SENSS

Implementing Cisco Edge Network Security Solutions

Version 1.0 **Lab Guide**

Part Number: 97-3331-01

https://t.me/learningnets

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS" AND AS SUCH MAY INCLUDE TYPOGRAPHICAL, GRAPHICS, OR FORMATTING ERRORS. CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

©2014 Cisco Systems, I

https://t.me/learningnets

Table of Contents

Lab 2-1: Configure Control and Management Plane Security Controls	***L-5***
Visual Objective	L-6
Required Resources	L-6
Command List	L-6
Job Aids	L-8
Task 1: Configure Management Plane Security Controls on Cisco IOS Software	L-12
Task 2: Configure Management Plane Security Controls on Cisco ASA	L-23
Task 3: Configure Management Access AAA on Cisco IOS Software	L-34
Task 4: Configure Management Access AAA on Cisco ASA	L-38
Lab 2-2: Configure Traffic Telemetry Methods	***L-47***
Visual Objective	L-48
Required Resources	L-48
Command List	L-48
Job Aids	L-49
Task 1: Configure Traffic Telemetry Methods on Cisco IOS Software	L-53
Task 2: Configure Traffic Telemetry Methods on Cisco ASA	L-62
Lab 2-3: Configure Layer 2 Data Plane Security Controls	***L-75***
Visual Objective	L-76
Required Resources	L-76
Command List	L-76
Job Aids	L-77
Task 1: Configure DHCP Snooping	L-81
Task 2: Configure ARP Inspection	L-92
Lab 2-4: Configure Layer 3 Data Plane Security Controls	***L-99***
Visual Objective	L-100
Required Resources	L-100
Command List	L-100
Job Aids	L-101
Task 1: Configure uRPF on the Cisco IOS Router	L-105
Task 2: Configure uRPF on the Cisco ASA	L-108
Task 3: Configure IP Source Guard on the Cisco IOS Catalyst Switch	L-114
Lab 3-1: Configure Cisco ASA NAT	***L-119***
Visual Objective	L-120
Required Resources	L-120
Command List	L-120
Job Aids	L-120
Task 1: Configure Static NAT	L-124
Task 2: Configure Dynamic NAT	L-133
Task 3: (Optional) Configure Twice NAT	L-138
Lab 3-2: Configure Cisco IOS Software NAT	***L-149***

https://t.me/learningnets

Visual Objective L-150
Required Resources L-150
Command List L-150
Job Aids L-151
Task 1: Configure Static NAT L-155
Task 2: Configure Dynamic NAT L-158

Lab 4-1: Configure Basic Cisco ASA Access Policies L-163

Visual Objective L-164
Required Resources L-164
Command List L-165
Job Aids L-165
Task 1: Configure Object Groups L-169
Task 2: Configure Interface ACLs L-176
Task 3: Configure Global ACL L-182
Task 4: Verify Connectivity Across the ASA L-184

Lab 4-2: Configure Advanced Cisco ASA Access Policies L-199

Visual Objective L-200
Required Resources L-200
Command List L-200
Job Aids L-200
Task 1: Tune OSI Layer 3-4 Stateful Inspection L-204
Task 2: Examine Support for Dynamic Protocols L-215
Task 3: Configure Application Inspection for HTTP Traffic L-220
Task 4: Configure Application Inspection for FTP Traffic L-231

Lab 4-3: Configure Cisco ASA Botnet Traffic Filter L-241

Visual Objective L-242
Required Resources L-242
Command List L-242
Job Aids L-242
Task 1: Configure the Botnet Traffic Filter using Dynamic Database L-246
Task 2: Configure the Botnet Traffic Filter using Static Database L-257

Lab 4-4: Configure Cisco ASA Identity Firewall L-261

Visual Objective L-262
Required Resources L-262
Command List L-262
Job Aids L-263
Task 1: Configure Cisco CDA L-267
Task 2: Configure the Cisco ASA for Active Directory Integration L-275
Task 3: Configure the Cisco ASA with Identity Options L-277
Task 4: Configure the Cisco ASA Identity-Based Access Rules L-278

Lab 5-1: Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies L-293

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Visual Objective L-294
Required Resources L-294
Command List L-294
Job Aids L-295
Task 1: Configure Security Zones L-299
Task 2: Configure Access Control Between the INSIDE and OUTSIDE Zones L-300
Task 3: Configure Access Control Between the VPN and INSIDE Zones L-307
Task 4: Configure Access Control for Management Traffic Between the SELF and OUTSIDE Zones L-309

Lab 5-2: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies L-315

Visual Objective L-316
Required Resources L-316
Command List L-316
Job Aids L-317
Task 1: Configure HTTP Application-Layer Inspection L-321

Lab Answer Keys L-327

Lab 2-1: Configure Control and Management Plane Security Controls L-327
Lab 2-2: Configure Traffic Telemetry Methods L-331
Lab 2-3: Configure Layer 2 Data Plane Security Controls L-332
Lab 2-4: Configure Layer 3 Data Plane Security Controls L-333
Lab 3-1: Configure Cisco ASA NAT L-334
Lab 3-2: Configure Cisco IOS Software NAT L-334
Lab 4-1: Configure Basic Cisco ASA Access Policies L-335
Lab 4-2: Configure Advanced Cisco ASA Access Policies L-336
Lab 4-3: Configure Cisco ASA Botnet Traffic Filter L-337
Lab 4-4: Configure Cisco ASA Identity Firewall L-337
Lab 5-1: Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies L-337
Lab 5-2: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies L-340

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 2-1: Configure Control and Management Plane Security Controls

Activity Objective

The company Secure-X has a network topology as shown in the figure. The company recently hired a new Chief Security Officer that wants to secure control and management plane of network devices in the Secure-X headquarters network.

You are the network security engineer for the Secure-X network. The CSO tasked you with implementing suitable control and management plane security controls on the Cisco ASA and Cisco IOS Software router in order to harden both devices, and to implement secure management access with usage of cryptographically protected management protocols and authentication, authorization, and accounting capabilities.

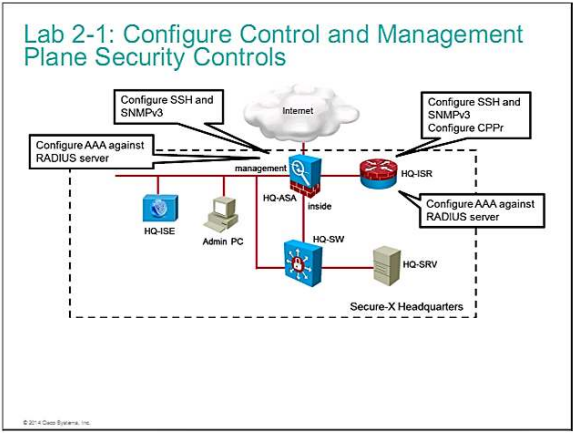
In this activity you will configure different control and management plane security controls:

- Enable SSH and SNMPv3 access, and Control Plane Policing on the Cisco IOS router
- Enable SSH and SNMPv3 access on the Cisco ASA
- Enable external AAA for management access on the Cisco IOS router
- Enable external AAA for management access on the Cisco ASA

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco IOS Commands

Command	Description
aaa accounting exec *name* **start-stop group radius**	Creates accounting method lists for exec attempts against a RADIUS server.
aaa authentication login *name* **group radius local**	Creates authentication method lists for login attempts against a RADIUS server and local database as backup.
aaa authorization exec *name* **group radius local**	Creates authorization method lists for exec attempts against a RADIUS server and local database as backup.
aaa new-model	Enables the authentication, authorization, and accounting (AAA) access control model.
accounting exec *name*	Applies accounting method list to lines.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command	Description
address ipv4 *ip_address* **auth-port 1645 acct-port 1646**	Adds RADIUS server to the RADIUS server group.
authorization exec *name*	Applies exec authorization method list to lines.
class *class_name*	Refers to a class map inside a policy map.
class-map *class_name*	Creates s class map.
control-plane host	Enter control plane host subinterface mode.
crypto key generate rsa modulus *modulus*	Generate RSA key pair.
ip access-list extended *acl_name*	Creates an extended ACL.
ip domain name *domain_name*	Configures domain name.
ip ssh version 2	Enables SSH version 2.
key *key*	Configures RADIUS preshared key for a RADIUS server.
line vty 0 1114	Enters VTY line configuration mode.
login authentication *name*	Applies authentication method list to lines.
login local	Enables local authentication in line configuration mode.
match access-group *acl_name*	Specifies matching criteria inside an class map.
permit *protocol source destination* **eq** *port*	Creates ACL permi statement.
police rate *rate* **bps burst** *burst_size* **bytes conform-action transmit exceed-action drop violate-action drop**	Applies policing action to a class map inside a policy map.
policy-map *policy_map_name*	Creates a policy map and enters policy map configuration mode.
radius server *group_name*	Creates a RADIUS server group.
service-policy input *policy_map_name*	Applies policy map.
show snmp user	Displays configured SNMP users.
show policy-map control-plane host	Displays operation of Control Plane Protection.
show processes cpu sorted	Displays CPU utilization by processes.
snmp-server contact *contact*	Configures SNMP contact.
snmp-server enable traps	Enables SNMP traps.
snmp-server group *group_name* **v3 priv**	Creates SNMPv3 group with priv security level.
snmp-server host *snmp_host* **version 3 priv** *username*	Configured SNMP host to send traps to.
snmp-server location *location*	Configures SNMP location.
snmp-server user *username group* **v3 auth sha** *password* **priv aes 128** *password*	Create SNMPv3 user.

https://t.me/learningnets

Command	Description
transport input ssh	Enables SSH on VTY lines.
username *username* **privilege** *level* **secret** *password*	Creates user account in the local user database.

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

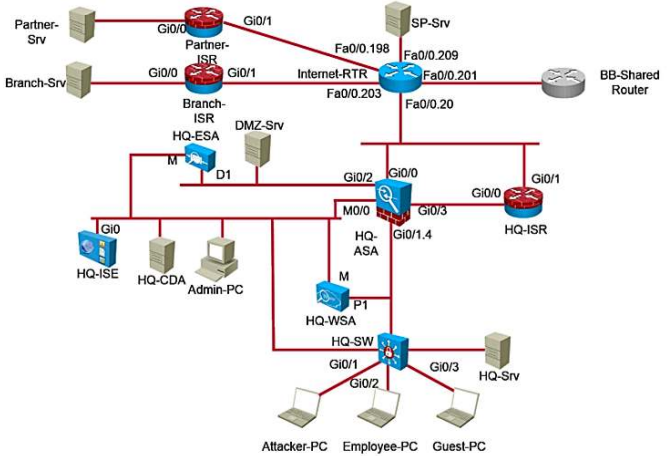
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

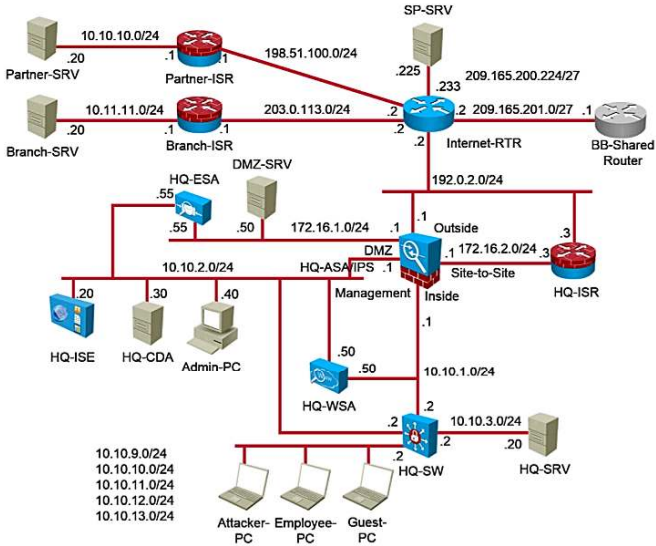
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

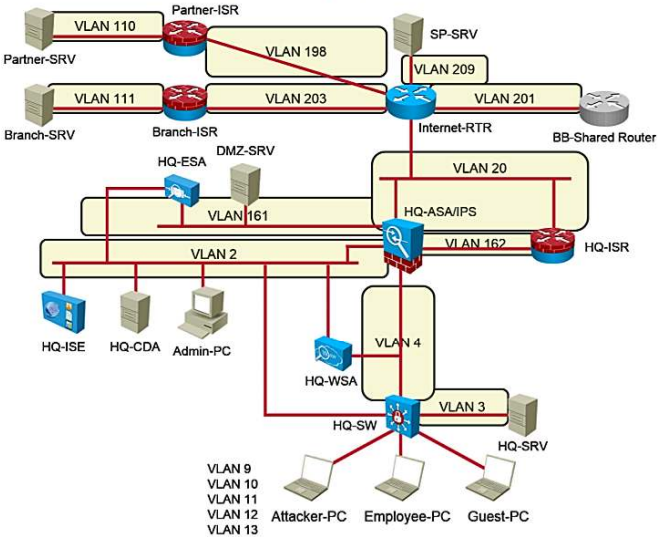
The figure shows the IP addresses that are used in this lab setup.



https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure Management Plane Security Controls on Cisco IOS Software

In this task you will protect the management plane on the Cisco IOS router. You will first enable SSH protocol with local authentication on the HQ-ISR router. Then, you will enable SNMPv3 with encryption and authentication on the HQ-ISR. Finally, you will rate limit traffic to protect control and management plane using Control Plane Protection feature.

Activity Procedure

Complete the following steps:

Step 1

Access the console of the HQ-ISR.

Step 2

Set the domain name on the router to **secure-x.local**. The hostname and domain name are used on the router to create a name for an RSA key pair.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

On the HQ-ISR router, create an RSA key pair with modulus 2048.

Step 4

On the HQ-ISR router, enable SSH version 2.

Step 5

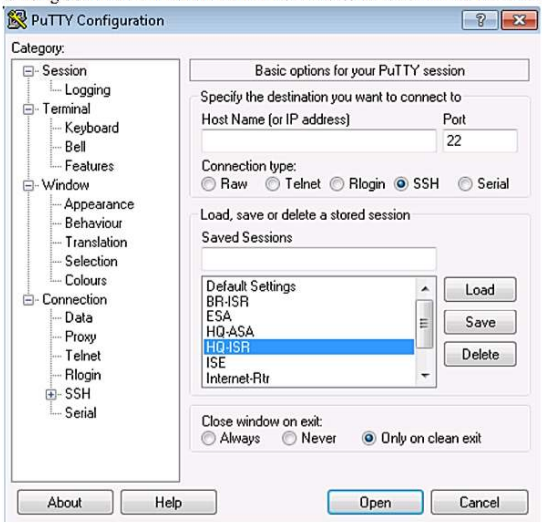
On the HQ-ISR router, create a local user with **admin** username, privilege level 15, and **Ci5coAdmin** password. This user will be used for local SSH authentication.

Step 6

On the HQ-ISR router, allow only SSH protocol on all VTY lines. Enable local authentication on all VTY lines.

Step 7

Access the Admin PC. Open the Putty by double-clicking the Putty icon on the desktop. Connect to the HQ-ISR at 172.16.2.3 using SSH. You can double-click the saved session to connect to the router.

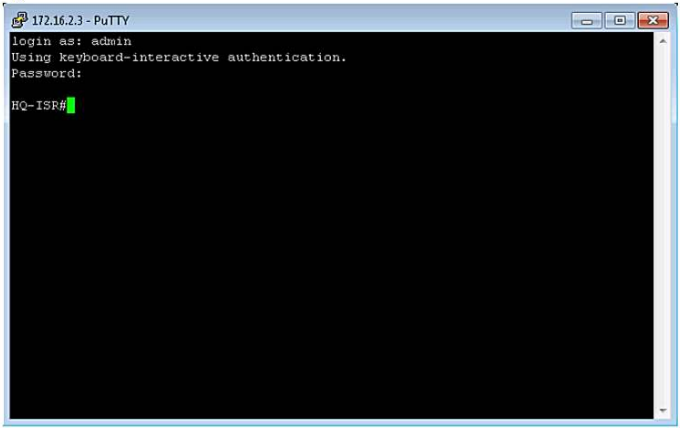


https://t.me/learningnets

Step 8

Accept the router's public key fingerprint by clicking **Yes** when you see the warning.

Log in using **admin** username and **Ci5coAdmin** password after you accepted the public key fingerprint. The SSH session with the router will establish. This verifies that the SSH access to the router is indeed working.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 9

Return to the console of the HQ-ISR router. In the next few steps you will enable SNMPv3 access.

Step 10

On the HQ-ISR router, configure a SNMP contact and SNMP location, as shown in the table:

SNMP Contact	Admin
SNMP Location	Secure-X HQ

Step 11

On the HQ-ISR router, configure a SNMPv3 group with Priv security model. Use **SECURE-X** as the name of the group.

Step 12

On the HQ-ISR router, configure a SNMPv3 user with the following parameters:

Username	admin
Group name	SECURE-X
SNMP Version	3
Authentication algorithm	SHA
Authentication key	Ci5coAdmin
Encryption algorithm	AES 128
Encryption key	Ci5coAdmin

Step 13

On the HQ-ISR router, configure the Admin PC at 10.10.2.40 as the SNMP server to send SNMP traps to and enable sending of traps. Use the following parameters:

SNMP server	10.10.2.40
SNMP Version	3
Username	admin

https://t.me/learningnets

Step 14

On the HQ-ISR router, display configured SNMP users. The output should look like this:

```
HQ-ISR# show snmp user
User name: admin
Engine ID: 800000090300B0FAEB64B388
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: SECURE-X
```

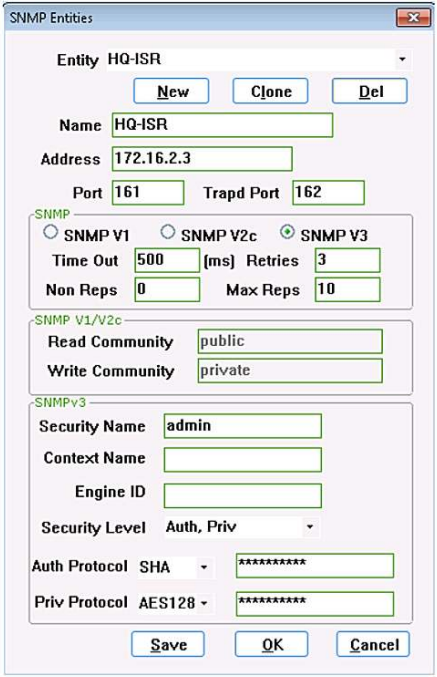

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 15

Return to the Admin PC. Open the HiliSoft MIB Browser by double-clicking the icon on the desktop. Navigate to **Tools > SNMP Entities**. Add the HQ-ISR router as SNMP entity with the following parameters:

Entity	HQ-ISR
Name	HQ-ISR
Address	172.16.2.3
SNMP Version	SNMP V3
Security Name (username)	admin
Security Level	Auth, Priv
Authentication protocol	SHA
Authentication key	Ci5coAdmin
Encryption protocol	AES 128
Encryption key	Ci5coAdmin

https://t.me/learningnets

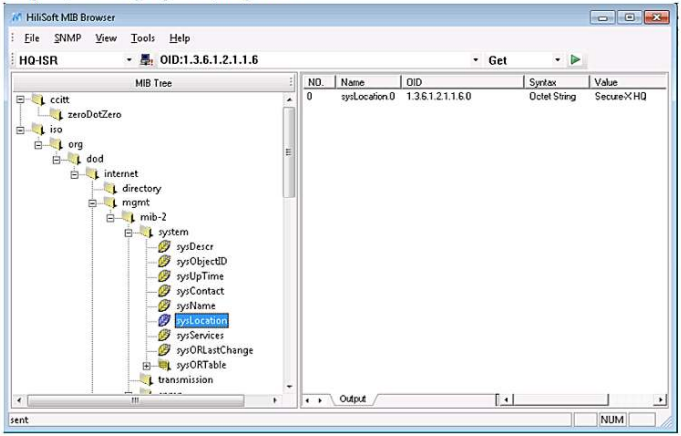


Click **Save** and **OK**.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 16

In the HiliSoft MIB Browser window, make sure that HQ-ISR is selected in the drop-down menu on the left. In the MIB Tree navigate to **iso > org > dod > internet > mgmt > mib-2 > system**. Select the **sysLocation** object. Select **Get** from the drop-down menu on the right and click the green "Play" button next to the drop-down menu. This procedure will obtain value of the sysLocation SNMP object from the router using SNMPv3. This step verifies that SNMPv3 access is working. You can also verify value of other SNMP objects, such as **sysUpTime**, or **sysName**.



Step 17

In the following steps, you will demonstrate how an attacker can overwhelm an SNMP enabled router with many SNMP requests. You will use the Attacker PC and the snmpwalk application to generate many SNMP requests that will overwhelm the HQ-ISR router's CPU.

Step 18

Access the Attacker PC. Open three terminal windows and use the snmpwalk program in all of them to walk through the entire SNMP management information base on the router. This action will overwhelm the router with SNMP requests.

```
root@attacker-pc:~# snmpwalk -v3 -l authPriv -u admin -a SHA -A Ci5coAdmin -x AES -X
Ci5coAdmin 172.16.2.3 1
```


https://t.me/learningnets

Step 19

Return to the console of the HQ-ISR router. Verify the CPU utilization. You should see that the SNMP process overwhelmed the CPU on the router, which may be unable to respond to legitimate requests on the control and management plane.

```
HQ-ISR# show processes cpu sorted
CPU utilization for five seconds: 94%/3%; one minute: 63%; five minutes: 57%
  PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
  257      267832      185679       1442 70.07% 35.54% 41.91%   0 SNMP ENGINE
  175       35732      364108         98  8.63%  9.91%  5.31%   0 IP SNMP
  251       25476      183488        138  6.39%  7.45%  3.97%   0 PDU DISPATCHER
  121       28704      347706         82  4.79%  5.34%  2.90%   0 IP Input
    6     1037128      174796       5933  0.47%  0.14%  0.11%   0 Check heaps
  128          92   135655264          0  0.23%  0.20%  0.15%   0 Ethernet Msec Ti
  179         116     4183233          0  0.07%  0.00%  0.00%   0 SSS Feature Time
    7           0       17851          0  0.00%  0.00%  0.00%   0 Pool Manager
    8           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
    9           0           2          0  0.00%  0.00%  0.00%   0 Timers
   10           0         620          0  0.00%  0.00%  0.00%   0 WATCH_AFS
```

Step 20

Return to the Attacker PC. Stop the snmpwalk on all three terminal windows by using the **CTRL-C** command sequence. Leave the terminal windows open as they will be used in a later step.

Step 21

On the HQ-ISR router, configure the following ACLs. These ACLs will be used to identify traffic going to the router's management and control plane to configure Control Plane Protection.

ACL Name	Protocol	Source IP Address	Destination IP Address	Destination Port
SSH_MGMT	TCP	Any	Any	22
SNMP_MGMT	UDP	Any	Any	161

Step 22

On the HQ-ISR router, configure the following class maps. These class maps will be used to classify traffic for Control Plane Protection.

Class Map Name	Match
SSH_MGMT	ACL Name: SSH_MGMT
SNMP_MGMT	ACL Name: SNMP_MGMT

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 23

On the HQ-ISR router, configure a policy map with name CPPR. This policy map will be used to apply policing actions to the previously configured traffic classes.

Class Name	Action
SSH_MGMT	Police to 64 kbs with 1500 B burst size
SNMP_MGMT	Police to 64 kbs with 1500 B burst size
Class-default	Police to 128 kbs with 1500 B burst size

Step 24

On the HQ-ISR router, apply the CPPR policy map to the host control plane subinterface.

Step 25

Return to the Attacker PC. Use the **snmpwalk** program again in all three terminal windows.

```
root@attacker-pc:~# snmpwalk -v3 -l authPriv -u admin -a SHA -A Ci5coAdmin -x AES -X
Ci5coAdmin 172.16.2.3 1
```

Step 26

Return to the console of the HQ-ISR router. Verify the CPU utilization again. You should see that the CPU utilization is very low due to the Control Plane Protection feature, which is policing SNMP traffic coming to the router.

```
HQ-ISR# show processes cpu sorted
CPU utilization for five seconds: 2%/0%; one minute: 1%; five minutes: 0%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   6     1046004      176272       5934  0.87%  0.14%  0.10%   0 Check heaps
 257      478764      226175       2116  0.31%  0.19%  0.05%   0 SNMP ENGINE
 175       45732      442762        103  0.23%  0.12%  0.03%   0 IP SNMP
 121       34724      401998         86  0.15%  0.07%  0.02%   0 IP Input
 128         144   136739381          0  0.15%  0.18%  0.17%   0 Ethernet Msec Ti
 251       32716      221851        147  0.15%  0.09%  0.02%   0 PDU DISPATCHER
  87         608     1079759          0  0.07%  0.02%  0.00%   0 Per-Second Jobs
 118        2552     2159044          1  0.07%  0.02%  0.00%   0 BPSM stat Proces
   9           0           2          0  0.00%  0.00%  0.00%   0 Timers
  10           0         672          0  0.00%  0.00%  0.00%   0 WATCH_AFS
```


https://t.me/learningnets

Step 27

On the HQ-ISR router, verify operation of Control Plane Protection. Observe number of matched packets in all classes.

```
HQ-ISR# show policy-map control-plane host
 Control Plane Host
  Service-policy input: CPPR
    Class-map: SSH_MGMT (match-all)
      19 packets, 1518 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name SSH_MGMT
      police:
          rate 64000 bps, burst 1500 bytes, peak-burst 1500 bytes
        conformed 19 packets, 1518 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps, violated 0000 bps
    Class-map: SNMP_MGMT (match-all)
      2515 packets, 452266 bytes
      5 minute offered rate 14000 bps, drop rate 3000 bps
      Match: access-group name SNMP_MGMT
      police:
          rate 64000 bps, burst 1500 bytes, peak-burst 1500 bytes
        conformed 2237 packets, 402202 bytes; actions:
          transmit
        exceeded 278 packets, 50064 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 14000 bps, exceeded 3000 bps, violated 0000 bps
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      police:
          rate 128000 bps, burst 1500 bytes, peak-burst 1500 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps, violated 0000 bps
```

Step 28

Return to the Attacker PC. Stop the snmpwalk on all three terminal windows by using the **CTRL-C** command sequence.

Activity Verification

No verification is needed in this task.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Task 2: Configure Management Plane Security Controls on Cisco ASA

In this task you will first protect the management plane on the Cisco ASA. You will first allow HTTPS and SSH access only from the Admin PC, using local authentication. Then, you will configure and verify SNMPv3 with encryption and authentication.

Activity Procedure

Complete the following steps:

Step 1

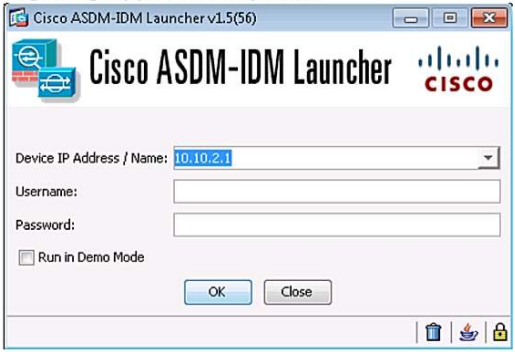
Access the console of the HQ-ASA.

Step 2

Enable HTTPS server on the HQ-ASA and enable Cisco ASDM access from the Admin PC at 10.10.2.40 through the management interface. After this step, you will be able to access the ASA using Cisco ASDM.

Step 3

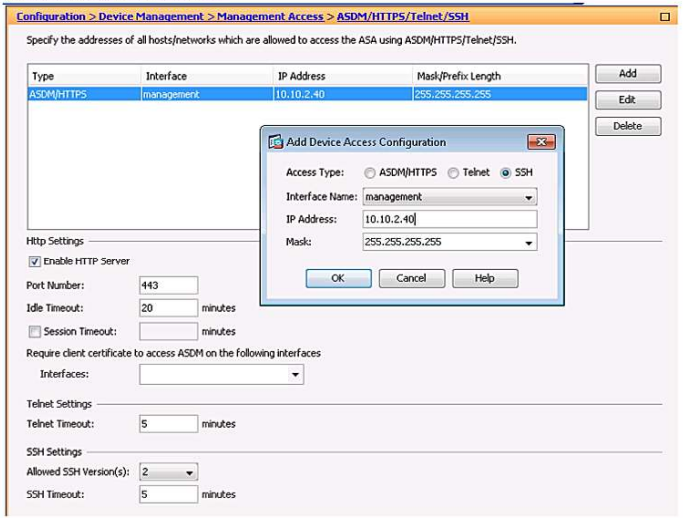
Return to the Admin PC. Start Cisco ASDM by double-clicking its icon on the desktop. Connect to the HQ-ASA at 10.10.2.1. Log in using empty username and password.



https://t.me/learningnets

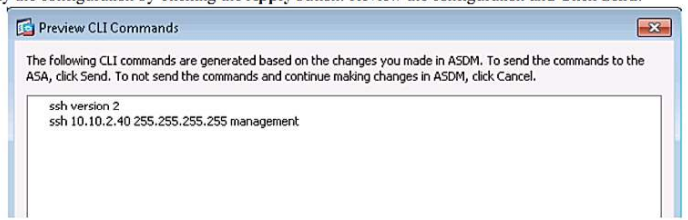
Step 4

In the Cisco ASDM, navigate to Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH. Allow SNMP access from the Admin PC at 10.10.2.40 through the management interface. Allow only SSH version 2.



Step 5

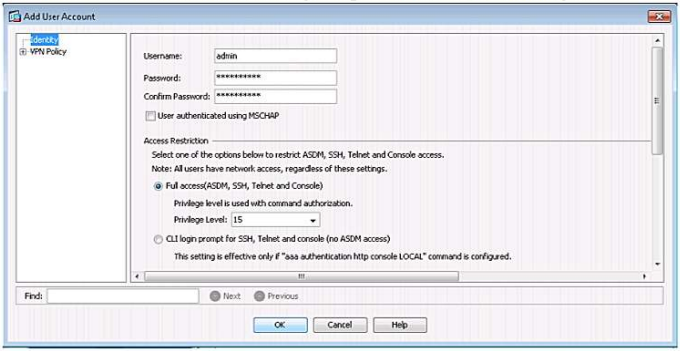
Apply the configuration by clicking the **Apply** button. Review the configuration and Click **Send**.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

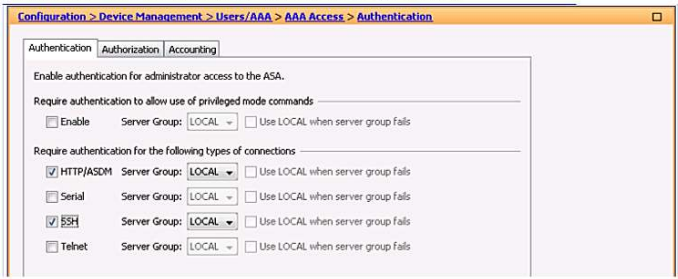
Step 6

In the Cisco ASDM, navigate to Configuration > Device Management > Users/AAA > User Accounts. Create local user account with **admin** username, privilege level 15, and **Ci5coAdmin** password.



Step 7

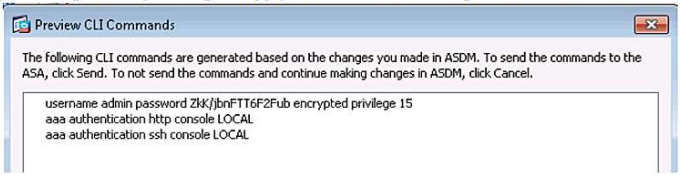
In the Cisco ASDM, navigate to Configuration > Device Management > Users/AAA > AAA Access > Authentication. Enable local authentication for SSH and ASDM access.



https://t.me/learningnets

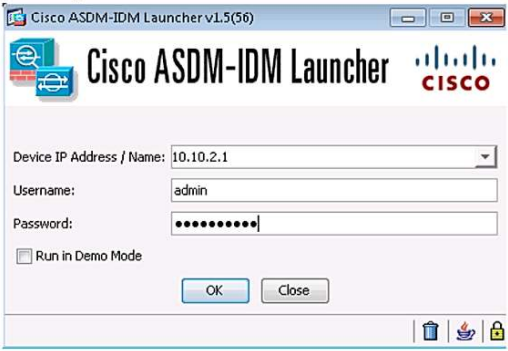
Step 8

Apply the configuration by clicking the **Apply** button. Review the configuration and Click **Send**.



Step 9

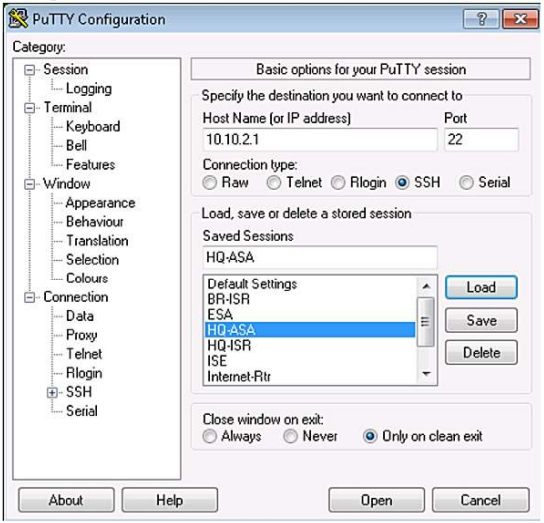
Close the existing ASDM session and open a new one. This time you are required to log in using **admin** username and **Ci5coAdmin** password.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 10

On the Admin PC, open the Putty by double-clicking the Putty icon on the desktop. Connect to the HQ-ASA at 10.10.2.1 using SSH. You can double-click the saved session to connect to the ASA.

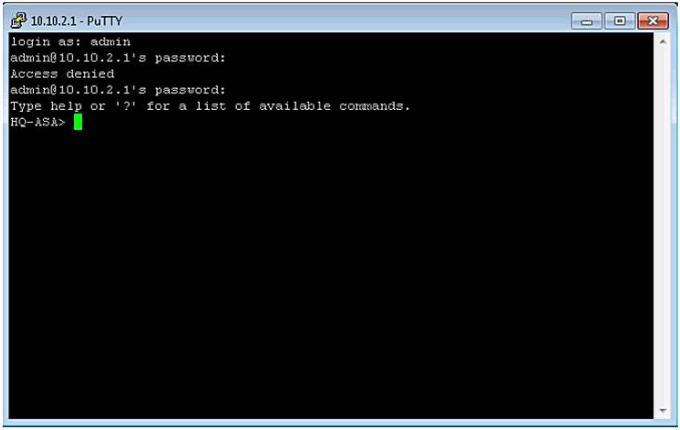


https://t.me/learningnets

Step 11

Accept the ASA's public key fingerprint by clicking **Yes** when you see the warning.

Log in using **admin** username and **Ci5coAdmin** password after you accepted the public key fingerprint. The SSH session with the ASA will establish. This verifies that the SSH access to the ASA is indeed working.



Step 12

In the Cisco ASDM, navigate to Configuration > Device Management > Management Access > SNMP. Configure a SNMP contact and SNMP location, as shown in the table:

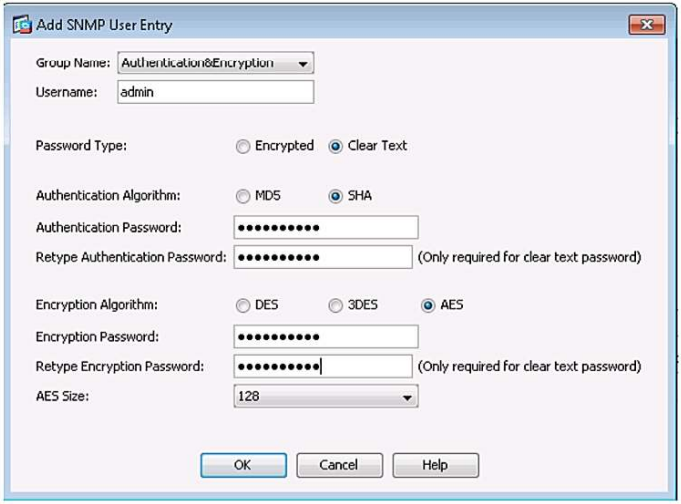
SNMP Contact	Admin
SNMP Location	Secure-X HQ

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 13

In the same Cisco ASDM window, click **Add** to add SNMPv3 user. Add the user with parameters as shown in the table:

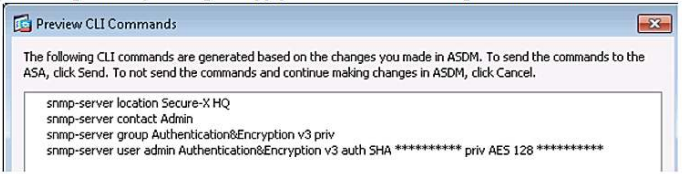
Username	admin
Group name	Authentication&Encryption
Authentication algorithm	SHA
Authentication key	Ci5coAdmin
Encryption algorithm	AES 128
Encryption key	Ci5coAdmin



https://t.me/learningnets

Step 14

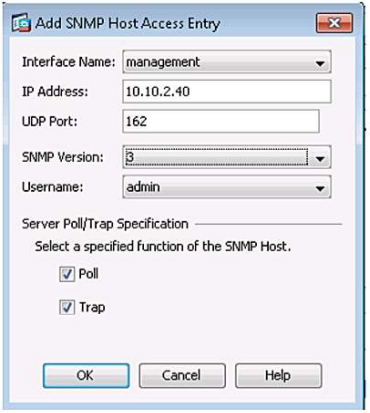
Apply the configuration by clicking the **Apply** button. Review the configuration and Click **Send**.



Step 15

In the same Cisco ASDM window, click **Add** to add SNMPv3 host. Add the Admin PC as the SNMP management station as shown in the table bellow:

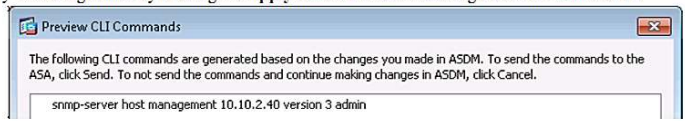
Interface	management
IP Address	10.10.2.40
SNMP Version	3
Username	admin



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 16

Apply the configuration by clicking the **Apply** button. Review the configuration and Click **Send**.



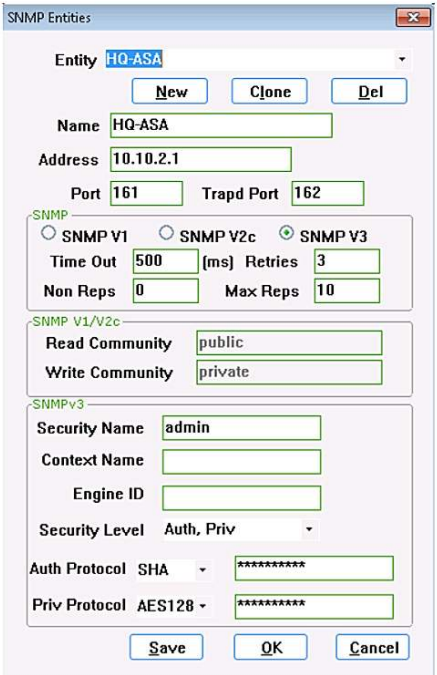
https://t.me/learningnets

Step 17

Return to the Admin PC. Open the HiliSoft MIB Browser if not already opened. Navigate to **Tools > SNMP Entities**. Add the HQ-ASA as SNMP entity with the following parameters:

Entity	HQ-ASA
Name	HQ-ASA
Address	10.10.2.1
SNMP Version	SNMP V3
Security Name (username)	admin
Security Level	Auth, Priv
Authentication protocol	SHA
Authentication key	Ci5coAdmin
Encryption protocol	AES 128
Encryption key	Ci5coAdmin

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

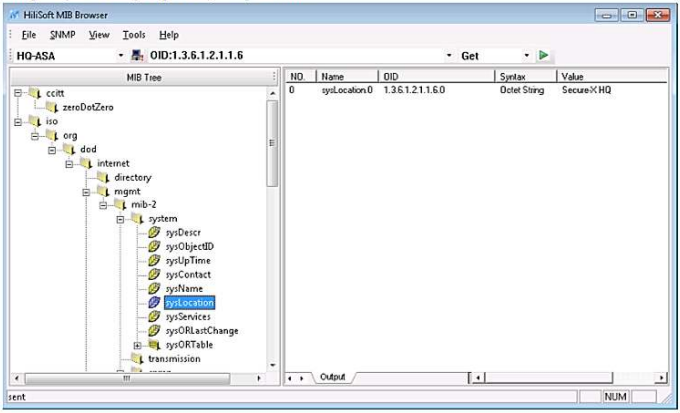


Click **Save** and **OK**.

https://t.me/learningnets

Step 18

In the HiliSoft MIB Browser window, make sure that HQ-ASA is selected in the drop-down menu on the left. In the MIB Tree navigate to **iso > org > dod > internet > mgmt > mib-2 > system**. Select the **sysLocation** object. Select **Get** from the drop-down menu on the right and click the green "Play" button next to the drop-down menu. This procedure will obtain value of the sysLocation SNMP object from the ASA using SNMPv3. This step verifies that SNMPv3 access is working. You can also verify value of other SNMP objects, such as **sysUpTime**, or **sysName**.



Activity Verification

You have completed this task when you attain this result:

Step 1

No verification is needed in this task.

Task 3: Configure Management Access AAA on Cisco IOS Software

In this task you will configure management access AAA on the HQ-ISR router against the external RADIUS server. The Cisco Identity Service Engine will be used as the RADIUS server, which has been preconfigured with policies and users to authenticate users when accessing the router. In the task, you will enable external authentication, exec authorization, and accounting on the router for SSH access.

Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

Access the console of the HQ-ISR.

Step 2

On the HQ-ISR router, enable the authentication, authorization, and accounting (AAA) access control model.

Step 3

On the HQ-ISR router, create a RADIUS server group named **MY-RADIUS**. Add HQ-ISE server at 10.10.2.20 to the server group as the RADIUS server. Use **cisco** as the preshared RADIUS key.

Step 4

On the HQ-ISR router, configure authentication method list for login attempts against the RADIUS server. Use the local database as backup. Use **MGMT_ACCESS** as the name for the method list.

Step 5

On the HQ-ISR router, configure authorization method list for exec attempts against the RADIUS server. Use the local database as backup. Use **MGMT_ACCESS** as the name for the method list.

Step 6

On the HQ-ISR router, configure accounting method list for exec attempts against the RADIUS server. Use **MGMT_ACCESS** as the name for the method list.

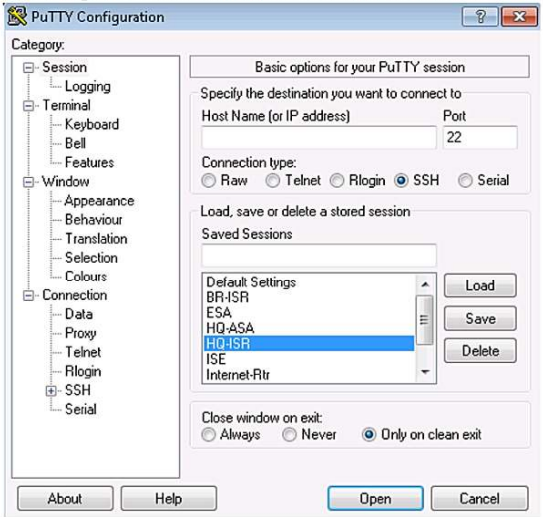
Step 7

On the HQ-ISR router, apply configured authentication, authorization, and accounting method lists to all VTY lines

https://t.me/learningnets

Step 8

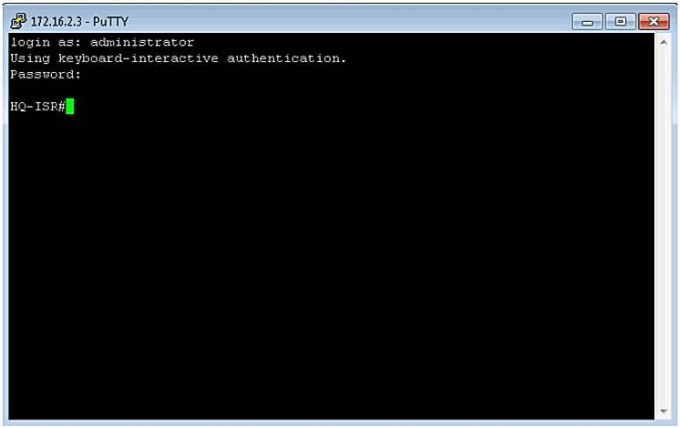
Return to the Admin PC. Open the Putty by double-clicking the Putty icon on the desktop. Connect to the HQ-ISR at 172.16.2.3 using SSH. You can double-click the saved session to connect to the router.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 9

Log in using **administrator** username and **Ci5coAdmin** password. This is the user account that has been preconfigured on the HQ-ISE RADIUS server. The user is configured with privilege level 15 and shell exec privileges. The SSH session with the router will establish.

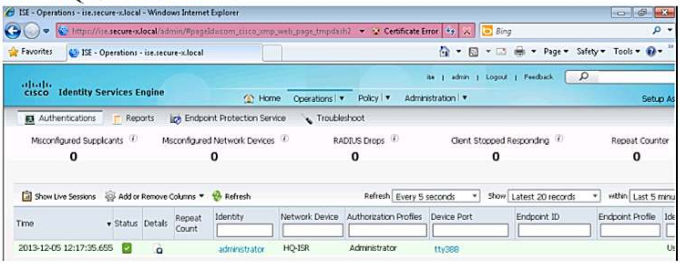


Step 10

On the Admin PC, open the Internet Explorer and navigate to Cisco ISE management web page at **https://ise.secure-x.local**. Login using **admin** username and **CI5coAdmin** password.

Step 11

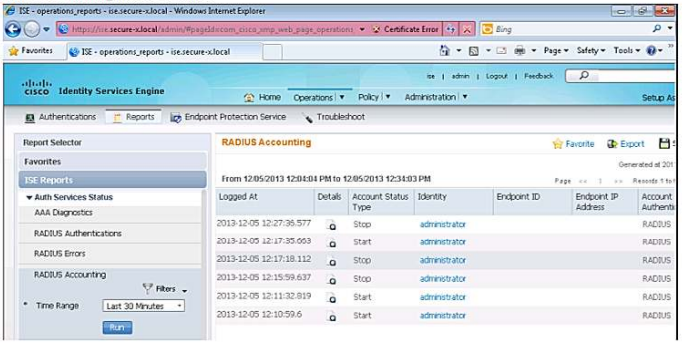
In the Cisco ISE user interface, navigate to **Operations > Authentications**. The page where you can monitor authentication requests, should be displayed. You should see one successful authentication request, sent from the HQ-ISR network device.



https://t.me/learningnets

Step 12

In the Cisco ISE user interface, navigate to **Operations > Reports > ISE Reports > Auth Services Status > RADIUS Accounting**. Run a report for the last 30 minutes. Examine the report. In the accounting report, you should see when **administrator** user accessed the HQ-ISR device, and when the user or the router terminated the management session.



Activity Verification

No verification is needed in this task.

Task 4: Configure Management Access AAA on Cisco ASA

In this task you will configure management access AAA on the HQ-ASA against the external RADIUS server. Similarly as in the previous task, Cisco Identity Service Engine will be used as the RADIUS server. In the task, you will enable external authentication, exec authorization, and accounting on the ASA for SSH access.

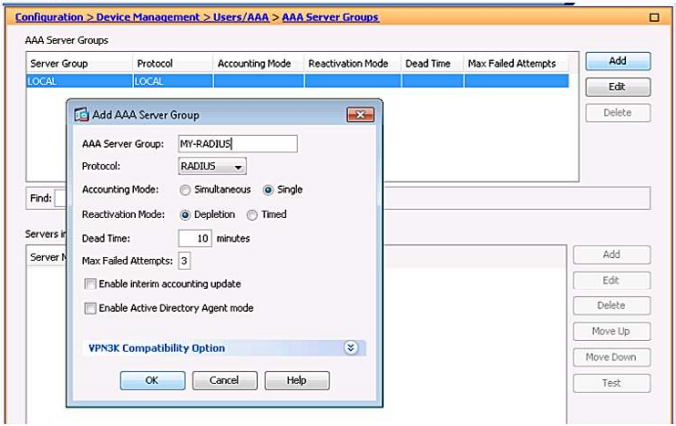
Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

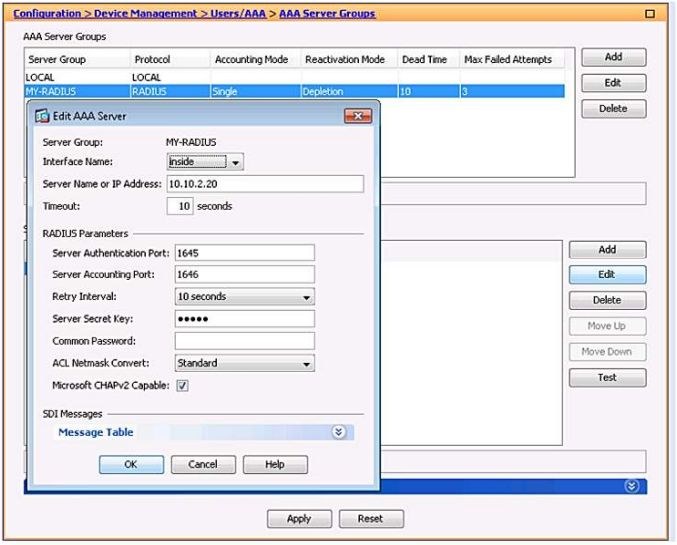
Return to the Cisco ASDM session on the Admin PC. Navigate to **Configuration > Device Management > Users/AAA > AAA Server Groups**. Click **Add** to add a server group. Add the RADIUS server group with name **MY-RADIUS**.



https://t.me/learningnets

Step 2

In the same Cisco ASDM window, select the configured AAA server group and click **Add** to add a server to the selected group. Add the HQ-ISE server at 10.10.2.20, accessible through the inside interface, as the RADIUS server. Use **cisco** as the RADIUS preshared key.



