, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: INSIDE Size: 200, Chain: 1, Timeout: 5, Reassembly: virtual

    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

Generate fragmented packets through the ASA, and verify that they are dropped:

https://t.me/learningnets

```
ASA34/pri/act# ping 150.1.6.6 size 2000

Type escape sequence to abort.
Sending 5, 2000-byte ICMP Echos to 150.1.6.6, timeout is 2 seconds:?????
Success rate is 0 percent (0/5)
!
!ASA2# show fragment DMZ

Interface: DMZ
    Size: 200, Chain: 1, Timeout: 5, Reassembly: virtualQueue: 0, Assembled: 0, Fail: 5, Overflow: 0
```

Task 6.2 Solution

```
ASA3:

access-list VLAN75_CONTROL_PLANE permit udp 172.16.6.0 255.255.255.0 any eq 500
access-list VLAN75_CONTROL_PLANE permit udp 172.16.6.0 255.255.255.0 any eq 4500
access-list VLAN75_CONTROL_PLANE permit esp 172.16.6.0 255.255.255.0 any
access-list VLAN75_CONTROL_PLANE deny udp any any eq 500
access-list VLAN75_CONTROL_PLANE deny udp any any eq 4500
access-list VLAN75_CONTROL_PLANE deny esp any any
!
access-group VLAN75_CONTROL_PLANE in interface VLAN75 control-plane
```

Task 6.2 Verification

Initiate the IKEv1 IPsec tunnel from **TEST-PC-B**, and verify that it still works; send some traffic through the tunnel and confirm that the ACL hits on the ASA:

```
ASA34/pri/act# show access-list VLAN75_CONTROL_PLANE
access-list VLAN75_CONTROL_PLANE; 6 elements; name hash: 0x24bcaa3e
access-list VLAN75_CONTROL_PLANE line 1 extended permit udp 172.16.6.0 255.255.255.0 any eq isakmp (hitcnt=1) 0x0dd1
access-list VLAN75_CONTROL_PLANE line 2 extended permit udp 172.16.6.0 255.255.255.0 any eq 4500 (hitcnt=0) 0xd45cb1
access-list VLAN75_CONTROL_PLANE line 3 extended permit esp 172.16.6.0 255.255.255.0 any (hitcnt=1) 0xbe58a4f8

access-list VLAN75_CONTROL_PLANE line 4 extended deny udp any any eq isakmp (hitcnt=0) 0x892097cb
access-list VLAN75_CONTROL_PLANE line 5 extended deny udp any any eq 4500 (hitcnt=0) 0xf32e2a2f
access-list VLAN75_CONTROL_PLANE line 6 extended deny esp any any (hitcnt=0) 0x3bf76038
```

https://t.me/learningnets

Task 6.3 Solution

```
R6:

ip access-list extended RFC1918_ACL
 permit ip host 172.16.5.100 any
 deny ip 10.0.0.0 0.255.255.255 any log RFC1918_FILTER
 deny ip 172.16.0.0 0.15.255.255 any log RFC1918_FILTER
 deny ip 192.168.0.0 0.0.255.255 any log RFC1918_FILTER
 permit ip any any
!
ip access-list log-update threshold 1
!
interface FastEthernet0/1
 ip access-group RFC1918_ACL in
```

Task 6.3 Verification

Verify the ACL configuration:

```
R6#show ip access-lists RFC1918_ACL
Extended IP access list RFC1918_ACL
    10 permit ip host 172.16.5.100 any (2 matches)
    20 deny ip 10.0.0.0 0.255.255.255 any log (tag = RFC1918_FILTER)
    30 deny ip 172.16.0.0 0.15.255.255 any log (31 matches) (tag = RFC1918_FILTER)
    40 deny ip 192.168.0.0 0.0.255.255 any log (tag = RFC1918_FILTER)
    50 permit ip any any
!
!R6#show ip interface fastEthernet0/1 | i Inbound
 Inbound  access list is RFC1918_ACL
```

Task 6.4 Solution

```
ASA2:

logging timestamp
logging enable
logging buffer-size 65536
logging buffered debugging
```

https://t.me/learningnets

```
!
logging ftp-bufferwrap
logging ftp-server 180.1.46.99 / asalogging asapassword
!
logging list TRACK_DEFAULT_ROUTE message 622001
logging mail TRACK_DEFAULT_ROUTE
logging from-address asa2firewall@inelab.local
logging recipient-address admin@inelab.local level informational
smtp-server 180.1.46.99 180.1.46.100
```