Step 3

Apply the configuration by clicking the **Apply** button. Review the configuration and Click **Send**.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 4

In the Cisco ASDM, navigate to **Configuration > Device Management > Users/AAA > AAA Access > Authentication**. Enable external authentication against the MY-RADIUS server group for SSH access. Use LOCAL group as backup.

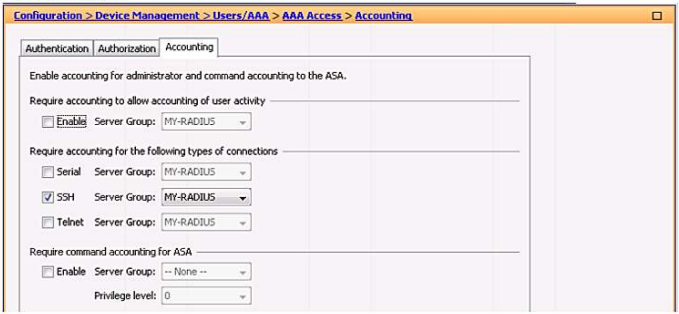
Step 5

In the Cisco ASDM, navigate to **Configuration > Device Management > Users/AAA > AAA Access > Authorization**. Enable external exec shell authorization against the external server.

https://t.me/learningnets

Step 6

In the Cisco ASDM, navigate to **Configuration > Device Management > Users/AAA > AAA Access > Accounting**. Enable accounting for SSH access. The accounting information should be sent to the MY-RADIUS server group.



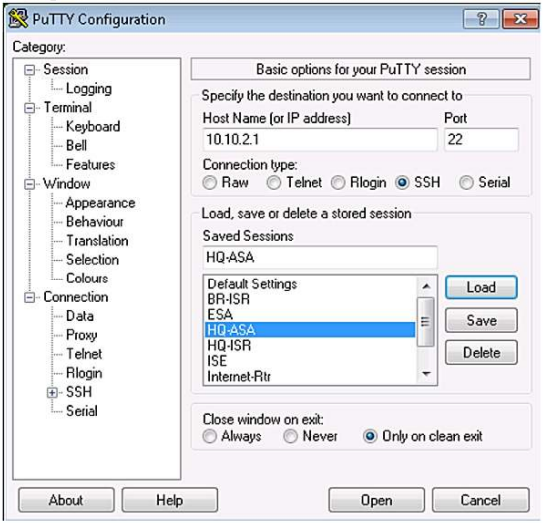
Step 7

Apply the configuration by clicking the **Apply** button. Review the configuration and Click **Send**.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 8

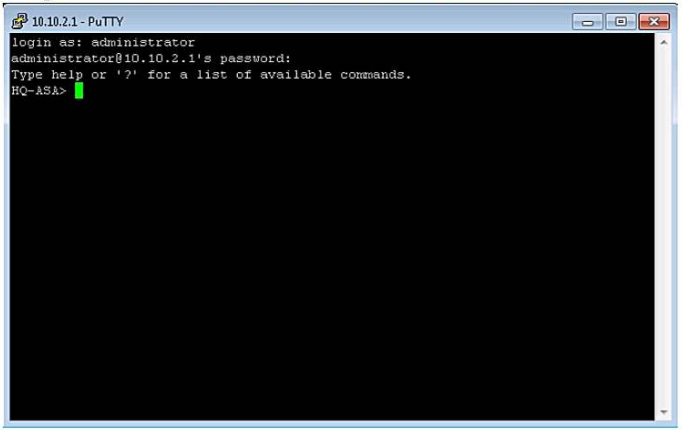
On the Admin PC, open the Putty by double-clicking the Putty icon on the desktop. Connect to the HQ-ASA at 10.10.2.1 using SSH. You can double-click the saved session to connect to the ASA.



https://t.me/learningnets

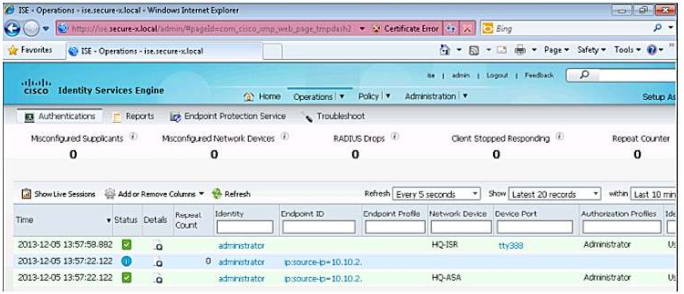
Step 9

Log in using **administrator** username and **Ci5coAdmin**. The SSH session with the ASA will establish.



Step 10

Return to the Cisco ISE user interface and navigate to **Operations > Authentications**. Now you should see another successful authentication request, sent from the HQ-ASA network device.



Step 11

In the Cisco ISE user interface, navigate to **Operations > Reports > ISE Reports > Auth Services Status > RADIUS Accounting**. Run a report for the last hour. This time, you should see accounting information for management session to both HQ-ISR and HQ-ASA devices.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Activity Verification

You have completed this task when you attain this result:

Step 1

No verification is needed in this task.

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 2-2: Configure Traffic Telemetry Methods

Activity Objective

The company Secure-X has a network topology as shown in the figure. The company recently hired a new Chief Security Officer that wants to get insight what is going on in the Secure-X network. The CSO knows that this can be achieved by configuring device and network event logging, and by exporting network flows using NetFLow to NetFlow collector. The CSO also requires that devices in the network have synchronized clock using NTP for better event correlation and readability.

You are the network security engineer for the Secure-X network. The CSO tasked you with implementing traffic telemetry methods in the network.

In this activity you will configure network telemetry methods on the Cisco IOS Software routers and on the Cisco ASA:

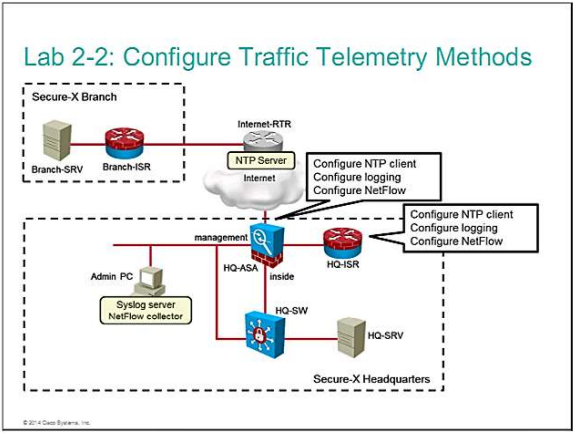
Configure NTP, logging, and NetFlow on the Cisco IOS router

Configure NTP, logging, and NetFlow on the Cisco ASA

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

Command List

The table describes the Cisco IOS Software commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco IOS Commands

Command	Description
clock timezone *timezone_name utc_offset*	Sets timezone.
destination *destination*	Configures NetFlow export destination.
export-protocol netflow-v9	Configures NetFlow export protocol.
exporter *exporter_name*	Specifies NetFlow exporter inside NetFlow monitor.
flow exporter *exporter_name*	Creates NetFlow exporter and enters configuration mode.
flow monitor *monitor_name*	Creates NetFlow monitor and enters configuration mode.
interface *interface*	Enters interface configuration mode.
ip flow monitor *monitor_name* **output**	Applies NetFlow monitor to an interface in outbound direction.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command	Description
logging buffered debugging	Enables logging of debugging messages to internal buffer.
logging host *ip_address*	Configures syslog server.
logging on	Globally enables logging.
logging trap debugging	Enables logging of debugging messages to a syslog server.
ntp authenticate	Enables NTP authentication.
ntp authentication-key *key_id* **md5** *key*	Specifies NTP authentication key.
ntp server *ip_address* **key** *key_id*	Configures NTP server.
ntp trusted-key *key_id*	Designates NTP authentication key as trusted.
record netflow ipv4 original-output	Defines NetFlow record inside NetFlow monitor.
show flow exporter statistics	Displays NetFlow data export statistics.
show flow monitor *monitor_name* **cache format table**	Displays content in a NetFlow monitor's cache.
show ntp associations [detail]	Displays status of NTP association.
show logging	Displays logging setup and content of the internal logging buffer.
transport udp *port*	Defines transport protocol in a NetFlow exporter.

The table describes the Cisco ASA commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco IOS Commands

Command	Description
show flow-export counters	Displays NetFlow runtime counters, including statistical data and error data.
show ntp associations [detail]	Displays status of NTP association.
show logging	Displays logging setup and content of the internal logging buffer.

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

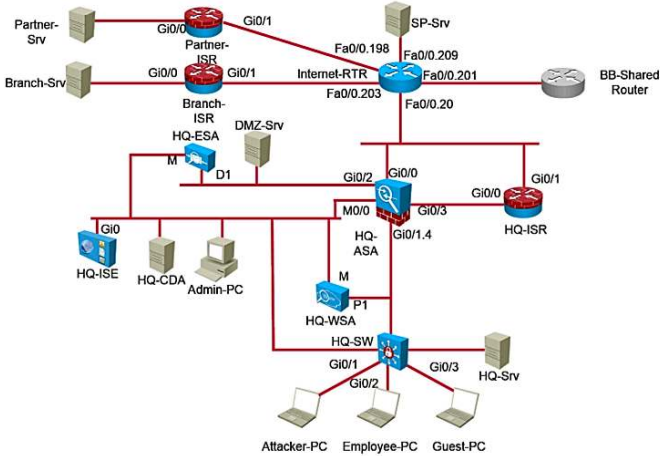
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

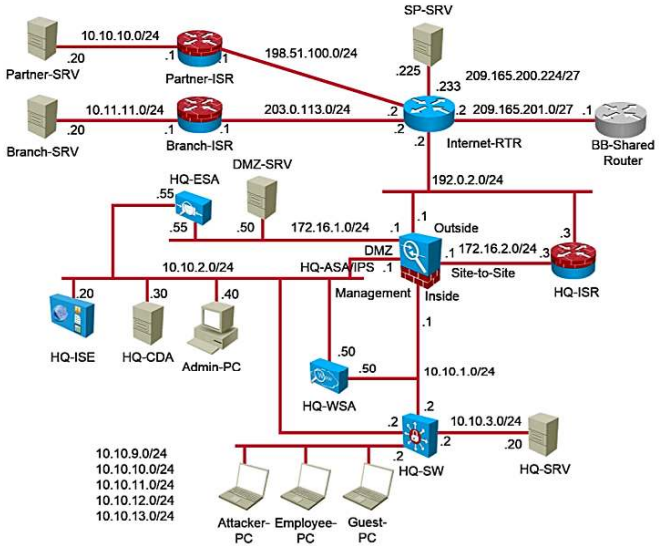
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



https://t.me/learningnets

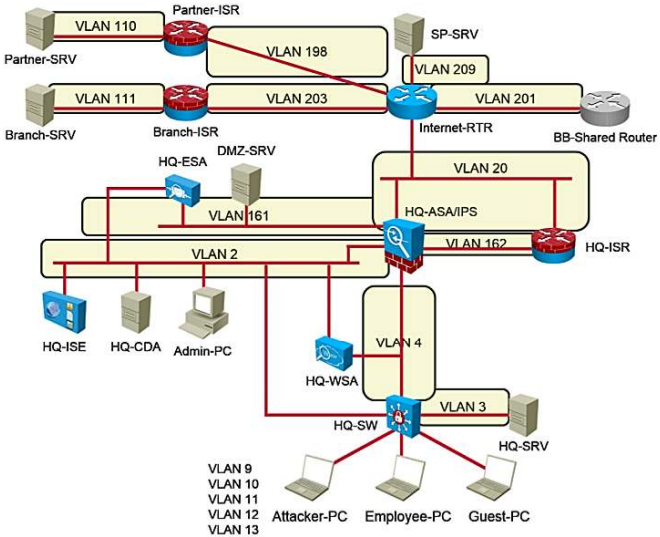
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure Traffic Telemetry Methods on Cisco IOS Software

In this task you will configure traffic telemetry methods on the Cisco IOS router. You will first make sure that clock is synchronized by configuring NTP client on the HQ-ISR router. Then, you will enable logging on the HQ-ISR router. Finally, you will configure flexible Netflow on the router to send information about flows to the NetFlow collector running on the Admin PC.

Activity Procedure

Complete the following steps:

Step 1

Access the console of the HQ-ISR.

Step 2

On the HQ-ISR router, set the time zone to the Pacific Standard Time zone (UTC/GMT -8 hours).

https://t.me/learningnets

Step 3

On the HQ-ISR router, configure authenticated NTP session with NTP server running on the Internet-RTR. Use the parameters as shown in the table. The NTP server has been preconfigured with clock and NTP settings.

NTP server	192.0.2.2
Authentication key ID	1
Authentication key	Ci5coAdmin

Step 4

On the HQ-ISR router, verify NTP association status. The clock should be synchronized to the NTP server. You should also see that stratum of the NTP server is 2.

```
HQ-ISR# show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~192.0.2.2       64.103.34.15     2    923   1024   377  1.549  -1.187  0.112
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Display also details about NTP association status. You will see that the NTP session is authenticated.

```
HQ-ISR# show ntp associations detail
192.0.2.2 configured, ipv4, authenticated, our_master, sane, valid, stratum 2
ref ID 64.103.34.15    , time D64C0E9F.A0966839 (00:51:43.627 PT Fri Dec 6 2013)
our mode client, peer mode server, our poll intvl 1024, peer poll intvl 1024
root delay 171.89 msec, root disp 0.97, reach 377, sync dist 103.35
delay 1.54 msec, offset -1.1870 msec, dispersion 0.11, jitter 0.03 msec
precision 2**16, version 4
assoc id 53125, assoc name 192.0.2.2
```

Note If clock is not synchronized, wait for a few minutes or proceed with the following steps and return to verification of NTP later.

Step 5

In the following steps, you will configure and verify logging on the HQ-ISR router.

Step 6

On the HQ-ISR router, make sure that logging is globally enabled.

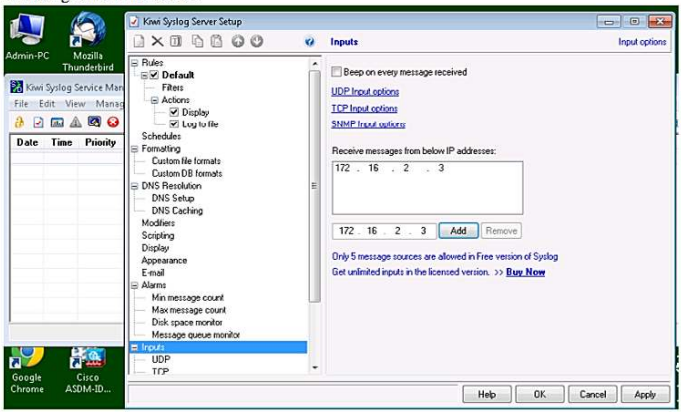
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 7

On the HQ-ISR router, enable logging of debugging events to the local buffer and syslog server on the Admin PC at 10.10.2.40.

Step 8

Access the Admin PC. Open the Kiwi Syslog Server Console by double-clicking the icon on the desktop. In the Kiwi Syslog Server Console, navigate to **File > Setup**. In the setup window, click the **Inputs** option in the menu on the left. Add the HQ-ISR router at 172.16.2.3 to the list on the right side to allow the server to receive messages from the router.

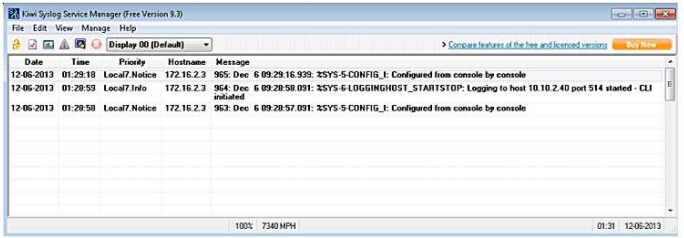


Click **OK**.

https://t.me/learningnets

Step 9

Return to the HQ-ISR router and trigger an event that will create logging message, for example enter and exit global configuration mode. Return to the Admin PC and observe the message in the Kiwi Syslog Server Console.



Seeing the message confirms that logging to the syslog server is working.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 10

On the HQ-ISR router, verify logging setup and content of the internal logging buffer. You should see a similar output:

```
HQ-ISR# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
    Console logging: level debugging, 4291 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 3338 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
No active filter modules.
    Trap logging: level debugging, 965 message lines logged
        Logging to 172.16.200.51  (udp port 514, audit disabled,
              link up),
              906 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging to 10.10.2.40  (udp port 514, audit disabled,
              link up),
              3 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:
Log Buffer (8192 bytes):
Dec  6 09:28:57.091: %SYS-5-CONFIG_I: Configured from console by console
Dec  6 09:28:58.091: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.10.2.40 port
514 started - CLI initiated
Dec  6 09:29:16.939: %SYS-5-CONFIG_I: Configured from console by console
```

Step 11

In the following steps, you will configure and verify flexible NetFlow on the HQ-ISR router.

https://t.me/learningnets

Step 12

On the HQ-ISR router, configure NetFlow exporter with the following parameters:

NetFlow exporter name	MY_EXPORTER
Destination	10.10.2.40
Transport	UDP 9996
Export protocol	NetFlow v9

Step 13

On the HQ-ISR router, configure NetFlow monitor with the following parameters:

NetFlow monitor name	MY_MONITOR
Record	IPv4 Original Output
Exporter	MY_EXPORTER

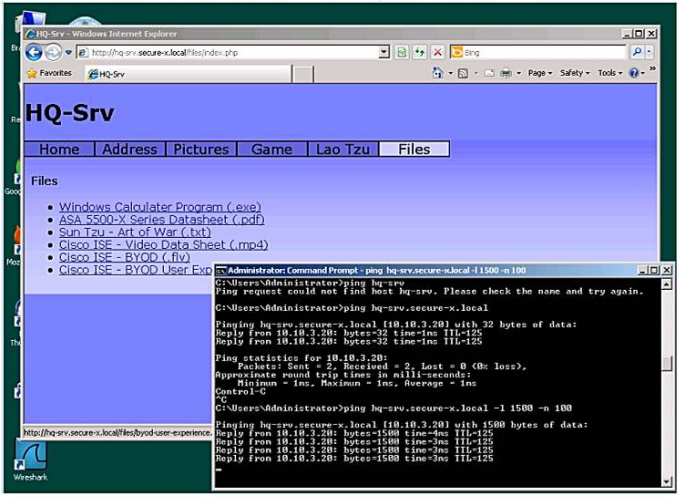
Step 14

On the HQ-ISR router, apply the configured NetFlow monitor to the GigabitEthernet0/0 interface in the outbound direction:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

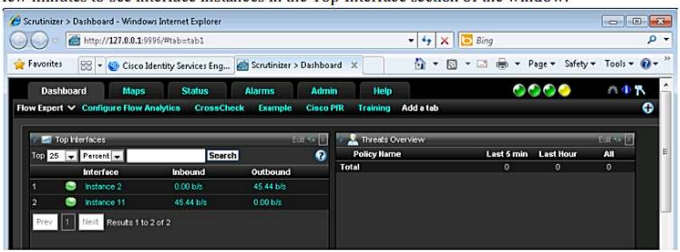
Step 15

Before verifying NetFlow, you have to trigger some traffic to flow over the HQ-ISR router over the GigabitEthernet0/0 interface in the outbound direction. Access the Branch-SRV, and open a web browser. Navigate to the web page of the HQ-SRV at **http://hq-srv.secure-x.local** and download some files from the web page or view videos that are available in the **Files** menu on the web page. At the same time, ping the HQ-SRV using many 1500 bytes long packets. IPsec VPN is established between the Secure-X headquarters and branch office in order to allow connectivity between the offices.



Step 16

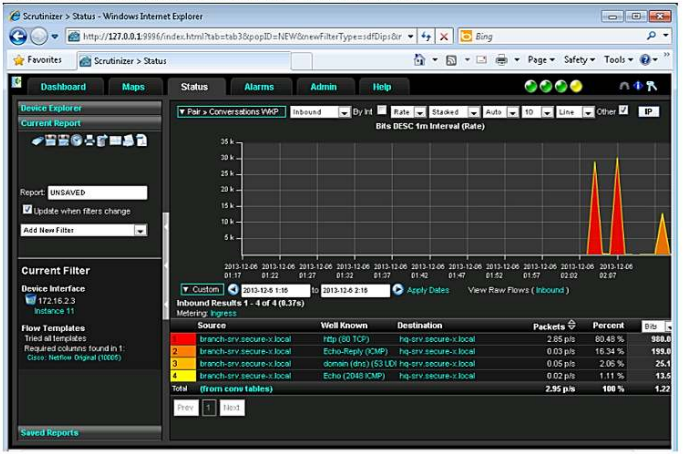
Return to the Admin PC. Open the Scrutinizer by double-clicking the icon on the desktop. Scrutinizer is a NetFlow collector software. If prompted to log in, use a username of **admin** and password of Ci5coAdmin. Wait few minutes to see interface instances in the Top Interface section of the window.



https://t.me/learningnets

Step 17

In the Top Interfaces section of the Scrutinizer, click the second interface instance. Another browser window should display where you can examine traffic flows across the router. You should see ICMP, HTTP, and DNS traffic flows between HQ-SRV and Branch-SRV.



Step 18

Return to the console of the HQ-ISR router. Verify NetFlow data export statistics. You should see non-zero numbers in the output, which means that flows are exported to the collector.

```
HQ-ISR# show flow exporter statistics
Flow Exporter MY_EXPORTER:
  Packet send statistics (last cleared 02:03:58 ago):
    Successfully sent:         231                    (26552 bytes)
  Client send statistics:
    Client: Flow Monitor MY_MONITOR
      Records added:           248
        - sent:                248
      Bytes added:             13144
        - sent:                13144
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 19

On the HQ-ISR router, show the content in the MY_MONITOR monitor's cache. You should see HTTP, DNS and ICMP flows between HQ-SRV and Branch-SRV.

```
HQ-ISR# show flow monitor MY_MONITOR cache format table
  Cache type:                               Normal
  Cache size:                                 4096
  Current entries:                               9
  High Watermark:                               21
  Flows added:                                 283
  Flows aged:                                  274
    - Active timeout      (  1800 secs)          0
    - Inactive timeout    (    15 secs)        274
    - Event aged                                 0
    - Watermark aged                             0
    - Emergency aged                             0
IPV4 SRC ADDR    IPV4 DST ADDR    TRNS SRC PORT  TRNS DST PORT  INTF OUTPUT
 FLOW SAMPLER ID  IP TOS  IP PROT  ip src as  ip dst as   ipv4 next hop addr
 ipv4 src mask  ipv4 dst mask  tcp flags  intf input  bytes   pkts
 time first   time last
================================================================================
10.11.11.20      10.10.3.20             0           2048         Gi0/0
       0           0x00      1          0           0          172.16.2.1
 /24             /24              0x00       Tu0        4900    49
 03:56:15.828  03:57:03.820
10.11.11.20      10.10.3.20             0            0         Gi0/0
       0           0x00      1          0           0          172.16.2.1
 /24             /24              0x00       Tu0       71932    98
 03:56:15.828  03:57:03.820
10.11.11.20      10.10.3.20          1059            80         Gi0/0
       0           0x00      6          0           0          172.16.2.1
 /24             /24              0x1B       Tu0       84076  2041
 03:56:53.340  03:57:01.676
10.11.11.20      10.10.3.20         62082            53         Gi0/0
       0           0x00     17          0           0          172.16.2.1
 /24             /24              0x00       Tu0         189     3
 03:56:53.948  03:56:55.956
10.11.11.20      10.10.3.20         60569            53         Gi0/0
       0           0x00     17          0           0          172.16.2.1
 /24             /24              0x00       Tu0         189     3
 03:56:57.064  03:56:59.080
10.11.11.20      10.10.3.20          1060            80         Gi0/0
       0           0x00      6          0           0          172.16.2.1
 /24             /24              0x1E       Tu0         450     5
 03:57:01.676  03:57:01.680
10.11.11.20      10.10.3.20         57213            53         Gi0/0
       0           0x00     17          0           0          172.16.2.1
 /24             /24              0x00       Tu0         189     3
 03:57:02.044  03:57:04.068
10.11.11.20      10.10.3.20          1061            80         Gi0/0
       0           0x00      6          0           0          172.16.2.1
 /24             /24              0x1E       Tu0         579     6
 03:57:02.100  03:57:02.108
10.11.11.20      10.10.3.20          1062            80         Gi0/0
       0           0x00      6          0           0          172.16.2.1
 /24             /24              0x1E       Tu0         672     8
 03:57:02.100  03:57:02.108
```


https://t.me/learningnets

Activity Verification

No verification is needed in this task.

Task 2: Configure Traffic Telemetry Methods on Cisco ASA

In this task you will configure traffic telemetry methods on the Cisco ASA. Similarly as in the previous task, you will first make sure that clock is synchronized by configuring NTP client on the HQ-ASA. Then, you will enable logging on the HQ-ASA. Finally, you will configure Netflow (NSEL) on the HQ-ASA to send information about flows to the NetFlow collector running on the Admin PC.

Activity Procedure

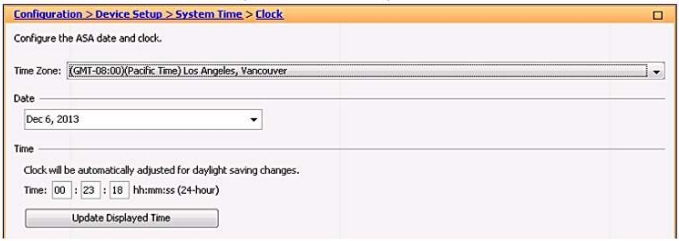
Complete the following steps:

Step 1

Access the Admin PC. Start the Cisco ASDM and connect to the HQ-ASA at 10.10.2.1. Log in using **admin** as the username and **Ci5coAdmin** as the password.

Step 2

In the Cisco ASDM, navigate to **Configuration > Device Setup > System Time > Clock**. Set the time zone to the Pacific Standard Time zone (UTC/GMT -8 hours).

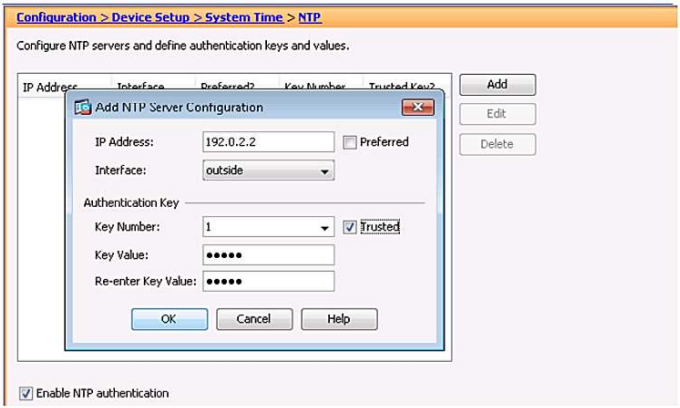


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

In the Cisco ASDM, navigate to **Configuration > Device Setup > System Time > NTP**. Enable NTP authentication and configure authenticated NTP session with NTP server running on the Internet-RTR. Use the parameters as shown in the table.

NTP server	192.0.2.2
Interface	outside
Authentication key ID	1
Authentication key	Ci5coAdmin



Step 4

Apply the configuration by clicking the **Apply** button. Review the configuration and Click **Send**.

https://t.me/learningnets

Step 5

Access the console of the HQ-ASA and verify NTP association status. The clock should be synchronized to the NTP server. You should also see that stratum of the NTP server is 2.

```
HQ-ASA# show ntp associations
      address         ref clock     st  when  poll reach  delay  offset    disp
*~192.0.2.2       64.103.34.15      2    25  1024  377     1.3   -0.45    15.9
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Display also details about NTP association status. You will see that the NTP session is authenticated.

```
HQ-ASA# show ntp associations detail
192.0.2.2 configured, authenticated, our_master, sane, valid, stratum 2
ref ID 64.103.34.15, time d64c41c0.7229e2a1 (04:29:52.445 PST Fri Dec 6 2013)
our mode client, peer mode server, our poll intvl 1024, peer poll intvl 1024
root delay 187.50 msec, root disp 4.24, reach 377, sync dist 114.502
delay 1.27 msec, offset -0.4453 msec, dispersion 15.88
precision 2**16, version 3
```

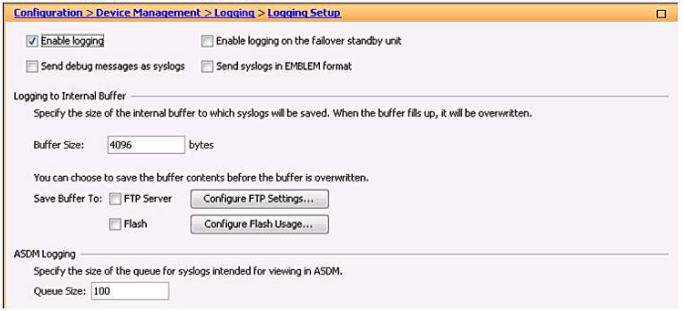
Note If clock is not synchronized, wait for a few minutes or proceed with the following steps and return to verification of NTP later.

Step 6

In the following steps, you will configure and verify logging on the HQ-ASA.

Step 7

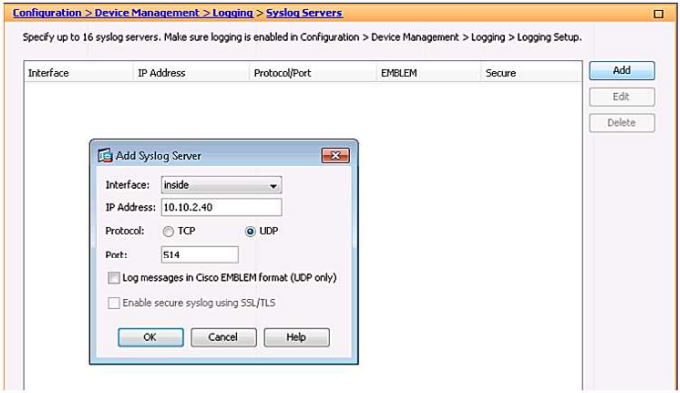
In the Cisco ASDM, navigate to **Configuration > Device Management > Logging > Logging Setup**. Make sure that logging is enabled globally.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 8

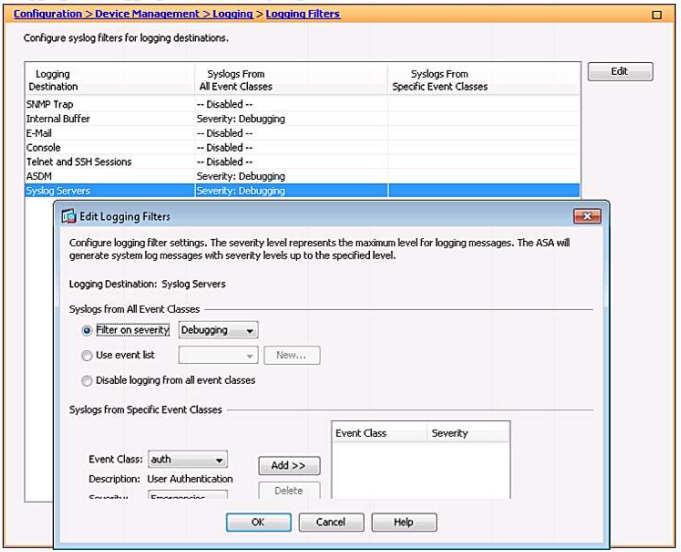
In the Cisco ASDM, navigate to **Configuration > Device Management > Logging > Syslog Servers**. Add the Admin PC at 10.10.2.40 as the syslog server. The server is accessible through the inside interface. Use the default UDP port for transport.



https://t.me/learningnets

Step 9

In the Cisco ASDM, navigate to **Configuration > Device Management > Logging > Logging Filters**. Enable logging of debugging events to the syslog server, ASDM, and internal buffer.



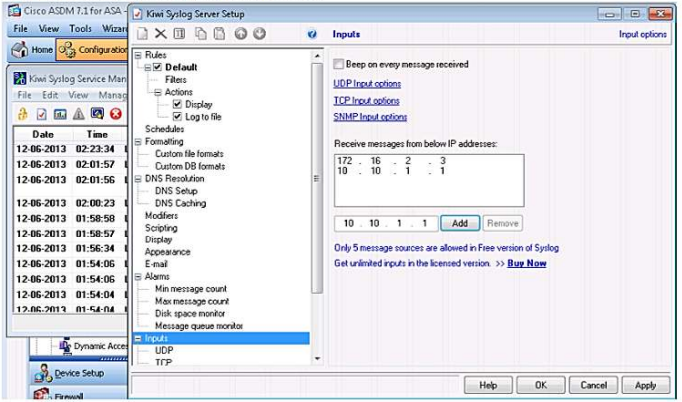
Step 10

Apply the configuration by clicking the **Apply** button. Review the configuration and Click **Send**.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 11

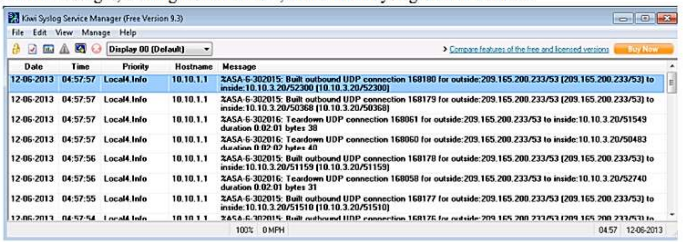
On the Admin PC, open the Kiwi Syslog Server Console by double-clicking the icon on the desktop if it is not already opened. In the Kiwi Syslog Server Console, navigate to **File > Setup**. In the setup window, click the **Inputs** option in the menu on the left. Add the HQ-ASA at 10.10.1.1 to the list on the right side to allow the server to receive messages from the ASA.



Click **OK**.

Step 12

Observe the messages, coming from the ASA, in the Kiwi Syslog Server Console.



Seeing the messages confirms that logging to the syslog server is working.

https://t.me/learningnets

Step 13

Access the HQ-ASA console and verify logging setup and content of the internal logging buffer. You should see a similar output:

```
HQ-ASA# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 347770 messages logged
    Trap logging: level debugging, facility 20, 701827 messages logged
        Logging to inside 10.10.2.40
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level debugging, 357997 messages logged
down UDP connection 170135 for outside:209.165.200.233/53 to inside:10.10.3.20/52445
duration 0:02:03 bytes 79
%ASA-6-302016: Teardown UDP connection 170137 for outside:209.165.200.233/53 to
inside:10.10.3.20/51493 duration 0:02:01 bytes 32
%ASA-6-302016: Teardown UDP connection 170269 for DMZ:172.16.1.55/50922 to inside:
10.10.3.20/53 duration 0:00:03 bytes 60
<output omitted>
```

Step 14

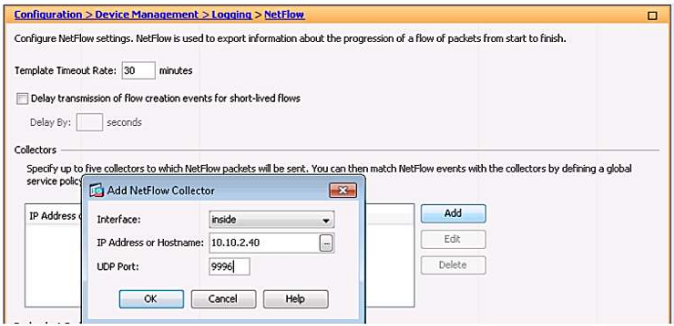
In the following steps, you will configure and verify NetFlow on the HQ-ASA.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 15

Return to the Cisco ASDM session on the Admin PC and navigate to **Configuration > Device Management > Logging > NetFlow**. Add NetFlow collector using the following parameters:

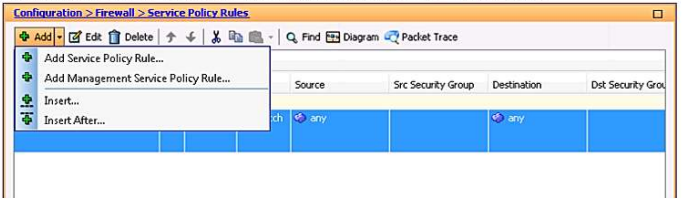
IP address	10.10.2.40
Interface	inside
Port	9996



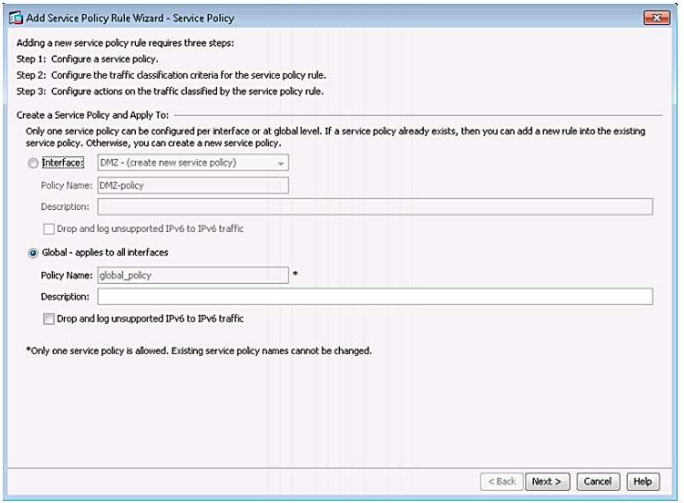
https://t.me/learningnets

Step 16

In this step, you will use Cisco ASA Modular Policy Framework to enable sending of traffic flows to the NetFlow collector. In the Cisco ASDM, navigate to **Configuration > Firewall > Service Policy Rules**. Select the configured traffic class **inspection_default** and click **Add > Insert After**.

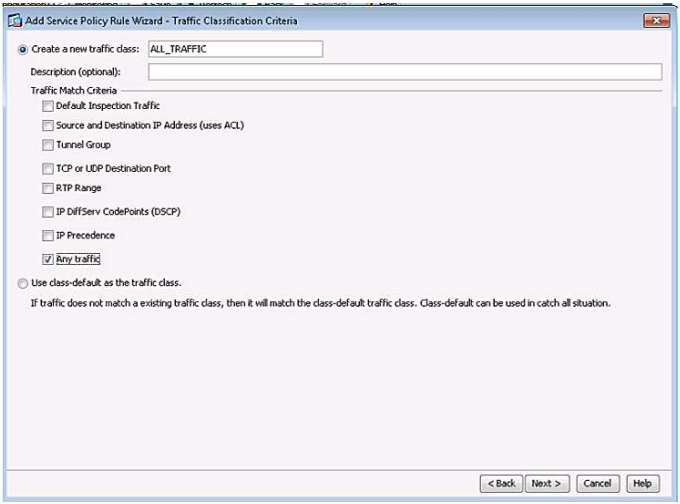


The Add Service Policy Rule Wizard window will display. Make sure that **Global - applies to all interfaces** radio button is selected and click **Next**.

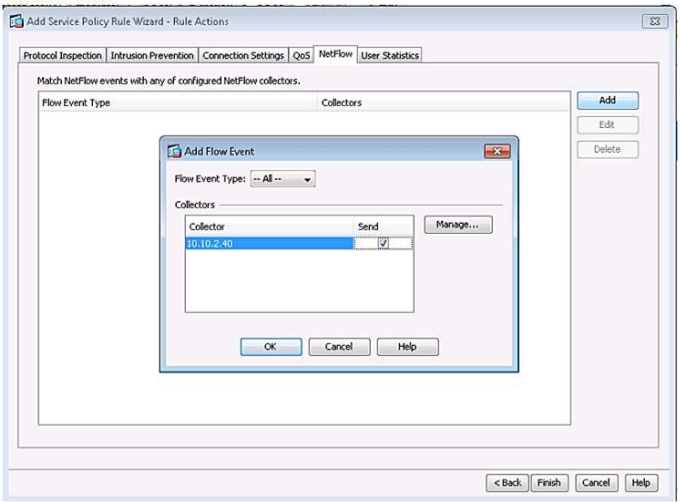


In the next window, create new traffic class with name **ALL_TRAFFIC** and use **Any traffic** checkbox as matching criteria. Click **Next**.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

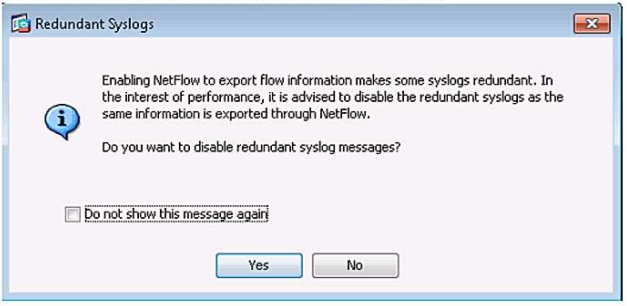


In the next window, select the **NetFlow** tab and add the previously configured collector to send flows to. Click **OK** and **Finish**.



https://t.me/learningnets

When prompted to disable redundant syslog logging messages, click **No**.

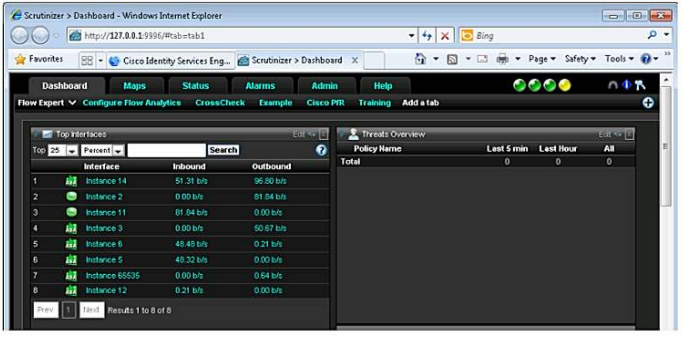


Step 17

Apply the configuration by clicking the **Apply** button. Review the configuration and Click **Send**.

Step 18

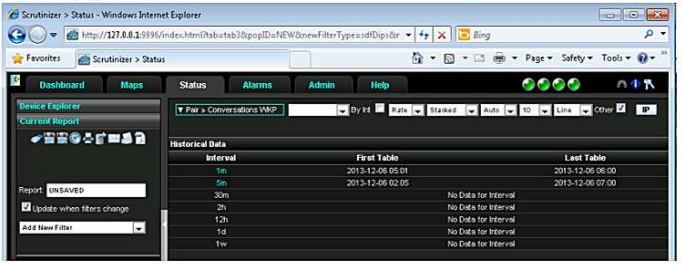
On the Admin PC, open the Scrutinizer by double-clicking the icon on the desktop, if not already opened. Wait few minutes and then refresh the Scrutinizer web page. You should see ASA interface instances in the Top Interfaces section of the Scrutinizer.



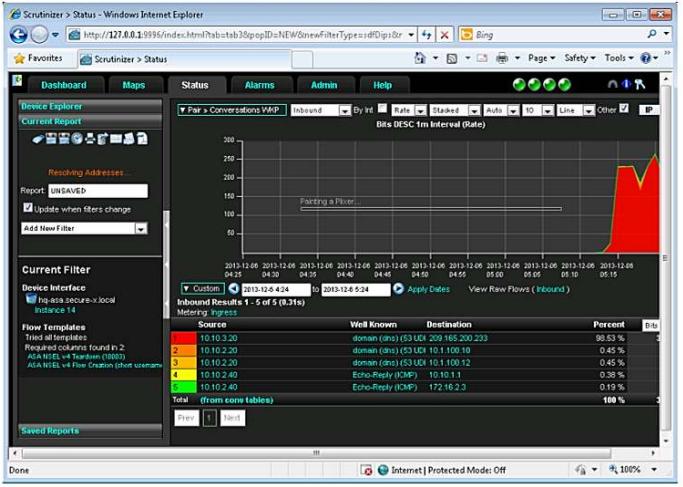
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 19

In the Top Interfaces section of the Scrutinizer, click the first ASA interface instance. Another browser window will display.



Click the **1m** link in the Interval column of the table. Another browser window will display where you can examine traffic flows across the HQ-ASA. You should see at least ICMP and DNS traffic flows.



https://t.me/learningnets

Step 20

Return to the console of the HQ-ASA. Verify NetFlow runtime counters, including statistical data and error data. You should see non-zero numbers in the output, which means that flows are exported to the collector.

```
HQ-ASA# show flow-export counters
destination: inside 10.10.2.40 9996
  Statistics:
    packets sent                                        181
  Errors:
    block allocation failure                              0
    invalid interface                                     0
    template send failure                                 0
    no route to collector                                 0
    source port allocation failure                        0
```

Activity Verification

No verification is needed in this task.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lab 2-3: Configure Layer 2 Data Plane Security Controls

Activity Objective

The company Secure-X has a network topology as shown in the figure. The company recently hired a new Chief Security Officer that wants to improve all of the current network security controls with the latest technologies to support the most recent company security policy.

You are the network security engineer for the Secure-X network. The Secure-X headquarters network has been experiencing layer 2 type attacks recently. The CSO tasked you with implementing suitable security controls to mitigate such attacks in the future.

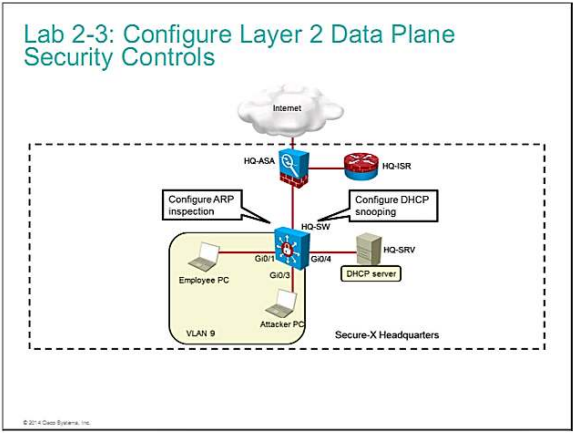
In this activity you will configure layer 2 network infrastructure protection features on Cisco IOS switches:

- Configure DHCP snooping to prevent DHCP server spoofing attacks
- Configure ARP inspection to mitigate ARP spoofing attacks

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco IOS Commands

Command	Description
interface range *interface-range*	Enters interface range configuration mode.
ip arp inspection limit rate *rate*	Tunes the ARP rate limit.
ip arp inspection trust	Configures interswitch links to other ARP-inspecting switches or router-switch links as trusted.
ip arp inspection vlan *vlan-range*	Enables ARP inspection in a specific VLAN.
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping database *location*	Configures the DHCP snooping binding database agent.
ip dhcp snooping limit rate *rate*	Configures a DHCP request rate limit on untrusted ports.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command	Description
ip dhcp snooping trust	Configures the DHCP server ports as trusted and configures interswitch links as trusted if DHCP snooping is deployed on the neighboring switch or if the DHCP server is reachable over other switches.
ip dhcp snooping vlan *vlan-list*	Enables DHCP snooping in a specific VLAN.
show ip arp inspection	Displays the overall status of ARP inspection.
show ip arp inspection *interface*	Displays the ARP inspection interface status.
show ip dhcp snooping	Displays the overall status of DHCP snooping.
show ip dhcp snooping binding	Displays the mappings in the binding database.
show ip dhcp snooping database	Displays the operation of the mapping database.
switchport port-security	Enables port security.
switchport port-security maximum *maximum_mac_addresses*	Sets maximum number of MAC addresses on a switchport.

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

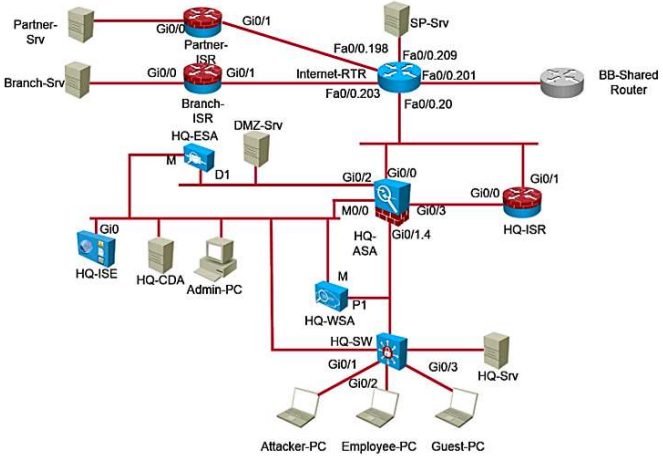
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

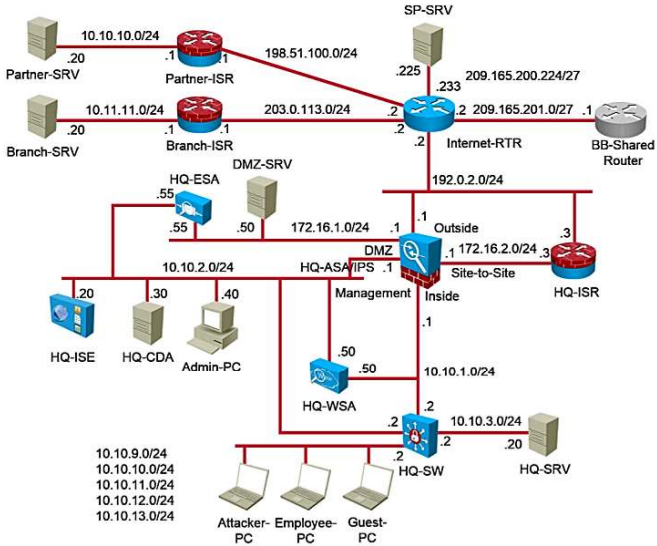
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



https://t.me/learningnets

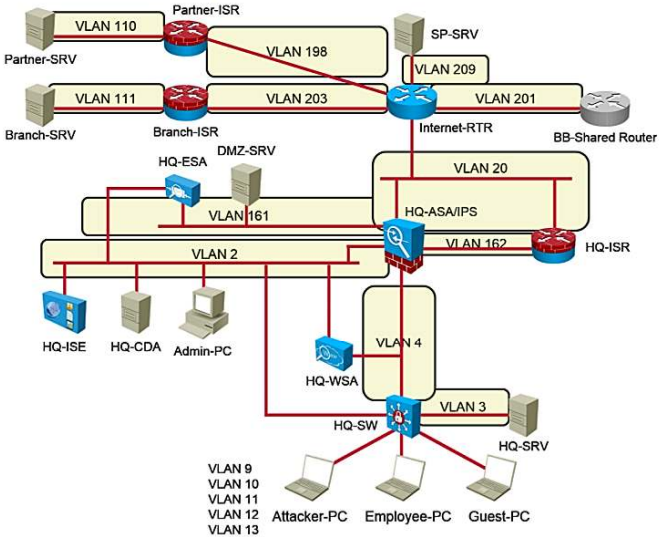
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure DHCP Snooping

DHCP snooping is a security feature which is available on the Cisco switches to protect from DHCP attacks. It validates DHCP messages received from untrusted sources and filters out invalid messages, rate-limits DHCP traffic from untrusted sources, and builds a DHCP binding table which can be used for other security features. In this task, you will first demonstrate how to perform a DHCP spoofing attack using the Attacker PC. Then you will enable and verify DHCP snooping feature on the switch in the Secure-X network to prevent DHCP attacks.

Activity Procedure

Complete the following steps:

Step 1

Access the Attacker PC.

Step 2

On the Attacker PC, start the terminal window.

https://t.me/learningnets

Step 3

On the Attacker PC, verify an IP address on an interface.

```
root@attacker-pc:~# ifconfig
eth2      Link encap:Ethernet  HWaddr a0:36:9f:1a:b2:b3
          inet addr:10.10.9.19  Bcast:10.10.9.255  Mask:255.255.255.0
          inet6 addr: fe80::a236:9fff:fe1a:b2b3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19400 errors:0 dropped:0 overruns:0 frame:0
          TX packets:237070051 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2181610 (2.0 MiB)  TX bytes:67801762963 (63.1 GiB)
          Memory:d2500000-d2600000
<output omitted>
```

Write down the IP address of the Ethernet interface because it will be used in the later step.

Note	Your Ethernet interface identifier and IP address may differ from the one in the output.

Step 4

On the Attacker PC, verify if the forwarding of IP packets is enabled. The value "1" means that IP forwarding is enabled, and the value "0" means that IP forwarding is disabled.

```
root@attacker-pc:~#cat /proc/sys/net/ipv4/ip_forward
0
```

Step 5

If the forwarding of IP packets is disabled, enable it by using the following command. This way, the Attacker PC will forward received IP packets to make sure that the victims of DHCP spoofing attack will not be aware of the attack.

```
root@attacker-pc:~# echo 1 >> /proc/sys/net/ipv4/ip_forward
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

On the Attacker PC, start a rogue DHCP server using the following command (replace the x with the IP address of the Attacker PC):

```
root@attacker-pc:~# dnsmasq -d -F 10.10.9.100,10.10.9.200,255.255.255.0,1d --dhcp-
option=3,10.10.9.x --dhcp-option=15,"secure-x.local" --dhcp-option=6,10.10.9.x -p 0
```

This command will start rogue DHCP server on the Attacker PC using the following parameters:

IP address pool: 10.10.9.100-10.10.9.200

Network mask: 255.255.255.0

Lease time: 1 day

Default gateway: 10.10.9.x

DNS server: 10.10.9.x

Domain name: secure-x.local

Step 7

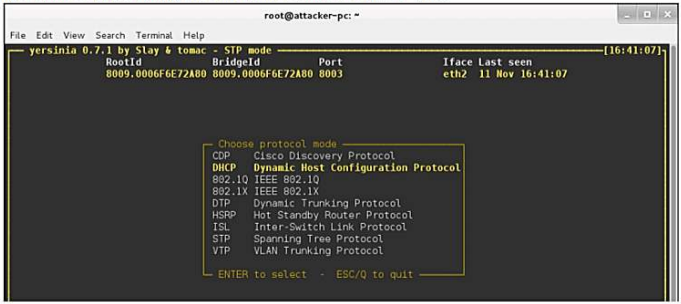
Open another terminal window on the Attacker PC. Start the Yersinia tool using the following command:

```
root@attacker-pc:~#yersinia -I
```

This command will start the Yersinia tool in the interactive mode. The tool can be used to perform different spoofing attacks.

Step 8

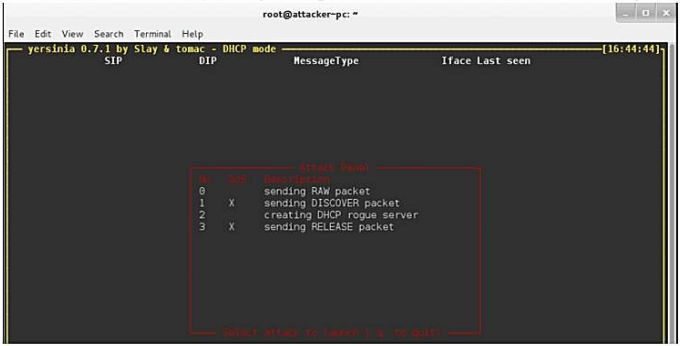
In the Yersinia tool, press the **G** key. This will invoke a menu. Select **DHCP Dynamic Host Configuration Protocol** using the **Up/Down** arrows and press **Enter**.



https://t.me/learningnets

Step 9

In the Yersinia tool, press the **x** key, then the **1** key. This will perform an exhaustion attack against the legitimate DHCP server on the HQ-SRV by sending a continuous stream of DHCP DISCOVER packets.



The Attacker PC will send many DHCP DISCOVER packets to the DHCP server, using a spoofed MAC address each time. The DHCP server's pool of IP address will quickly exhaust and valid DHCP requests will be unanswered.

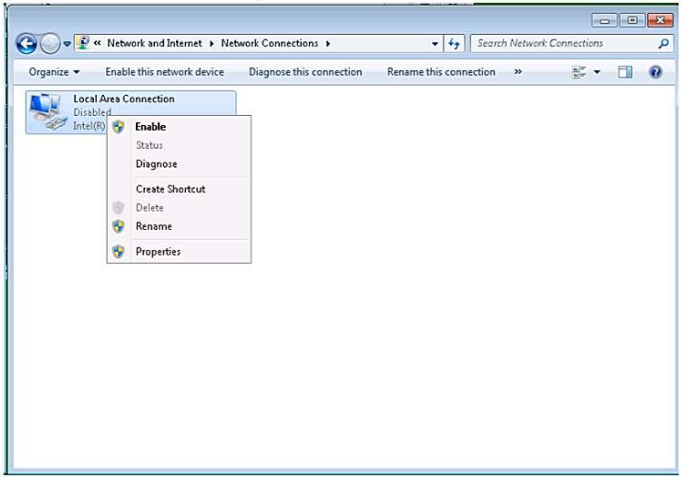
Step 10

Access the Employee PC. Log in using **SECURE-X\it1** username and **cisco** password. Navigate to **Control Panel\Network and Internet\Network Connections**.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 11

On the Employee PC, right-click the **Local Area Connection** adapter and disable it and enable it back. The PC will obtain the IP address automatically.



Step 12

On the Employee PC, open a command prompt. Verify IP settings using the **ipconfig** command.

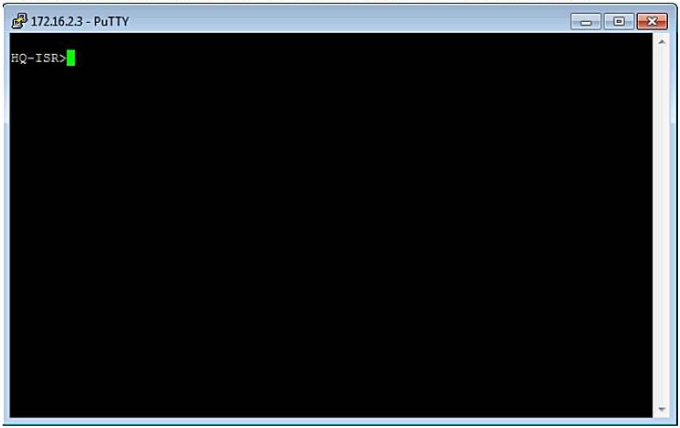
```
C:\Users\it1>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . : secure-x.local
   Link-local IPv6 Address . . . . . : fe80::1926:99f3:1417:bf09%15
   IPv4 Address. . . . . . . . . . . : 10.10.9.113
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.9.19
Tunnel adapter isatap.secure-x.local:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : secure-x.local
Tunnel adapter 6TO4 Adapter:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

You should see that the PC received IP settings from the rogue DHCP server running on the Attacker PC. The default gateway and DNS server are both set to the IP address of the Attacker PC, which will cause the Employee PC to sent all traffic over the Attacker PC, where it can be intercepted and examined using a packet capture tool such as Wireshark.

https://t.me/learningnets

Step 13

On the Employee PC, open a Putty client by double-clicking its icon on the desktop. Connect to the HQ-ISR at 172.16.2.3 switch using Telnet. This way you will test that the PC indeed has a connectivity even though traffic flows through the Attacker PC, as indicated by the default gateway settings.



Step 14

In the next few steps you will mitigate the DHCP spoofing attack by enabling DHCP snooping on the HQ-SW switch. Access the switch console.

Step 15

On the HQ-SW switch, enable console logging.

Enter the following commands on the HQ-SW switch:

```
HQ-SW# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-SW(config)# logging console
HQ-SW(config)# end
```

Step 16

On the HQ-SW switch, enable DHCP snooping globally.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 17

On the HQ-SW switch, specify the location of the persistent DHCP snooping binding database.

The DHCP snooping binding database should be stored in the **flash:/dhcp-snooping.db** file.

Observe the warning that is received on the console.

```
Apr 24 23:36:45.320: %DHCP_SNOOPING-4-DHCP_SNOOPING_DATABASE_FLASH_WARNING: Saving
DHCP snooping bindings to flash can fill up your device causing the writes of
bindings to device, to fail.
Apr 24 23:36:46.335: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping
database Write succeeded.
```

Step 18

On the HQ-SW switch, designate the port that forwards traffic toward the DHCP server as trusted.

The DHCP server is connected to the port GigabitEthernet0/4.

Step 19

On the HQ-SW switch, enable DHCP snooping on VLAN 9.

Verify which ports are connected to VLAN 9 by entering the following command on the HQ-SW switch:

```
HQ-SW# show vlan brief | include VLAN0009
9    VLAN0009                         active    Gi0/1, Gi0/2, Gi0/3
```

Ports GigabitEthernet0/1, GigabitEthernet0/2, and GigabitEthernet0/3 are connected to VLAN 9.

https://t.me/learningnets

Step 20

On the HQ-SW switch, configure DHCP rate limiting to 10 and configure port security to allow only 2 MAC addresses on each untrusted port in VLAN 9.

When the rate of incoming DHCP packets exceeds the configured limit, the switch places the port in the error disabled state. The port remains in that state until you intervene or you enable error-disable recovery so that ports automatically emerge from this state after a specified timeout period.

Port security allows you to configure Layer 2 interfaces that allow inbound traffic from only a restricted set of MAC addresses. The MAC addresses in the restricted set are called secure MAC addresses. In addition, number of MAC addresses that can be seen on interface can be set, thus preventing MAC spoofing, which is used in the DHCP exhaustion attack.

After you enabled port security, you should see the following message on the switch console:

```
.Apr  2 23:05:56.425: %PM-4-ERR_DISABLE: psecure-violation error detected on Gi0/3,
putting Gi0/3 in err-disable state
.Apr  2 23:05:56.459: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address ba88.4424.acf6 on port GigabitEthernet0/3.
.Apr  2 23:05:57.466: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/3, changed state to down
.Apr  2 23:05:58.464: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to
down
```

The switch put the GigabitEthernet0/3 to error disabled state, because the number of MAC addresses seen on the interface exceeded 2 MAC addresses. This way, the DHCP exhaustion attack was mitigated.

Step 21

Return to the Employee PC. Disable the Local Area Connection adapter and enable it back. The PC will obtain the IP address automatically from the legitimate DHCP server now, since the port connecting to the Attacker PC is now error disabled. Even if the port was not disabled, the switch would not allow the DHCP messages coming from the Attacker PC, because the port was configured as DHCP snooping untrusted port.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 22

On the Employee PC, open a command prompt. Verify IP settings using the **ipconfig** command.

```
C:\Users\itl>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . : secure-x.local
   Link-local IPv6 Address . . . . . : fe80::1926:99f3:1417:bf09%15
   IPv4 Address. . . . . . . . . . . : 10.10.9.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.9.2
Tunnel adapter isatap.{643B7808-C75C-4DBD-B60F-CFDDC9B33594}:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
Tunnel adapter 6TO4 Adapter:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

You should see that the PC received IP settings from the legitimate DHCP server running on the HQ-SRV.

Step 23

Return to the Attacker PC and cancel the DHCP exhaustion attack in the Yersinia tool by pressing the **q** key.

https://t.me/learningnets

Step 24

On the HQ-SW switch, verify the general DHCP snooping configuration.

```
HQ-SW# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
9
DHCP snooping is operational on following VLANs:
9
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0006.f6e7.2a80 (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)
-----------------------    -------    ------------    ----------------
GigabitEthernet0/1         no         no              10
  Custom circuit-ids:
GigabitEthernet0/2         no         no              10
  Custom circuit-ids:
GigabitEthernet0/3         no         no              10
  Custom circuit-ids:
GigabitEthernet0/4         yes        yes             unlimited
  Custom circuit-ids:
```

Step 25

On the HQ-SW switch, verify the dynamically discovered bindings in the DHCP snooping binding database.

```
HQ-SW# show ip dhcp snooping binding
MacAddress         IpAddress     Lease(sec) Type           VLAN Interface
-----------------  ------------  ---------- -------------  ---- --------------
A0:36:9F:1A:B2:B3 10.10.9.19    691075     dhcp-snooping  9    GigabitEthernet0/3
A0:36:9F:1A:B2:B1 10.10.9.10    689355     dhcp-snooping  9    GigabitEthernet0/1
Total number of bindings: 2
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 26

On the HQ-SW switch, verify the status of the binding database.

```
HQ-SW# show ip dhcp snooping database
Agent URL : flash:dhcp-snooping.db
Write delay Timer : 300 seconds
Abort Timer : 300 seconds
Agent Running : No
Delay Timer Expiry : 145 (00:02:25)
Abort Timer Expiry : Not Running
Last Succeded Time : 14:48:39 PT Sat Apr 2 2011
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts       :        3   Startup Failures :        0
Successful Transfers :        3   Failed Transfers :        0
Successful Reads     :        1   Failed Reads     :        0
Successful Writes    :        2   Failed Writes    :        0
Media Failures       :        0
```

Step 27

On the HQ-SW switch, verify the status of port security settings.

```
HQ-SW# show port-security interface GigabitEthernet0/3
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : eeba.206d.b7cf:9
Security Violation Count   : 1
```

Step 28

Return to the HQ-SW and enable the error disabled GigabitEthernet0/3 port.

Activity Verification

No verification is needed in this task.

https://t.me/learningnets

Task 2: Configure ARP Inspection

ARP inspection is a security feature that is available on the Cisco switches to protect from ARP attacks. ARP inspection intercepts, logs, and discards ARP packets with invalid IP to MAC address bindings. IP to MAC address bindings are verified against the DHCP snooping database for DHCP enabled hosts, or against a static ARP access list for statically addressed hosts. ARP inspection protects the network from ARP-based man-in-the-middle attacks. In this task you will first demonstrate how to perform the ARP spoofing attack using the Attacker PC. Then you will enable and verify ARP inspection feature on the switch in the Secure-X network to prevent ARP attacks.

Activity Procedure

Complete the following steps:

Step 1

Return to the Employee PC. Verify the IP address and the default gateway of the Employee PC, which will be the target of the ARP spoofing attack.

```
C:\Users\it1>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . : secure-x.local
   Link-local IPv6 Address . . . . . : fe80::1926:99f3:1417:bf09%15
   IPv4 Address. . . . . . . . . . . : 10.10.9.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.9.2
Tunnel adapter isatap.{643B7808-C75C-4DBD-B60F-CFDDC9B33594}:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
Tunnel adapter 6TO4 Adapter:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Note The actual IP address of the Employee PC may differ from the one in the output.

Step 2

Return to the Attacker PC. Open a terminal window and perform ARP poisoning for traffic from the Employee PC to its default gateway by using the following command. Change the IP address of the Employee PC in the following command to match your configuration, if needed.

```
root@attacker-pc:~# arpspoof -i eth2 -t 10.10.9.10 10.10.9.2
a0:36:9f:1a:b2:b3 a0:36:9f:1a:b2:b1 0806 42: arp reply 10.10.9.2 is-at a0:36:9f:
1a:b2:b3
<output omitted>
```

The tool called arpspoof redirects the packets from a target host (or all hosts) on the LAN that are intended for another host on the LAN by forging ARP replies.

You should see that the Attacker PC started to send out the spoofed ARP replies.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Note	If the Attacker PC does not have the eth2 interface, examine the available interfaces using the **ifconfig** command. Use the interface that you see in the **ifconfig** output. This also applies to the later steps.

Step 3

Open another terminal window on the Attacker PC. Configure ARP poisoning also for the traffic in the opposite direction, from the default gateway to the Employee PC, by using the following command. Change the IP address of the Employee PC in the following command to match your configuration, if needed.

```
root@attacker-pc:~# arpspoof -i eth2 -t 10.10.9.2 10.10.9.10
a0:36:9f:1a:b2:b3 0:6:f6:e7:2a:c3 0806 42: arp reply 10.10.9.10 is-at a0:36:9f:
1a:b2:b3
<output omitted>
```

Step 4

On the Attacker PC, start the Wireshark application by choosing **Applications > Kali Linux > Top 10 Security Tools > Wireshark**.

Step 5

Start capturing traffic on the eth2 interface by choosing **Capture > Interfaces**, selecting `eth2`, and clicking **Start**.

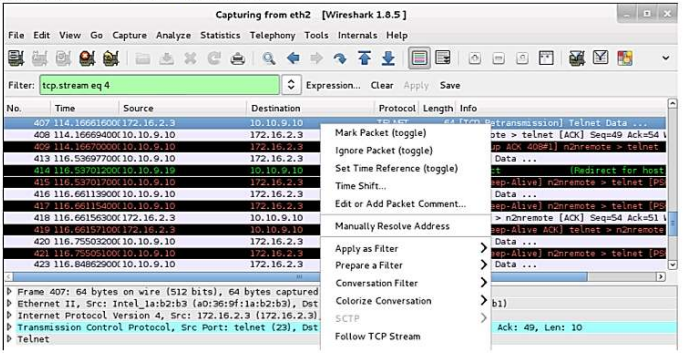
Step 6

On the Employee PC, run the PuTTY application and connect using Telnet to the HQ-ISR router at **172.16.2.3**. Enter the privileged EXEC mode using the **enable** command. Use **cisco** as the enable password.

https://t.me/learningnets

Step 7

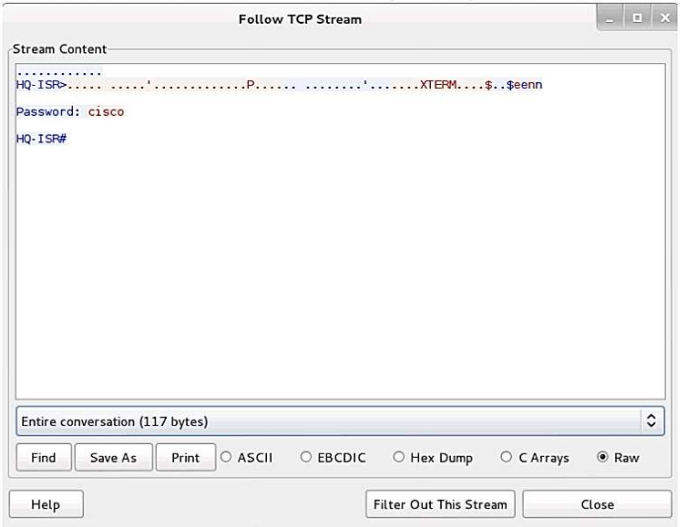
Observe the output of the traffic capture on the Attacker PC. You should see Telnet traffic with the source and destination IP addresses of the Employee PC and its default gateway. Right-click the appropriate line in the capture and click **Follow TCP Stream**.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 8

The **Follow TCP Stream** window opens. You should see the enable password that you used on the HQ-ISR router. The man-in-the-middle attack was successful because you intercepted the Telnet session.



Step 9

In the next few steps you will enable and verify ARP inspection to prevent ARP-based man-in-the-middle attacks. Return to the console of the HQ-SW switch.

Step 10

On the HQ-SW switch, enable ARP inspection on VLAN 9. This will configure all ports that are in VLAN 9 as ARP inspection untrusted ports.

https://t.me/learningnets

Step 11

You should see the following messages on the switch console after the ARP inspection has been enabled:

```
.Apr  3 01:58:45.172: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Gi0/3,
vlan 9.([a036.9f1a.b2b3/10.10.9.2/a036.9f1a.b2b1/10.10.9.10/17:58:44 PT Sat Apr 2
2011])
.Apr  3 01:58:46.179: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Gi0/3,
vlan 9.([a036.9f1a.b2b3/10.10.9.10/0006.f6e7.2ac3/10.10.9.2/17:58:45 PT Sat Apr 2
2011])
```

The messages are indicating that the switch is seeing and dropping invalid ARP responses on GigabitEthernet0/3 interface for 10.10.9.2 and 10.10.9.10 IP addresses. The ARP responses were verified against the DHCP snooping database. This way the switch prevented the ARP spoofing attacks.

Note The consequences of the ongoing ARP attack are still in place because the ARP cache on the Employee PC and its default gateway still include spoofed MAC addresses. To mitigate the ongoing attack, you should clear ARP cache on the Employee PC and on the default gateway. This way, both the PC and the default gateway would issue ARP requests again and both would reply with ARP replies with legitimate ARP messages.

Step 12

Return to the Attacker PC and interrupt the ARP spoofing attacks in both terminal windows using the **Ctrl-C** key combination.

Step 13

Also on the Attacker PC, stop the Wireshark traffic capture and close the application.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 14

On the HQ-SW switch, display general ARP inspection configuration. Observe the number of allowed and denied ARP messages.

```
HQ-SW# show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   9      Enabled          Active
 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
    9     Deny             Deny              Off
 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
    9            62           1292           1292              0
 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
    9             62             0               0                     0
 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
    9                   0                        0                      0
```

Step 15

On the HQ-SW switch, display the ARP inspection trust mode of all switch interfaces. You should see that all interfaces are configured as untrusted.

```
HQ-SW# show ip arp inspection interfaces
 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Gi0/1            Untrusted               15                 1
 Gi0/2            Untrusted               15                 1
 Gi0/3            Untrusted               15                 1
<output omitted>
```

Activity Verification

No verification is needed in this task.

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 2-4: Configure Layer 3 Data Plane Security Controls

Activity Objective

The company Secure-X has a network topology as shown in the figure. The company recently hired a new Chief Security Officer that wants to improve all of the current network security controls with the latest technologies to support the most recent company security policy.

You are the network security engineer for the Secure-X network. The Secure-X headquarters and branch networks has been experiencing IP spoofing attacks recently. The CSO tasked you with implementing suitable security controls to mitigate such attacks in the future.

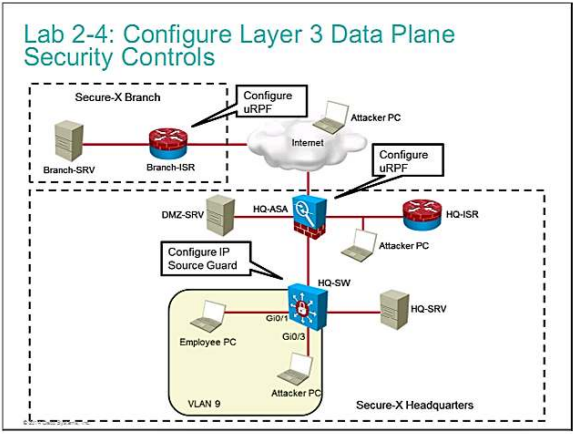
In this activity you will configure layer 3 data plane protection features on Cisco devices:

- Configure uRPF on the Cisco IOS router to prevent IP spoofing attacks
- Configure uRPF on the Cisco ASA to prevent IP spoofing attacks
- Configure IP Source Guard on the Cisco IOS Catalyst switch to prevent IP spoofing attacks

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

Command List

The table describes the Cisco IOS Software commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco IOS Commands

Command	Description
interface range *interface-range*	Enters interface range configuration mode.
ip verify unicast source reachable-via rx	Enables strict uRPF on an interface.
ip verify unicast source reachable-via rx allow-default	Enables strict uRPF on the interface and allows usage of a default route.
ip verify source	Enables IP Source Guard on an interface.
ip verify source port-security	Enables IP Source Guard with port security on an interface.
show ip interface *interface*	Displays status and statistics of an interface.
show ip verify source	Displays IP Source Guard information.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

The table describes the Cisco ASA commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco ASA Commands

Command	Description
show ip verify statistics	Displays uRPF statistics.

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

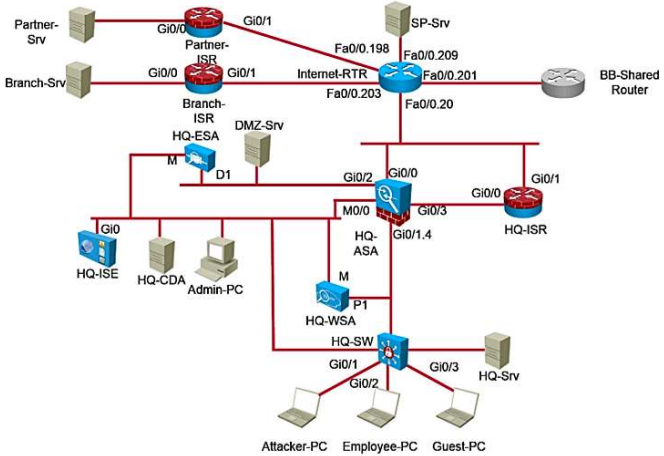
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

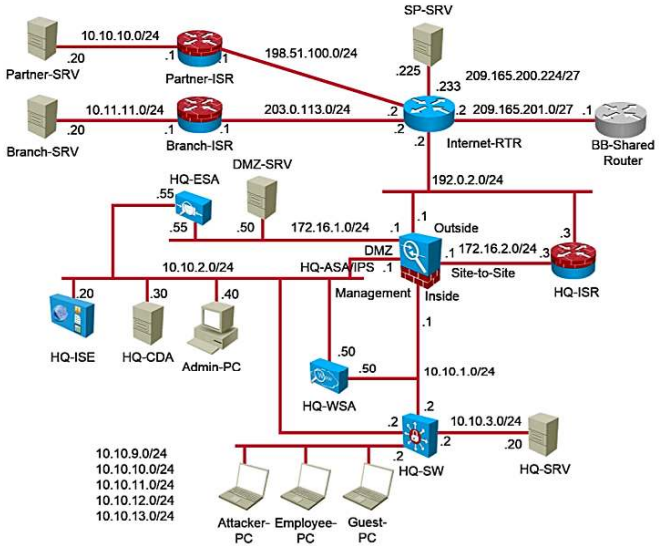
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



https://t.me/learningnets

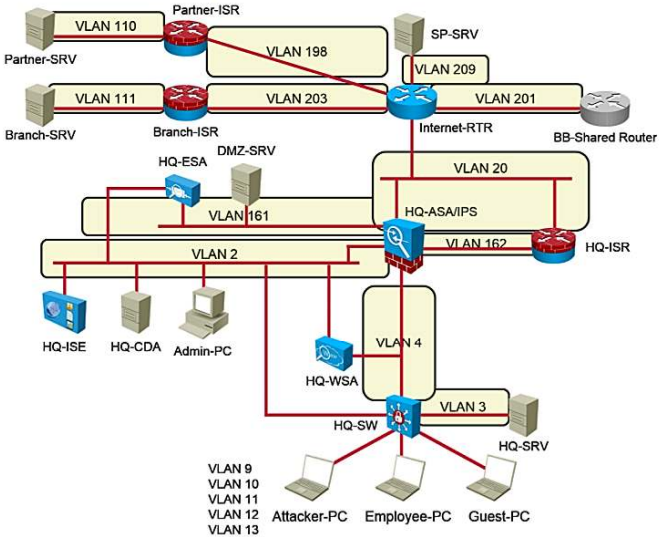
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure uRPF on the Cisco IOS Router

In this task, you will configure the Cisco IOS uRPF feature on the Branch-ISR router to protect the Secure-X branch from IP spoofing attacks. First you will use the Attacker PC to ping the Branch-ISR router. You will spoof the source IP address of the ping packets with IP address of the Branch-SRV. The Branch-ISR will then respond with ping replies to the Branch-SRV. Such an attack, when amplified with several attackers, could lead to a DoS attack on the victim. Then you will enable uRPF on the router and observe what effect it has on the spoofing attack.

Activity Procedure

Complete the following steps:

https://t.me/learningnets

Step 1

Access the console of the HQ-SW switch. Move the Attacker PC to VLAN 203 by using the following commands:

```
configure terminal
interface GigabitEthernet0/3
 switchport access vlan 203
 shutdown
 no shutdown
```

The Attacker PC will get a correct IP address from a DHCP server.

Step 2

Access the Attacker PC.

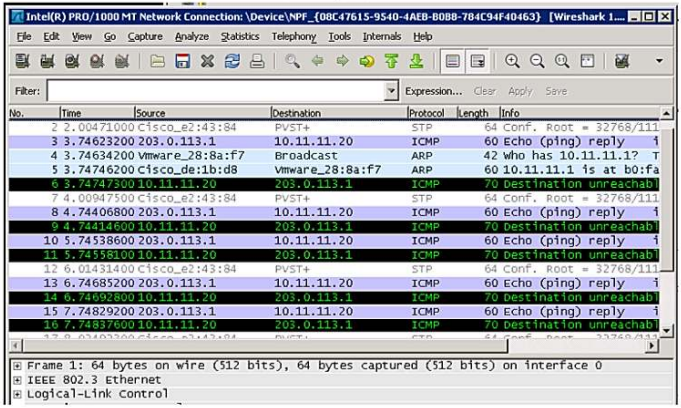
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

Open a terminal window on the Attacker PC and use the nping tool to ping the GigabitEthernet0/1 interface of the Branch-ISR router. Spoof the source IP address of the ICMP packets and use the IP address of the Branch-SRV as the source IP address.

```
root@attacker-pc:~# nping 203.0.113.1 -S 10.11.11.20 -c 200
Starting Nping 0.6.25 ( http://nmap.org/nping ) at 2013-06-13 23:31 EDT
SENT (0.0120s) ICMP 10.11.11.20 > 203.0.113.1 Echo request (type=8/code=0) ttl=64
id=3323 iplen=28
SENT (1.0125s) ICMP 10.11.11.20 > 203.0.113.1 Echo request (type=8/code=0) ttl=64
id=3323 iplen=28
SENT (2.0139s) ICMP 10.11.11.20 > 203.0.113.1 Echo request (type=8/code=0) ttl=64
id=3323 iplen=28
SENT (3.0152s) ICMP 10.11.11.20 > 203.0.113.1 Echo request (type=8/code=0) ttl=64
id=3323 iplen=28
SENT (4.0164s) ICMP 10.11.11.20 > 203.0.113.1 Echo request (type=8/code=0) ttl=64
id=3323 iplen=28
```

In the meantime, access the Branch-SRV and start the interface packet capture by using Wireshark. The router should have responded to the ICMP echo request packets, but instead it responded to Branch-SRV, because its IP address was spoofed by the Attacker PC. This way, an attacker could perform a DoS attack by sending a large amount of traffic with a spoofed source IP address to many hosts, which would then respond to the victim and overwhelm it with ICMP replies.



Step 4

Access the console of the Branch-ISR router and enable strict uRPF on GigabitEthernet0/0 and GigabitEthernet0/1 interfaces to prevent IP spoofing attacks. Allow the usage of the default route on the GigabitEthernet0/1 interface.

https://t.me/learningnets

Step 5

Return to the Attacker PC and perform the spoofing attack again.

```
root@attacker-pc:~# nping 203.0.113.1 -S 10.11.11.20 -c 200
Starting Nping 0.6.25 ( http://nmap.org/nping ) at 2013-06-13 23:31 EDT
SENT (0.0120s) ICMP 10.11.11.20 > 203.0.113.1 Echo request (type=8/code=0) ttl=64
id=3323 iplen=28
SENT (1.0125s) ICMP 10.11.11.20 > 203.0.113.1 Echo request (type=8/code=0) ttl=64
id=3323 iplen=28
SENT (2.0139s) ICMP 10.11.11.20 > 203.0.113.1 Echo request (type=8/code=0) ttl=64
id=3323 iplen=28
SENT (3.0152s) ICMP 10.11.11.20 > 203.0.113.1 Echo request (type=8/code=0) ttl=64
id=3323 iplen=28
SENT (4.0164s) ICMP 10.11.11.20 > 203.0.113.1 Echo request (type=8/code=0) ttl=64
id=3323 iplen=28
```

Observe the Wireshark output on the Branch-SRV. You should see that the server did not receive the ICMP echo replies because the router dropped them as a result of the uRPF checks.

Step 6

Return to the Branch-ISR and verify the uRPF statistics on the GigabitEthernet0/1 interface.

```
Branch-ISR# show ip interface GigabitEthernet0/1 | begin IP verify
  IP verify source reachable-via RX, allow default
    76 verification drops
    0 suppressed verification drops
    0 verification drop-rate
```

You should see dropped packets because of uRPF checks.

Activity Verification

No verification is needed in this task.

Task 2: Configure uRPF on the Cisco ASA

In this task, you will configure uRPF feature on the HQ-ASA to protect the Secure-X headquarters from IP spoofing attacks. First you will use the Attacker PC to ping the DMZ-SRV. You will spoof the source IP address of the ping packets with IP address of the HQ-SRV. The DMZ-SRV will then respond with ping replies to the HQ-SRV. Such an attack, when amplified with several attackers, could lead to a DoS attack on the victim. Then you will enable uRPF on the ASA to protect from the spoofing attack.

Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

Return to the console of the HQ-SW switch. Move the Attacker PC to VLAN 162 by using the following commands:

```
configure terminal
interface GigabitEthernet0/3
 switchport access vlan 162
 shutdown
 no shutdown
```

VLAN 162 is a segment between the HQ-ASA and the HQ-ISR router. The Attacker PC will get a correct IP address from a DHCP server.

Step 2

Return to the Attacker PC.

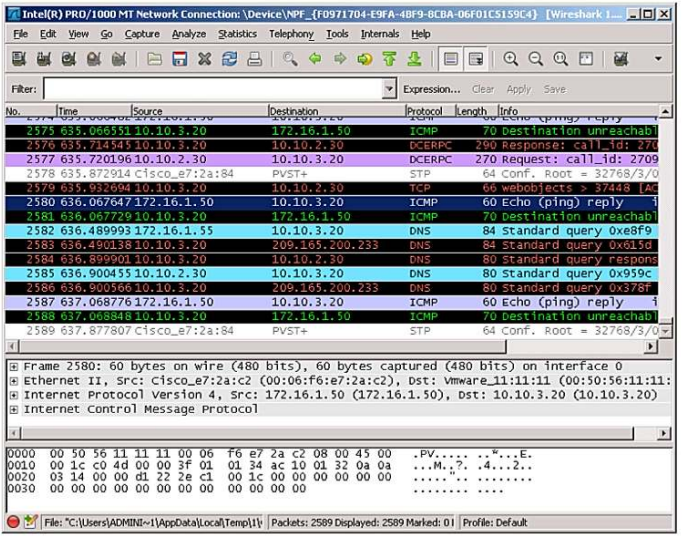
https://t.me/learningnets

Step 3

Open a terminal window on the Attacker PC and use the nping tool to ping DMZ-SRV. Spoof the source IP address of the ICMP packets and use the IP address of the HQ-SRV as the source IP address.

```
root@attacker-pc:~# nping 172.16.1.50 -S 10.10.3.20 -c 200
Starting Nping 0.6.25 ( http://nmap.org/nping ) at 2013-11-14 13:44 GMT
SENT (0.1792s) ICMP 10.10.3.20 > 172.16.1.50 Echo request (type=8/code=0) ttl=64
id=60691 iplen=28
SENT (1.1794s) ICMP 10.10.3.20 > 172.16.1.50 Echo request (type=8/code=0) ttl=64
id=60691 iplen=28
SENT (2.1806s) ICMP 10.10.3.20 > 172.16.1.50 Echo request (type=8/code=0) ttl=64
id=60691 iplen=28
SENT (3.1818s) ICMP 10.10.3.20 > 172.16.1.50 Echo request (type=8/code=0) ttl=64
id=60691 iplen=28
```

In the meantime, access the HQ-SRV and start the interface packet capture by using Wireshark. The DMZ-SRV should have responded to the ICMP echo request packets, but instead it responded to HQ-SRV, because its IP address was spoofed by the Attacker PC.



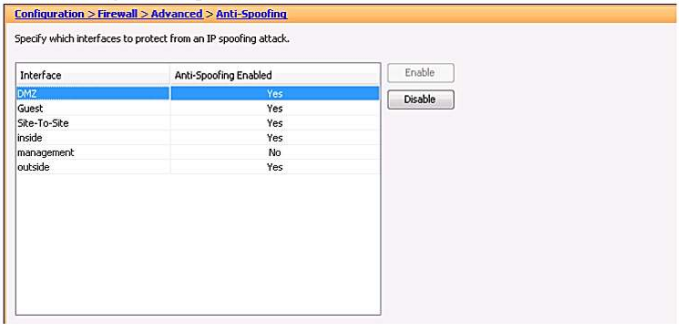
Step 4

Access the Admin PC. Start the Cisco ASDM and connect to the HQ-ASA at 10.10.2.1. Log in using **admin** as the username and **Ci5coAdmin** as the password.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 5

In the Cisco ASDM, navigate to **Configuration > Firewall > Advanced > Anti-Spoofing** and enable uRPF on all interfaces, except the management interface.



Step 6

Apply the configuration by clicking the **Apply** button. Review the configuration and Click **OK**.

Step 7

Return to the Attacker PC and perform the spoofing attack again.

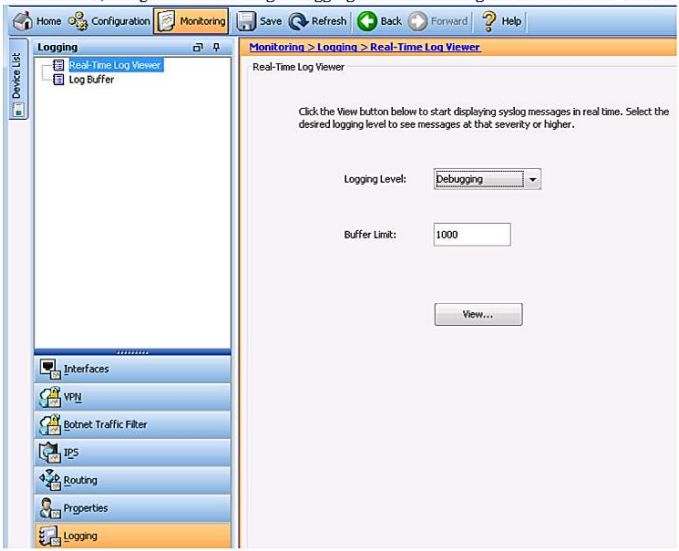
```
root@attacker-pc:~# nping 172.16.1.50 -S 10.10.3.20 -c 200
Starting Nping 0.6.25 ( http://nmap.org/nping ) at 2013-11-14 13:44 GMT
SENT (0.1792s) ICMP 10.10.3.20 > 172.16.1.50 Echo request (type=8/code=0) ttl=64
id=60691 iplen=28
SENT (1.1794s) ICMP 10.10.3.20 > 172.16.1.50 Echo request (type=8/code=0) ttl=64
id=60691 iplen=28
SENT (2.1806s) ICMP 10.10.3.20 > 172.16.1.50 Echo request (type=8/code=0) ttl=64
id=60691 iplen=28
SENT (3.1818s) ICMP 10.10.3.20 > 172.16.1.50 Echo request (type=8/code=0) ttl=64
id=60691 iplen=28
```

Observe the Wireshark output on the HQ-SRV. You should see that the server did not receive the ICMP echo replies because the ASA dropped them as a result of the uRPF checks.

https://t.me/learningnets

Step 8

In the Cisco ASDM, navigate to **Monitoring > Logging > Real-Time Log Viewer**. Click the **View** button.

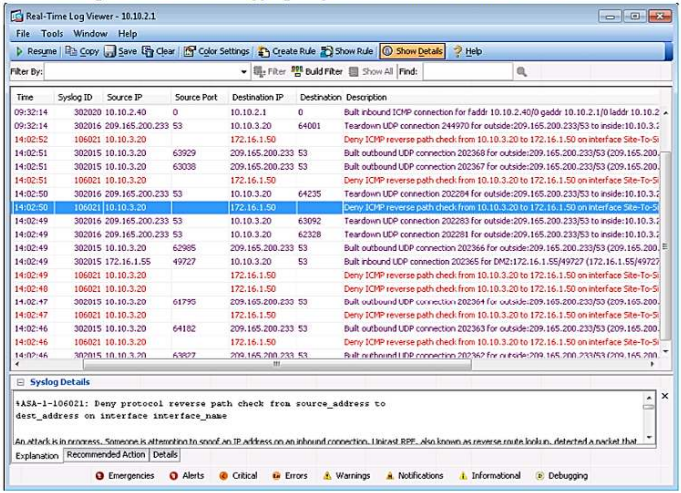


The Real-Time Log Viewer will open.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 9

Observe the messages about the ASA dropping the packets because of the uRPF check.



Step 10

Access the HQ-ASA console and verify uRPF statistics.

```
HQ-ASA# show ip verify statistics
interface outside: 0 unicast rpf drops
interface inside: 519 unicast rpf drops
interface Guest: 0 unicast rpf drops
interface DMZ: 0 unicast rpf drops
interface Site-To-Site: 167 unicast rpf drops
interface management: 0 unicast rpf drops
```

You should see dropped packets on the Site-To-Site interface because of the uRPF checks.

Activity Verification

No verification is needed in this task.

https://t.me/learningnets

Task 3: Configure IP Source Guard on the Cisco IOS Catalyst Switch

In this task, you will configure the IP Source Guard feature on the HQ-SW to protect the Secure-X headquarters from IP spoofing attacks at the network access layer. First you will use the Attacker PC to spoof the IP address of the Employee PC when pinging its default gateway. To prevent IP spoofing attacks within the same VLAN you cannot use uRPF, since uRPF is deployed on boundaries between different IP subnets. Therefore you will enable IP Source Guard on the HQ-SW switch to protect the network from the spoofing attack.

Activity Procedure

Complete the following steps:

Step 1

Return to the console of the HQ-SW switch. Move the Attacker PC to VLAN 9 by using the following commands:

```
configure terminal
interface GigabitEthernet0/3
 switchport access vlan 9
 shutdown
 no shutdown
```

The Attacker PC will get a correct IP address from a DHCP server.

Step 2

Return to the Attacker PC.

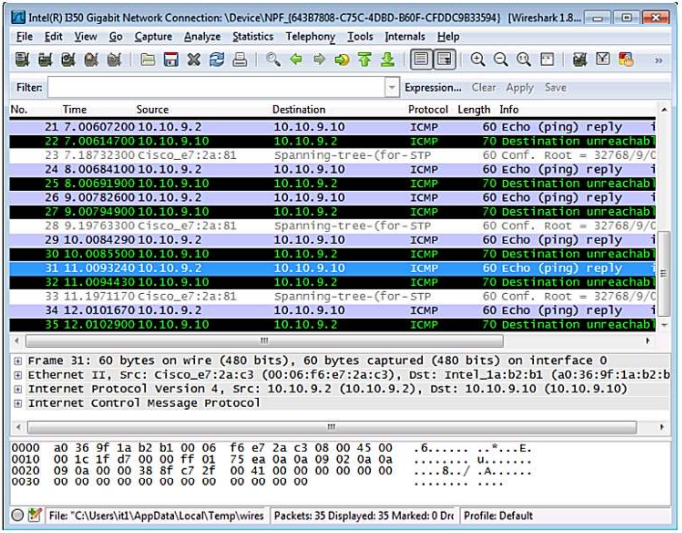
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 3

Open a terminal window on the Attacker PC and use the nping tool to ping the default gateway in VLAN 9 at 10.10.9.2. Spoof the source IP address of the ICMP packets and use the IP address of the Employee PC as the source IP address. Verify the Employee PC's IP address by accessing it and verifying its IP address.

```
root@attacker-pc:~# nping 10.10.9.2 -S 10.10.9.10 -c 200
Starting Nping 0.6.25 ( http://nmap.org/nping ) at 2013-11-15 09:12 GMT
SENT (0.1458s) ICMP 10.10.9.10 > 10.10.9.2 Echo request (type=8/code=0) ttl=64
id=63388 iplen=28
SENT (1.1462s) ICMP 10.10.9.10 > 10.10.9.2 Echo request (type=8/code=0) ttl=64
id=63388 iplen=28
```

In the meantime, return to the Employee PC and start the interface packet capture by using Wireshark. The default gateway should have responded to the ICMP echo request packets, but instead it responded to Employee PC, because its IP address was spoofed by the Attacker PC.



Step 4

Return to the HQ-SW console. Enable IP Source Guard on the GigabitEthernet0/1, GigabitEthernet0/2, and GigabitEthernet0/3 interfaces.

https://t.me/learningnets

Step 5

Return to the Attacker PC and perform the spoofing attack again. Again, use the IP address of your Employee PC as the source IP address.

```
root@attacker-pc:~# nping 10.10.9.2 -S 10.10.9.10 -c 200
Starting Nping 0.6.25 ( http://nmap.org/nping ) at 2013-11-15 09:12 GMT
SENT (0.1458s) ICMP 10.10.9.10 > 10.10.9.2 Echo request (type=8/code=0) ttl=64
id=63388 iplen=28
SENT (1.1462s) ICMP 10.10.9.10 > 10.10.9.2 Echo request (type=8/code=0) ttl=64
id=63388 iplen=28
```

Observe the Wireshark output on the Employee PC. You should see that the PC did not receive the ICMP echo replies because the switch dropped them as a result of the IP Source Guard checks.

Step 6

On the HQ-SW console, display the IP Source Guard information.

```
HQ-SW# show ip verify source
Interface  Filter-type  Filter-mode  IP-address  Mac-address          Vlan  Log
---------  -----------  -----------  ----------  -----------          ----  ---
Gi0/1      ip           active       10.10.9.10                        9    disabled
Gi0/2      ip           active       10.10.9.11                        9    disabled
Gi0/3      ip           active       10.10.9.19                        9    disabled
```

You should see that the switch is verifying only IP addresses and no MAC addresses, as indicated by the empty Mac-address column. The switch allows only traffic coming from the 10.10.9.19 IP address on the GigabitEthernet0/3 interface. Your IP address may differ from what is shown in the example.

Step 7

On the HQ-SW, change the IP Source Guard configuration to also verify MAC addresses.

Note	Port security configuration is required on a switch to enable IP Source Guard to verify MAC addresses. Port security configuration should in place from the previous lab.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 8

On the HQ-SW console, display the IP Source Guard information again.

```
HQ-SW# show ip verify source
Interface  Filter-type  Filter-mode  IP-address  Mac-address          Vlan  Log
---------  -----------  -----------  ----------  -----------          ----  ---
Gi0/1      ip-mac       active       10.10.9.10  A0:36:9F:1A:B2:B1    9     disabled
Gi0/2      ip-mac       active       10.10.9.11  A0:36:9F:1A:B2:B2    9     disabled
Gi0/3      ip-mac       active       10.10.9.19  A0:36:9F:1A:B2:B3    9     disabled
```

You should see that the switch is verifying also MAC addresses. The switch allows only traffic coming from the 10.10.9.19 IP address and A0:36:9F:1A:B2:B3 MAC address on the GigabitEthernet0/3 interface. Your IP address may differ from what is shown in the example.

Activity Verification

No verification is needed in this task.

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 3-1: Configure Cisco ASA NAT

Activity Objective

The company Secure-X has a network topology as shown in the figure. The company recently hired a new Chief Security Officer that wants to improve all of the current network security controls with the latest technologies to support the most recent company security policy.

You are the network security engineer for the Secure-X network. The Secure-X network requires network address translation in order to hide internal addressing and to enable connectivity from the network to the Internet. The CSO tasked you with implementing dynamic NAT with PAT on the Cisco ASA for the hosts that require only outbound connectivity. The CSO also tasked you to configure static NAT for servers that require also inbound connectivity.

The Secure-X network was recently connected to the Partner network using IPsec VPN connection. However, one of the internal Secure-X networks is using the same address space as the Partner network. The CSO tasked you to also configure twice NAT on the Cisco ASA to overcome the problem of overlapping address space.