Task 6.4 Verification

Verify logging configuration:

```
ASA2# show logging

Syslog logging: enabled
    Facility: 20 Timestamp logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled Buffer logging: level debugging, 32 messages logged
    Trap logging: disabled
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled Mail logging: list TRACK_DEFAULT_ROUTE, 0 messages logged

    ASDM logging: disabled
```

Task 6.5 Solution

```
ASA2:

access-list IM_TRAFFIC deny ip 180.1.34.0 255.255.255.0 180.1.46.0 255.255.255.0
access-list IM_TRAFFIC deny ip 180.1.46.0 255.255.255.0 180.1.34.0 255.255.255.0
access-list IM_TRAFFIC permit ip any any
!
class-map type inspect im match-any IM_PROTOCOL
 match protocol msn-im
 match protocol yahoo-im
!
class-map IM_CLASS
```

https://t.me/learningnets

```
 match access-list IM_TRAFFIC
!
policy-map type inspect im IM_POLICY
 class IM_PROTOCOL
  drop-connection log
!
policy-map global_policy
 class IM_CLASS
  inspect im IM_POLICY
```

Task 6.5 Verification

Verify the configuration:

```
ASA2# show service-policy inspect im


Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
    Class-map: IM_CLASS
      Inspect: im IM_POLICY, packet 0, drop 0, reset-drop 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
        class IM_PROTOCOL (match-any)
          Match: protocol msn-im , 0 packets
          Match: protocol yahoo-im , 0 packets
          drop-connection log, packet 0
```

Task 6.6 Solution

```
SW1 - SW6:

no mac address-table learning vlan 88
!
mac address-table static 0034.aa12.f0a1 vlan 88 drop
```

Task 6.6 Verification

https://t.me/learningnets

For example, verify the dynamic MAC address table of SW2 for VLAN 88, before applying the policy:

```
SW2#show mac address-table dynamic vlan 88

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  88    0000.0c07.ac00    DYNAMIC     Fa1/0/1
  88    001b.d58b.2196    DYNAMIC     Fa1/0/20
  88    001d.70df.2b75    DYNAMIC     Fa1/0/20
  88    0050.56a8.0802    DYNAMIC     Fa1/0/20
  88    48f8.b32e.2532    DYNAMIC     Fa1/0/20
  88    d48c.b5da.d549    DYNAMIC     Fa1/0/1
  88    d867.d9e0.bbc1    DYNAMIC     Fa1/0/2
Total Mac Addresses for this criterion: 7
```

Verify after applying the configuration:

```
SW2#show mac address-table dynamic vlan 88
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----SW2#
```

Verify that traffic to or from the specified MAC address will be silently dropped, for example on SW2:

```
SW2#show mac address-table static vlan 88 | e CPU
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    ----- 88    0034.aa12.f0a1    STATIC      Drop
Total Mac Addresses for this criterion: 21
!
!SW2#show platform forward fastEthernet 1/0/1 0034.aa12.f0a1 aaaa.aaaa.bbbb
Ingress:
Global Port Number: 3, lpn: 2 Asic Number: 0
Source Vlan Id: Real 88, Mapped 7. L2EncapType 0, L3EncapType 3
```

https://t.me/learningnets

```
Hashes: L2Src 0x02 L2Dst 0x0B L3Src 0x02 L3Dst 0x0B
 Lookup                    Key-Used                  Index-Hit    A-Data
Classify 68_00F0AAAA_AAAABBBB-00_00000034_AA12F0A1     017FC   00000000
InputACL 20_00F0AAAA_AAAABBBB-00_00000034_AA12F0A1     01FF8   01000000
L2LrnMsk FF_03FFFFFF_FFFFFFFF-00_000003FF_00000000
L2Learn  83_00070034_AA12F0A1-C3_00001C03_00000000     00E61   000000C7 Secure Port violation
L2FwdMsk FF_03FFFFFF_FFFFFFFF
L2Fwd    83_0007AAAA_AAAABBBB                          01820   00000044
Station Descriptor: 02FF0000, DestIndex: 0306, RewriteIndex: F007
Secure port violation. New destIndex is 0x02EA.

========================================
Egress: Asic 0, switch 1
        CPU queues: 14.
Source Vlan Id: Real 88, Mapped 7. L2EncapType 0, L3EncapType 3
portMap 0x0, non-SPAN portMap 0x0

Output Packets:
```

https://t.me/learningnets

CCIE Security v4 Technologies Workbook - CCIE Security V4 Lab Resources

Security Rack Rental and Hardware Guide

Click here for the Security V4.0 Rack Rental and Hardware Guides

https://t.me/learningnets