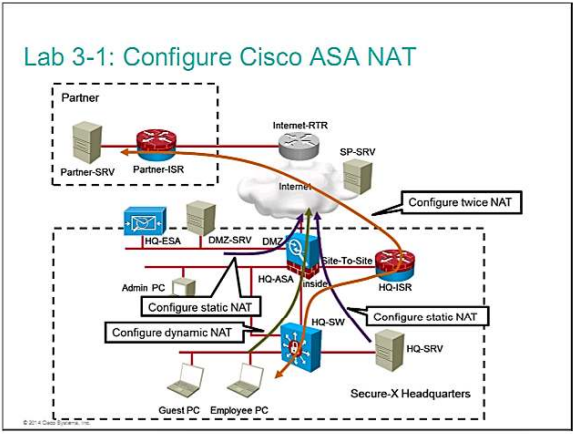
In this activity you will configure NAT on the Cisco ASA:

- Configure static NAT using network object NAT on the Cisco ASA
- Configure dynamic NAT using network object NAT on the Cisco ASA
- Configure twice NAT using manual NAT on the Cisco ASA

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

Command List

The table describes the Cisco ASA commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco ASA Commands

Command	Description
show nat	Displays NAT table.
show xlate	Displays NAT translations.

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

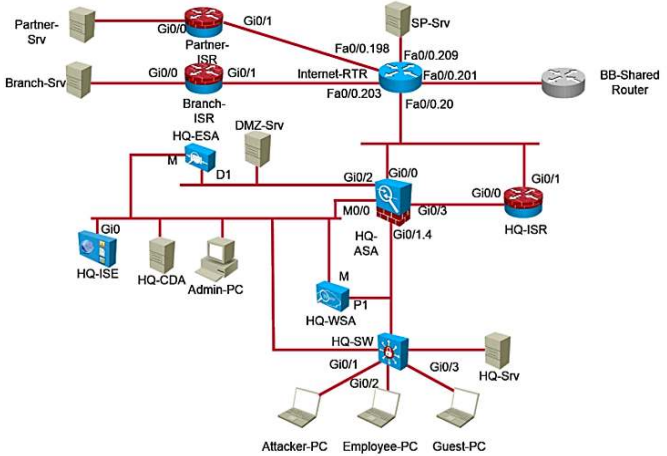
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

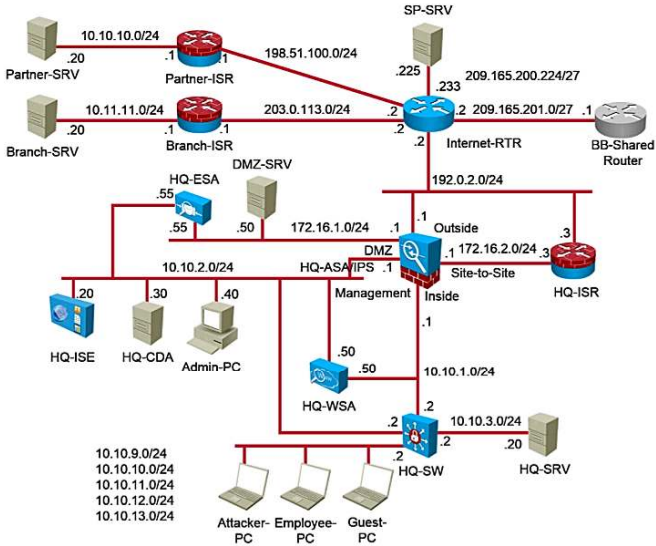
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

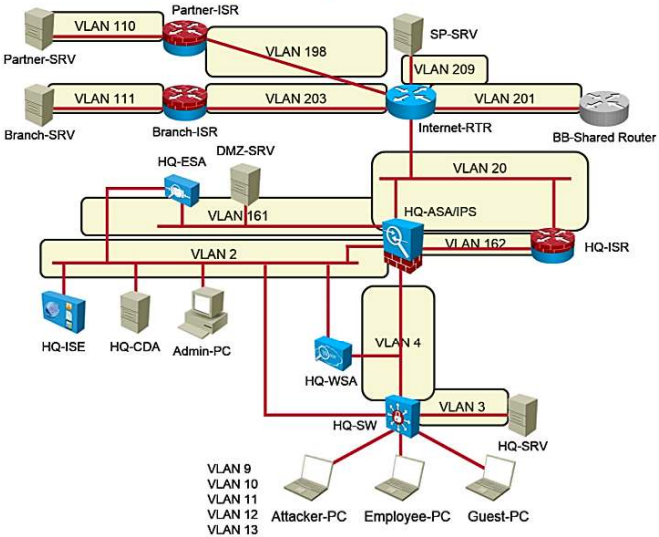
The figure shows the IP addresses that are used in this lab setup.



https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure Static NAT

In this task, you will configure static NAT using network object (auto) NAT on the HQ-ASA. Static NAT will translate IP addresses of all hosts in the Secure-X network that may require inbound connectivity from the outside networks. Such hosts are DMZ-SRV, HQ-ESA, and HQ-SRV. The DMZ-SRV requires inbound connectivity for DNS, HTTP, and FTP services, while the HQ-ESA acts as a mail transfer agent (MTA) for the email server on the HQ-SRV and requires inbound connectivity for SMTP. The HQ-SRV does not require any inbound connectivity at this time. You will verify NAT configuration by accessing the SP-SRV from all three hosts the static NAT will be configured for. Actual inbound connectivity will be verified in a later lab when configuring inbound access rules.

Activity Procedure

Complete the following steps:

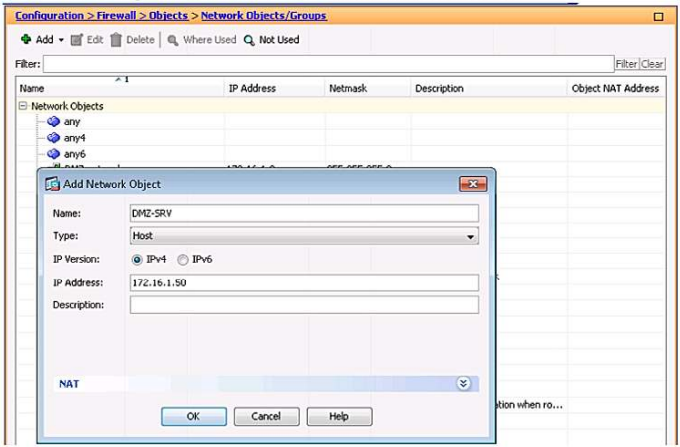
Step 1

Access the Admin PC. Start Cisco ASDM by double-clicking its icon on the desktop. Connect to the HQ-ASA at 10.10.2.1. Log in using **admin** as the username and **Ci5coAdmin** as the password.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

When Cisco ASDM opens, navigate to **Configuration > Firewall > Objects > Network Objects/Groups**. Create a new network object with name DMZ-SRV and IP address 172.16.1.50.



https://t.me/learningnets

Step 3

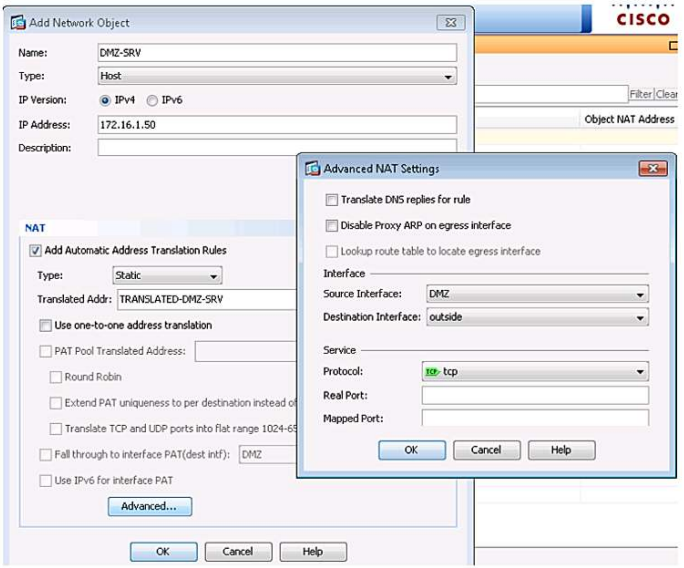
Expand the **NAT** option in the Add Network Object window. Enable the **Add Automatic Address Translation Rules** check box. Configure static NAT with the following parameters.

Translated IP address: 192.0.2.50

Object name for the translated IP address: **TRANSLATED-DMZ-SRV**

Source interface: **DMZ**

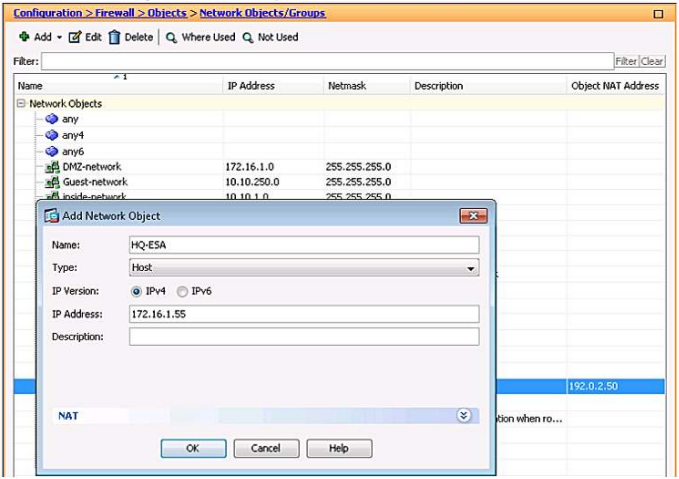
Destination interface: **outside**



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 4

Create another network object with name HQ-ESA and IP address 172.16.1.55.



https://t.me/learningnets

Step 5

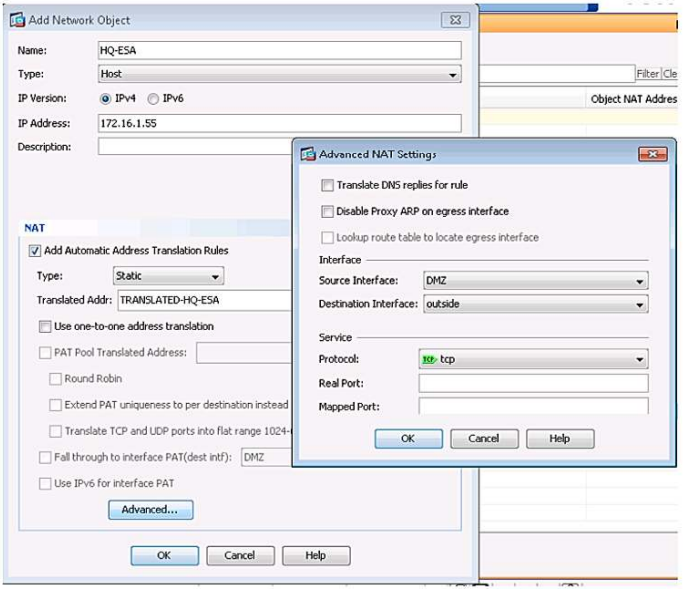
Expand the **NAT** option in the Add Network Object window. Enable the **Add Automatic Address Translation Rules** check box. Configure static NAT with the following parameters.

Translated IP address: 192.0.2.55

Object name for the translated IP address: **TRANSLATED-HQ-ESA**

Source interface: **DMZ**

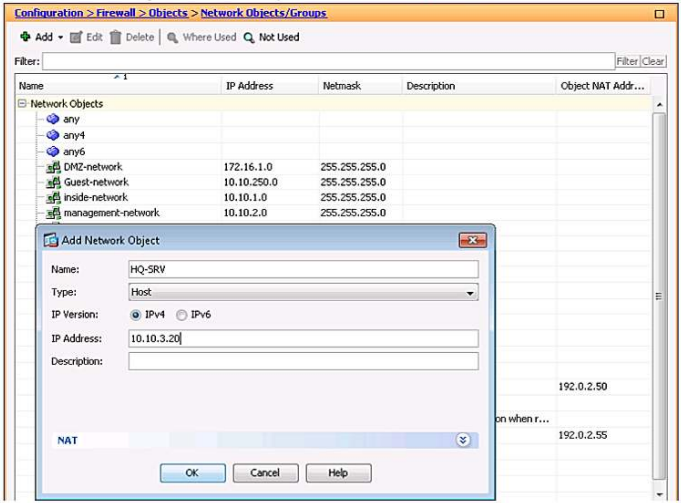
Destination interface: **outside**



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

Create another network object with name HQ-SRV and IP address 10.10.3.20.



https://t.me/learningnets

Step 7

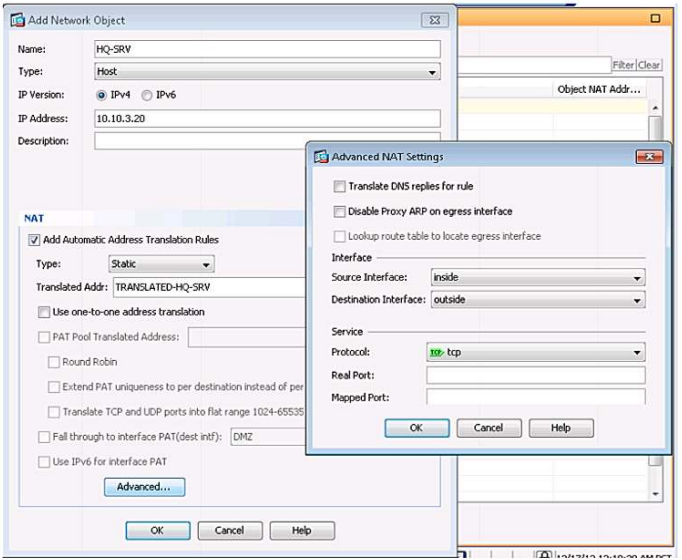
Expand the **NAT** option in the Add Network Object window. Enable the **Add Automatic Address Translation Rules** check box. Configure static NAT with the following parameters.

Translated IP address: 192.0.2.20

Object name for the translated IP address: **TRANSLATED-HQ-SRV**

Source interface: **inside**

Destination interface: **outside**



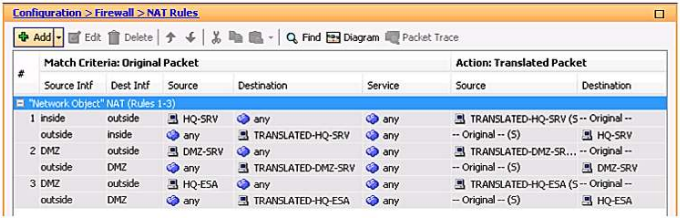
Step 8

Apply the configuration by clicking the **Apply** button.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

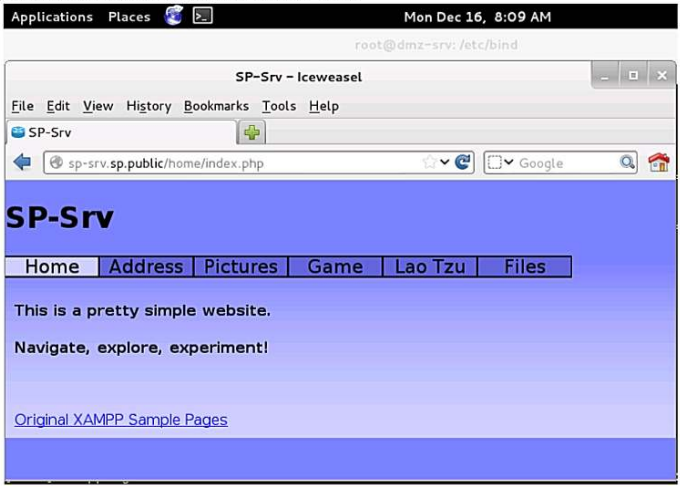
Step 9

In the Cisco ASDM, navigate to **Configuration > Firewall > NAT Rules**. Observe the auto generated NAT rules. You should see three static NAT rules; for the DMZ-SRV, for the HQ-ESA, and for the HQ-SRV.



Step 10

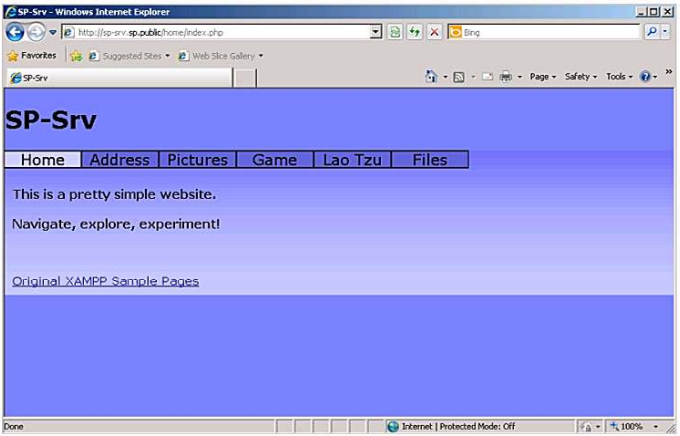
Access the DMZ-SRV. Open the Iceweasel Web Browser and navigate to **http://sp-srv.sp.public**. This will generate traffic from the DMZ-SRV to the SP-SRV.



https://t.me/learningnets

Step 11

Access the HQ-SRV. Open Internet Explorer and navigate to **http://sp-srv.sp.public**. This will generate traffic from the HQ-SRV to the SP-SRV.



Step 12

Access the console of the HQ-ESA. Log in using **admin** username and **Ci5coAdmin** password. Telnet to **sp-srv.sp.public** using port 25. This will generate traffic from the HQ-ESA to the SP-SRV.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Tue Dec 17 07:58:57 2013
Copyright (c) 2001-2013, Cisco Systems, Inc.
AsyncOS 8.0.0 for Cisco C100V build 550
Welcome to the Cisco C100V Email Security Virtual Appliance
esa.secure-x.local> telnet sp-srv.sp.public 25
Trying 209.165.200.233...
Connected to sp-srv.sp.public.
Escape character is '^]'.
220 ********************
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 13

Access the HQ-ASA console. Display the NAT table. You should see three auto NAT policies in the second section of the NAT table. You should also see statistics for translated packets.

```
HQ-ASA# show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source static HQ-SRV TRANSLATED-HQ-SRV
    translate_hits = 38, untranslate_hits = 0
2 (DMZ) to (outside) source static DMZ-SRV TRANSLATED-DMZ-SRV
    translate_hits = 3841, untranslate_hits = 32
3 (DMZ) to (outside) source static HQ-ESA TRANSLATED-HQ-ESA
    translate_hits = 70, untranslate_hits = 1762
```

Step 14

On the HQ-ASA console, display the translation table. You should see 3 static translations, all marked with s flag.

```
HQ-ASA# show xlate
3 in use, 5 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from inside:10.10.3.20 to outside:192.0.2.20
    flags s idle 0:00:34 timeout 0:00:00
NAT from DMZ:172.16.1.50 to outside:192.0.2.50
    flags s idle 0:13:17 timeout 0:00:00
NAT from DMZ:172.16.1.55 to outside:192.0.2.55
    flags s idle 0:00:12 timeout 0:00:00
```

Activity Verification

No verification is needed in this task.

Task 2: Configure Dynamic NAT

In this task, you will configure dynamic NAT with PAT using network object (auto) NAT on the HQ-ASA. Dynamic NAT with PAT will translate IP addresses of all internal hosts in the Secure-X network that require only outbound connectivity. Such hosts are Employee PC and Guest PC. You will configure dynamic NAT with PAT for all internal hosts to translate source IP addresses to a single IP address of 192.0.2.100 when internal hosts are routed to the outside interface. You will verify dynamic NAT configuration by accessing the SP-SRV from two internal hosts.

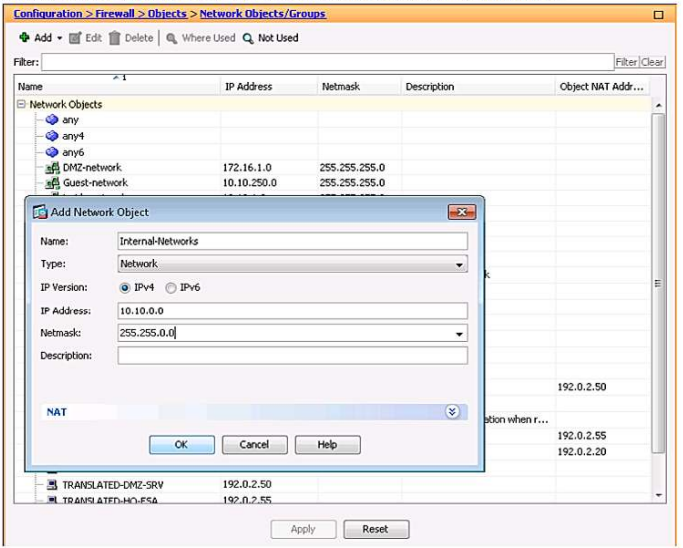
Activity Procedure

Complete the following steps:

https://t.me/learningnets

Step 1

Return to the Admin PC. Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**. Create a new network object with name Internal-Networks and IP subnet 10.10.0.0/16.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

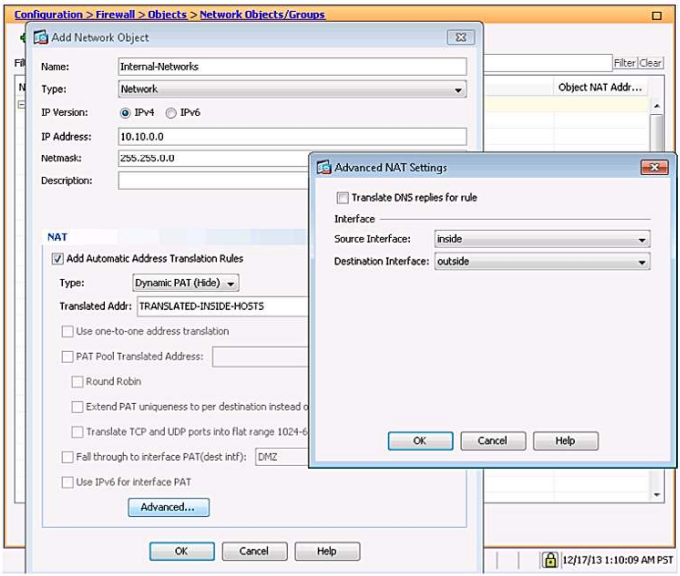
Expand the **NAT** option in the Add Network Object window. Enable the **Add Automatic Address Translation Rules** check box. Configure dynamic NAT with PAT with the following parameters.

Translated IP address: 192.0.2.100

Object name for the translated IP address: **TRANSLATED-INSIDE-HOSTS**

Source interface: **inside**

Destination interface: **outside**



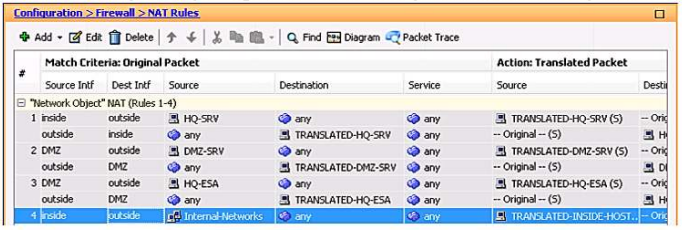
Step 3

Apply the configuration by clicking the **Apply** button.

https://t.me/learningnets

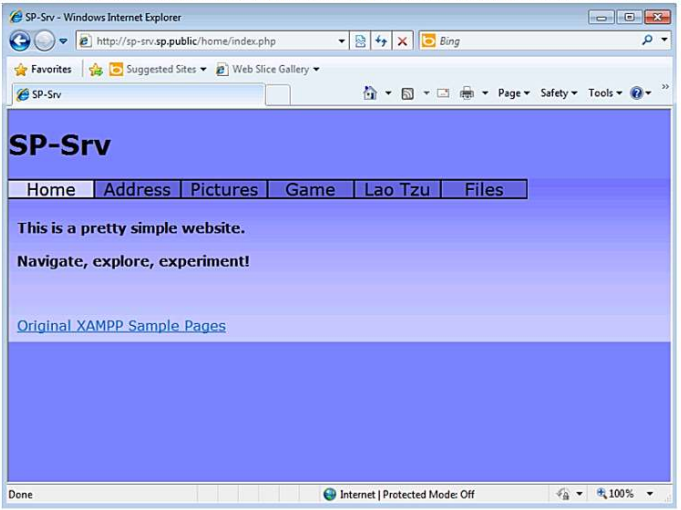
Step 4

In the Cisco ASDM, navigate to **Configuration > Firewall > NAT Rules**. Observe the auto generated NAT rules. In addition to the previously configured static NAT rules, you should also see the dynamic NAT rule.



Step 5

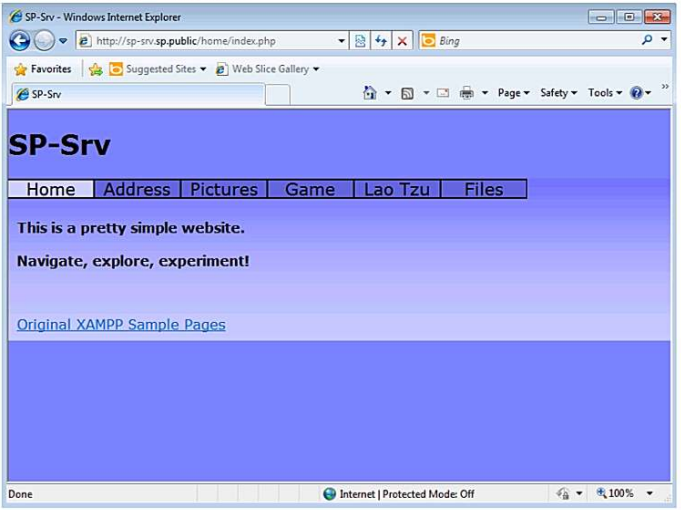
Access the Employee PC. Login as **it1** user and **cisco** password if required. Open Internet Explorer and navigate to **http://sp-srv.sp.public**. This will generate traffic from the Employee PC to the SP-SRV.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

Access the Guest PC. Open Internet Explorer and navigate to **http://sp-srv.sp.public**. This will generate traffic from the Guest PC to the SP-SRV.



Step 7

Return to the HQ-ASA console. Display the NAT table. You should see the configured dynamic NAT policy in the second section of the NAT table. You should also see statistics for translated packets.

```
HQ-ASA# show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source static HQ-SRV TRANSLATED-HQ-SRV
    translate_hits = 252, untranslate_hits = 6
2 (DMZ) to (outside) source static DMZ-SRV TRANSLATED-DMZ-SRV
    translate_hits = 3863, untranslate_hits = 32
3 (DMZ) to (outside) source static HQ-ESA TRANSLATED-HQ-ESA
    translate_hits = 195, untranslate_hits = 1762
4 (inside) to (outside) source dynamic Internal-Networks TRANSLATED-INSIDE-HOSTS
    translate_hits = 188, untranslate_hits = 1
```


https://t.me/learningnets

Step 8

On the HQ-ASA console, display the Xlate table. You should see dynamic translations for the Employee PC (from 10.10.9.10 IP address) and for the Guest PC (from 10.10.9.11 IP address).

All dynamic translations are marked with r and i flags. Observe how both inside private IP addresses translate to the same public IP address, but using different ports.

```
HQ-ASA# show xlate
7 in use, 55 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from inside:10.10.3.20 to outside:192.0.2.20
    flags s idle 0:00:01 timeout 0:00:00
NAT from DMZ:172.16.1.50 to outside:192.0.2.50
    flags s idle 0:01:38 timeout 0:00:00
NAT from DMZ:172.16.1.55 to outside:192.0.2.55
    flags s idle 0:00:14 timeout 0:00:00
TCP PAT from inside:10.10.9.11/1122 to outside:192.0.2.100/1122 flags ri idle 0:00:05
timeout 0:00:30
TCP PAT from inside:10.10.9.10/9297 to outside:192.0.2.100/9297 flags ri idle 0:00:01
timeout 0:00:30
TCP PAT from inside:10.10.9.10/9296 to outside:192.0.2.100/9296 flags ri idle 0:00:02
timeout 0:00:30
TCP PAT from inside:10.10.9.10/9293 to outside:192.0.2.100/9293 flags ri idle 0:00:04
timeout 0:00:30
```

Note	Your IP addresses my differ from the ones in the output.

Note	Dynamic NAT with PAT translations are short lived and expire in 30 seconds by default. If you do not the translations, return to the Employee PC and Guest PC and refresh the web page in Internet Explorer. Quickly return to the HQ-ASA and display the Xlate table again.

Activity Verification

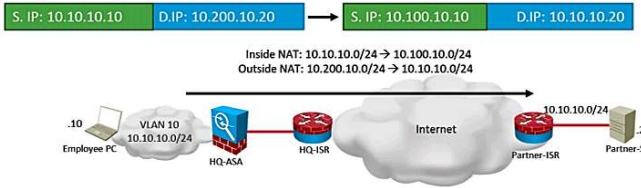
No verification is needed in this task.

Task 3: (Optional) Configure Twice NAT

In this task, you will configure twice NAT using manual NAT on the HQ-ASA. The Partner office and the Secure-X headquarters network are connected using IPsec VPN tunnel. The Partner network and the VLAN 10 in the Secure-X headquarters network use the same IP address space (10.10.10.0/24). To make communication between these networks possible, NAT has to be configured. Because it is unlikely that NAT will be done on the Partner-ISR router, NAT has to be configured in the Secure-X headquarters for both source and destination IP addresses (inside and outside NAT). You will verify twice NAT by putting the Employee PC into VLAN 10 and and accessing the Partner-SRV.

The following diagram illustrates how IP addresses can be translated to enable communication between the Partner and headquarters offices.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.



When traffic goes from the VLAN 10 to the Partner network, the destination IP addresses should be 10.200.10.x. This is how the Partner network is seen from the perspective of the headquarters. When the traffic goes over the Cisco ASA, the source IP address (e.g. 10.10.10.10) is translated to an IP address from the 10.100.10.0/24 network. This is how the inside VLAN 10 is seen from the perspective of the Partner network. The destination IP address is at the same time translated from 10.200.10.x to 10.10.10.x.

Activity Procedure

Complete the following steps:

https://t.me/learningnets

Step 1

Return to the Admin PC. Navigate to **Configuration > Firewall > NAT Rules**. Create a new manual NAT rule before the network object rules. Configure twice NAT to statically translate source IP addresses from VLAN 10 to 10.100.10.0/24 network. At the same time, the NAT rule should translate destination IP addresses from 10.200.10.0/24 (Partner network as seen from the headquarters) to 10.10.10.0/24 (Partner network as seen locally). Use the following parameters to configure NAT rule:

Original source IP network: 10.10.10.0/24

Object name for the original source IP network: **REAL-VLAN10**

Translated source IP network: 10.100.10.0/24

Object name for the translated source IP network: **TRANSLATED-VLAN10**

Translated destination IP network: 10.200.10.0/24

Object name for the translated destination IP network: **TRANSLATED-PARTNER**

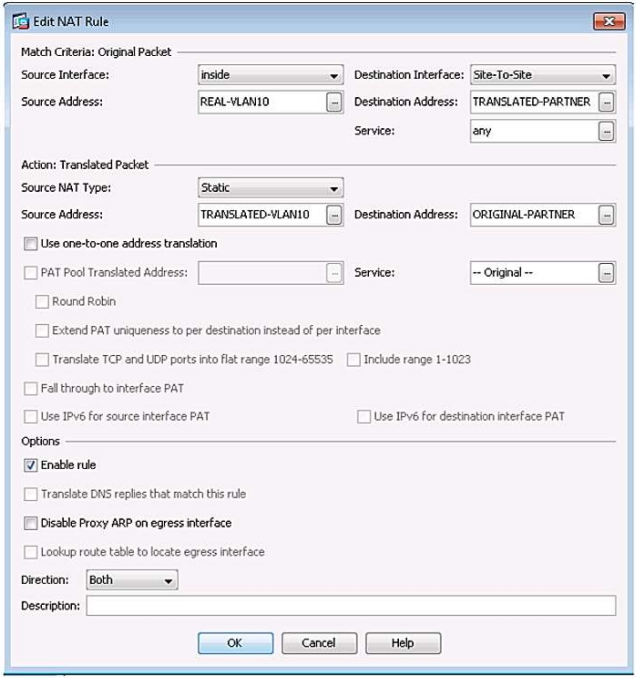
Original destination IP network: 10.10.10.0/24

Object name for the original destination IP network: **ORIGINAL-PARTNER**

Source interface: inside

Destination interface: Site-To-Site

https://t.me/learningnets
© 2014 Cisco Systems, Inc.



Step 2

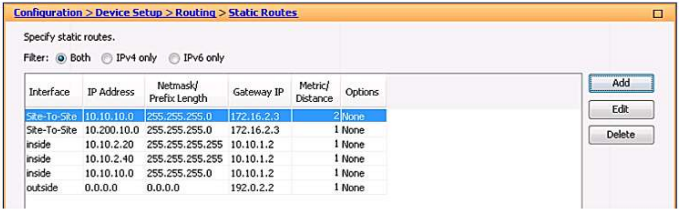
Apply the configuration by clicking the **Apply** button.

https://t.me/learningnets

Step 3

In the Cisco ASDM, navigate to **Configuration > Device Setup > Routing > Static Routes**. Add the following static routes:

Interface	Network	Gateway	Distance
Site-To-Site	10.10.10.0/24	172.16.2.3	2
Site-To-Site	10.200.10.0/24	172.16.2.3	1
inside	10.10.10.0/24	10.10.1.2	1



These three routes are needed in addition to the twice NAT rule to overcome the problem of the overlapping address space. Two routes are needed for the 10.10.10.0/24 network. One should point to the inside interface, and the other should point to the site-to-site interface. One route is needed to send traffic to the internal VLAN 10, and the other is needed to send traffic to the Partner network. Because the ASA cannot accept two same routes for the same destination, one route should be configured with the administrative distance set to 2.

When the traffic is sent from the internal VLAN 10 to the Partner office, the ASA first sees the destination IP address from the 10.200.10.0/24 (this is how the Partner office is seen from the headquarters' perspective). Because the ASA needs to find outgoing interfaces for such traffic (to apply the proper NAT rule and to route the traffic), there is also a route for the 10.200.10.0/24 network, which points to the site-to-site interface.

Step 4

Apply the configuration by clicking the **Apply** button.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 5

Access the console of the HQ-ISR router and examine the following configuration:

```
HQ-ISR# show running-config
<output omitted>
interface Tunnel1
 description IPsec VPN tunnel to Partner office
 ip address 172.16.101.1 255.255.255.0
 ip ospf message-digest-key 1 md5 cisco
 tunnel source GigabitEthernet0/1
 tunnel destination 198.51.100.1
 tunnel protection ipsec profile IPSEC_PROFILE
!
<output omitted>
!
router ospf 2
 redistribute static subnets route-map RED_OSPF
 network 172.16.101.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
ip http server
ip http authentication local
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.0.2.2
ip route 10.10.10.0 255.255.255.0 Tunnel1 172.16.101.2
ip route 10.100.10.0 255.255.255.0 172.16.2.1 tag 100
!
<output omitted>
!
route-map RED_OSPF permit 10
 match tag 100
```

The router is configured with IPsec VPN tunnel to the Partner office. The IP address of the tunnel interface is from the 172.16.101.0/24 subnet. The router is also configured with the static route for the mapped VLAN 10 address (10.100.10.0/24). The route points to the HQ-ASA IP address for the site-to-site interface and is required to send traffic from the Partner traffic to VLAN 10. This route is also redistributed into OSPF to advertise the network to the Partner router. Redistribution of static routes is done selectively using a tag and a route map to control which static routes are allowed to be redistributed into OSPF.

The router is also configured with a route for the Partner network (10.10.10.0/24) which points to the tunnel interface. This route is needed to allow the router to send traffic to the Partner network.

https://t.me/learningnets

Step 6

Access the console of the HQ-SW switch. Move the Employee PC to VLAN 10 by using the following commands:

```
configure terminal
interface GigabitEthernet0/1
 switchport access vlan 10
 shutdown
 no shutdown
```

The Employee PC will get a correct IP address from a DHCP server.

Step 7

Return to the Employee PC. The Employee PC should be in VLAN 10 now. Open a command prompt and verify the IP address on the PC:

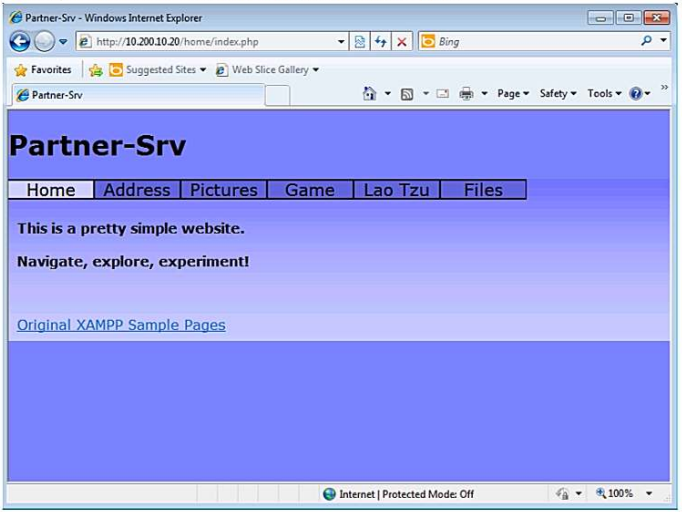
```
C:\Users\it1>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection 3:
   Connection-specific DNS Suffix  . : secure-x.local
   Link-local IPv6 Address . . . . . : fe80::ad39:69d6:419a:ef9c%20
   IPv4 Address. . . . . . . . . . . : 10.10.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
```

The IP address from the 10.10.10.0/24 subnet indicates that the PC is in VLAN 10.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

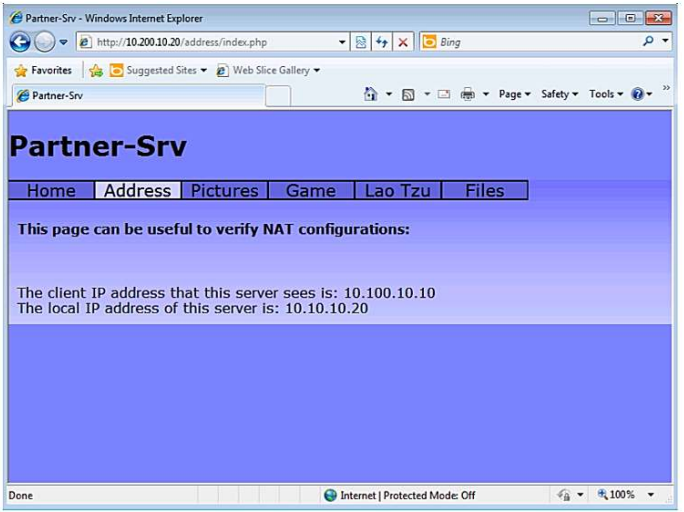
Step 8

Open Internet Explorer on the Employee PC and navigate to the translated IP address of the Partner-SRV (10.200.10.20). This is how the inside VLAN 10 sees the Partner-SRV.



You should be successful. Navigate to the **Address** link on the web page. The web page that opens will show you that the Partner-SRV sees your connection as coming from the translated IP address (10.100.10.10) of the Employee PC. You should also see the local IP address of the server which is 10.10.10.20. Recall that when you made the connection from the Employee PC, the source IP address was that of the Employee PC (10.10.10.10 as indicated in the command prompt printout), and the destination IP address was the mapped IP address of the Partner-SRV (10.200.10.20 as written into the Internet Explorer address bar).

https://t.me/learningnets



Step 9

Return to the HQ-ASA console. Display the NAT table. You should see the configured twice NAT rule in the first section of the NAT table. You should also see statistics for translated packets.

```
HQ-ASA# show nat
Manual NAT Policies (Section 1)
1 (inside) to (Site-To-Site) source static REAL-VLAN10 TRANSLATED-
VLAN10   destination static TRANSLATED-PARTNER ORIGINAL-PARTNER
    translate_hits = 28, untranslate_hits = 28
Auto NAT Policies (Section 2)
1 (inside) to (outside) source static HQ-SRV TRANSLATED-HQ-SRV
    translate_hits = 660, untranslate_hits = 6
2 (DMZ) to (outside) source static DMZ-SRV TRANSLATED-DMZ-SRV
    translate_hits = 4073, untranslate_hits = 32
3 (DMZ) to (outside) source static HQ-ESA TRANSLATED-HQ-ESA
    translate_hits = 1075, untranslate_hits = 1763
4 (inside) to (outside) source dynamic Internal-Networks TRANSLATED-INSIDE-HOSTS
    translate_hits = 3361, untranslate_hits = 2
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 10

On the HQ-ASA console, display the Xlate table. You should see two static translations between the Employee PC (10.10.10.10) and the Partner-SRV. One is used to translate source IP address, and the other is used to translate destination IP address.

Observer that both translations are marked with s and T flags.

```
HQ-ASA# show xlate
7 in use, 55 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from inside:10.10.3.20 to outside:192.0.2.20
    flags s idle 0:00:01 timeout 0:00:00
NAT from DMZ:172.16.1.50 to outside:192.0.2.50
    flags s idle 0:26:35 timeout 0:00:00
NAT from DMZ:172.16.1.55 to outside:192.0.2.55
    flags s idle 0:00:02 timeout 0:00:00
NAT from inside:10.10.10.0/24 to Site-To-Site:10.100.10.0/24
    flags sT idle 0:00:04 timeout 0:00:00
NAT from Site-To-Site:10.10.10.0/24 to inside:10.200.10.0/24
    flags sT idle 0:00:04 timeout 0:00:00
TCP PAT from inside:10.10.2.40/20674 to outside:192.0.2.100/20674 flags ri idle
0:00:53 timeout 0:00:30
TCP PAT from inside:10.10.2.40/20673 to outside:192.0.2.100/20673 flags ri idle
0:00:53 timeout 0:00:30
```

Activity Verification

No verification is needed in this task.

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 3-2: Configure Cisco IOS Software NAT

Activity Objective

The partner company of the Secure-X company has a network topology as shown in the figure. The partner company requested help with configuration of their Cisco IOS Software router. The partner company requires outbound connectivity to the Internet for clients in the network, and inbound connectivity from the Internet to the server.

You are the network security engineer for the Secure-X network. The CSO of the Secure-X network tasked you to help the partner network to configure NAT on their Cisco IOS Software router. You will have to configure static NAT to enable inbound connectivity to the server, and dynamic NAT with PAT to enable outbound connectivity from the internal clients to the Internet.

In this activity you will configure NAT on Cisco IOS router:

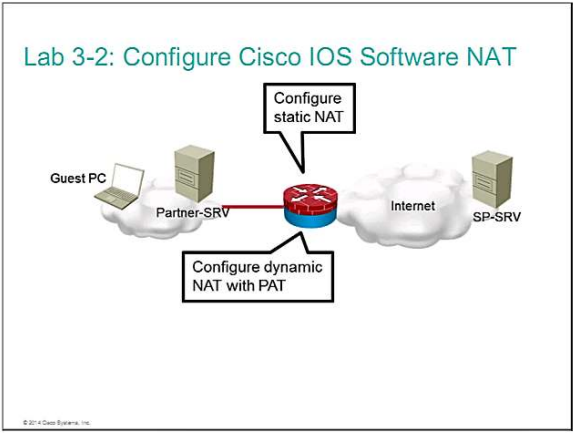
Configure static NAT on the Cisco IOS Software router

Configure dynamic NAT with PAT on the Cisco IOS Software router

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Commands

Command	Description
debug ip nat	Enables NAT debugging.
interface *interface*	Enters interface configuration mode.
ip access-list standard *ACL-name*	Creates a standard ACL and enters ACL configuration mode.
ip nat inside source list *ACL-name* **pool** *pool_name* **overload**	Creates a dynamic NAT rule that translates the source network to the IP address(es) in a pool. The **overload** keyword permits more IP addresses to be translated into a single IP address.
ip nat inside source static *inside-local-IP inside-global-IP*	Creates a static one-to-one address translation.
ip nat {outside | inside}	Enables NAT and tags the interface as NAT outside or NAT inside.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command	Description
ip nat pool *pool_name start_ip end_ip* **netmask** *mask*	Creates a pool of IP address(es) for NAT translations.
{permit | deny} *source-network wildcard-mask*	Creates a statement in the ACL configuration.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays a NAT translation table.

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

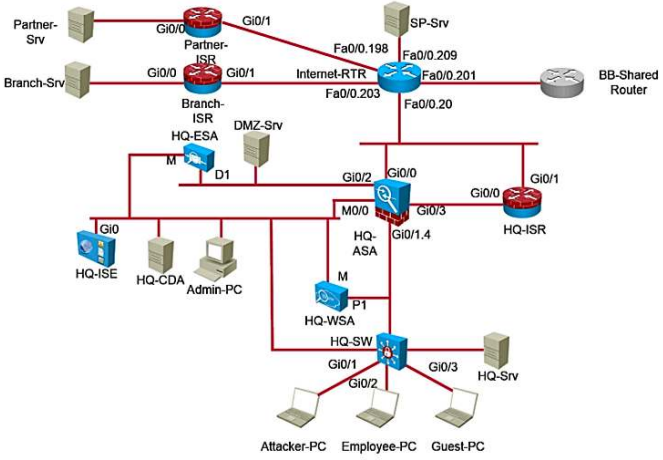
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

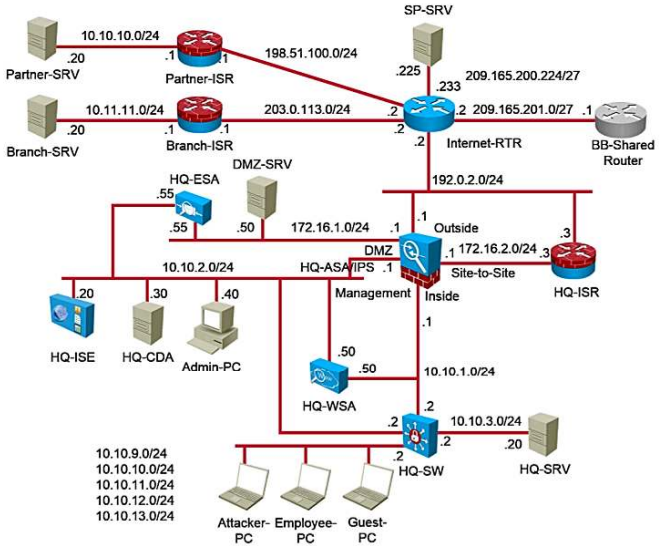
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



https://t.me/learningnets

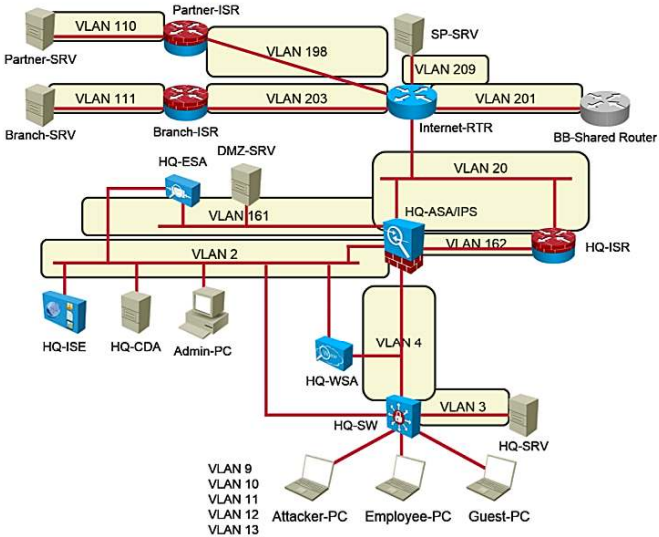
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure Static NAT

In this task, you will configure static NAT on the Partner-ISR router. Static NAT will translate IP address of the Partner-SRV to a public address and expose the server to the outside networks. Then you will verify static NAT configuration by triggering and inbound traffic to the Partner-SRV.

Activity Procedure

Complete the following steps:

Step 1

Access the Partner-ISR router console.

Step 2

On the Partner-ISR router, enable NAT on the GigabitEthernet0/1 interface and tag the interface as NAT outside.

https://t.me/learningnets

Step 3

On the Partner-ISR router, enable NAT on the GigabitEthernet0/0 interface and tag the interface as NAT inside.

Step 4

On the Partner-ISR router, configure static NAT translation for the Partner-SRV at 10.10.10.20. The server should translate to 198.51.100.20.

Step 5

Access the SP-SRV. Open Internet Explorer and navigate to the translated IP address of the Partner-SRV (198.51.100.20). You should be successful.

Step 6

Quickly return to the Partner-ISR console and display active NAT translations. You should see a similar output:

```
Partner-ISR# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 198.51.100.20:80   10.10.10.20:80     209.165.200.233:1183 209.165.200.233:1183
tcp 198.51.100.20:80   10.10.10.20:80     209.165.200.233:1184 209.165.200.233:1184
--- 198.51.100.20      10.10.10.20        ---                ---
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 7

On the Partner-ISR router, display NAT statistics.

```
Partner-ISR# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 23, occurred 02:33:37 ago
Outside interfaces:
  GigabitEthernet0/1
Inside interfaces:
  GigabitEthernet0/0
Hits: 15851  Misses: 0
CEF Translated packets: 15774, CEF Punted packets: 77
Expired translations: 85
Dynamic mappings:
<output omitted>
```

Step 8

On the Partner-ISR router, enable NAT debugging.

```
Partner-ISR# debug ip nat
```

Step 9

Return to the SP-SRV and refresh the web page on the Partner-SRV.

Step 10

Return to the Partner-ISR router and observe debugging messages. In the first line of the output you should see how is the destination IP address of the traffic from the SP-SRV to the Partner-SRV translated from 198.51.100.20 to 10.10.10.20. In the second line of the output you should see how the source IP address of the returning traffic is translated from 10.10.10.20 to 198.51.100.20.

```
Partner-ISR#
*Dec 19 13:23:02.727: NAT*: s=209.165.200.233, d=198.51.100.20->10.10.10.20 [28705]
*Dec 19 13:23:02.739: NAT*: s=10.10.10.20->198.51.100.20, d=209.165.200.233 [21357]
*Dec 19 13:23:02.739: NAT*: s=209.165.200.233, d=198.51.100.20->10.10.10.20 [28706]
*Dec 19 13:23:02.739: NAT*: s=209.165.200.233, d=198.51.100.20->10.10.10.20 [28707]
*Dec 19 13:23:02.743: NAT*: s=10.10.10.20->198.51.100.20, d=209.165.200.233 [21358]
```

Step 11

On the Partner-ISR router, disable NAT debugging.

```
Partner-ISR# no debug ip nat
```


https://t.me/learningnets

Activity Verification

No verification is needed in this task.

Task 2: Configure Dynamic NAT

In this task, you will configure dynamic NAT with PAT on the Partner-ISR router. Dynamic NAT with PAT will translate IP addresses of the hosts in the 10.10.10.0/24 to a public address and thus enable outside connectivity. You will verify dynamic NAT configuration by moving the Guest PC into the Partner network and triggering outbound traffic.

Activity Procedure

Complete the following steps:

Step 1

Return to the Partner-ISR router console.

Step 2

On the Partner-ISR router, create a standard ACL that will permit traffic from the inside Partner network (10.10.10.0/24). Use **NAT** as the name for the ACL.

Step 3

On the Partner-ISR router, create a pool for translated IP address. The pool should consist of a single IP address 198.51.100.100. Use **POOL** as the name for the pool.

Step 4

On the Partner-ISR router, configure dynamic NAT with PAT translation for hosts on the inside network. Use the previously configured ACL and NAT pool.

Step 5

Access the console of the HQ-SW switch. Move the Guest PC to VLAN 110 by using the following commands:

```
configure terminal
interface GigabitEthernet0/2
 switchport access vlan 110
 shutdown
 no shutdown
```

VLAN 110 is the VLAN in the Partner network. The Guest PC will get a correct IP address from a DHCP server.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

On the Guest PC, open Internet Explorer and navigate to **http://sp-srv.sp-public**. You should be successful.

Step 7

Quickly return to the Partner-ISR console and display active NAT translations. You should see a number of translations similar to the output shown below. In the output bellow, you should see three dynamic translations. The last one is translation for DNS traffic from the Guest PC to the SP-SRV, and the first two are for HTTP traffic from the Guest PC to the SP-SRV.

```
Partner-ISR# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 198.51.100.20      10.10.10.20        ---                ---
tcp 198.51.100.100:1192 10.10.10.200:1192 209.165.200.233:80 209.165.200.233:80
tcp 198.51.100.100:1193 10.10.10.200:1193 209.165.200.233:80 209.165.200.233:80
udp 198.51.100.100:53831 10.10.10.200:53831 209.165.200.233:53 209.165.200.233:53
```


https://t.me/learningnets

Step 8

On the Partner-ISR router, display NAT statistics.

```
Partner-ISR# show ip nat statistics
Total active translations: 4 (1 static, 3 dynamic; 3 extended)
Peak translations: 47, occurred 19:16:17 ago
Outside interfaces:
  GigabitEthernet0/1
Inside interfaces:
  GigabitEthernet0/0
Hits: 55688  Misses: 0
CEF Translated packets: 55112, CEF Punted packets: 576
Expired translations: 448
Dynamic mappings:
-- Inside Source
[Id: 2] access-list NAT pool POOL refcount 3
 pool POOL: netmask 255.255.255.0
        start 198.51.100.100 end 198.51.100.100
        type generic, total addresses 1, allocated 1 (100%), misses 0
<output omitted>
```

Step 9

On the Partner-ISR router, enable NAT debugging.

```
Partner-ISR# debug ip nat
```

Step 10

Return to the Guest PC and refresh the web page in the Internet Explorer.

Step 11

Return to the Partner-ISR router and observe debugging messages. In the first line of the output you should see how the source IP address of the traffic from the Guest PC to the SP-SRV translated from 10.10.10.200 to 198.51.100.100. In the second line of the output you should see how the destination IP address of the returning traffic is translated from 198.51.100.100 to 10.10.10.200.

```
Partner-ISR#
*Dec 20 09:05:51.991: NAT*: s=10.10.10.200->198.51.100.100, d=209.165.200.233 [826]
*Dec 20 09:05:51.995: NAT*: s=209.165.200.233, d=198.51.100.100->10.10.10.200 [1305]
*Dec 20 09:05:51.995: NAT*: s=10.10.10.200->198.51.100.100, d=209.165.200.233 [827]
*Dec 20 09:05:51.995: NAT*: s=10.10.10.200->198.51.100.100, d=209.165.200.233 [828]
*Dec 20 09:05:51.999: NAT*: s=209.165.200.233, d=198.51.100.100->10.10.10.200 [1306]
*Dec 20 09:05:52.003: NAT*: s=10.10.10.200->198.51.100.100, d=209.165.200.233 [829
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 12

On the Partner-ISR router, disable NAT debugging.

```
Partner-ISR# no debug ip nat
```

Activity Verification

No verification is needed in this task.

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 4-1: Configure Basic Cisco ASA Access Policies

Activity Objective

The company Secure-X has a network topology as shown in the figure. The company recently hired a new Chief Security Officer that wants to improve all of the current network security controls with the latest technologies to support the most recent company security policy.

You are the network security engineer for the Secure-X network. The Secure-X network requires connectivity between various internal hosts, internal servers, DMZ servers, and external servers. NAT configuration is already in place, but the ACLs that are currently configured on the ASA do not suffice to the connectivity requirements. The CSO tasked you with implementing ACLs on the Cisco Adaptive Security Appliance to allow connectivity between the devices in the network and in the Internet. The CSO also instructed to allow only minimal inbound connectivity, as specified by the requirements for individual publicly available servers.

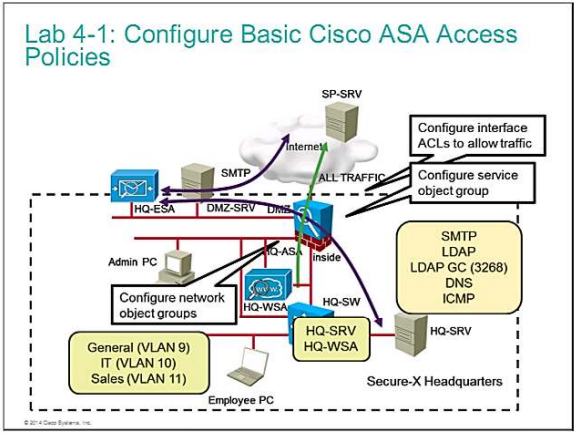
In this activity you will configure basic Cisco ASA access control features:

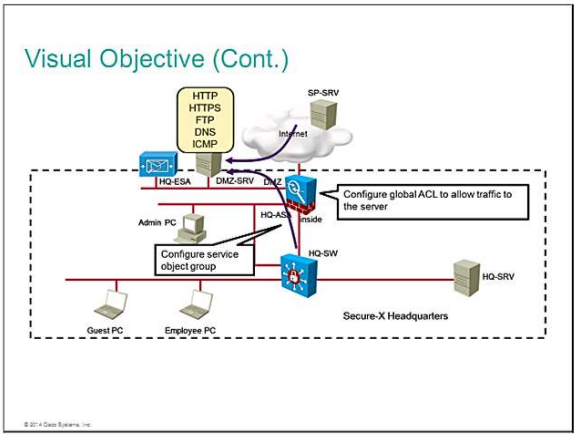
- Configure object groups
- Configure interface ACLs
- Configure global ACLs
- Verify ACLs

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.





Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command List

The table describes the Cisco ASA commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco ASA Commands

Command	Description
show access-list	Displays ACL configuration and statistics.

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

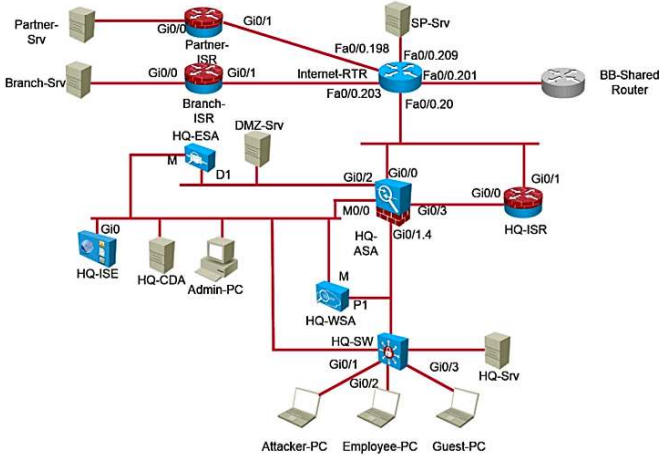
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

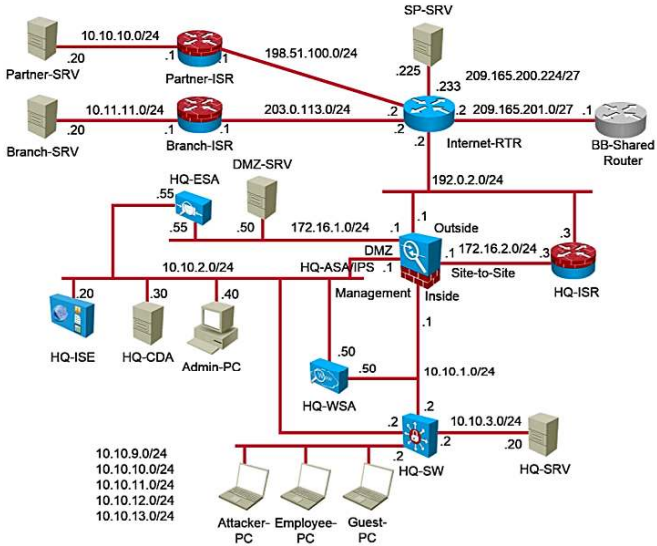
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



https://t.me/learningnets

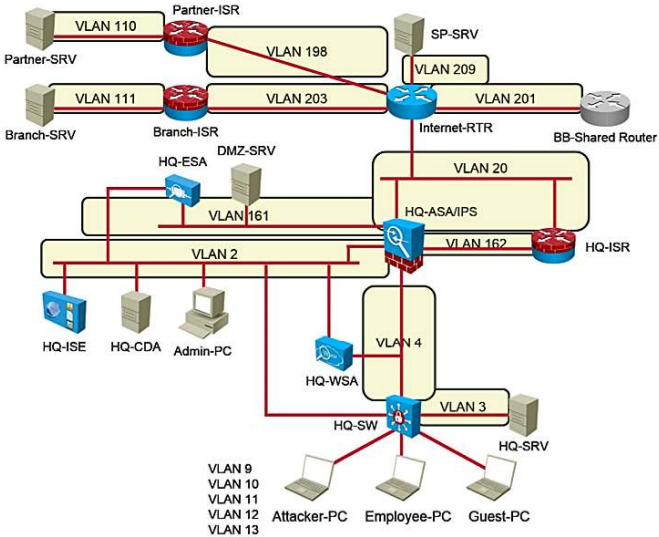
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure Object Groups

In this task, you will create network objects, network object groups, and service object groups, which will be needed in the later tasks to enable connectivity over HQ-ASA.

Activity Procedure

Complete the following steps:

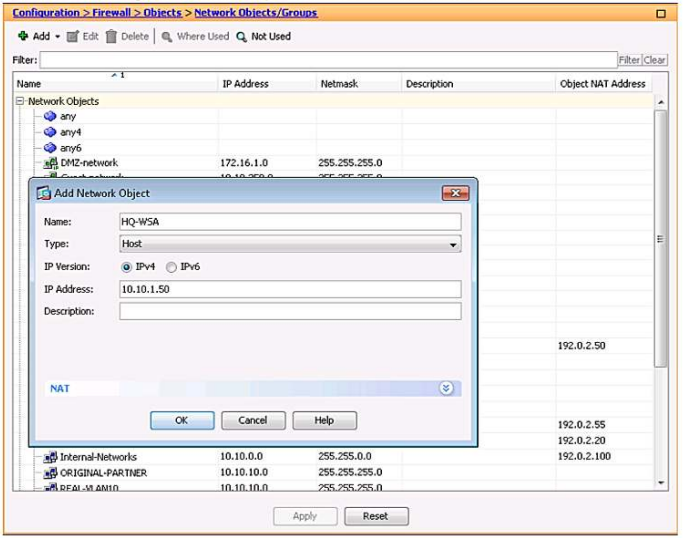
Step 1

Access the Admin PC. Start Cisco ASDM by double-clicking its icon on the desktop. Connect to the HQ-ASA at 10.10.2.1. Log in using **admin** as the username and **Ci5coAdmin** as the password.

https://t.me/learningnets

Step 2

When Cisco ASDM opens, navigate to **Configuration > Firewall > Objects > Network Objects/Groups**. Create a new network object with name HQ-WSA and IP address 10.10.1.50.



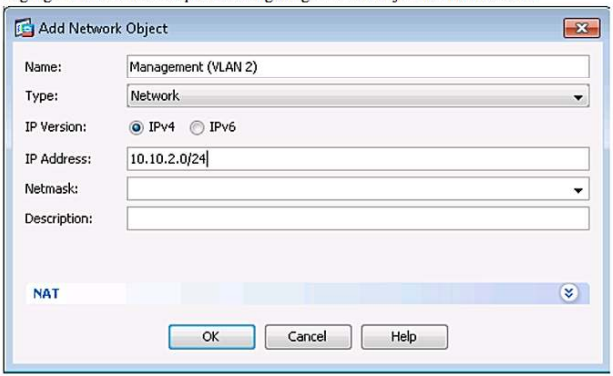
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

Repeat the previous step and configure the following network objects:

Network Object Name	Description	Network Object IP Address
Management	VLAN 2	10.10.2.0/24
General	VLAN 9	10.10.9.0/24
IT	VLAN 10	10.10.10.0/24
Sales	VLAN 11	10.10.11.0/24

The following figure shows an example of configuring network object for 10.10.2.0/24.



https://t.me/learningnets

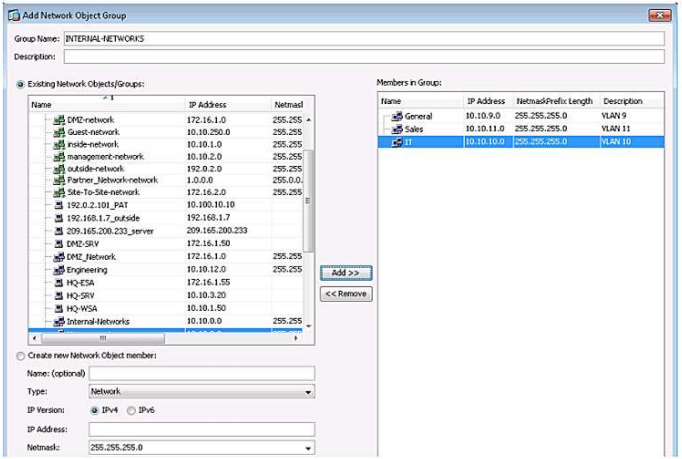
Step 4

In the same Cisco ASDM window, create a network object group and name it **INTERNAL-NETWORKS**. Include the following objects in the group:

General

IT

Sales



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

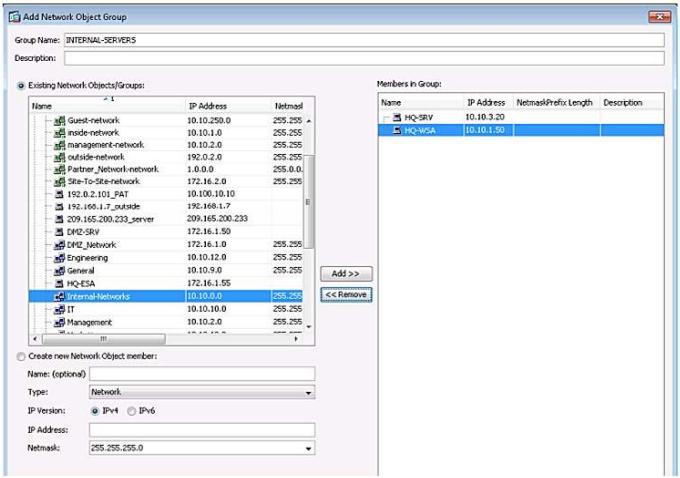
Step 5

Create another network object group and name it **INTERNAL-SERVERS**.

Include the following objects in the group:

HQ-SRV

HQ-WSA



https://t.me/learningnets

Step 6

In the Cisco ASDM, navigate to **Configuration > Firewall > Objects > Service Objects/Groups**. Create an IP service group and name it **DMZ-SRV-SERVICES**.

Include the following services in the group:

TCP/HTTP

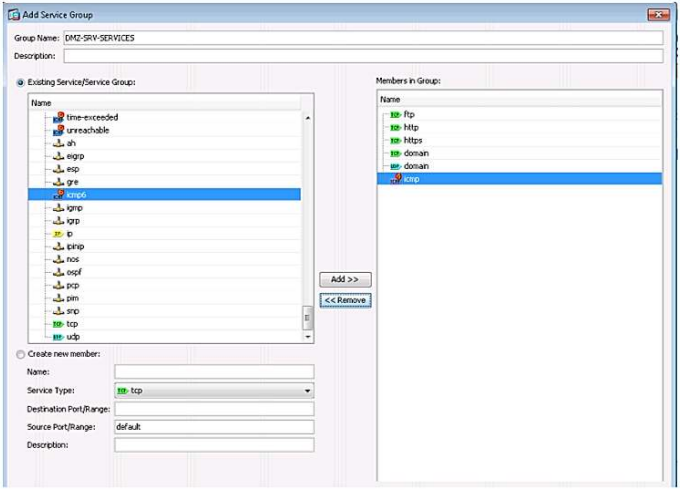
TCP/HTTPS

TCP/FTP

TCP/DNS

UDP/DNS

ICMP



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 7

Create another IP service group and name it **HQ-SRV-SERVICES**.

Include the following services in the group:

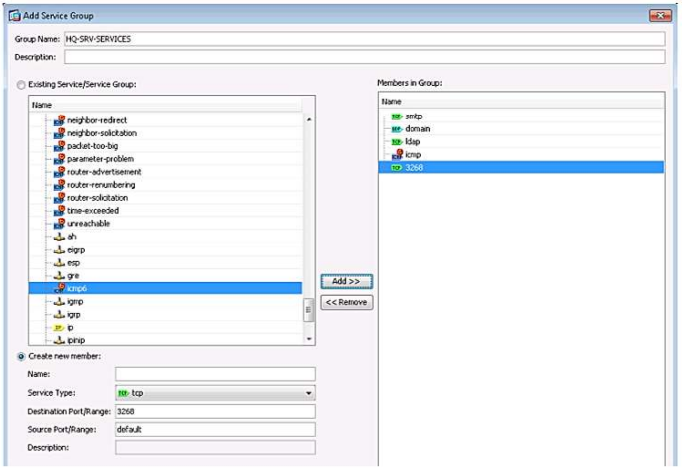
TCP/SMTP

TCP/LDAP

TCP/3268 (LDAP Global Catalogue)

UDP/DNS

ICMP



Step 8

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

Activity Verification

No verification is needed in this task.

https://t.me/learningnets

Task 2: Configure Interface ACLs

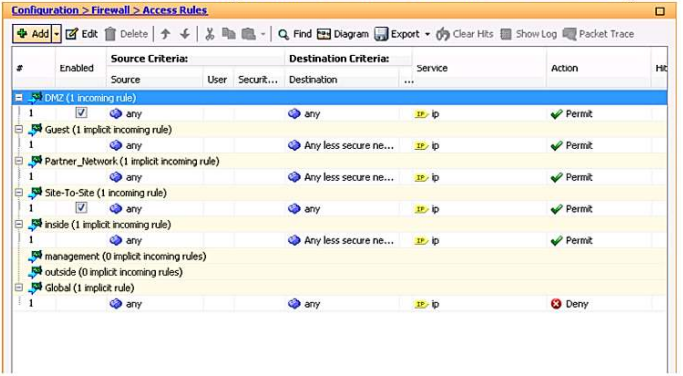
In this task, you will configure ACLs on the HQ-ASA to allow connectivity as required by using the previously configured object groups. First, you will allow all IP connectivity from the internal networks to the outside. Then, you will enable DNS, SMTP, and LDAP connectivity from the HQ-ESA mail transfer agent to the internal mail server on the HQ-SRV, deny connectivity from the DMZ network to the internal networks, and allow all other IP connectivity from the DMZ network to outside. Finally, you will enable SMTP connectivity from the outside to the HQ-ESA mail transfer agent to allow receiving emails from external senders.

Activity Procedure

Complete the following steps:

Step 1

In the Cisco ASDM, navigate to **Configuration > Firewall > Access Rules**. Review the existing ACLs.



You should see there are only two explicit ACLs configured; one on the DMZ interface and another on the Site-To-Site interface. Both are allowing all IP traffic through the interfaces in the inbound direction.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

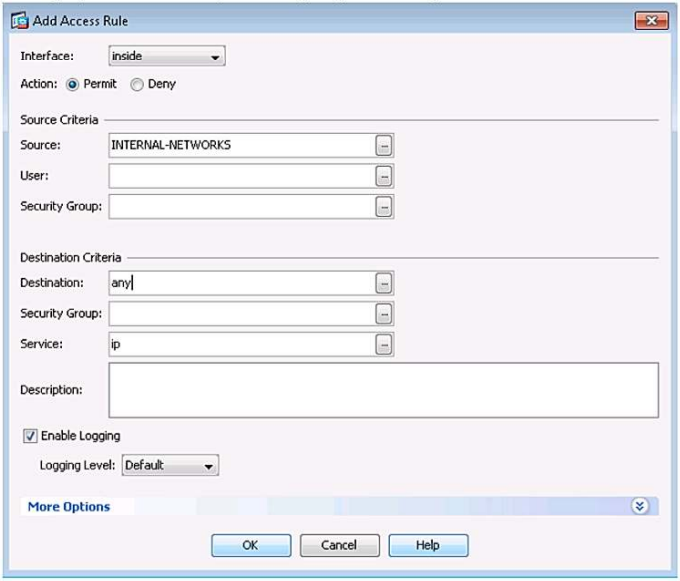
Step 2

Create an ACL on the inside interface with the following ACL entries:

Source	Destination	Service	Action
Management	any	ip	Permit
INTERNAL-NETWORKS	any	ip	Permit
INTERNAL-SERVERS	any	ip	Permit

This ACL is needed to allow connectivity from the internal hosts and networks to all destinations.

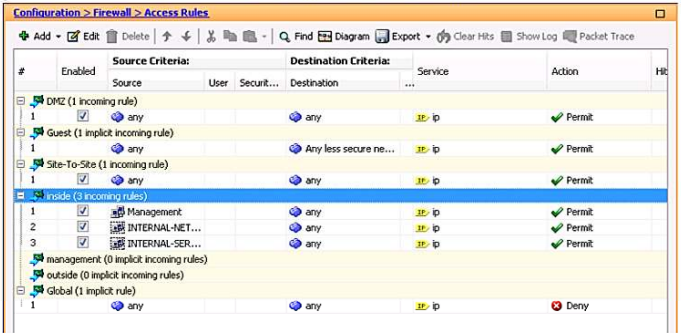
The following figure shows an example of configuring the first entry.



https://t.me/learningnets

Step 3

After you added all the rules, the Access Rules table should look like this:



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

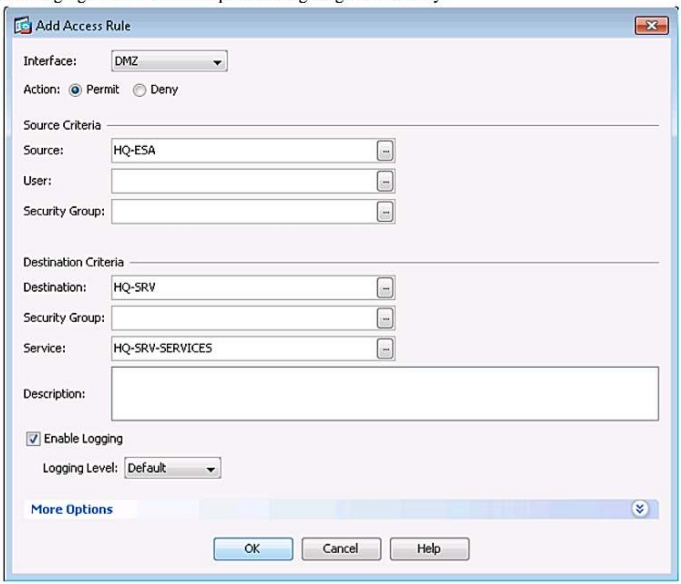
Step 4

Delete the existing explicit permit-all rule ACL on the DMZ interface and create a new ACL with the following entries:

Source	Destination	Service	Action
HQ-ESA	HQ-SRV	HQ-SRV-SERVICES	Permit
any	INTERNAL-SERVERS	ip	Deny
any	INTERNAL-NETWORKS	ip	Deny
any	any	ip	Permit

This ACL is needed to allow the HQ-ESA to send emails to the HQ-SRV mail server, and to make DNS and LDAP queries to the HQ-SRV. The DNS and LDAP queries are required for successful HQ-ESA operations. The ACL also prevents all other communication from the DMZ network to the internal networks and servers, and allows communication from DMZ to all other destinations.

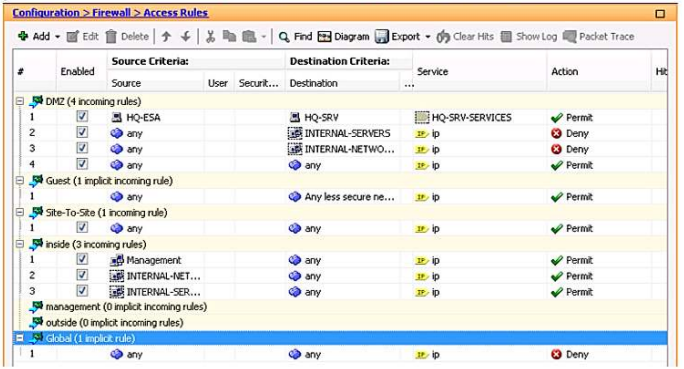
The following figure shows an example of configuring the first entry.



https://t.me/learningnets

Step 5

After you added all rules, the Access Rules table should look like shown below:



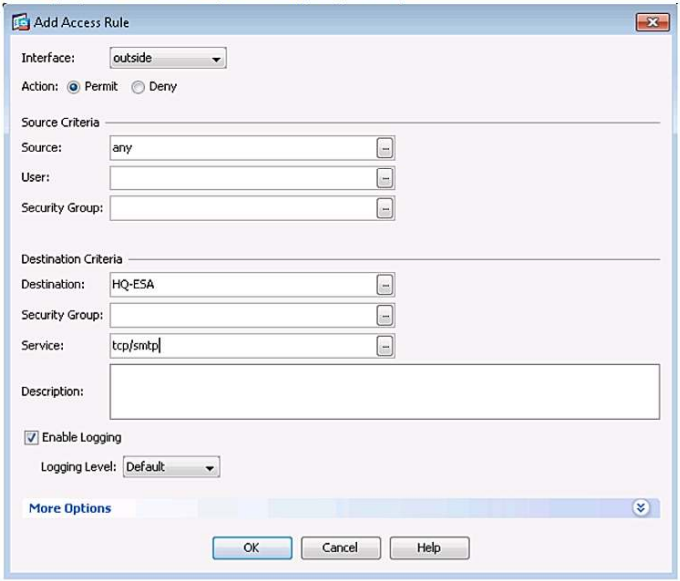
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

Create a new ACL on the outside interface with the following entry:

Source	Destination	Service	Action
any	HQ-ESA	tcp/smtp	Permit

The following figure shows an example of configuring the entry.

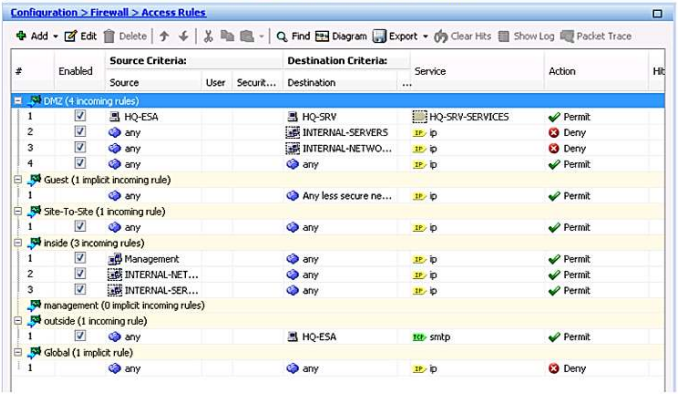


This ACL is needed to allow the external mail servers to send emails to the HQ-ESA.

https://t.me/learningnets

Step 7

After you added all the rules, the Access Rules table should look like this:



#	Enabled	Source Criteria: Source	User	Securit...	Destination Criteria: Destination	...	Service	Action	Hit
DMZ (4 incoming rules)									
1	✓	HQ-ESA			HQ-SRV		HQ-SRV-SERVICES	Permit	
2	✓	any			INTERNAL-SERVERS		ip	Deny	
3	✓	any			INTERNAL-NETWO...		ip	Deny	
4	✓	any			any		ip	Permit	
Guest (1 implicit incoming rule)									
1		any			Any less secure ne...		ip	Permit	
Site-To-Site (1 incoming rule)									
1	✓	any			any		ip	Permit	
inside (3 incoming rules)									
1	✓	Management			any		ip	Permit	
2	✓	INTERNAL-NET...			any		ip	Permit	
3	✓	INTERNAL-SER...			any		ip	Permit	
management (0 implicit incoming rules)									
outside (1 incoming rule)									
1	✓	any			HQ-ESA		smtp	Permit	
Global (1 implicit rule)									
1		any			any		ip	Deny	

Step 8

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

Activity Verification

No verification is needed in this task.

Task 3: Configure Global ACL

In this task, you will enable connectivity to the DMZ-SRV for the required DMZ services. This time you will use a global ACL, because connectivity to the server is required from inside and outside of the ASA.

Activity Procedure

Complete the following steps:

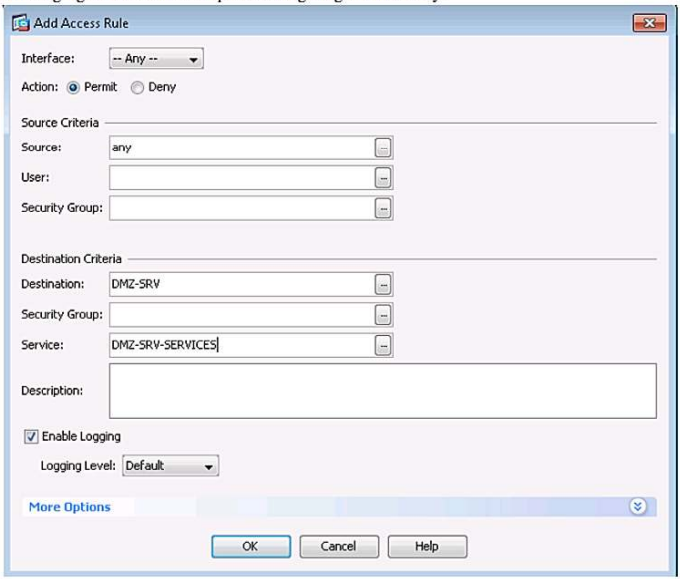
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

In the Cisco ASDM, navigate to **Configuration > Firewall > Access Rules**. Create a new global ACL with the following entries:

Source	Destination	Service	Action
any	DMZ-SRV	DMZ-SRV-SERVICES	Permit
any	any	ip	Deny

The following figure shows an example of configuring the first entry.

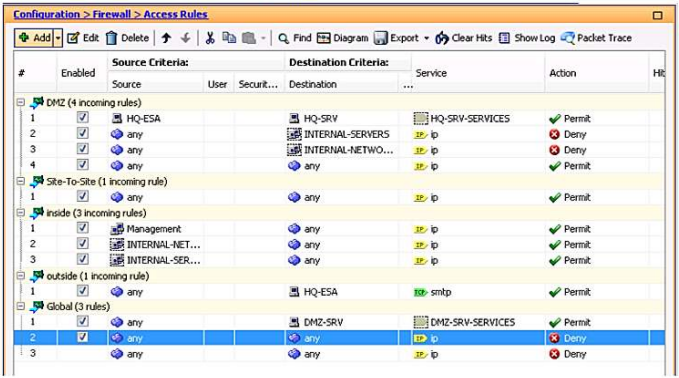


This ACL is needed to allow HTTP, HTTPS, FTP, DNS, and ICMP connectivity to the DMZ-SRV.

https://t.me/learningnets

Step 2

The final Access Rules table should look like this:



Step 3

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

Activity Verification

No verification is needed in this task.

Task 4: Verify Connectivity Across the ASA

In this task, you will verify connectivity across the HQ-ASA. You will trigger traffic across the ASA and observe the effect configured ACLs have on the traffic. You will also observe the logging messages that are produced by the ASA as the traffic is permitted or denied. You will also use the Packet Tracer tool to see how the ASA processes packets.

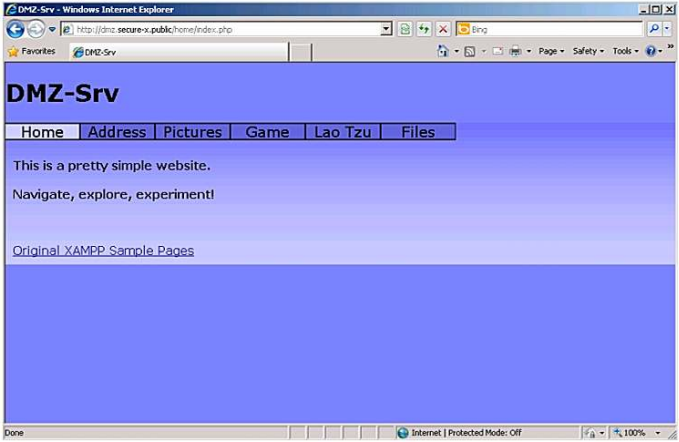
Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

Access the SP-SRV. Open the Internet Explorer browser and navigate to the web page on the DMZ-SRV at **http://dmz.secure-x.public**. This attempt will verify if DNS and HTTP traffic to the DMZ-SRV server is allowed.



The attempt should be successful.

https://t.me/learningnets

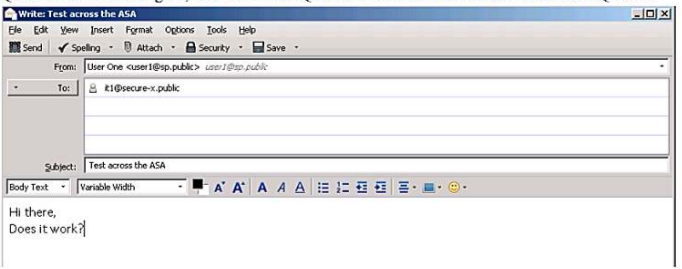
Step 2

On the SP-SRV, open a command prompt and use FTP to connect to the DMZ-SRV. Login using as **anonymous** as the username and anything as the password. This attempt will verify if FTP traffic to the DMZ-SRV server is allowed.

The attempt should be successful.

Step 3

On the SP-SRV, open the Mozzila Thunderbird email client by double-clicking its icon on the desktop. Compose a new email for the **it1@secure-x.public** user as shown below. This email account is created on the HQ-SRV email server. This attempt will test chain of DNS and SMTP connectivity from the outside to the HQ-ESA mail transfer agent, and from the HQ-ESA to the internal mail server on the HQ-SRV.



The email should be sent successfully.

Note The HQ-ESA, HQ-SRV, SP-SRV, and the Employee PC have been preconfigured with email settings to allow sending of emails from the Employee PC to the SP-SRV and vice versa..

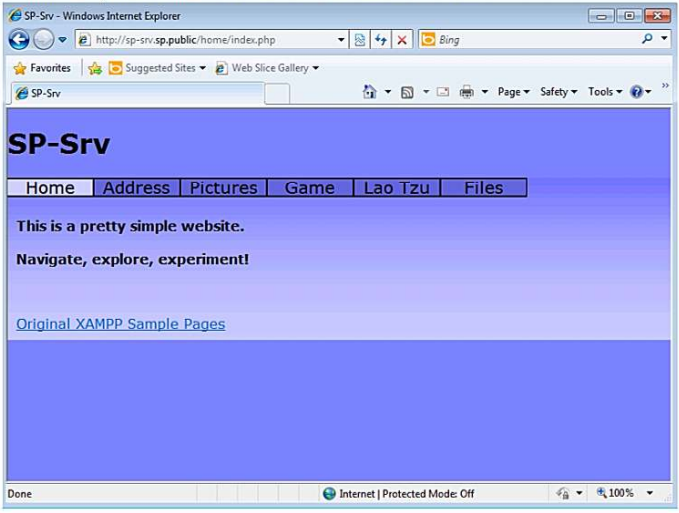
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 4

Access the Employee PC. Log in using **SECURE-X\it1** as the username and **cisco** as the password.

Step 5

On the Employee PC, open the Internet Explorer web browser and navigate to **http://sp-srv.sp.public**. This will test connectivity from the inside network to the SP-SRV on the outside.

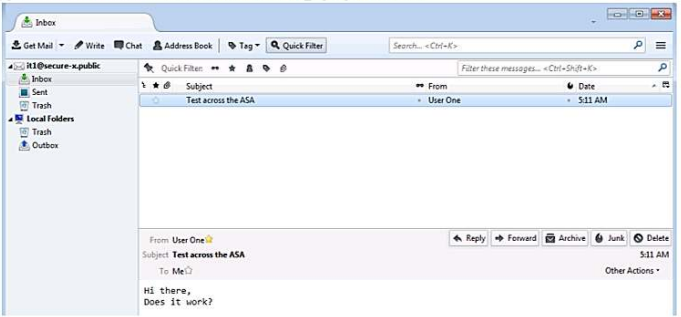


The attempt should be successful.

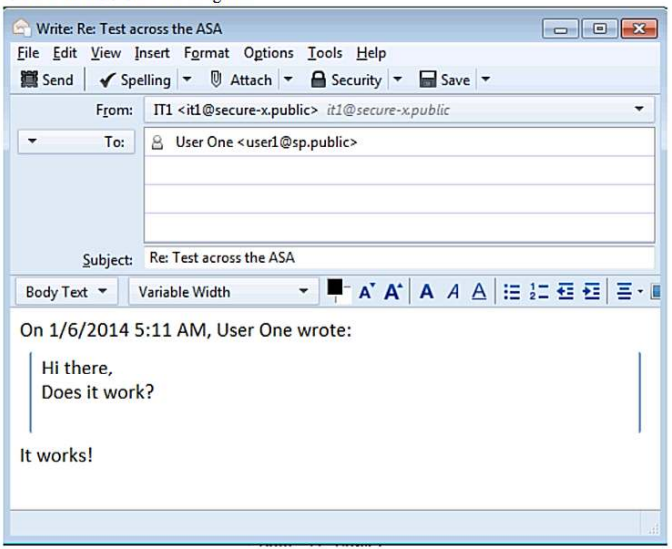
https://t.me/learningnets

Step 6

On the Employee PC, open the Mozzila Thunderbird email client by double-clicking its icon on the desktop. You should see a new email from user1@sp1.public user.



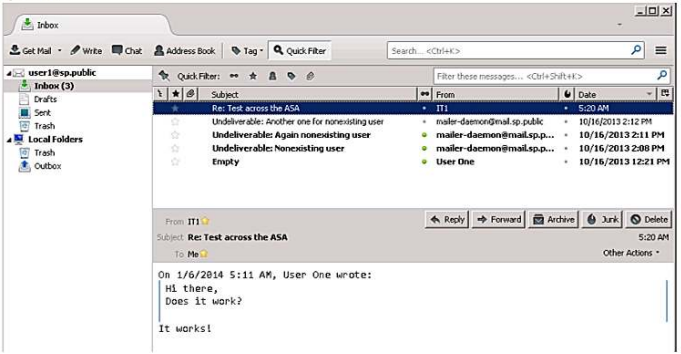
Reply to the email as shown in the figure:



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

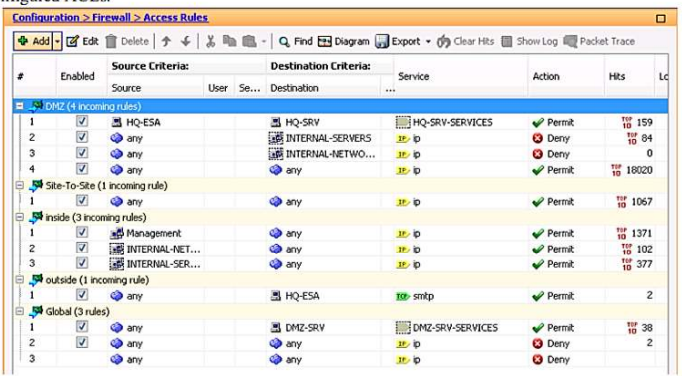
Step 7

Return to the Mozila Thunderbird client on the SP-SRV. You should see the reply that came from the Employee PC.



Step 8

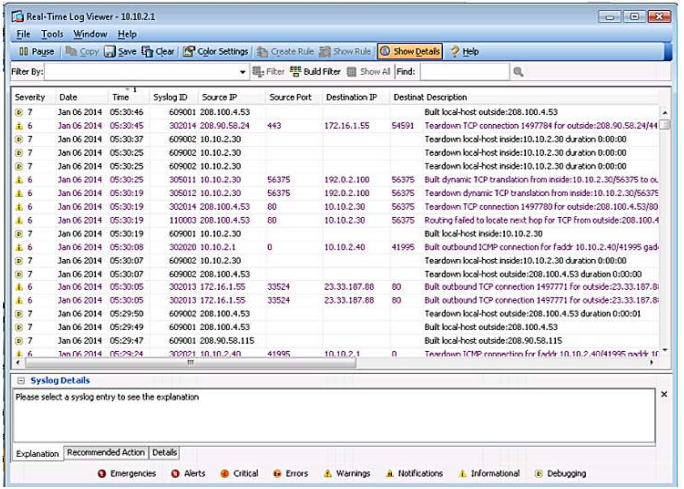
Return to the Cisco ASDM that is running on the Admin PC. Navigate to **Configuration > Firewall > Access Rules**. Observe the number of hits in the configured ACL rules. You should see a number of hits in all configured ACLs.



https://t.me/learningnets

Step 9

In the Cisco ASDM, navigate to **Monitoring > Logging > Real-Time Log Viewer**. Start the viewer by clicking the **View** button. The Real-Time Log Viewer should open.



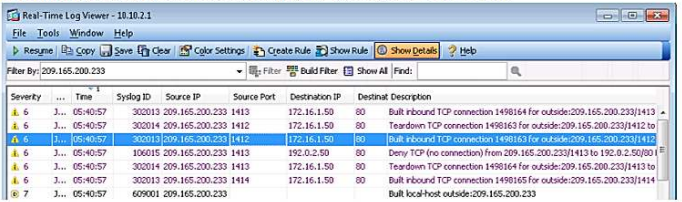
Step 10

Return to the SP-SRV and refresh the web page on the DMZ-SRV in the Internet Explorer. This will again trigger traffic from the SP-SRV to the DMZ-SRV.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 11

Return to the Cisco ASDM Real-Time Log Viewer on the Admin PC. Enter the IP address of the SP-SRV (209.165.200.233) into the Filter By input field and press Enter to filter the output based on IP address. Observe how the ASA built and torn down the connection from the SP-SRV to the DMZ-SRV. You can stop the incoming messages for better readability by clicking the **Pause** button.

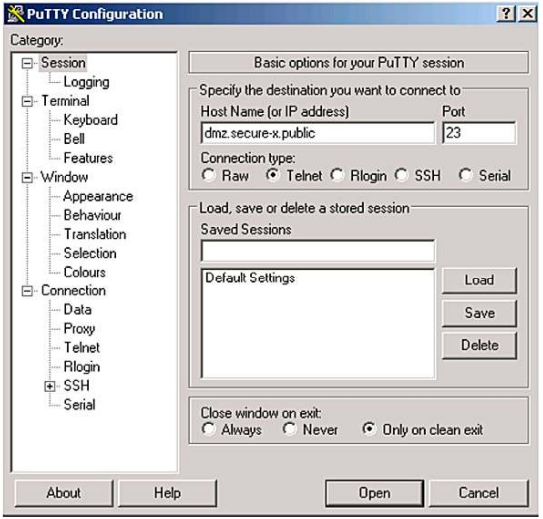


Click the **Resume** button when you are done with examining the logging messages.

https://t.me/learningnets

Step 12

Return to the SP-SRV and open the Putty client by double-clicking its icon on the desktop. Connect to **dmz.secure-x.public** using Telnet.

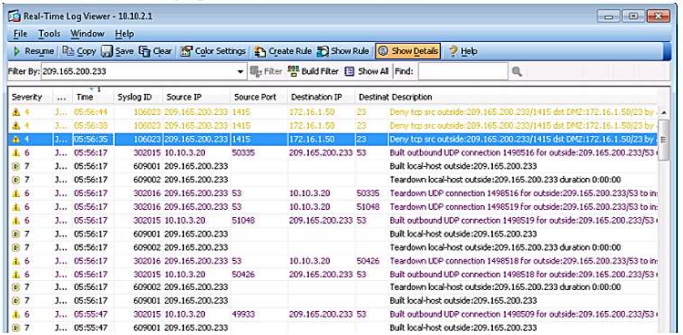


The attempt should not be successful, since Telnet traffic is not included in the DMZ-SRV-SERVICES service group.

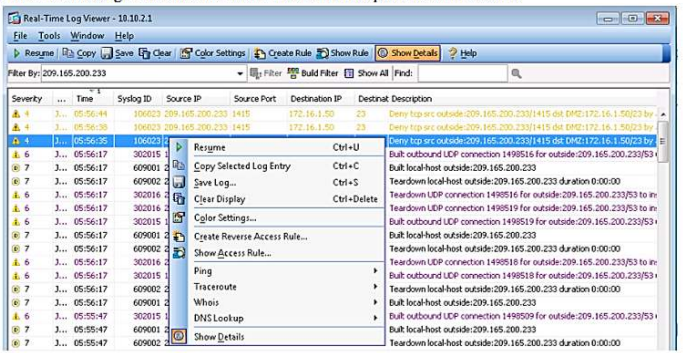
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 13

Return to the Cisco ASDM Real-Time Log Viewer on the Admin PC. Observe the logging messages with ID 106023 about the ASA denying Telnet traffic to the DMZ-SRV.

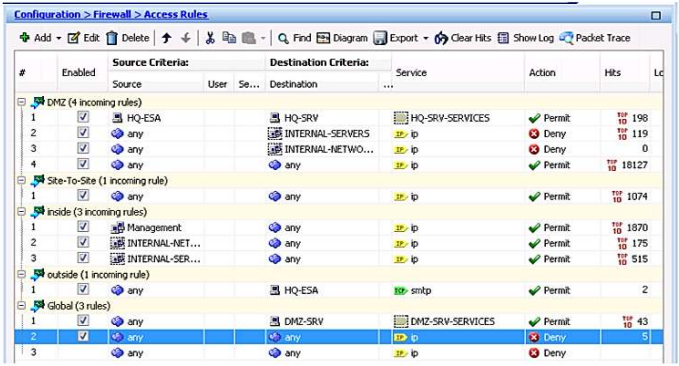


Right-click the message and click the **Show Access Rule** option from the menu.



The Cisco ASDM will display and highlight the rule that denied the connection. You should see that the explicit global deny-all rule denied the Telnet connection.

https://t.me/learningnets



This way, you can determine which ACL rule denied a connection and make necessary changes to ACL configuration if needed.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 14

Another way to determine what is a cause of denied packet is to use the Packet Tracer tool. Start the Packet Tracer in the Cisco ASDM by navigating to **Tools > Packet Tracer**.

Populate the Packet Tracer input fields with the following values:

Interface: outside

Packet Type: TCP

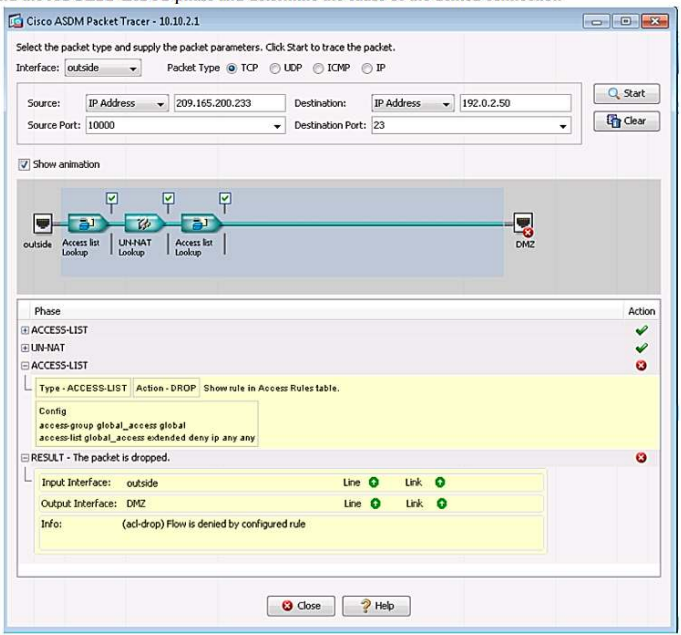
Source IP Address: 209.165.200.233 (SP-SRV)

Destination IP Address: 192.0.2.50 (translated IP addres of the DMZ-SRV)

Source Port: 10000

Destination Port: 23 (Telnet)

Start the packet capture by clicking the **Start** button. You should see that the connection was denied. Expand the **ACCESS-LISTS** phase and determine the cause of the denied connection



https://t.me/learningnets

Click the **Show rule in Access Rules table.** link to display the ACL rule in Cisco ASDM. You should again see that the explicit global deny-all rule denied the Telnet connection.

Step 15

Return to the Packet Tracer tool and perform a trace for a packet that should not be denied by the configured ACLs (for example, HTTP traffic from the SP-SRV to the DMZ-SRV).

Populate the Packet Tracer input fields with the following values:

Interface: outside

Packet Type: TCP

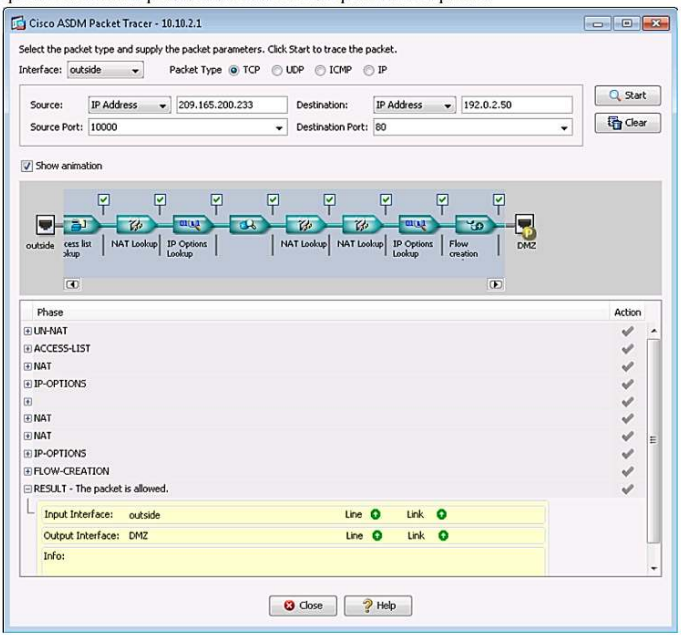
Source IP Address: 209.165.200.233 (SP-SRV)

Destination IP Address: 192.0.2.50 (translated IP addres of the DMZ-SRV)

Source Port: 10000

Destination Port: 80 (HTTP)

Start the packet capture by clicking the Start button. You should see that the connection was allowed. You can expand the individual phases to see how the ASA processed the packet.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 16

Access the HQ-ASA console. Examine the ACL statistics. Observer how the ASA expands object groups to allow monitoring of ACL hists for individual object elements.

```
HQ-ASA# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list DMZ_access_in; 11 elements; name hash: 0x76dc8ff6
access-list DMZ_access_in line 1 extended permit object-group HQ-SRV-SERVICES object
HQ-ESA object HQ-SRV (hitcnt=0) 0x545a6141
  access-list DMZ_access_in line 1 extended permit icmp host 172.16.1.55 host
10.10.3.20 (hitcnt=0) 0x7ed66c7c
  access-list DMZ_access_in line 1 extended permit tcp host 172.16.1.55 host
10.10.3.20 eq 3268 (hitcnt=150) 0xfe232532
  access-list DMZ_access_in line 1 extended permit tcp host 172.16.1.55 host
10.10.3.20 eq ldap (hitcnt=0) 0x23bb79c3
  access-list DMZ_access_in line 1 extended permit tcp host 172.16.1.55 host
10.10.3.20 eq smtp (hitcnt=9) 0x56f76a71
  access-list DMZ_access_in line 1 extended permit udp host 172.16.1.55 host
10.10.3.20 eq domain (hitcnt=63) 0x3cc0de2a
access-list DMZ_access_in line 2 extended deny ip any object-group INTERNAL-SERVERS
(hitcnt=140) 0x58ea2bee
  access-list DMZ_access_in line 2 extended deny ip any host 10.10.3.20 (hitcnt=140)
0x58a203a5
  access-list DMZ_access_in line 2 extended deny ip any host 10.10.1.50 (hitcnt=0)
0xd11891c0
access-list DMZ_access_in line 3 extended deny ip any object-group INTERNAL-NETWORKS
(hitcnt=0) 0x2dd012e3
  access-list DMZ_access_in line 3 extended deny ip any 10.10.9.0 255.255.255.0
(hitcnt=0) 0xc8f3130f
  access-list DMZ_access_in line 3 extended deny ip any 10.10.10.0 255.255.255.0
(hitcnt=0) 0x6001aa82
  access-list DMZ_access_in line 3 extended deny ip any 10.10.11.0 255.255.255.0
(hitcnt=0) 0x1d4b2dc0
access-list DMZ_access_in line 4 extended permit ip any any (hitcnt=18196) 0xc651a8ad
access-list Site-To-Site; 1 elements; name hash: 0x5472414d
access-list Site-To-Site line 1 extended permit ip any any (hitcnt=1082) 0x4c60fca3
access-list inside_access_in; 6 elements; name hash: 0x433a1af1
access-list inside_access_in line 1 extended permit ip object Management any
(hitcnt=1984) 0x36923111
  access-list inside_access_in line 1 extended permit ip 10.10.2.0 255.255.255.0 any
(hitcnt=1984) 0x36923111
access-list inside_access_in line 2 extended permit ip object-group INTERNAL-NETWORKS
any (hitcnt=177) 0x0f732587
  access-list inside_access_in line 2 extended permit ip 10.10.9.0 255.255.255.0 any
(hitcnt=0) 0x47ecc094
  access-list inside_access_in line 2 extended permit ip 10.10.10.0 255.255.255.0 any
(hitcnt=177) 0x8049be2a
  access-list inside_access_in line 2 extended permit ip 10.10.11.0 255.255.255.0 any
(hitcnt=0) 0xb5a7bbb7
access-list inside_access_in line 3 extended permit ip object-group INTERNAL-SERVERS
any (hitcnt=551) 0x6c03032f
  access-list inside_access_in line 3 extended permit ip host 10.10.3.20 any
(hitcnt=388) 0x299a12ef
  access-list inside_access_in line 3 extended permit ip host 10.10.1.50 any
(hitcnt=163) 0x50494b39
access-list outside_access_in; 1 elements; name hash: 0x6892a938
```


https://t.me/learningnets

```
access-list outside_access_in line 1 extended permit tcp any object HQ-ESA eq smtp
(hitcnt=2) 0x07100b3c
  access-list outside_access_in line 1 extended permit tcp any host 172.16.1.55 eq
smtp (hitcnt=2) 0x07100b3c
access-list global_access; 8 elements; name hash: 0xbd6c87a7
access-list global_access line 1 extended permit object-group DMZ-SRV-SERVICES any
object DMZ-SRV (hitcnt=2) 0xa5321530
  access-list global_access line 1 extended permit icmp any host 172.16.1.50
(hitcnt=2) 0xc15d92d7
  access-list global_access line 1 extended permit tcp any host 172.16.1.50 eq domain
(hitcnt=0) 0x0f7fc249
  access-list global_access line 1 extended permit tcp any host 172.16.1.50 eq ftp
(hitcnt=10) 0xa94cc496
  access-list global_access line 1 extended permit tcp any host 172.16.1.50 eq www
(hitcnt=25) 0xb2005a0e
  access-list global_access line 1 extended permit tcp any host 172.16.1.50 eq https
(hitcnt=0) 0xff8ea212
  access-list global_access line 1 extended permit udp any host 172.16.1.50 eq domain
(hitcnt=7) 0x96531694
  access-list global_access line 1 extended permit tcp any host 172.16.1.50 eq telnet
(hitcnt=0) 0x27930285
access-list global_access line 2 extended deny ip any any (hitcnt=9) 0x0cac2fd5
```

Activity Verification

Successful task activity results verify the desired configuration performance.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 4-2: Configure Advanced Cisco ASA Access Policies

Activity Objective

The company Secure-X has a network topology as shown in the figure. The company recently hired a new Chief Security Officer that wants to improve all of the current network security controls with the latest technologies to support the most recent company security policy.

You are the network security engineer for the Secure-X network. Access control lists and NAT configuration on the firewall in the Secure-X headquarters network already allows connectivity as required by the enterprise's policy. However, the CSO required you to further optimize the Cisco ASA stateful inspection to enable ICMP inspection to allow responses to ICMP PINGs to reach internal networks. The CSO also required the Cisco ASA to be visible in traceroute outputs for easier troubleshooting of connectivity issues from the internal networks to the Internet.

The company also experienced unauthorized changes on the company's DMZ server. Specifically, someone deleted files from the FTP server and made changes to the Xampp web server through the Xampp management web interface. The CSO tasked you with protecting the FTP and HTTP server on the DMZ server by enabling application inspection on the Cisco ASA, thus preventing access to the Xampp management web page and deletion of files and folders from the FTP server.

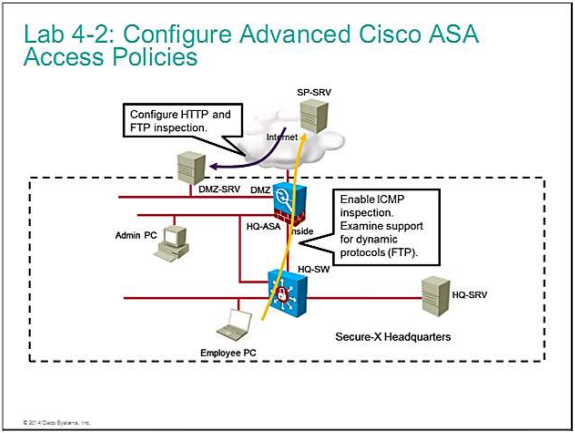
In this activity you will configure advanced Cisco ASA access control features:

- Tune OSI Layer 3-4 stateful inspection
- Examine support for dynamic protocols
- Configure HTTP application inspection
- Configure FTP application inspection

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

Command List

The table describes the Cisco ASA commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco ASA Commands

Command	Description
show conn address *ip_address* **detail**	Displays connection table details for the specified IP address
show service-policy	Displays service policy configuration and statistics

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

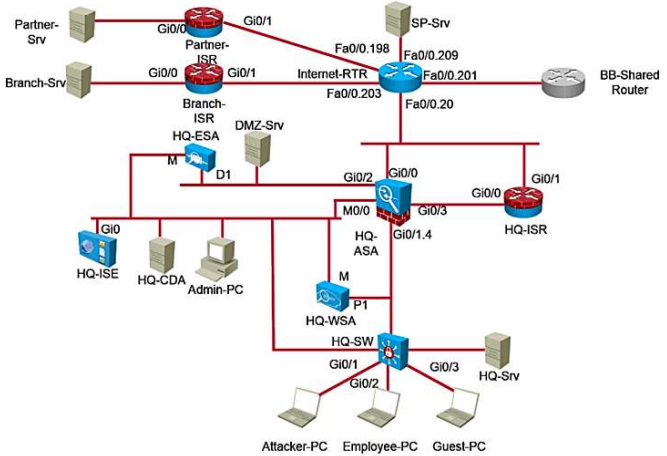
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

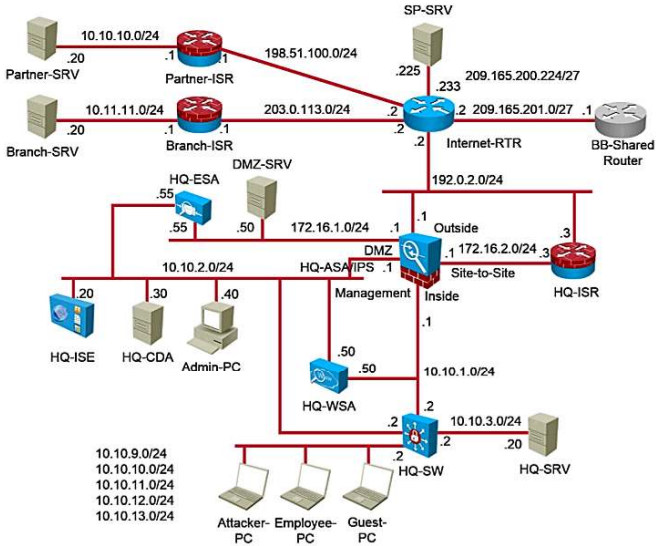
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

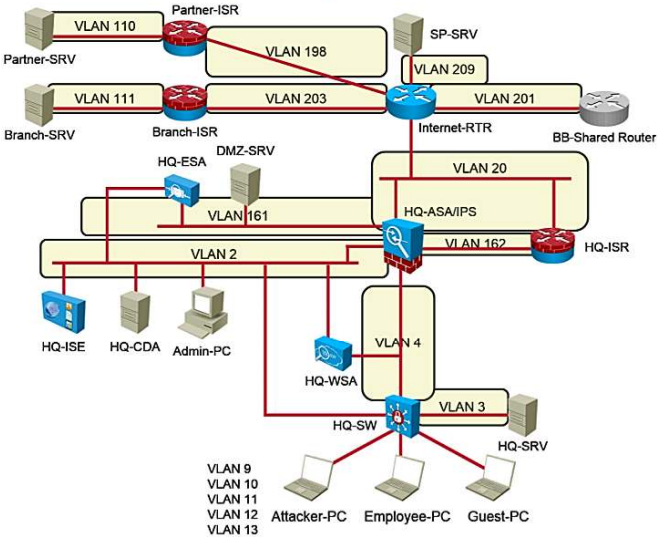
The figure shows the IP addresses that are used in this lab setup.



https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Tune OSI Layer 3-4 Stateful Inspection

In this task, you will first observe default Layer 3-4 stateful inspection on the HQ-ASA. You will first observe how the ASA treats ICMP Echo (PING) packets by default. Then, you will enable ICMP inspection to enable the ASA to allow returning ICMP Echo Reply messages without configuring an access list on an interface. Finally, you will observe and change the default ASA IP TTL behaviour.

Activity Procedure

Complete the following steps:

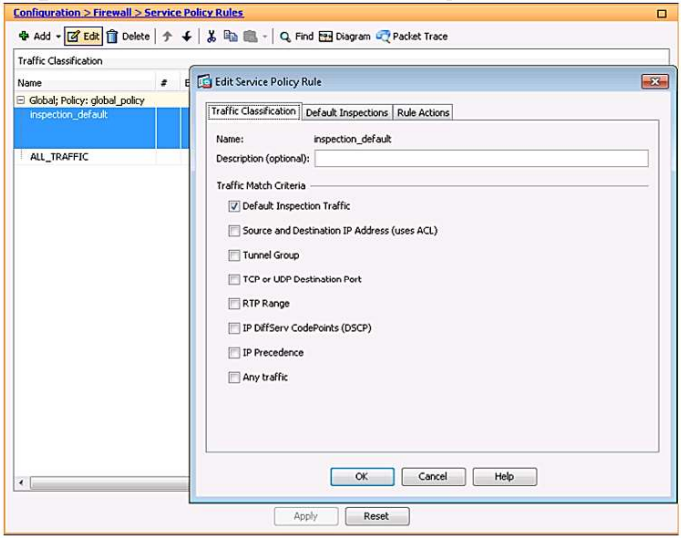
Step 1

Access the Admin PC. Start Cisco ASDM by double-clicking its icon on the desktop. Connect to the HQ-ASA at 10.10.2.1. Log in using **admin** as the username and **Ci5coAdmin** as the password.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

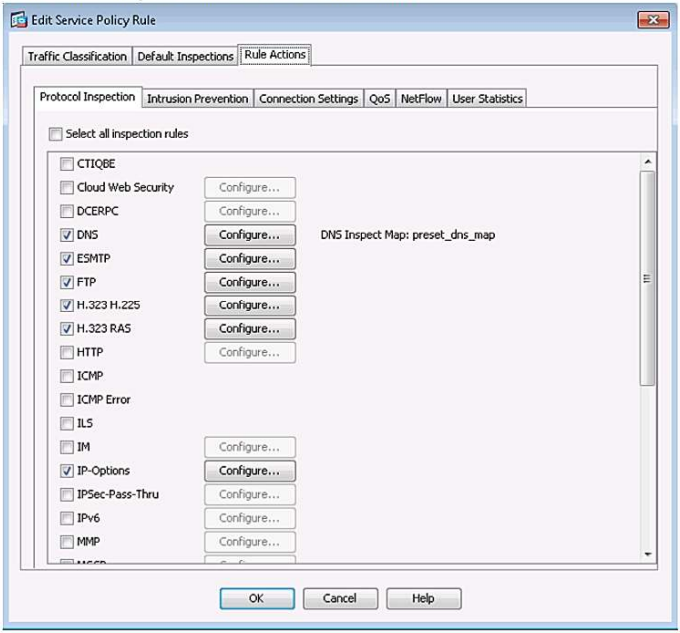
When Cisco ASDM opens, navigate to **Configuration > Firewall > Service Policy Rules**. Select the **inspection_defaullt** traffic class and click **Edit**. Observe the matching criteria for the traffic class.



https://t.me/learningnets

Step 3

In the **Edit Service Policy Rule** window, click the **Rule Actions** tab.



Observe enabled inspectors and populate the following table:

Protocol	Enabled
CTIQBE	
Cloud Web Security	
DCERPC	
DNS	
ESMTP	
FTP	
H.323 H.225	
H.323 RAS	

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

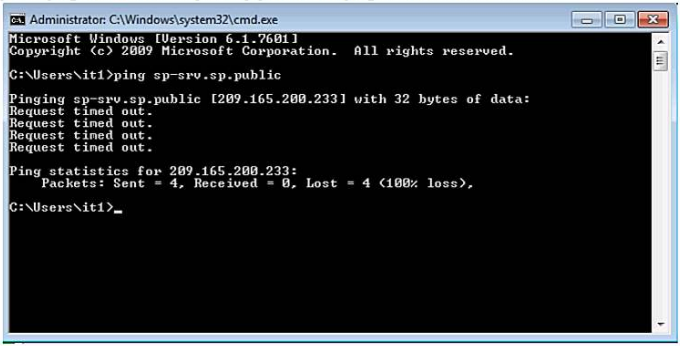
Protocol	Enabled
HTTP	
ICMP	
ICMP Error	
ILS	
IM	
IP-Options	
IPsec Pass-Thru	
IPv6	
MMP	
MGCP	
NETBIOS	
PPTP	
RSH	
RTSP	
SCCP (Skinny)	
SIP	
SNMP	
SQLNET	
SUNRPC	
TFTP	
WAAS	
XDMCP	

You should see that ICMP inspection is disabled.

https://t.me/learningnets

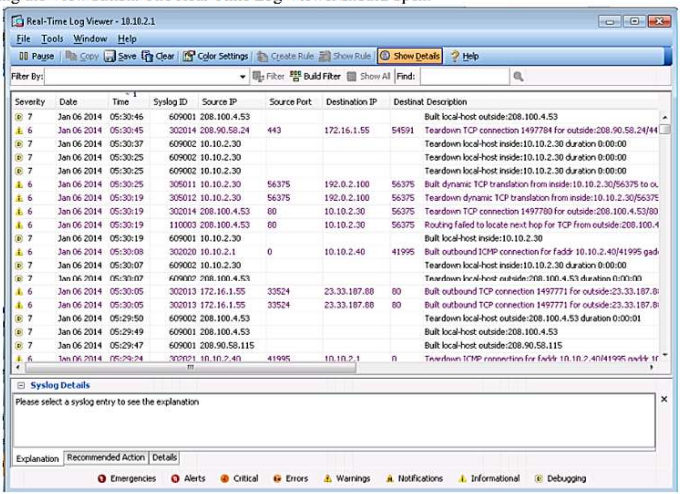
Step 4

Access the Employee PC. Log in using **it1** as the username and **cisco** as the password. Open a command prompt and ping the SP-SRV at **sp-srv.sp.public**. The ping should not be successful.



Step 5

In the Cisco ASDM, navigate to **Monitoring > Logging > Real-Time Log Viewer**. Start the viewer by clicking the **View** button. The Real-Time Log Viewer should open.



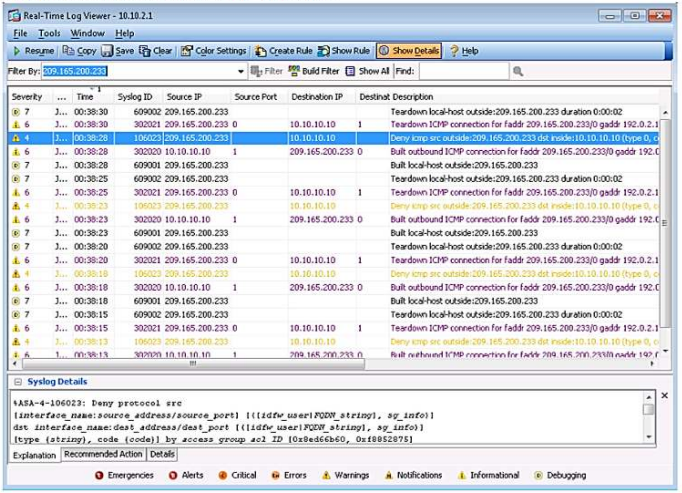
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

Return to the Employee PC and trigger the ping again..

Step 7

Return to the Cisco ASDM Real-Time Log Viewer on the Admin PC. Enter the IP address of the SP-SRV (209.165.200.233) into the Filter By input field and press Enter to filter the output based on IP address. Observe how the ASA denied incoming echo reply packet from the SP-SRV to the Employee PC. You can stop the incoming messages for better readability by clicking the **Pause** button. The reason the ASA denied the echo reply messages is disabled ICMP inspection.

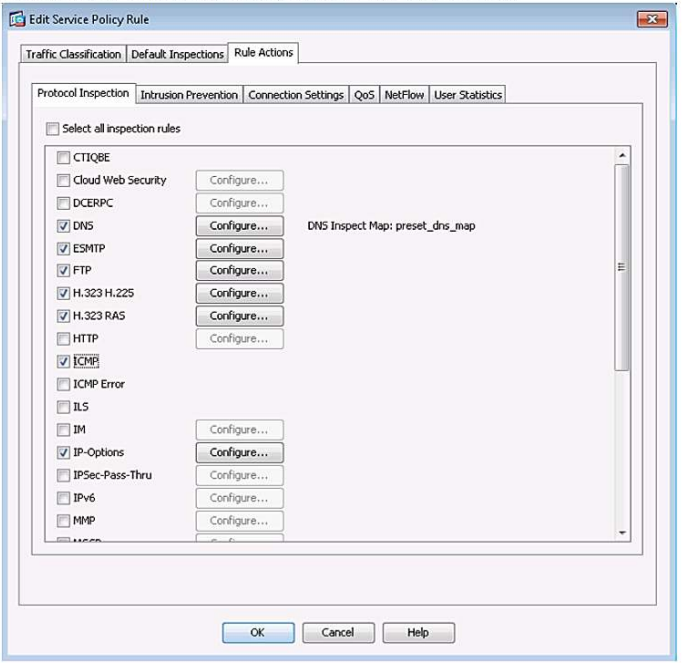


Click the **Resume** button when you are done with examining the logging messages.

https://t.me/learningnets

Step 8

In Cisco ASDM, navigate to **Configuration > Firewall > Service Policy Rules**. Select the **inspection_defaullt** traffic class and click **Edit**. Click the **Rule Actions** tab in the **Edit Service Policy Rule** window. Enable ICMP inspection by checking the **ICMP** checkbox. Click **OK**.



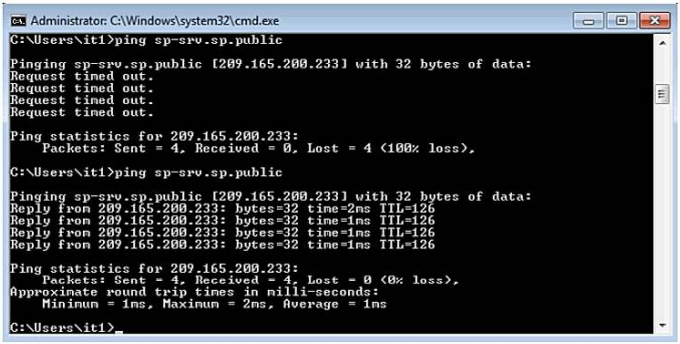
Step 9

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 10

Return to the Employee PC. Ping the SP-SRV at **sp-srv.sp.public** again. This time, the ping should be successful.



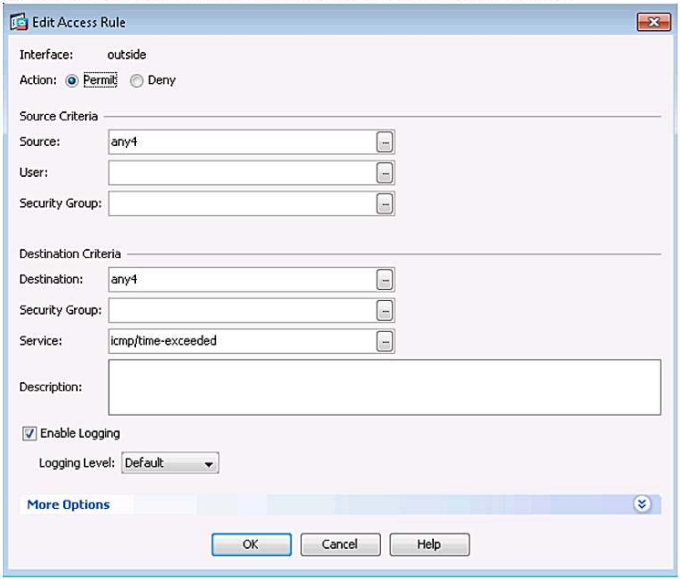
Step 11

In the next few steps, you will demonstrate the ASA IP TTL decrement behaviour.

https://t.me/learningnets

Step 12

Return to the Cisco ASDM session on the Admin PC and navigate to **Configuration > Firewall > Access Rules**. Edit the access rule on the outside interface by adding an additional rule to allow ICMP time-exceeded messages from any IPv4 host to any IPv4 host. This rule is required to allow ICMP time-exceeded messages to come from outside when traceroute is performed from the inside networks.



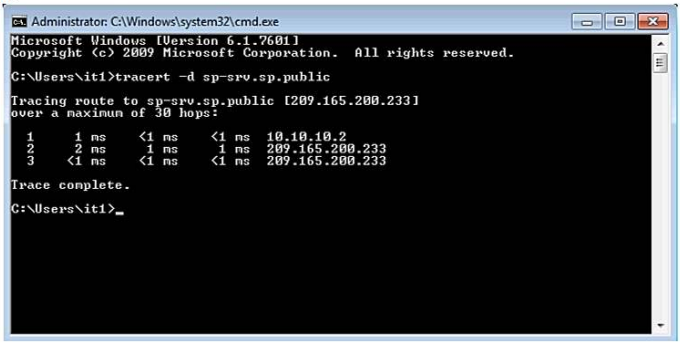
Step 13

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 14

Return to the Employee PC. Peform a traceroute to the SP-SRV at **sp-srv.sp.public**. You should see two hops between the Employee PC and the SP-SRV; the first one is HQ-SW, and the second is Internet-RTR. Recall that the ASA does not decrement TTL in IP packets by default and is therefore not seen in traceroute outputs.

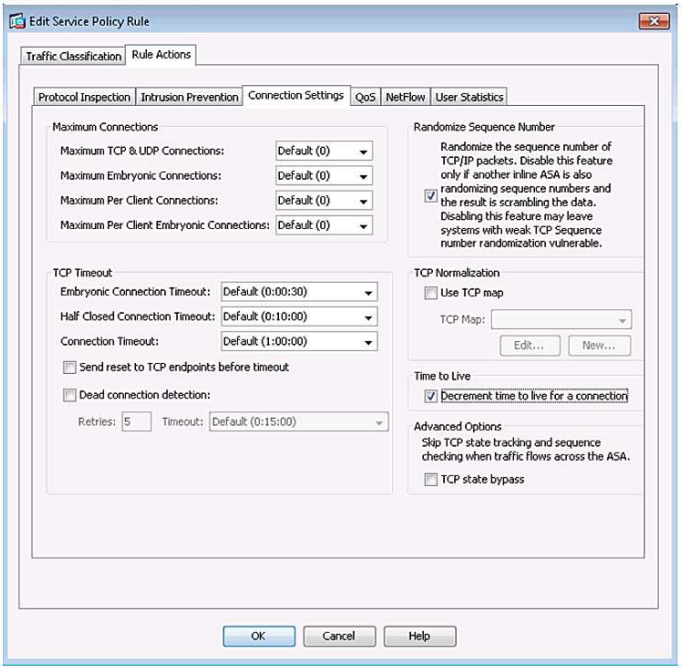


Note The ASA changes source IP address of the incoming ICMP time-exceeded messages to the IP address of the traceroute destination. This is the reason that you see IP address of the SP-SRV in both last two traceroute packets. You can disable such behaviour by enabling ICMP Error inspection on the ASA.

https://t.me/learningnets

Step 15

Return to the Cisco ASDM session on the Admin PC and navigate to **Configuration > Firewall > Service Policy Rules**. Select the **ALL_TRAFFIC** traffic class and click **Edit**. Click the **Connection Settings** tab and configure the ASA to decrement TTL in IP packets by checking the **Decrement time to live for a connection** checkbox. Click **OK**.



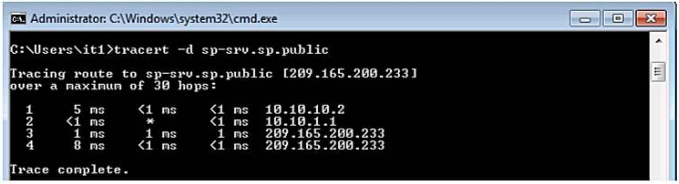
Step 16

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 17

Return to the Employee PC. Peform a traceroute to the SP-SRV at **sp-srv.sp.public** again. This time, you should see three hops between the Employee PC and the SP-SRV; the first one is HQ-SW, the second is HQ-ASA, and the third is Internet-RTR. This time, the ASA did decrement TTL in IP packets and is therefore seen in the traceroute output.



Activity Verification

No verification is needed in this task.

Task 2: Examine Support for Dynamic Protocols

In this task, you will examine the Cisco ASA support for dynamic protocols. You will observe how the ASA allows dynamic FTP data session to be established by default. Then, you will disable FTP inspection and observe the effect configuration has on FTP traffic between the Employee PC and SP-SRV.

Activity Procedure

Complete the following steps:

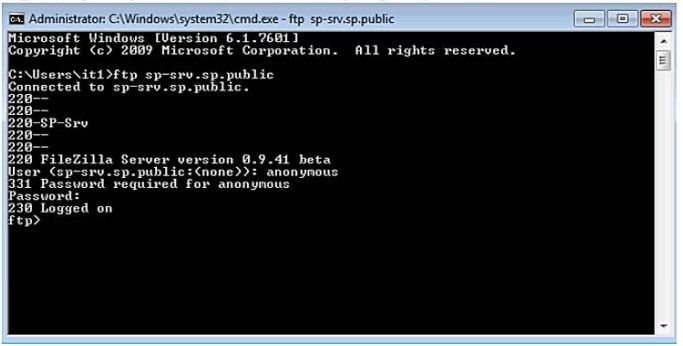
Step 1

In the first task, you already observed that FTP inspection is enabled on the HQ-ASA. FTP inspection allows establishment of dynamic FTP sessions. Dynamic FTP sessions, called data sessions, are established after a control session is established on TCP port 21, and are used to transfer data.

https://t.me/learningnets

Step 2

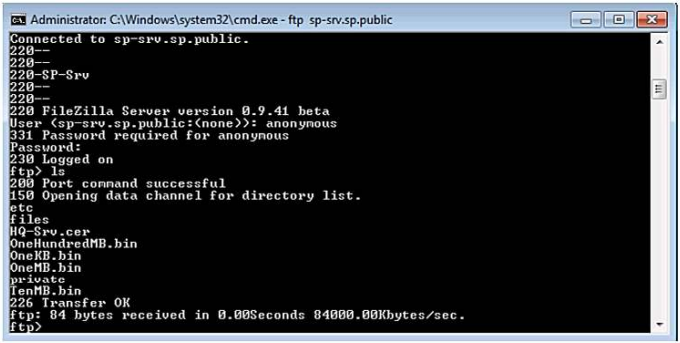
Return to the Employee PC. Open a command prompt and connect to the SP-SRV at **sp-srv.sp.public** using FTP. Log in using **anonymous** as the username and anything as a password.



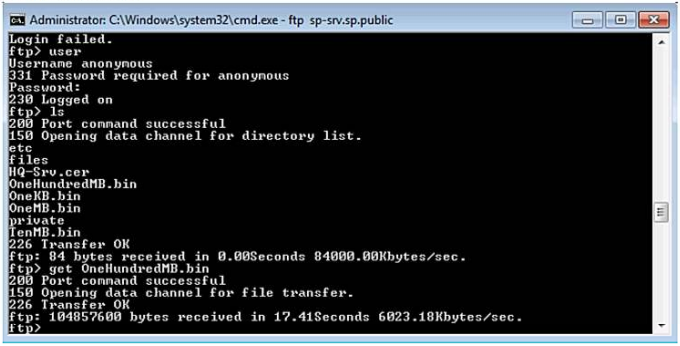
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

Inside the FTP session, list the files on the FTP server using the **ls** command. This will establish a data FTP session.



Transfer the **OneHundredMB.bin** file from the FTP server using the **get** command. This will establish another FTP data session.



https://t.me/learningnets

Step 4

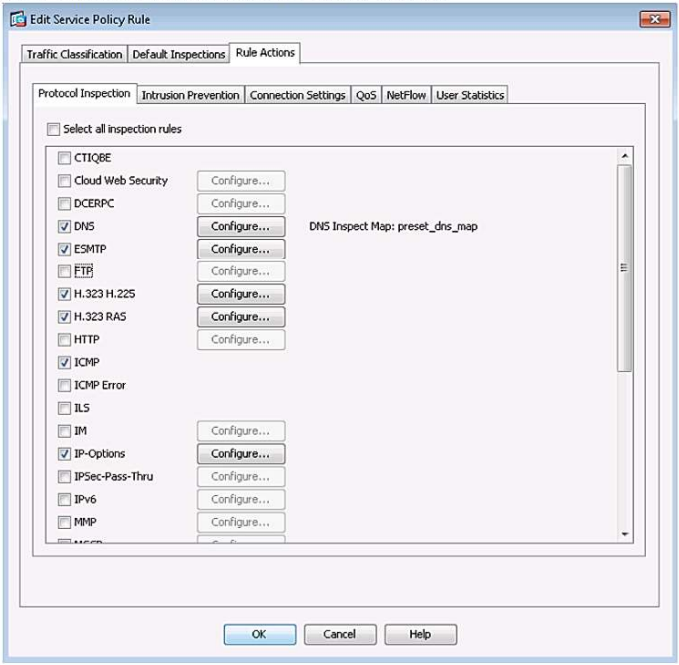
In the meantime, access the HQ-ASA console. Examine connection table details. List only connections that belong to the SP-SRV. You should see two connections; one is FTP control session, which is established from the PC to the server on TCP port 21, and the second is FTP data session, which is established from the server to the PC using source port 20 and a dynamically negotiated destination TCP port (4164 in the example below).

```
HQ-ASA# show conn address 209.165.200.233 detail
25 in use, 319 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, c - cluster centralized,
       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,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
TCP outside: 209.165.200.233/20 inside: 10.10.10.10/4164,
    flags UIB , idle 0s, uptime 6s, timeout 1h0m, bytes 36633596
TCP outside: 209.165.200.233/21 inside: 10.10.10.10/4157,
    flags UxIO , idle 0s, uptime 57s, timeout 1h0m, bytes 640
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 5

Return to the Cisco ASDM session on the Admin PC. Navigate to **Configuration > Firewall > Service Policy Rules**. Select the **inspection_defaullt** traffic class and click **Edit**. Click the **Rule Actions** tab. Disable FTP inspection by unchecking the **FTP** checkbox. Click **OK**.



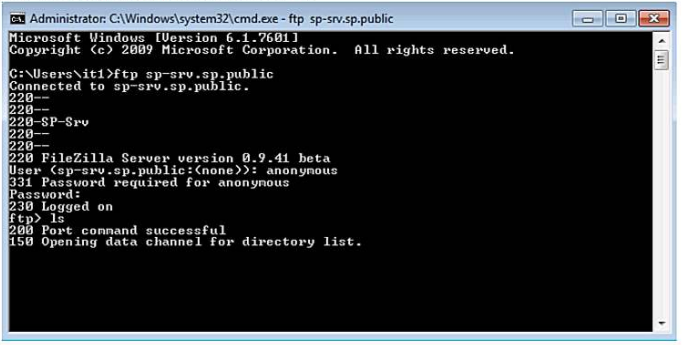
Step 6

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

https://t.me/learningnets

Step 7

Return to the Employee PC. Connect to the SP-SRV at **sp-srv.sp.public** using FTP again. Log in using **anonymous** as the username and anything as a password. List the files on the FTP server using the **ls** command again. This time, you should not be successful because the ASA does not allow the dynamic data session to be established from the server to the PC.



Step 8

Return to the ASDM session on the Admin PC and re-enable FTP inspection.

Step 9

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

Activity Verification

No verification is needed in this task.

Task 3: Configure Application Inspection for HTTP Traffic

In this task, you will configure HTTP application inspection on the HQ-ASA. You will configure the ASA to deny HTTP requests to the management page of Xampp web server that is running on the DMZ-SRV. Access to the management page should be denied only when it is access through the ASA outside interface.

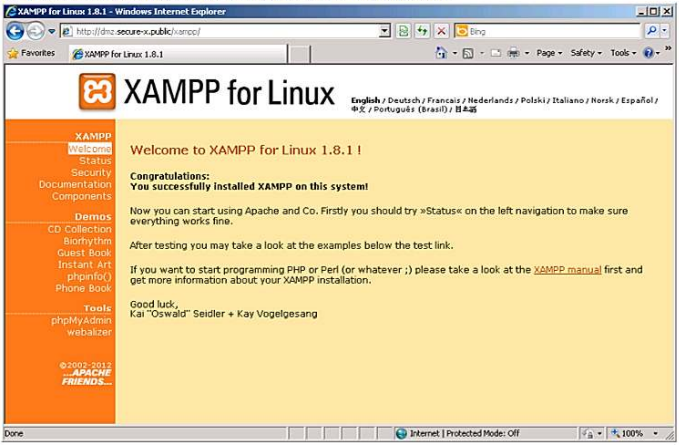
Activity Procedure

Complete the following steps:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 1

Access the SP-SRV. Open Internet Explorer web browser and navigate to **http://dmz.secure-x.public/xampp**. The management page of the Xampp web server should open.

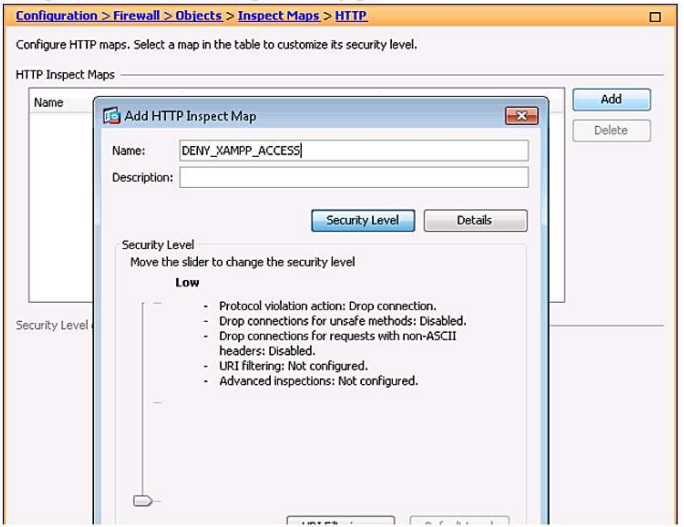


Since it is not desired to allow access to the Xampp management web page from the outside network, you will enable HTTP application inspection on the ASA that will deny access to the management web page, but will still allow access to other web pages on the DMZ server.

https://t.me/learningnets

Step 2

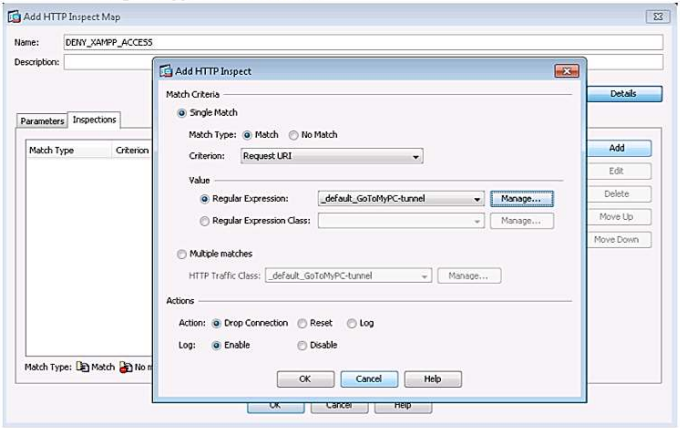
Return to the Cisco ASDM session on the Admin PC. Navigate to **Configuration > Firewall > Objects > Inspect Maps > HTTP**. Create a new HTTP inspect map (OSI Layer 5-7 policy map) and name it **DENY_XAMPP_ACCESS**. This policy map will match string "xampp" in HTTP request URIs and will deny and log access to the XAMPP management web page.



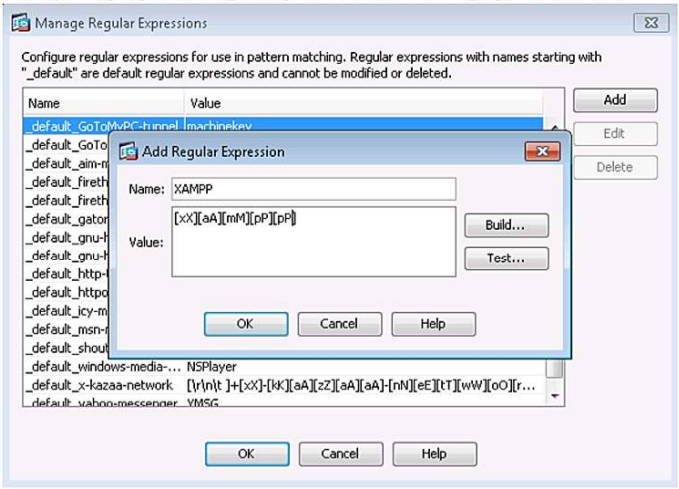
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

Click the **Details** button, select **Inspection** tab and create a new inspection policy that will deny HTTP requests that have string "xampp" in the URL field.

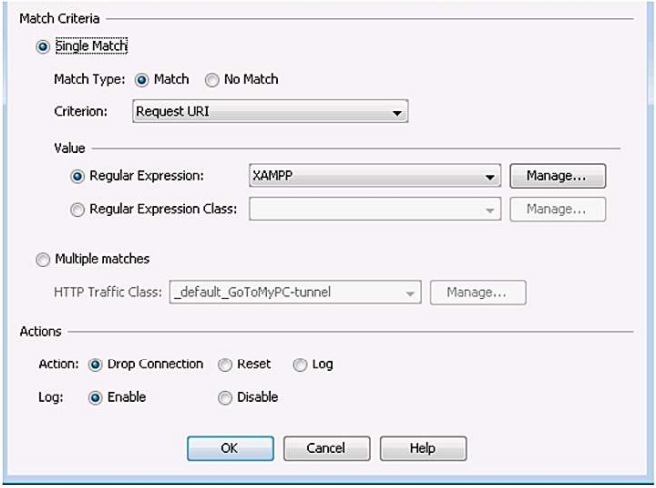


Use **[xX][aA][mM][pP][pP]** as the regular expression to match the string regardless of the case.



https://t.me/learningnets

Make sure that the regular expression is selected in the Add HTTP Inspect window.



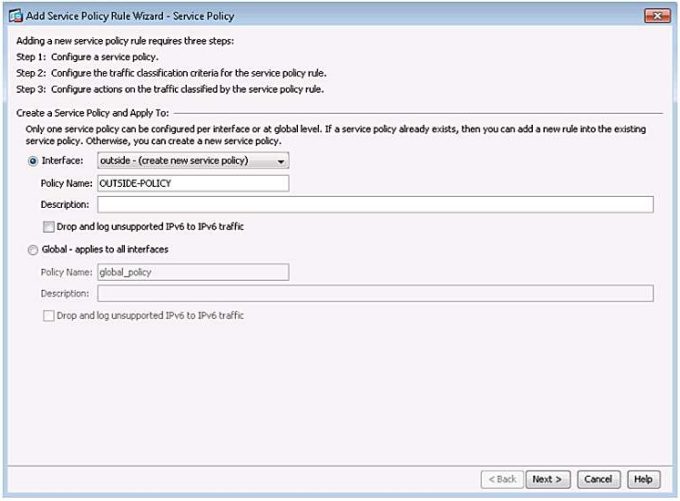
Step 4

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

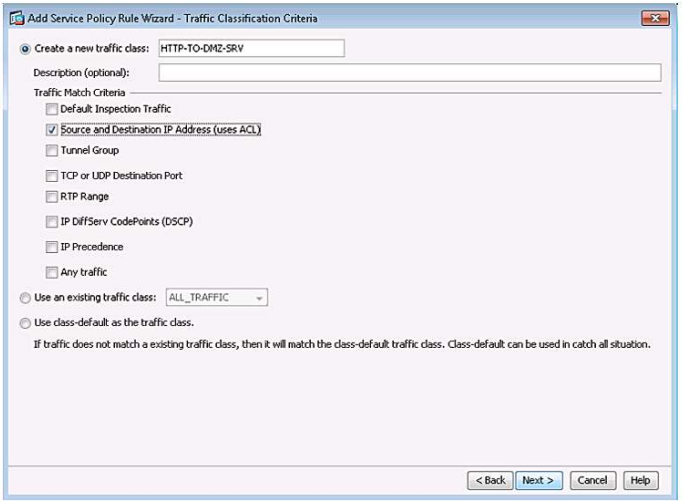
Step 5

In Cisco ASDM , navigate to **Configuration > Firewall > Service Policy Rules**. Create a new service policy rule on the outside interface. This policy will match HTTP traffic to the DMZ-SRV and will enable HTTP inspection with the previously configured HTTP inspect policy map. Use **OUTSIDE-POLICY** as the name of the policy.

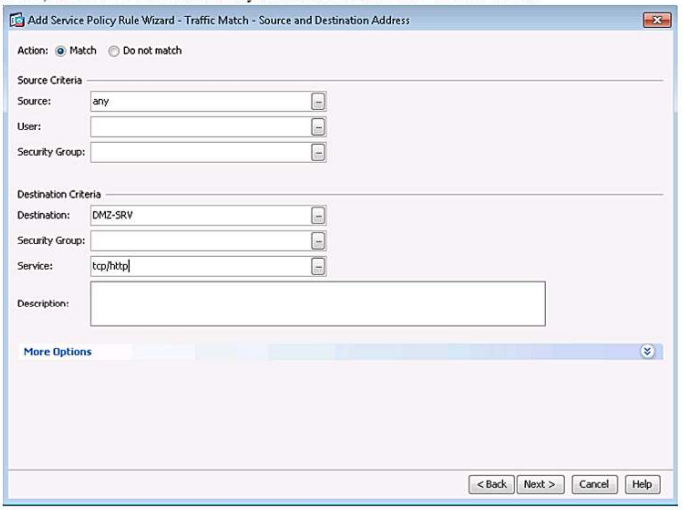


Use ACL in the traffic class definition. Use **HTTP-TO-DMZ-SRV** as the name of the traffic class.

https://t.me/learningnets

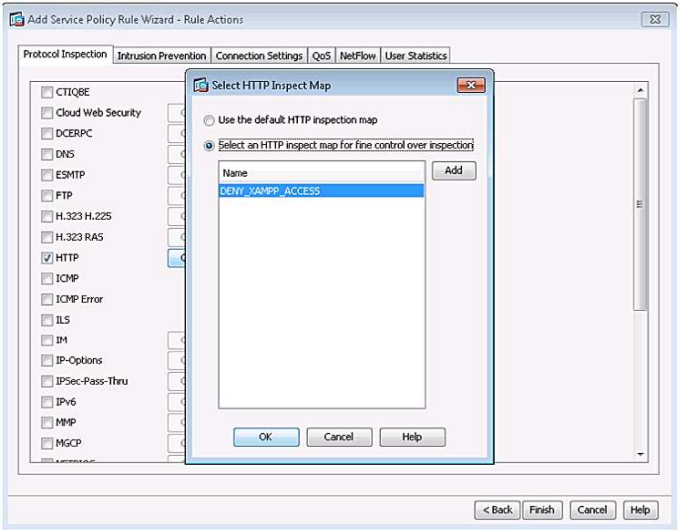


In the ACL, match HTTP traffic from any source to the DMZ-SRV at 172.16.1.50.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Enable HTTP inspection for the traffic class. Enable application inspection with the previously configured Layer 5-7 HTTP policy map.



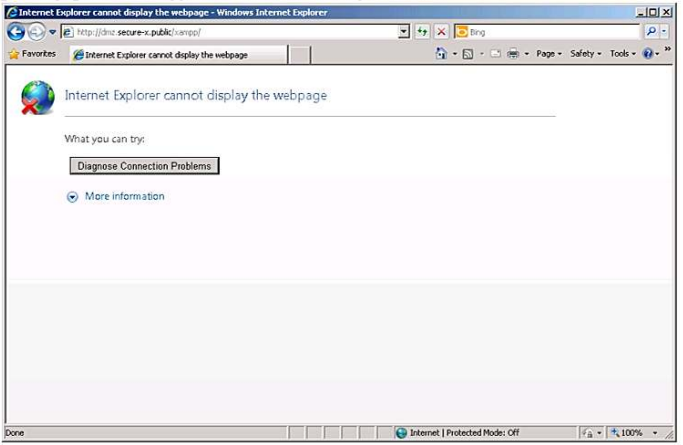
Step 6

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

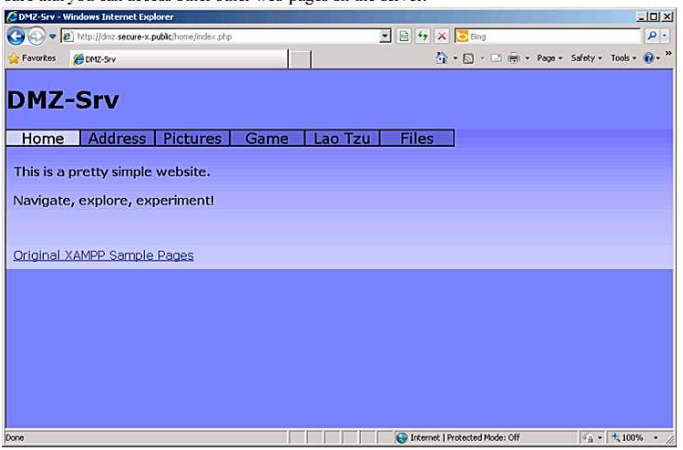
https://t.me/learningnets

Step 7

Return to the SP-SRV. Refresh the Xampp management web page in the Internet Explorer. The management page of the Xampp web server should not open this time.



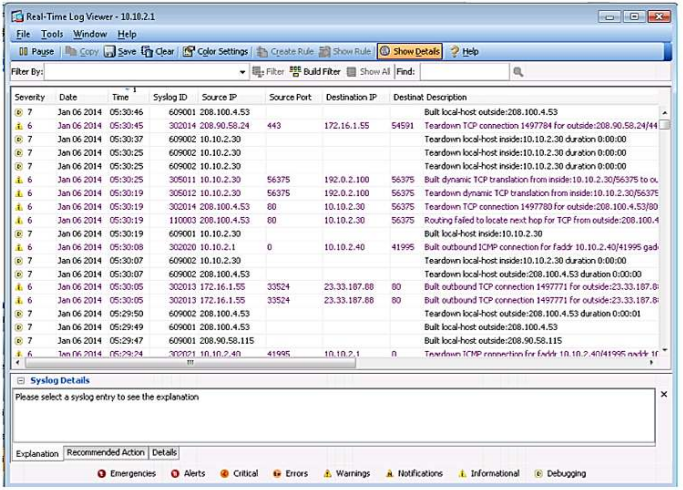
Using the Internet Explorer, navigate to the web page on the DMZ-SRV at **http://dmz.secure-x.public** to make sure that you can access other other web pages on the server.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 8

In the Cisco ASDM, navigate to **Monitoring > Logging > Real-Time Log Viewer**. Start the viewer by clicking the **View** button. The Real-Time Log Viewer should open.



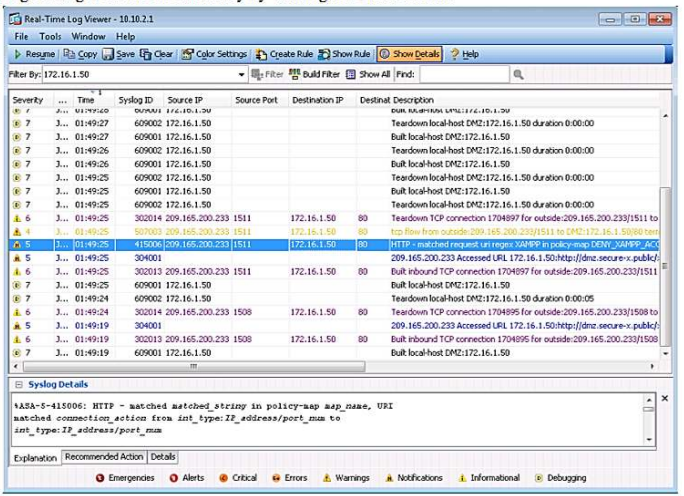
Step 9

Return to the SP-SRV and navigate to the Xampp management web page again.

https://t.me/learningnets

Step 10

Return to the Cisco ASDM Real-Time Log Viewer on the Admin PC. Enter the IP address of the DMZ-SRV (172.16.1.50) into the Filter By input field and press Enter to filter the output based on IP address. Observe how the ASA denied incoming HTTP request for the Xampp management page. You can stop the incoming messages for better readability by clicking the **Pause** button.



Click the **Resume** button when you are done with examining the logging messages.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 11

Access the HQ-ASA console. Examine service policy statistics. You should see a number of packets that matched HTTP-TO-DMZ-SRV traffic class and a number of packets that are dropped.

```
HQ-ASA# show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop
0, v6-fail-close 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop
0, v6-fail-close 0
      Inspect: ip-options _default_ip_options_map, packet 0, lock fail 0, drop 0,
reset-drop 0, v6-fail-close 0
      Inspect: netbios, packet 3, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: skinny , packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: esmtp _default_esmtp_map, packet 365828, lock fail 0, drop 0, reset-
drop 0, v6-fail-close 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: xdmcp, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: dns preset_dns_map, packet 1134065, lock fail 0, drop 3345, reset-drop
0, v6-fail-close 0
      Inspect: icmp, packet 11644, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
    Class-map: ALL_TRAFFIC
      Set connection policy:         drop 0
      Set connection decrement-ttl
Interface outside:
  Service-policy: OUTSIDE-POLICY
    Class-map: HTTP-TO-DMZ-SRV
      Inspect: http DENY_XAMPP_ACCESS, packet 8, lock fail 0, drop 2, reset-drop 0,
v6-fail-close 0
```

Activity Verification

No verification is needed in this task.

Task 4: Configure Application Inspection for FTP Traffic

In this task, you will configure FTP application inspection on the HQ-ASA. You will configure the ASA to reset FTP sessions to the DMZ-SRV if commands to delete a file or folder are seen in sessions. These commands should be only denied for FTP sessions from the outside interface.

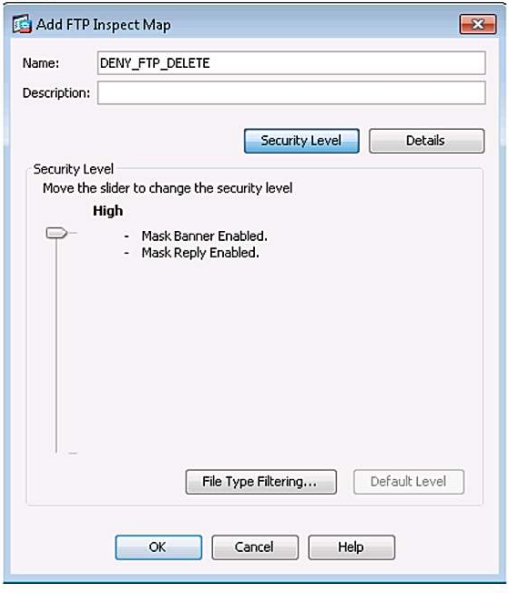
https://t.me/learningnets

Activity Procedure

Complete the following steps:

Step 1

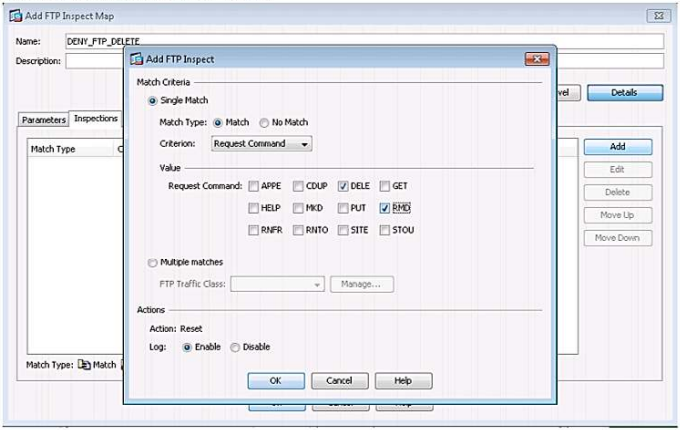
Return to the Cisco ASDM session on the Admin PC. Navigate to **Configuration > Firewall > Objects > Inspect Maps > FTP**. Create a new FTP inspect map (OSI Layer 5-7 policy map) and name it **DENY_FTP_DELETE**.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

Click the **Details** button, select **Inspection** tab and create a new inspection policy that will deny DELE and RMD FTP commands. The DELE command is used to delete files from an FTP server and RMD command is used to delete folders from an FTP server.



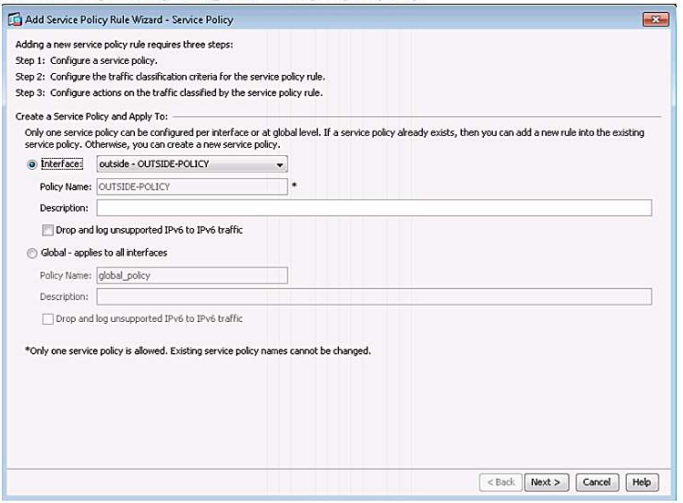
Step 3

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

https://t.me/learningnets

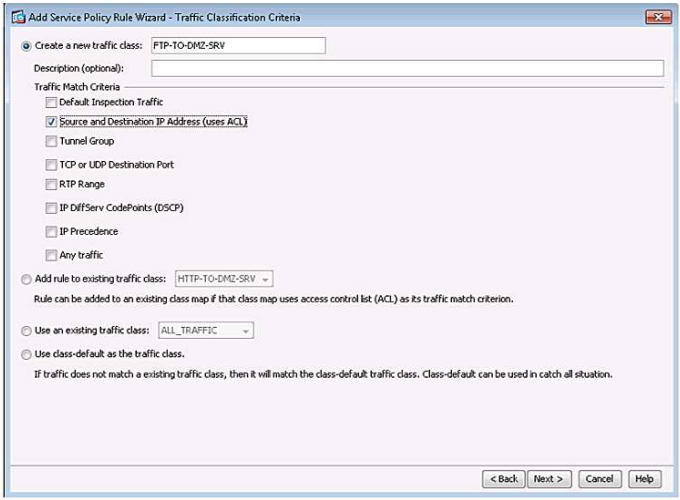
Step 4

In Cisco ASDM , navigate to **Configuration > Firewall > Service Policy Rules**. Edit the service policy rule on the outside interface to include a new rule (traffic class with associated action) to the service policy on the outside interface. This policy will match FTP traffic to the DMZ-SRV and will enable FTP inspection with the previously configured FTP inspect policy map.

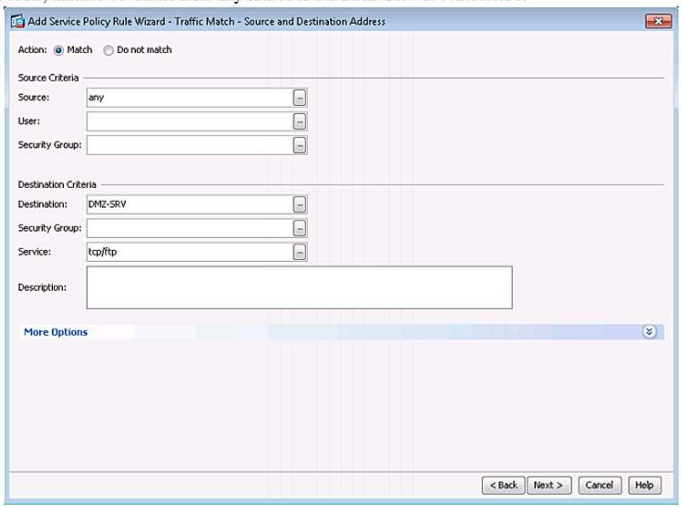


Use ACL in the traffic class definition. Use **FTP-TO-DMZ-SRV** as the name of the traffic class.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

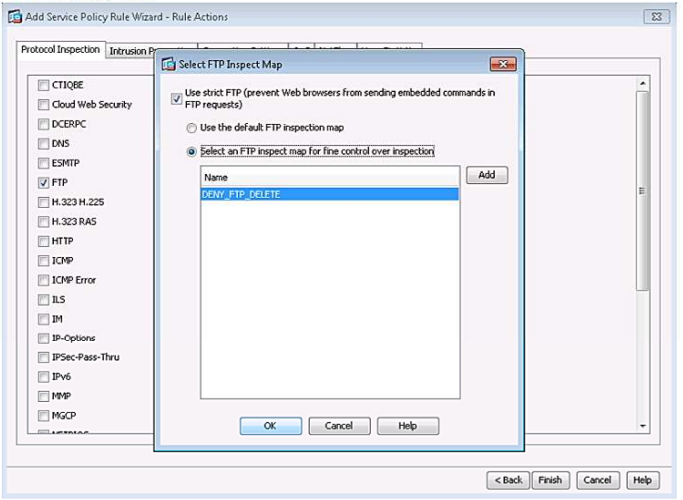


In the ACL, match FTP traffic from any source to the DMZ-SRV at 172.16.1.50.



https://t.me/learningnets

Enable FTP inspection for the traffic class. Enable application inspection with the previously configured Layer 5-7 FTP policy map.



Step 5

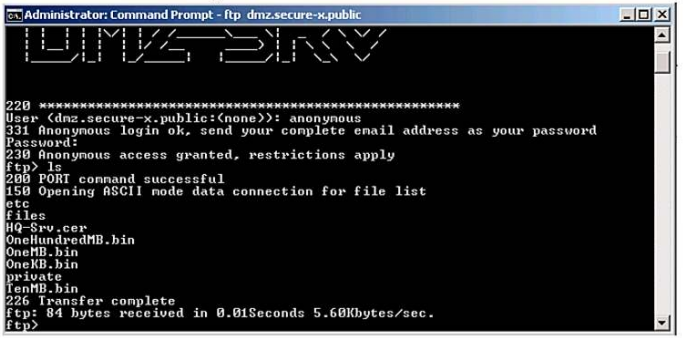
Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

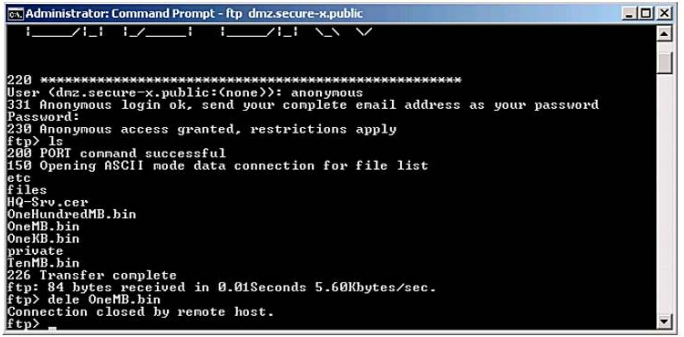
Return to the SP-SRV. Open a command prompt and connect to the **DMZ-SRV** at **dmz.secure-x.public** using FTP. Log in using **anonymous** as the username and anything as a password.

List the files on the FTP server using the **ls** command.



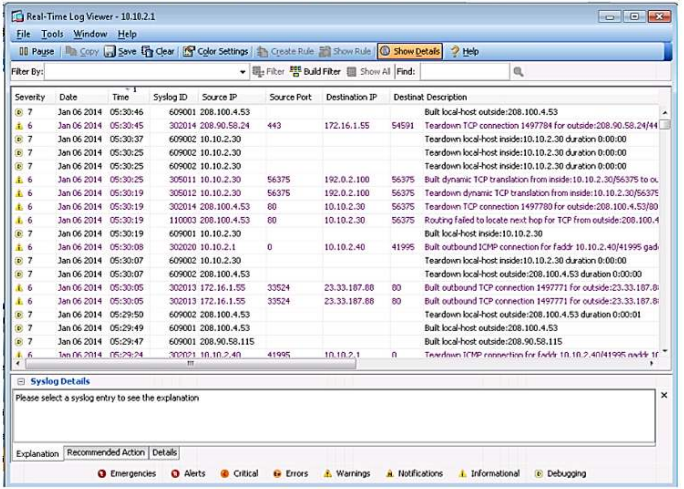
Try to delete the OneMB.bin file using the **dele** command. You should not be able to do so. The FTP session should close instead.

https://t.me/learningnets



Step 7

In the Cisco ASDM, navigate to **Monitoring > Logging > Real-Time Log Viewer**. Start the viewer by clicking the **View** button. The Real-Time Log Viewer should open.



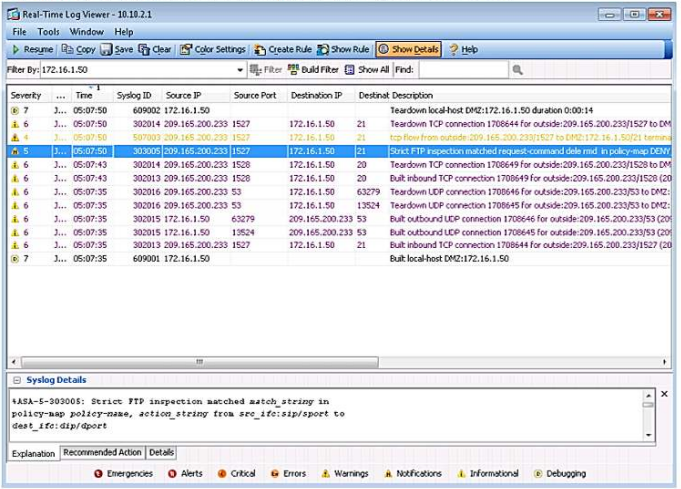
Step 8

Return to the SP-SRV, connect to the DMZ-SRV using FTP again, and try to delete the file again.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 9

Return to the Cisco ASDM Real-Time Log Viewer on the Admin PC. Enter the IP address of the DMZ-SRV (172.16.1.50) into the Filter By input field and press Enter to filter the output based on IP address. Observe how the ASA denied incoming FTP session when the FTP DELETE command was seen. You can stop the incoming messages for better readability by clicking the **Pause** button.



Click the **Resume** button when you are done with examining the logging messages.

https://t.me/learningnets

Step 10

Return to the HQ-ASA console. Examine service policy statistics. You should see a number of packets that matched FTP-TO-DMZ-SRV traffic class and a number of packets that were dropped with connection reset.

```
HQ-ASA# show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop
0, v6-fail-close 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop
0, v6-fail-close 0
      Inspect: ip-options _default_ip_options_map, packet 0, lock fail 0, drop 0,
reset-drop 0, v6-fail-close 0
      Inspect: netbios, packet 3, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: skinny , packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: esmtp _default_esmtp_map, packet 367308, lock fail 0, drop 0, reset-
drop 0, v6-fail-close 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: xdmcp, packet 0, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: dns preset_dns_map, packet 1134559, lock fail 0, drop 3345, reset-drop
0, v6-fail-close 0
      Inspect: icmp, packet 12074, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
      Inspect: ftp, packet 80, lock fail 0, drop 0, reset-drop 0, v6-fail-close 0
    Class-map: ALL_TRAFFIC
      Set connection policy:          drop 0
      Set connection decrement-ttl
Interface outside:
  Service-policy: OUTSIDE-POLICY
    Class-map: HTTP-TO-DMZ-SRV
      Inspect: http DENY_XAMPP_ACCESS, packet 8, lock fail 0, drop 2, reset-drop 0,
v6-fail-close 0
    Class-map: FTP-TO-DMZ-SRV
      Inspect: ftp strict DENY_FTP_DELETE, packet 68, lock fail 0, drop 0, reset-drop
2, v6-fail-close 0
```

Activity Verification

No verification is needed in this task.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 4-3: Configure Cisco ASA Botnet Traffic Filter

Activity Objective

The company Secure-X has a network topology as shown in the figure. The company recently hired a new Chief Security Officer that wants to improve all of the current network security controls with the latest technologies to support the most recent company security policy.

You are the network security engineer for the Secure-X network. The company has recently detected increase of traffic to malware infected destinations. The CSO deduced that some PCs in the internal networks are infected with malware and communicate with malware infected destinations.

The CSO tasked you with enabling Botnet Traffic FIlter on the Cisco ASA to detect and deny further connection attempts from infected PCs to malware destinations.

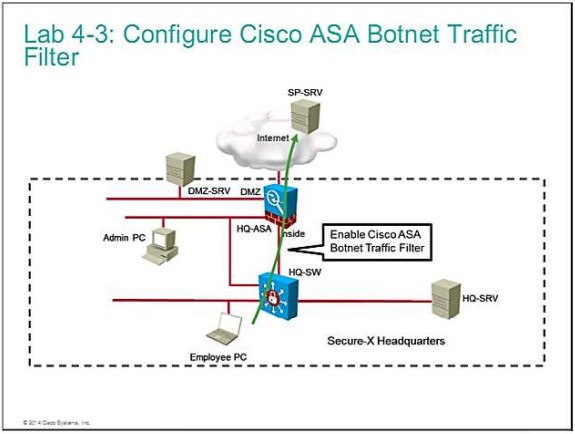
In this activity you will configure Cisco ASA Botnet Traffic Filter:

- Configure the Botnet Traffic Filter using dynamic database
- Configure the Botnet Traffic Filter using static database

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

Command List

The table describes the Cisco ASA commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco ASA Commands

Command	Description
show conn address *ip_address* **detail**	Displays connection table details for the specified IP address
show service-policy	Displays service policy configuration and statistics

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

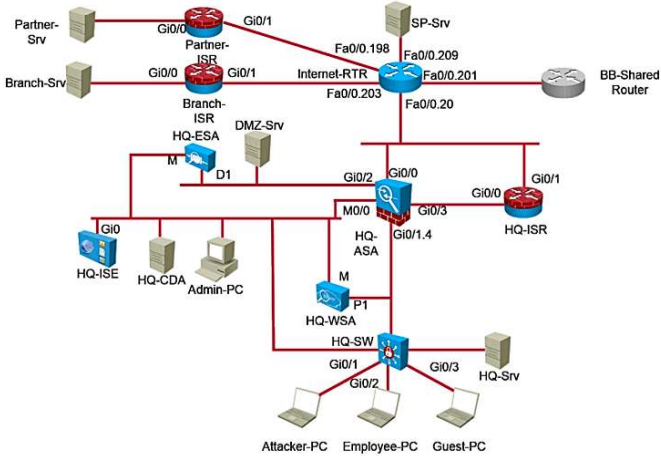
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

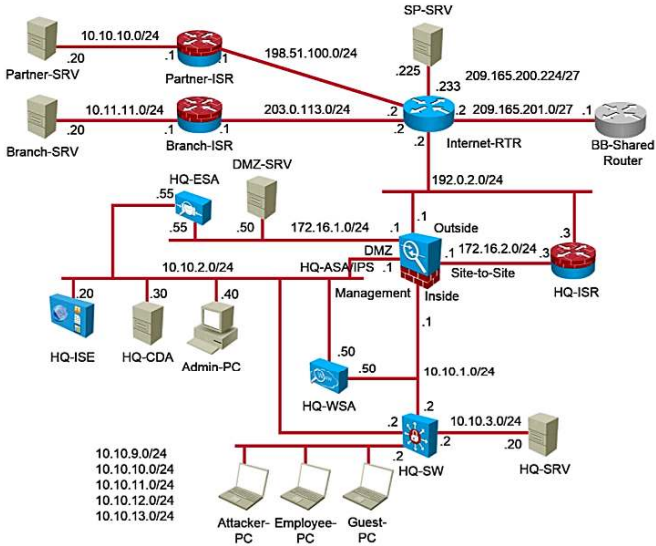
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

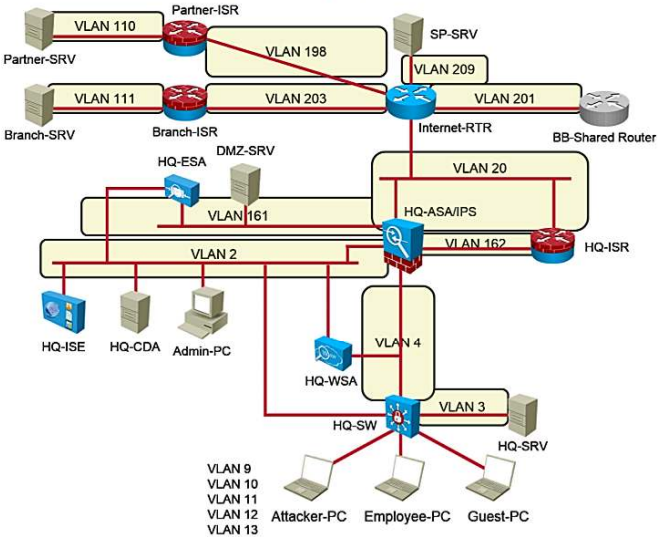
The figure shows the IP addresses that are used in this lab setup.



https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure the Botnet Traffic Filter using Dynamic Database

In this task, you will configure the Botnet Traffic Filter on the HQ-ASA. First you will download the dynamic database and enable use of it. Then you will enable the ASA to detect and drop blacklisted traffic using the dynamic database. Finally, you will verify that the ASA indeed drops traffic to blacklisted destinations.

Activity Procedure

Complete the following steps:

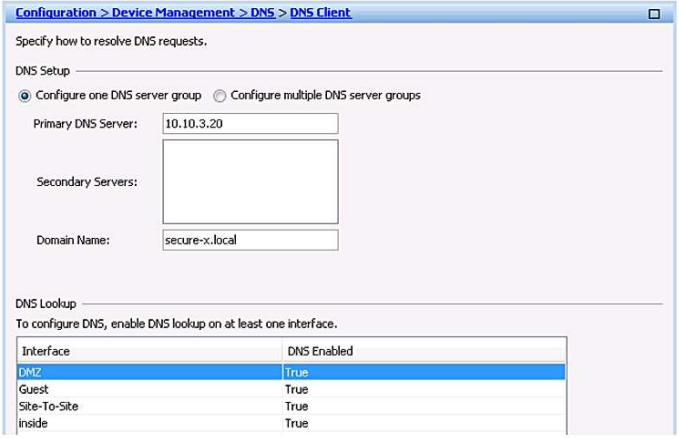
Step 1

Access the Admin PC and launch Cisco ASDM. Connect to 10.10.2.1 and log in as **admin** with password **Ci5coAdmin**.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

In Cisco ASDM, navigate to **Configuration > Device Management > DNS > DNS Client**. Make sure that DNS is enabled on the inside interface and set to the HQ-SRV (10.10.3.20). Set the Domain Name to **secure-x.local** if not already set.



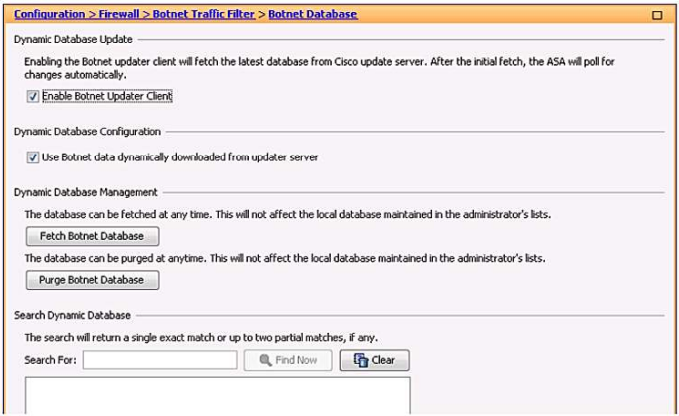
https://t.me/learningnets

Step 3

In Cisco ASDM, navigate to **Configuration > Firewall > Botnet Traffic Filter > Botnet Database**.

Check the **Enable Botnet Updater Client** check box to enable downloading of the dynamic database. The update server determines how often the security appliance polls the update server. Typically, this polling is done every hour, which is the default.

Check the **Use Botnet data dynamically downloaded from updater server** check box to enable the use of the dynamic database.



The database files are stored in running memory; they are not stored in flash memory. You also can use the **Fetch Botnet Database** button to manually fetch the database for testing purposes.

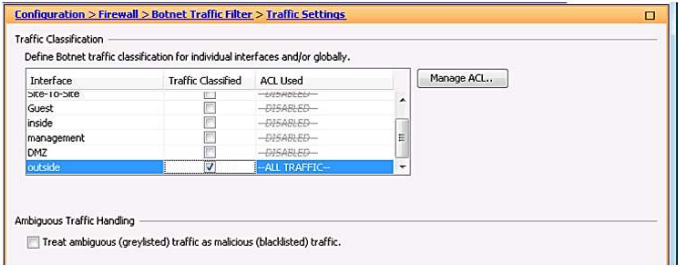
Step 4

In Cisco ASDM, choose **Configuration > Firewall > Botnet Traffic Filter > DNS Snooping**. Enable DNS snooping

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

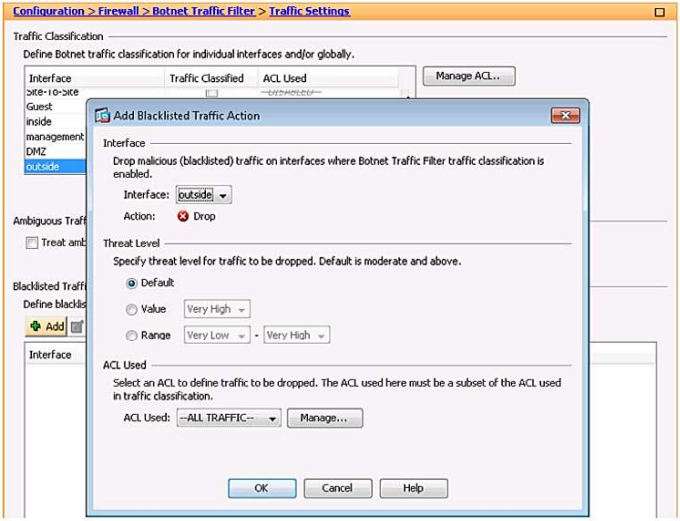
Step 5

In Cisco ASDM, choose **Configuration > Firewall > Botnet Traffic Filter > Traffic Settings**. Enable Botnet Traffic Filter classification on the outside interface for **All Traffic**.



Step 6

In the same Cisco ASDM window, configure the Botnet Traffic Filter to drop blacklisted traffic on the outside interface. Use the default Threat Level settings.



https://t.me/learningnets

Step 7

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

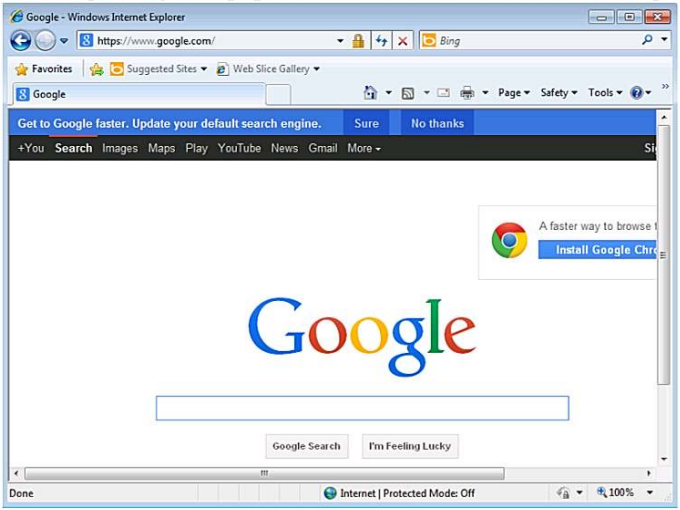
Step 8

In the Cisco ASDM, navigate to **Monitoring > Logging > Real-Time Log Viewer**. Start the viewer by clicking the **View** button. The Real-Time Log Viewer should open.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

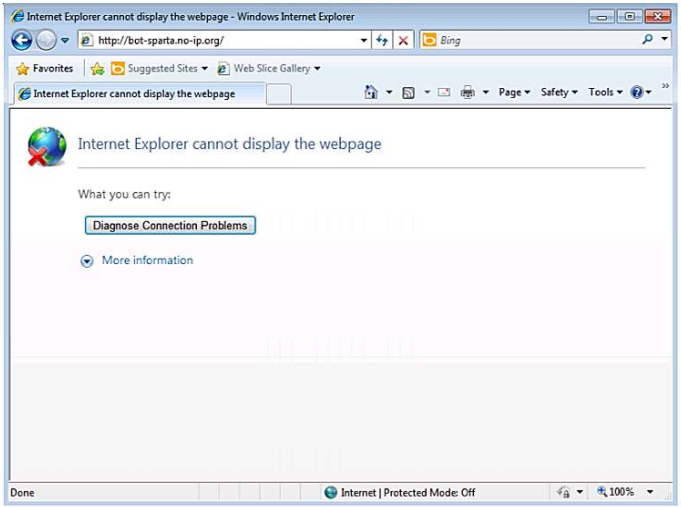
Step 9

Access the Employee PC. Log in using **it1** as the username and **cisco** as the password. Open Internet Explorer and navigate to **http://www.google.com** to make sure that access to the Internet is working.

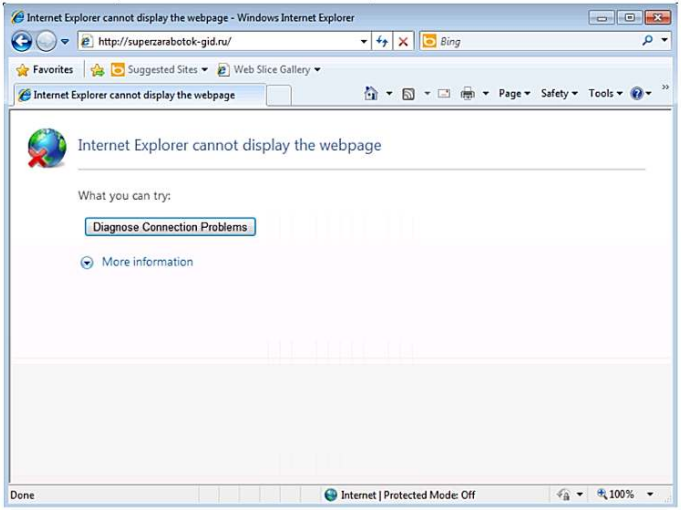


In the Internet Explorer, navigate to **http://bot-sparta.no-ip.org**. This destination is classified as malware destination by the Cisco SIO database. The attempt should not be successful.

https://t.me/learningnets



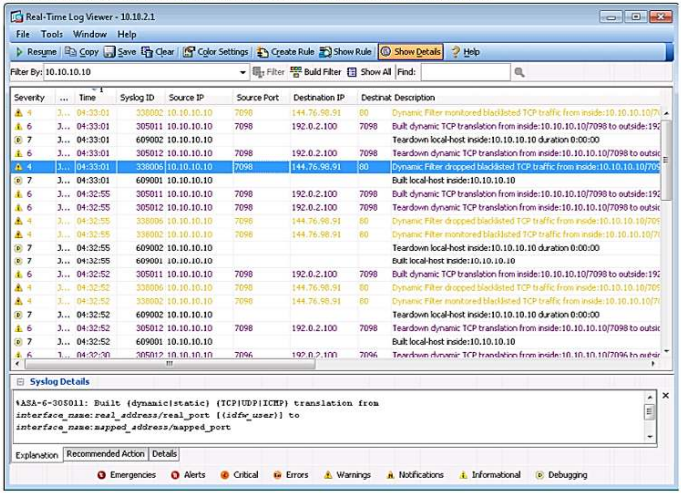
In the Internet Explorer, navigate to **http://superzarabotok-gid.ru/**. This destination is classified as malware destination by the Cisco SIO database. The attempt should not be successful.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 10

Return to the Cisco ASDM Real-Time Log Viewer on the Admin PC. Enter the IP address of the Employee PC (10.10.10.10 in the example) into the Filter By input field and press Enter to filter the output based on IP address. Observe how the ASA dropped blacklisted traffic to the web pages.



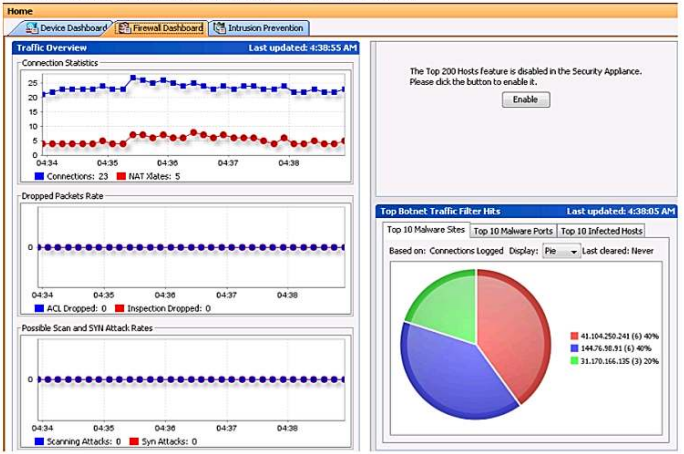
Click the **Resume** button when you are done with examining the logging messages.

Note It may take a while to see the logging message in the Cisco ASDM Real-Time Log Viewer.

https://t.me/learningnets

Step 11

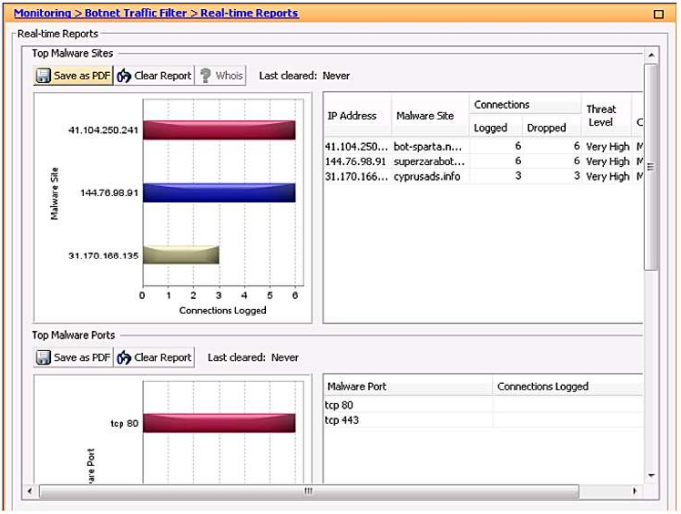
In Cisco ASDM, navigate to **Home > Firewall Dashboard**. Observe all three tabs of Botnet Traffic Filter statistics in the Top Botnet Traffic Filter Hist dashlet. In the **Top 10 Malware Sites** tab you should see at least two destinations that were accessed from the Employee PC.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 12

In Cisco ASDM, navigate to **Monitoring > Botnet Traffic Filter > Real-time Reports**. Observe the Botnet Traffic Filter real-time report. In the report you should again see the destinations that were accessed from the Employee PC.



https://t.me/learningnets

Step 13

Access the HQ-ASA console. Examine dynamic database information. You should see information about the downloaded dynamic database.

```
HQ-ASA# show dynamic-filter data
Dynamic Filter is using downloaded database version '1389687915'
Fetched at 03:50:46 PST Jan 14 2014, size: 2097130
Sample contents from downloaded database:
  dfgdsfgsdfg.com  guitarizmo.ru  3238d70829a17013664c960a52790b10.cz.cc  sportmarketi
ngrotterdam.nl
  travel-
cruise.ru  40373.dns7v.net  chwilowkanadowod.evenweb.com  fastloanforbadcredit.com
Sample meta data from downloaded database:
  threat-level: very-high,      category: Malware,
  description: "These are sources that use various exploits to deliver adware,
spyware and other malware to victim computers.  Some of these are associated with
rogue online vendors and distributors of dialers which deceptively call premium-rate
phone numbers."
  threat-level: high,   category: Bot and Threat Networks,
  description: "These are rogue systems that control infected computers.  They are
either systems hosted on threat networks or systems that are part of the botnet
itself."
  threat-level: moderate,       category: Malware,
  description: "These are sources that deliver deceptive or malicious anti-spyware,
anti-malware, registry cleaning, and system cleaning software."
  threat-level: low,    category: Ads,
  description: "These are advertising networks that deliver banner ads,
interstitials, rich media ads, pop-ups, and pop-unders for websites, spyware and
adware.  Some of these networks send ad-oriented HTML emails and email verification
services."
Total entries in Dynamic Filter database:
  Dynamic data: 80476 domain names , 4512 IPv4 addresses
  Local data: 2 domain names , 0 IPv4 addresses
Active rules in Dynamic Filter asp table:
  Dynamic data: 2 domain names , 4512 IPv4 addresses
  Local data: 4 domain names , 0 IPv4 addresses
```

Step 14

On the HQ-ASA console, examine report for top 10 malware sites. You should see the same information as before in the Cisco ASDM.

```
HQ-ASA# show dynamic-filter reports top malware-sites
Malware Sites (since last clear)
Site                            Connections Logged Dropped Threat-level Category
-------------------------------------------------------------------------------
41.104.250.241 (bot-sparta.no-ip.org)          6        6    very-high  Malware
144.76.98.91 (superzarabotok-gid.ru)           6        6    very-high  Malware
31.170.166.135 (cyprusads.info)                3        3    very-high  Malware
Last clearing of the top sites report: Never
```

Activity Verification

No verification is needed in this task.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Task 2: Configure the Botnet Traffic Filter using Static Database

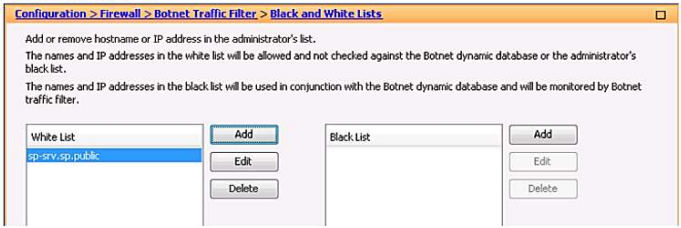
In this task, you will configure the Botnet Traffic Filter on the HQ-ASA to use manually populated static database. You will add the SP-SRV destination as the whitelisted destination to the Botnet Traffic Filter. Then you will observe how the Botnet Traffic Filter logs connection attempts to the whitelisted destination.

Activity Procedure

Complete the following steps:

Step 1

Return to the ASDM session on the Admin PC. Navigate to **Configuration > Firewall > Botnet Traffic Filter > Black and White Lists**. Add the **sp-srv.sp.public** to the Botnet Traffic Filter whitelist. Adding the destination to the whitelist will allow access to the web server, but a logging message will be logged when traffic for the server is seen.



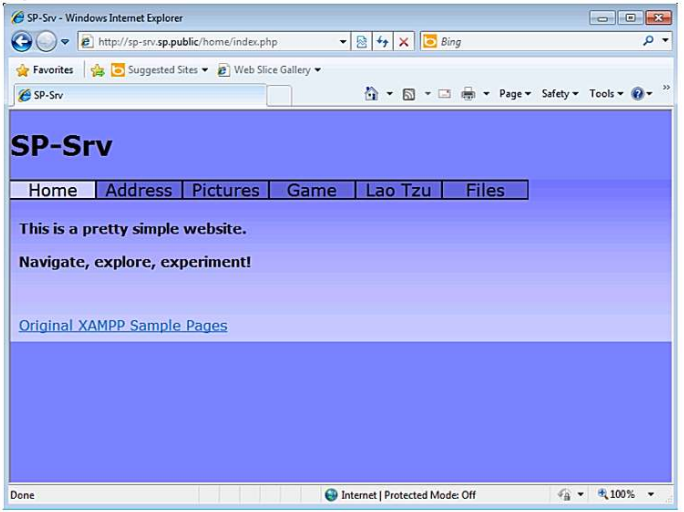
Step 2

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

https://t.me/learningnets

Step 3

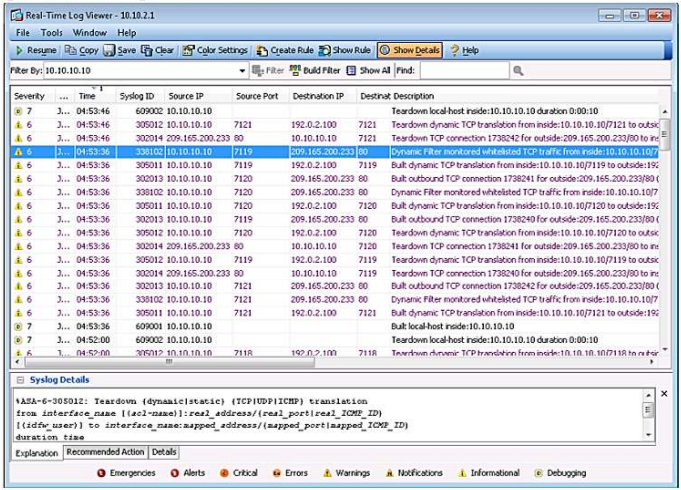
Return to the Employee PC. In the Internet Explorer, navigate to **http://sp-srv.sp.public**. The web page should open.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 4

Return to the Cisco ASDM Real-Time Log Viewer on the Admin PC. Observe how the ASA logged a message about monitoring whitelisted traffic.

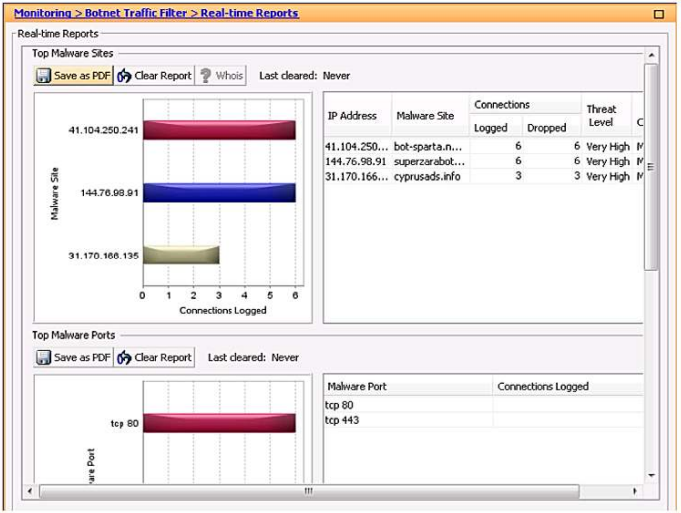


Note It may take a while to see the logging message in the Cisco ASDM Real-Time Log Viewer.

https://t.me/learningnets

Step 5

Return to Cisco ASDM Botnet Traffic Filter real-time reports by navigating to **Monitoring > Botnet Traffic Filter > Real-time Reports**. Observe that **sp.srv.sp.public** destination has not been logged under **Top Malware Sites** since it is whitelisted.



Activity Verification

No verification is needed in this task.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lab 4-4: Configure Cisco ASA Identity Firewall

Activity Objective

The company Secure-X has a network topology as shown in the figure. The company recently hired a new Chief Security Officer that wants to improve all of the current network security controls with the latest technologies to support the most recent company security policy.

Access control lists and NAT configuration on the firewall in the Secure-X headquarters network already allows all IP connectivity from the inside networks to the Internet. The CSO learned about the Cisco ASA Identity Firewall solution, which enables configuration of access rules based on Microsoft Active Directory domain groups and users. The CSO wants to improve the security policy to limit outbound traffic as required by employees' roles.

The CSO tasked you with enabling Cisco ASA Identity Firewall feature on the HQ-ASA to allow outbound access from the Marketing domain group using HTTP and HTTPS and from the Enginneering domain group using HTTP, HTTPS, FTP, and Telnet. The Secure-X enterprise also has to distuinigshed employees; it1 and sales1 users, which both require outbound access for all IP traffic.

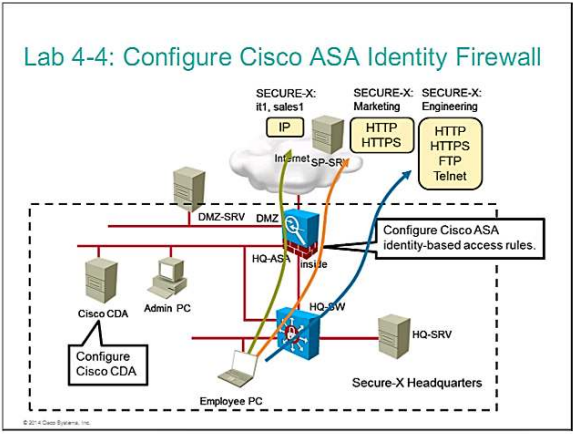
In this activity you will configure Cisco ASA Botnet Traffic Filter:

- Configure Cisco CDA
- Configure the Cisco ASA for Active Directory Integration
- Configure the Cisco ASA with Identity Options
- Configure the Cisco ASA Identity-Based Access Rules

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

Command List

The table describes the Cisco ASA commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco ASA Commands

Command	Description
show user-identity ad-agent	Displays the Cisco CDA and Microsoft Active Directory domain status
show user-identity user active list detail	Displays connection table details for the specified IP address

The table describes the Cisco CDA commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Cisco CDA Commands

Command	Description
show ntp	Displays NTP status
show running-config	Displays running configuration

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

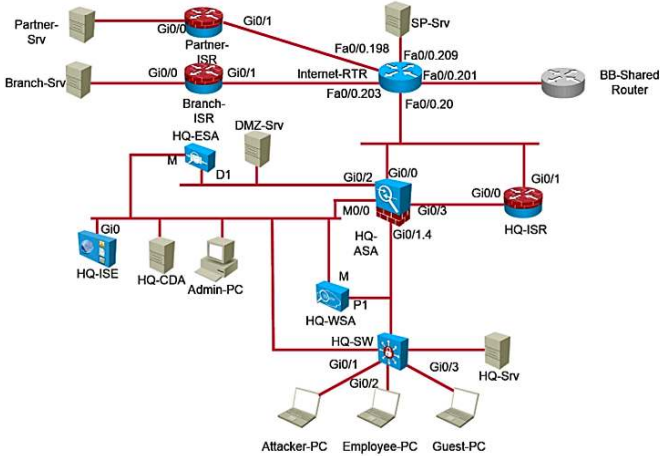
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

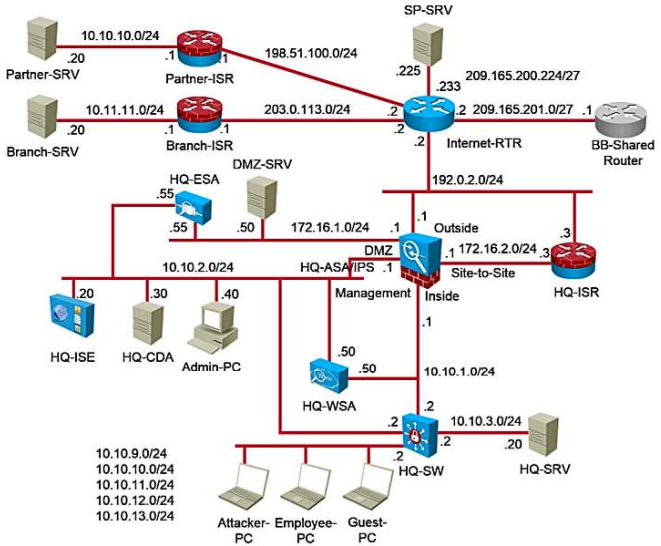
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



https://t.me/learningnets

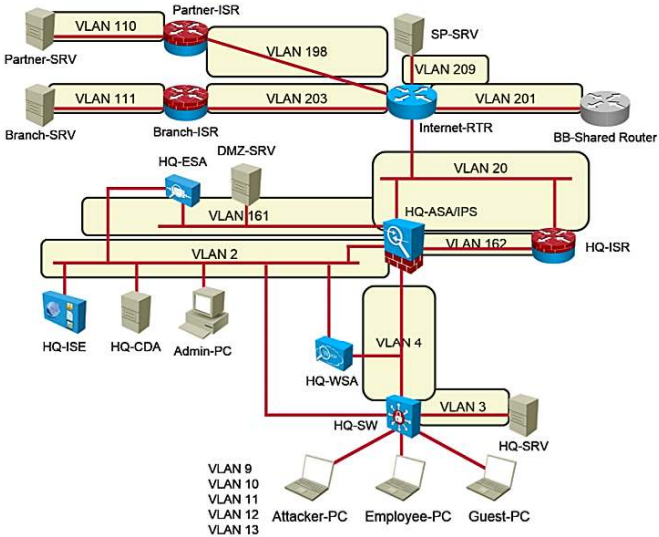
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure Cisco CDA

In this task, you will integrate the HQ-CDA server with the Active Directory domain controller running on the HQ-SRV, and with the HQ-ASA. You will also add the HQ-CDA server to the HQ-ASA to be able to verify Cisco CDA and Cisco ASA integration.

Activity Procedure

Complete the following steps:

https://t.me/learningnets

Step 1

Access the console of the **HQ-CDA**. Log in using **admin** as the username and **Ci5coAdmin** as the password. Examine the running configuration. You should see that the CDA is configured with basic networking settings.

```
cda/admin# show running-config
Generating configuration...
!
hostname cda
!
ip domain-name secure-x.local
!
interface GigabitEthernet 0
  ip address 10.10.2.30 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 10.10.3.20
!
ip default-gateway 10.10.2.2
!
clock timezone US/Pacific
!
ntp server 10.10.3.20
!
username admin password hash $1$RnbOgAat$.V5rWj1kQ9CPggSO.qwuM. role admin
username administrator password hash $1$8y3nejqJ$HBam1cPDgx0uDe/9XvjDR. role adm
in
!
service sshd
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

On the HQ-CDA console, verify NTP status. The Cisco CDA should have clock synchronized with the HQ-SRV at 10.10.3.20.

```
cda/admin# show ntp
Primary NTP   : 10.10.3.20
synchronised to NTP server (10.10.3.20) at stratum 3
   time correct to within 86 ms
   polling server every 256 s
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 127.127.1.0     .LOCL.          10 l    64   64  377    0.000    0.000   0.001
*10.10.3.20      64.103.34.15     2 u     7  256  377    0.516   -7.557   5.468
Warning: Output results may conflict during periods of changing synchronization.
```

Step 3

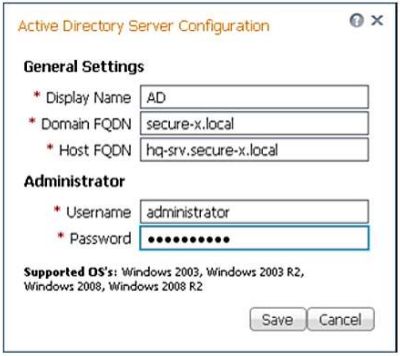
Access the Admin PC and start Mozilla Firefox browser. Connect to the HQ-CDA (at 10.10.2.30) by navigating to **https://cda.secure-x.local** and log in as **admin** with password **Ci5coAdmin**.

https://t.me/learningnets

Step 4

In the Cisco CDA GUI, add the Active Directory server running on the HQ-SRV. Use the following parameters when adding the server:

Setting	Value
Display Name	AD
Domain FQDN	secure-x.local
Host FQDN	hq-srv.secure-x.local
Username	administrator
Password	Cis5oAdmin



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 5

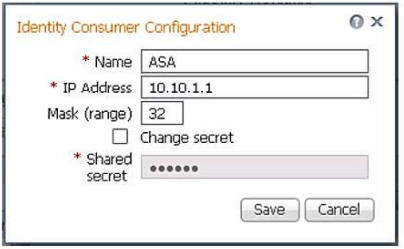
Wait for few minutes and refresh the **Home** dashboard in the Cisco CDA. You should see the HQ-CDA being connected to the AD server.

https://t.me/learningnets

Step 6

In Cisco CDA GUI, add the Cisco ASA as the consumer device. Use the following parameters when adding the server:

Setting	Value
Name	ASA
IP Address	10.10.1.1
Mask	255.255.255.255
Shared secret	cisco123



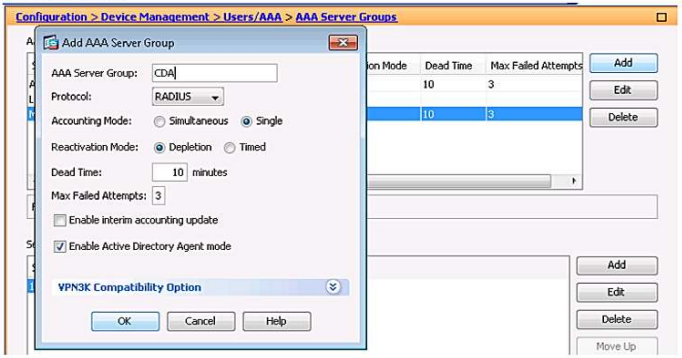
Step 7

On the Admin PC, launch Cisco ASDM. Connect to 10.10.2.1 and log in as **admin** with password **Ci5coAdmin**.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 8

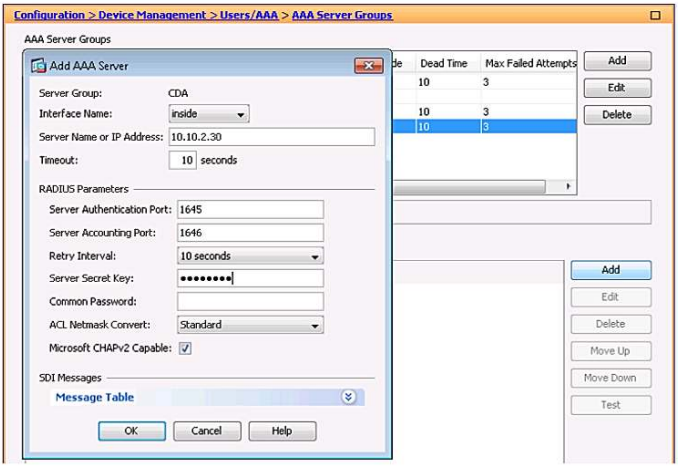
In the Cisco ASDM, navigate to **Configuration > Device Management > Users/AAA > AAA Server Groups**. Add the RADIUS AAA server group. Use CDA as the name of the group. Enable Active Directory Agent mode.



https://t.me/learningnets

Step 9

In the same Cisco ASDM window, add the HQ-CDA server at 10.10.2.30 to the CDA server group. The HQ-CDA server is accessible through the ASA inside interface. Use **cisco123** as the preshared RADIUS key.

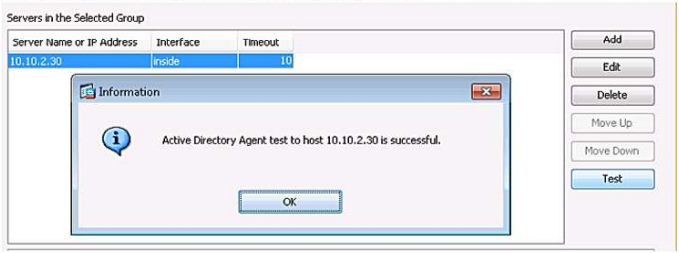


Step 10

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

Step 11

In the same Cisco ASDM window, test the connectivity to the HQ-CDA server by selecting the HQ-CDA server and clicking the **Test** button. The test should be successful.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 12

On the Admin PC, return to the Cisco CDA GUI. Navigate to **Registered Devices**. You should see the **HQ-ASA** as the registered device.

Activity Verification

No verification is needed in this task.

Task 2: Configure the Cisco ASA for Active Directory Integration

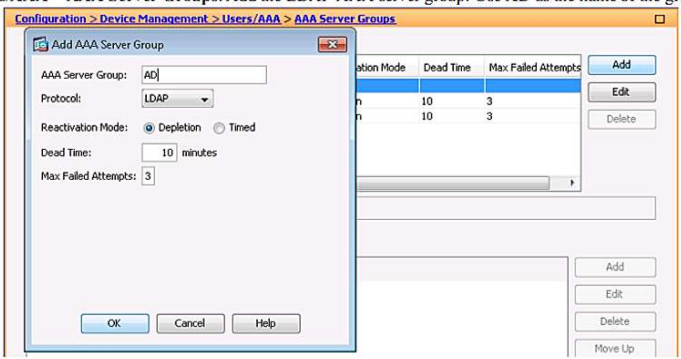
In this task, you will configure integration between the HQ-ASA and the Active Directory domain controller running on the HQ-SRV. This will be done by adding the HQ-SRV as the LDAP server to the HQ-ASA.

Activity Procedure

Complete the following steps:

Step 1

Return to the Cisco ASDM sesion on the Admin PC. Navigate to **Configuration > Device Management > Users/AAA > AAA Server Groups**. Add the LDAP AAA server group. Use **AD** as the name of the group.

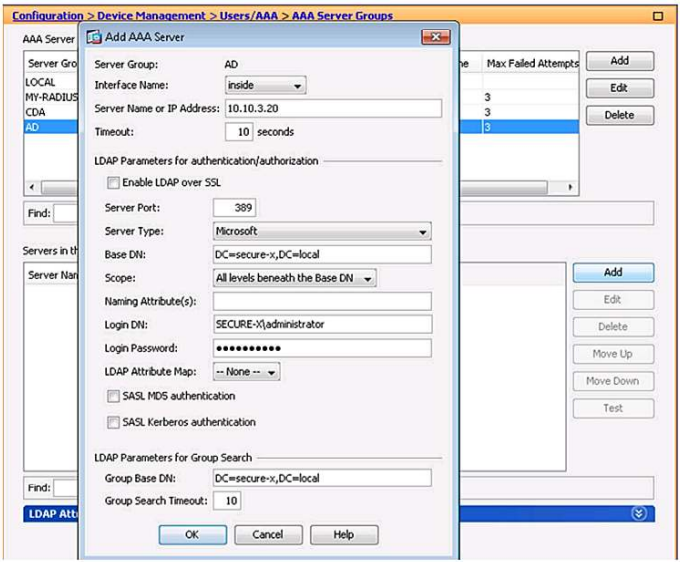


https://t.me/learningnets

Step 2

In the same Cisco ASDM window, add the HQ-SRV server at 10.10.3.20 to the LDAP server group. The HQ-SRV server is accessible through the ASA inside interface. Use the following LDAP settings:

Setting	Value
Server Type	Microsoft
Base DN	DC=secure-x,DC=local
Scope	All levels beneath the Base DN
Login DN	SECURE-X\administrator
Login Password	Ci5coAdmin
Group Base DN	DC=secure-x,DC=local



Step 3

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 4

In the same Cisco ASDM window, test the connectivity to the HQ-SRV server by selecting the HQ-SRV server and clicking the **Test** button. Select the **Authentication** radio button and enter **it1** as the username and **cisco** as the password. The test should be successful.

Activity Verification

No verification is needed in this task.

Task 3: Configure the Cisco ASA with Identity Options

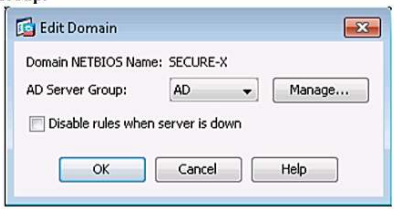
Before configuring identity-based access rules, you have to configure the Cisco ASA with identity options. In this task, you will configure the HQ-ASA with identity user options.

Activity Procedure

Complete the following steps:

Step 1

Return to the Cisco ASDM session on the Admin PC. Navigate to **Configuration > Firewall > Identity Options**. Add the **SECURE-X** domain to the list of domains. Use the previously configured **AD** server group as the **AD Server Group.**



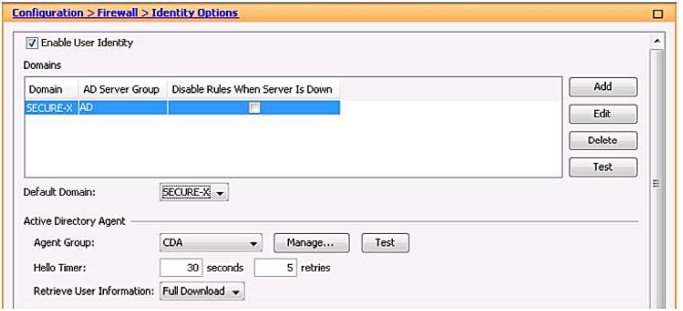
https://t.me/learningnets

Step 2

In the same Cisco ASDM window, select the **SECURE-X** domain as the default domain. The default domain is used for all users and user groups when a domain has not been explicitly configured for those users or groups.

Step 3

In the same Cisco ASDM window, select the previously configured **CDA** server group as the **Active Directory Agent** server group. Leave the other settings at their default values.



Step 4

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

Activity Verification

No verification is needed in this task.

Task 4: Configure the Cisco ASA Identity-Based Access Rules

In this task, you will configure and verify identity-based access rules on the HQ-ASA to allow outbound connectivity as specified by the requirements. You will start by configuring service object groups and local user object that will be used later when configuring identity-based access rules.

Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

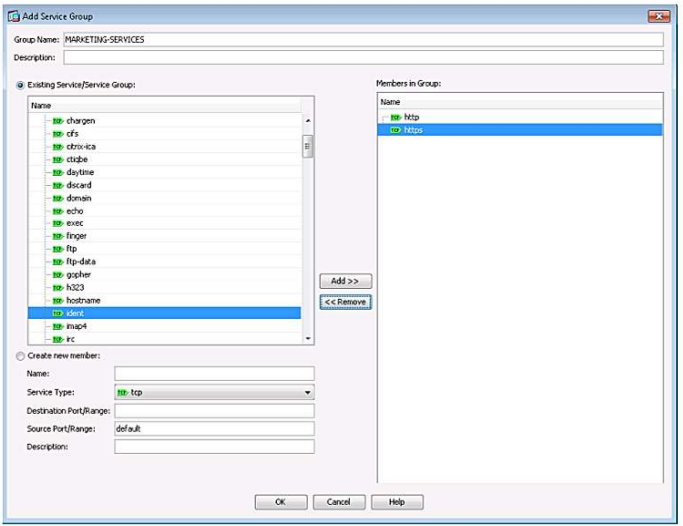
Step 1

In the Cisco ASDM session on the Admin PC, navigate to **Configuration > Firewall > Objects > Service Objects/Groups**. Create an IP service group. Use **MARKETING-SERVICES** as the name of the group.

Add the following services to the group:

HTTP

HTTPS



https://t.me/learningnets

Step 2

Create another IP service group. Use **ENGINEERING-SERVICES** as the name of the group.

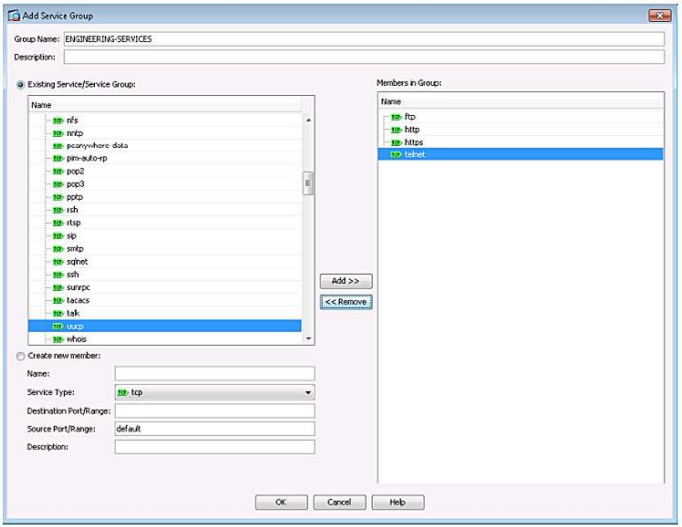
Add the following services to the group:

HTTP

HTTPS

FTP

Telnet



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

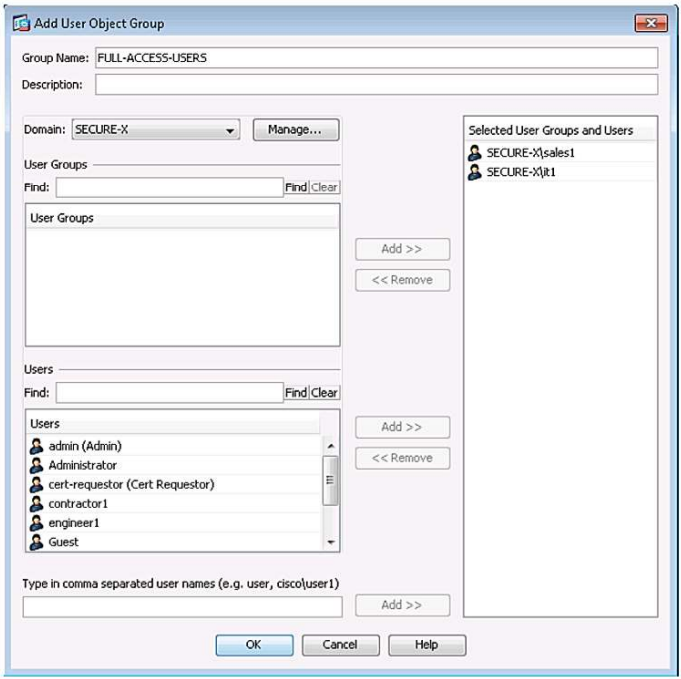
Step 3

In the Cisco ASDM, navigate to **Configuration > Firewall > Objects > Local User Groups**. Create a local user group and use **FULL-ACCESS-USERS** as the name of the group.

Add the following users to the local user group:

SECURE-X\it1

SECURE-X\sales1



Step 4

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

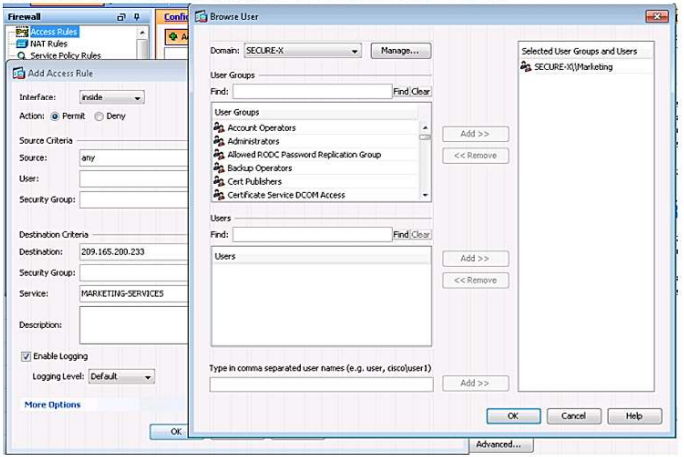
https://t.me/learningnets

Step 5

In the Cisco ASDM , navigate to **Configuration > Firewall > Access Rules**. Remove the access rule, which allows all IP traffic from the INTERNAL-NETWORKS object group to all destinations, from the inside interface. This access rule will be replaced by identity-based access rules that will be configure based on the roles Active Directory domain groups and users have.

Step 6

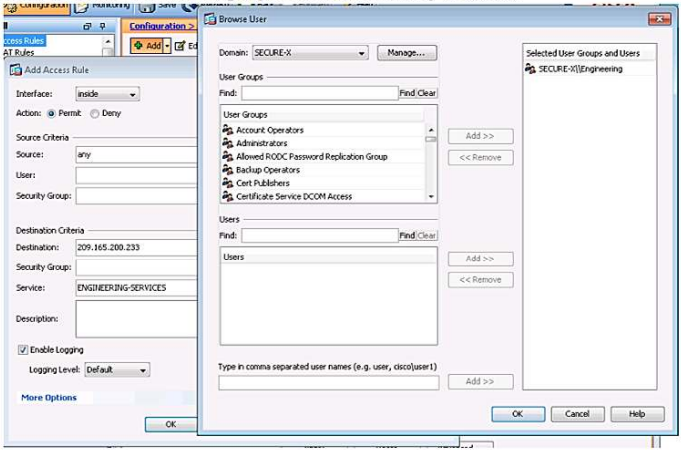
In the same Cisco ASDM window, add a new access rule on the inside interface that will allow traffic from the Active Directory SECURE-X\Marketing group to the SP-SRV at 209.165.200.233 using the MARKETING-SERVICES service group. The users can have any IP address.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 7

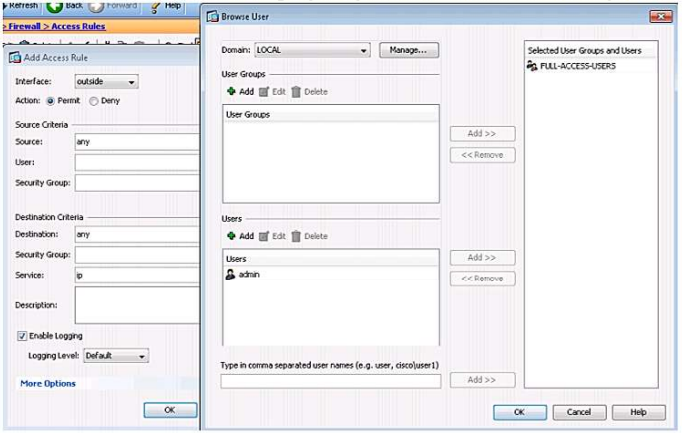
In the same Cisco ASDM window, add a new access rule on the inside interface that will allow traffic from the Active Directory SECURE-X\Engineering group to the SP-SRV at 209.165.200.233 using the ENGINEERING-SERVICES service group. The users can have any IP address.



https://t.me/learningnets

Step 8

In the same Cisco ASDM window, add a new access rule on the inside interface that will allow all IP traffic from the FULL-ACCESS-USERS local user group to any destination. The users can have any IP address.



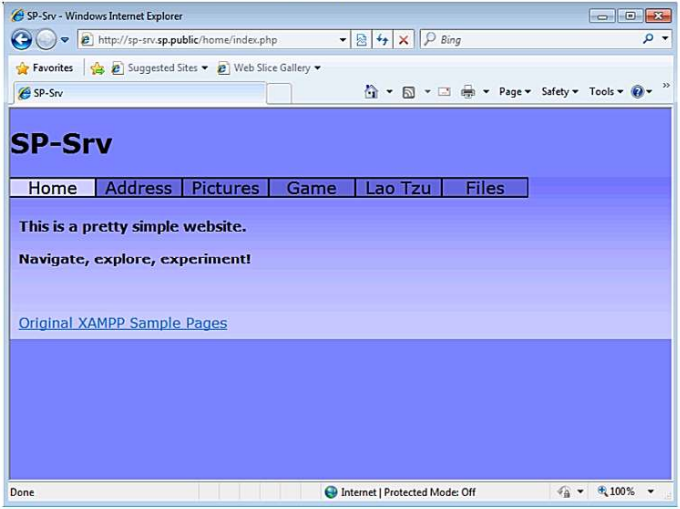
Step 9

Apply the configuration by clicking the **Apply** button, and **Send** the configuration to the appliance.

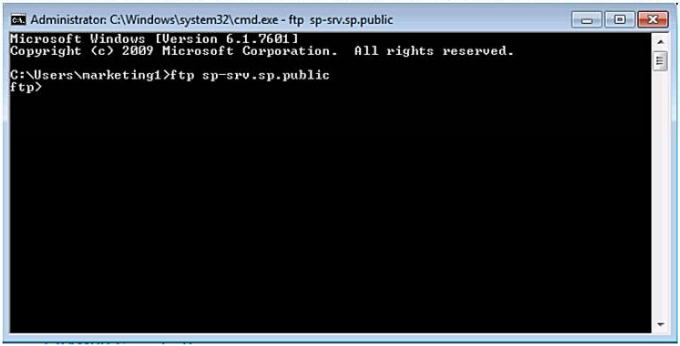
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 10

Access the Employee PC. Log in as the **SECURE-X\marketing1** user with **cisco** password. Open Internet Explorer web browser and navigate to **http://sp-srv.sp.public**. You should be successful since HTTP traffic is allowed from the Marketing Active Directory group.



On the Employee PC, open the command prompt and use FTP to connect to the **sp-srv.sp.public**. The attempt should not be successful because FTP is not allowed from the Marketing Active Directory group.



https://t.me/learningnets

Step 11

Access the HQ-ASA console. Display the active users on the HQ-ASA. Observe the mapping between the SECURE-X\marketing1 Active Directory domain user and IP address:

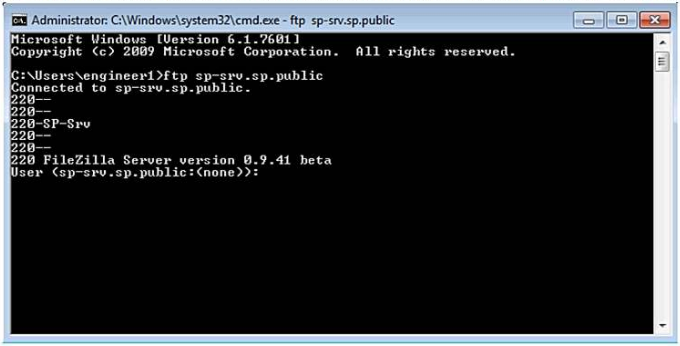
```
HQ-ASA# show user-identity user active list detail
Total active users: 1    Total IP addresses: 1
  LOCAL: 0 users, 0 IP addresses
  SECURE-X: 1 users, 1 IP addresses
  SECURE-X\marketing1: 0 active conns; idle 21 mins
    10.10.10.10: login 70 mins, idle 21 mins, 0 active conns
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 12

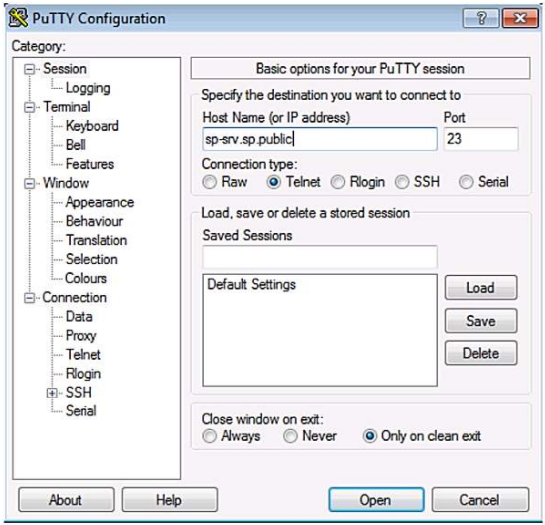
Return to the Employee PC. Log out and log in again as the **SECURE-X\engineer1** user with **cisco** password.

On the Employee PC, open the command prompt and use FTP to connect to the **sp-srv.sp.public**. The attempt should be successful because FTP is allowed from the Engineering Active Directory domain group.



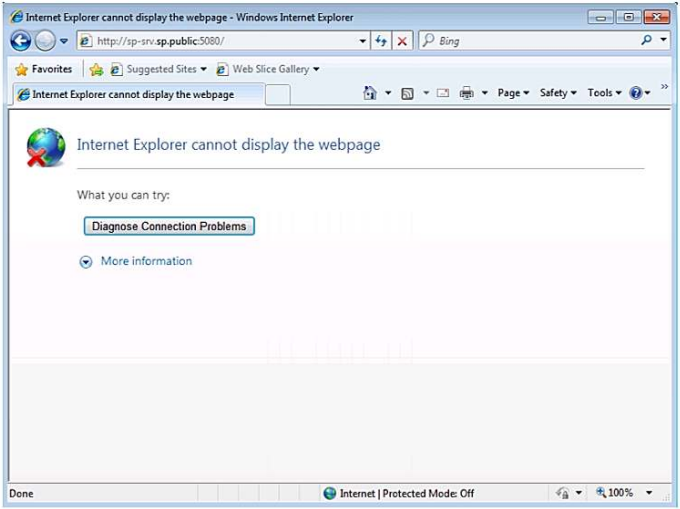
On the Employee PC, open Putty and use Telnet to connect to the **sp-srv.sp.public**. The attempt should be successful because Telnet is allowed from the Engineering Active Directory domain group.

https://t.me/learningnets



On the Employee PC, open Internet Explorer web browser and navigate to **http://sp-srv.sp.public:5080.** You should not be successful since TCP 5080 traffic is not allowed from the Engineering Active Directory domain group.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



Step 13

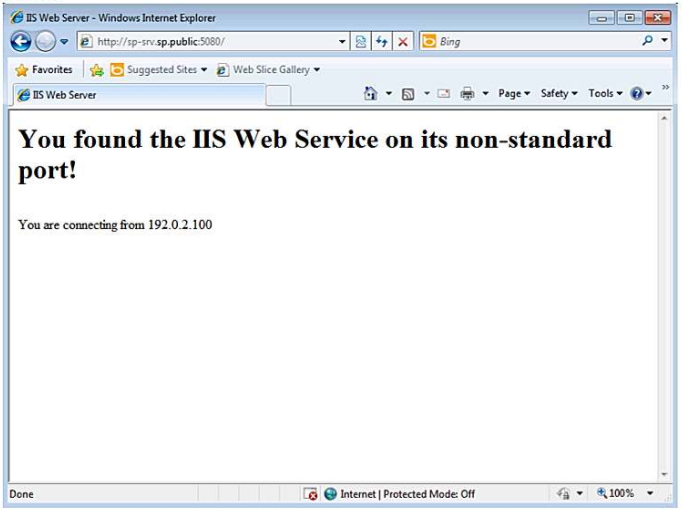
Return to the HQ-ASA console. Display the active users on the HQ-ASA. Observe the mapping between the SECURE-X\engineer1 Active Directory domain user and IP address. The same IP address is now mapped to the different Active Directory domain user.

```
HQ-ASA# show user-identity user active list detail
Total active users: 1    Total IP addresses: 1
  LOCAL: 0 users, 0 IP addresses
  SECURE-X: 1 users, 1 IP addresses
  SECURE-X\engineer1: 1 active conns; idle 0 mins
    10.10.10.10: login 11 mins, idle 0 mins, 1 active conns
```


https://t.me/learningnets

Step 14

Return to the Employee PC. Log out and log in again as the **SECURE-X\it1** user with **cisco** password. Open Internet Explorer web browser and navigate to **http://sp-srv.sp.public.:5080** again. You should be successful because all IP traffic (including TCP 5080) is allowed from the it1 or sales1 Active Directory domain users.



Step 15

Return to the HQ-ASA console. Display the active users on the ASA. Observe the mapping between the SECURE-X\it1 Active Directory domain user and IP address. The same IP address is now mapped to the different Active Directory domain user.

```
HQ-ASA# show user-identity user active list detail
Total active users: 1    Total IP addresses: 1
  LOCAL: 0 users, 0 IP addresses
  SECURE-X: 1 users, 1 IP addresses
  SECURE-X\it1: 0 active conns; idle 0 mins
    10.10.10.10: login 1 mins, idle 0 mins, 0 active conns
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

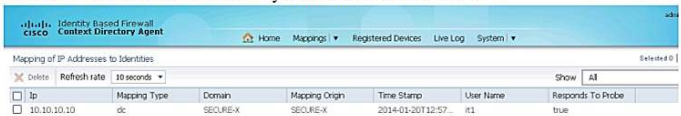
Step 16

On the HQ-ASA console, display the Cisco CDA and Microsoft Active Directory domain status. Both the Cisco CDA status and Active Directory domain status should be in the up state.

```
HQ-ASA# show user-identity ad-agent
Primary AD Agent:
 Status                  up (registered)
 Mode:                   full-download
 IP address:             10.10.2.30
 Authentication port:    udp/1645
 Accounting port:        udp/1646
 ASA listening port:     udp/3799
 Interface:              inside
 Up time:                3 days 2 hours
 Average RTT:            0 msec
AD Domain Status:
 Domain SECURE-X:        up
```

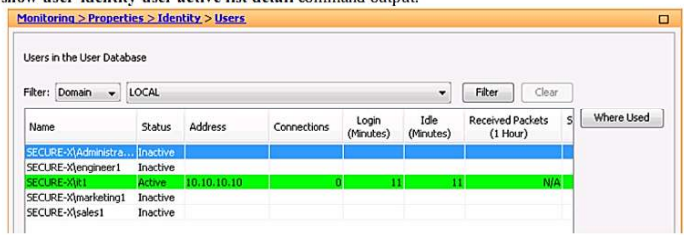
Step 17

Return to the Cisco CDA GUI session on the Admin PC. Navigate to **Mappings**. Observer the mapping between the SECURE-X\it1 Active Directory domain user and IP address.



Step 18

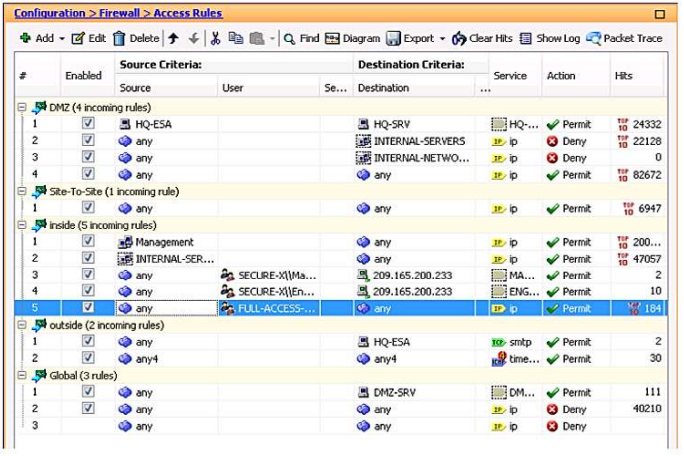
Return to the Cisco ASDM session on the Admin PC. Navigate to **Monitoring > Properties > Identity > Users**. Observe the mappings in the Cisco ASDM. The output should be similar than output in the ASA CLI **show user-identity user active list detail** command output.



https://t.me/learningnets

Step 19

In the Cisco ASDM, navigate to **Configuration > Firewall > Access Rules**. Non-zero hit counts next to the identity-based access rules indicate that packets indeed matched the access rules.



Activity Verification

No verification is needed in this task.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lab 5-1: Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies

Activity Objective

The partner company of the Secure-X company has a network topology as shown in the figure. The partner company has the Cisco IOS router that has been configured by you with NAT configuration to implement outbound connectivity to the Internet for clients in the network, and inbound connectivity from the Internet to the server.
The partner network wants to improve the security posture of their network and would like to implement Cisco IOS Zone-Based Policy Firewall to allow only required connectivity across the router.

You are the network security engineer for the Secure-X network. The CSO of the Secure-X network tasked you to help the partner company to configure Cisco IOS Zone-Based Policy Firewall on their Cisco IOS Software router. You will have to configure zones, zone pairs, and policies to allow connectivity between inside and outside networks, and between the inside network and the router's control and management plane. Because the Secure-X company is connected to the partner network via IPsec VPN tunnel, you will also have to configure Cisco IOS Zone-Based Policy Firewall for traffic coming from the VPN tunnel and going into the inside network.

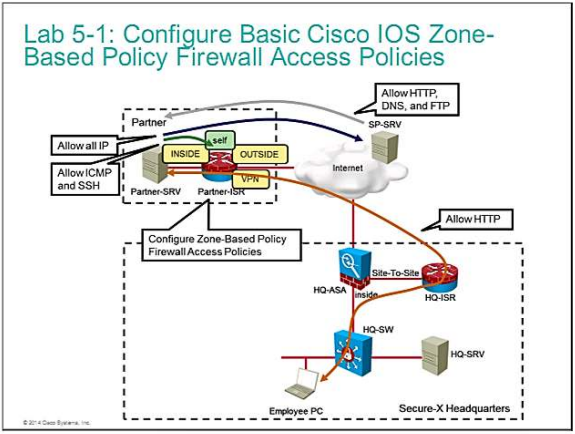
In this activity you will configure basic Cisco IOS Zone-Based Policy Firewall access policies:

- Configure security zones
- Configure access control between the INSIDE and OUTSIDE zones
- Configure access control between the VPN and INSIDE zones
- Configure access control for management traffic between the SELF and OUTSIDE zones

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

Command List

The table describes the Cisco IOS commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco IOS Commands

Command	Description
class-map type inspect [match-any | match-all] *class-map-name*	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect-type class map.
class type inspect *class-map-name*	Specifies the traffic (class) on which an action is to be performed in policy-map configuration mode.
drop [log]	Drops packets that are sent to the router in policy-map-class configuration mode.
inspect	Enables Cisco IOS stateful packet inspection in policy-map-class configuration mode.
interface *interface*	Enters interface configuration mode
ip access-list extended *access-list-name*	Defines the extended IP access list.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command	Description
match access-group {*access-group* | **name** *access-group-name*}	Configures the match criteria for a class map based on the specified ACL.
match protocol *protocol-name*	Configures the match criterion for a class map based on the specified protocol.
permit *source [source-wildcard]* **permit** *protocol source source-wildcard destination destination-wildcard*	Sets conditions to allow a packet to pass a named IP access list in access list configuration mode.
policy-map type inspect *policy-map-name*	Creates a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect-type policy map.
service-policy type inspect *policy-map-name*	Attaches a firewall policy map to a zone-pair in zone-pair configuration mode.
show policy-map type inspect zone-pair [*zone-pair-name*]	Displays the runtime inspect-type policy map statistics and other information such as sessions existing on a specified zone pair.
show zone security *security-zone-name*	Displays zone security information.
zone-member security *zone-name*	Attaches an interface to a security zone in interface configuration mode.
zone-pair security *zone-pair-name* **source** {*source-zone-name* | **self** | *default*} **destination** {*destination-zone-name* | **self** | **default**}	Creates a zone pair in global configuration mode.
zone security *zone-name*	Creates a security zone.

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

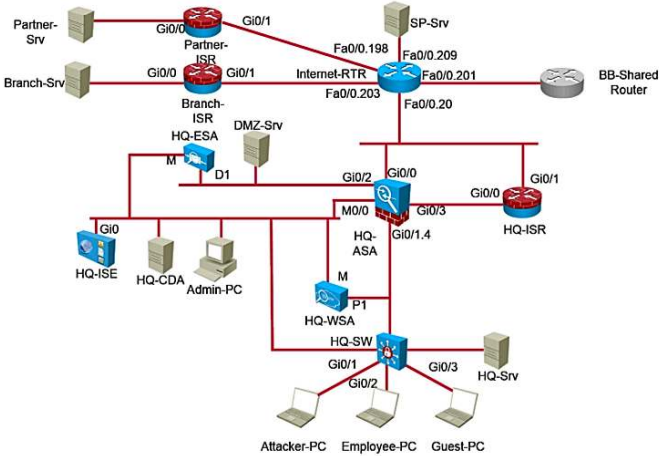
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

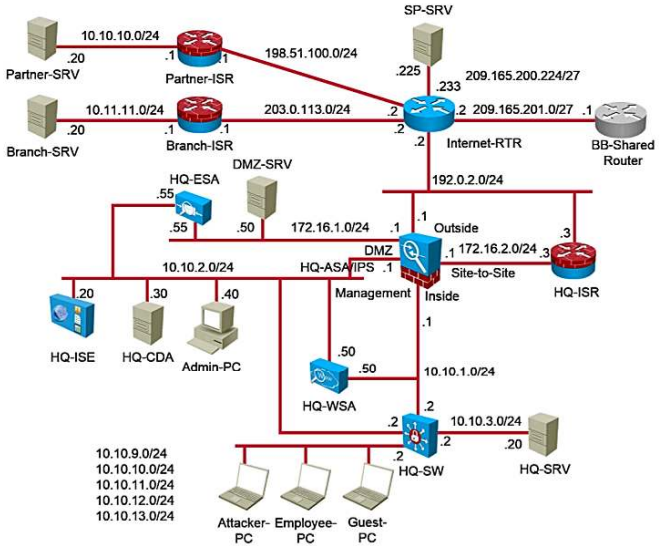
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



https://t.me/learningnets

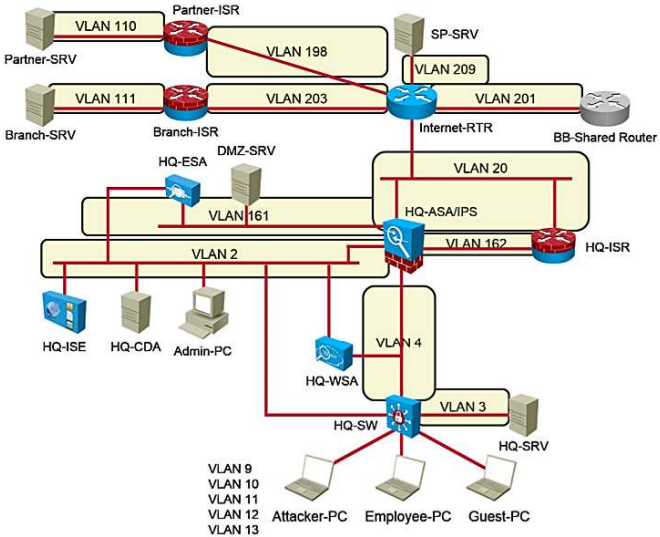
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure Security Zones

In this task, you will create three named security zones, assign router interfaces to zones, and create zone pairs that require interaction, on the Partner-ISR router.

Activity Procedure

Complete the following steps:

Step 1

Access the Partner-ISR router console.

Step 2

On the Partner-ISR router, globally create zones named INSIDE, VPN and OUTSIDE.

https://t.me/learningnets

Step 3

On the Partner-ISR router, assign interfaces to zones:

Assign the GigabitEthernet0/1 interface to zone OUTSIDE

Assign the GigabitEthernet0/0 interface to zone INSIDE

Assign the Tunnel0 interface to zone VPN

Step 4

Create zone pairs that will require interaction:

INSIDE to OUTSIDE

OUTSIDE to INSIDE

VPN to INSIDE

Step 5

On Partner-ISR display the zone descriptions and interfaces that are associated with the three zones:

```
Partner-ISR# show zone security
zone self
  Description: System defined zone
zone INSIDE
  Member Interfaces:
    GigabitEthernet0/0
zone OUTSIDE
  Member Interfaces:
    GigabitEthernet0/1
zone VPN
  Member Interfaces:
    Tunnel0
```

Activity Verification

No verification is needed in this task.

Task 2: Configure Access Control Between the INSIDE and OUTSIDE Zones

In this task, you will configure access control between the INSIDE and OUTSIDE zones.

Activity Procedure

Complete the following steps:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 1

On the Partner-ISR router, configure the access policy using the Zone-based Policy Firewall configuration language that will allow any host in the INSIDE zone to access to any host in the OUTSIDE zone, using any protocol (all IP traffic).

Create an access list that will match all IP traffic from any host to any host. Use **IN-TO-OUT-ACL** as the name of the ACL.

Create a class map that will match the **IN-TO-OUT-ACL** access list. Use **IN-TO-OUT-TRAFFIC** as the name of the class map.

Create a policy map, that will refer to the **IN-TO-OUT-TRAFFIC** class map and apply inspect action to it. Use **IN-TO-OUT-POLICY** as the name of the policy map.

Apply the **IN-TO-OUT-POLICY** policy map to the INSIDE to OUTSIDE zone pair.

Step 2

On the Partner-ISR router, configure the access policy using the Zone-based Policy Firewall configuration language that will allow any host in the OUTSIDE zone to access the Partner-SRV in the INSIDE zone, using HTTP, DNS and FTP. Deny and log all other attempts.

Create an access list that will match all IP traffic from any host to the Partner-SRV host (10.10.10.20). Use **OUT-TO-PARTNER-SRV-ACL** as the name of the ACL.

Create a class map that will match the **OUT-TO-PARTNER-SRV-ACL** access list AND HTTP protocol. Use **OUT-TO-PARTNER-SRV-HTTP-TRAFFIC** as the name of the class map.

Create a class map that will match the **OUT-TO-PARTNER-SRV-ACL** access list AND FTP protocol. Use **OUT-TO-PARTNER-SRV-FTP-TRAFFIC** as the name of the class map.

Create a class map that will match the **OUT-TO-PARTNER-SRV-ACL** access list AND DNS protocol. Use **OUT-TO-PARTNER-SRV-DNS-TRAFFIC** as the name of the class map.

Create a policy map. Use **OUT-TO-IN-POLICY** as the name of the policy map.

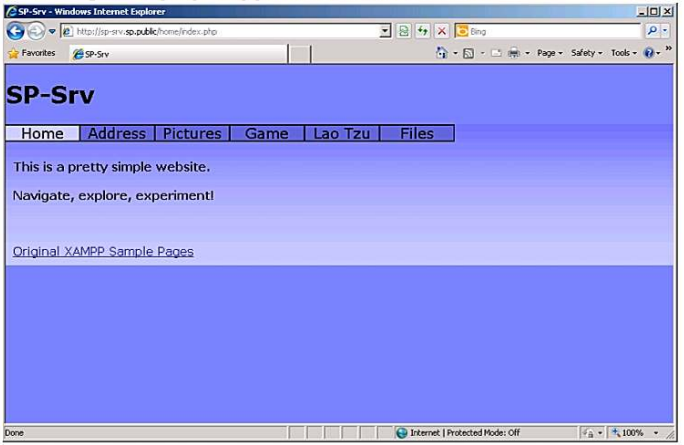
- Inside the policy map, refer to the **OUT-TO-PARTNER-SRV-HTTP-TRAFFIC** class map and apply inspect action to it.
- Inside the policy map, refer to the **OUT-TO-PARTNER-SRV-FTP-TRAFFIC** class map and apply inspect action to it.
- Inside the policy map, refer to the **OUT-TO-PARTNER-SRV-DNS-TRAFFIC** class map and apply inspect action to it.
- Inside the policy map, refer to the **class-default** class map and apply drop and log action to it.

Apply the **OUT-TO-IN-POLICY** policy map to the OUTSIDE to INSIDE zone pair.

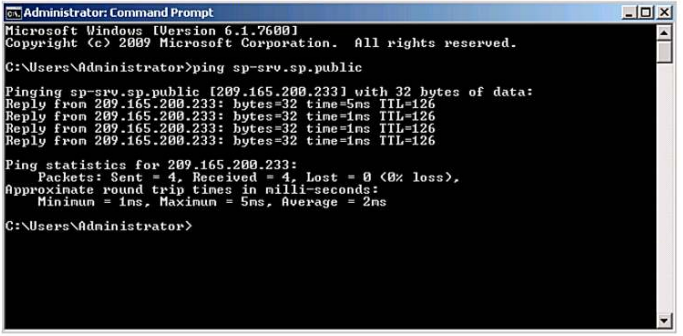
https://t.me/learningnets

Step 3

Access the Partner-SRV to test connectivity from the INSIDE zone to the OUTSIDE zone. Open Internet Explorer and navigate to **http://sp-srv.sp.public**. You should be successful.



On the Partner-SRV, open a command prompt and ping **sp-srv.sp.public**. You should be successful.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 4

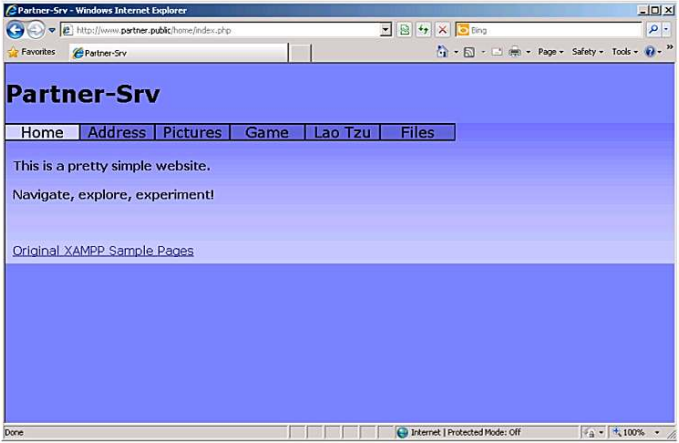
Return to the Partner-ISR console and display a policy map along with its class maps, and display session statistics. You should see a number of packets matching the **IN-TO-OUT-TRAFFIC** class map in the **IN-TO-OUT-POLICY** policy.

```
Partner-ISR# show policy-map type inspect zone-pair
policy exists on zp IN-TO-OUT
  Zone-pair: IN-TO-OUT
  Service-policy inspect : IN-TO-OUT-POLICY
    Class-map: IN-TO-OUT-TRAFFIC (match-all)
      Match: access-group name IN-TO-OUT-ACL
   Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [1:1193]
        udp packets: [120:1]
        icmp packets: [0:8]
        Session creations since subsystem startup or last reset 85
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [12:3:4]
        Last session created 00:00:40
        Last statistic reset never
        Last session creation rate 5
        Maxever session creation rate 49
        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: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
<output omitted>
```

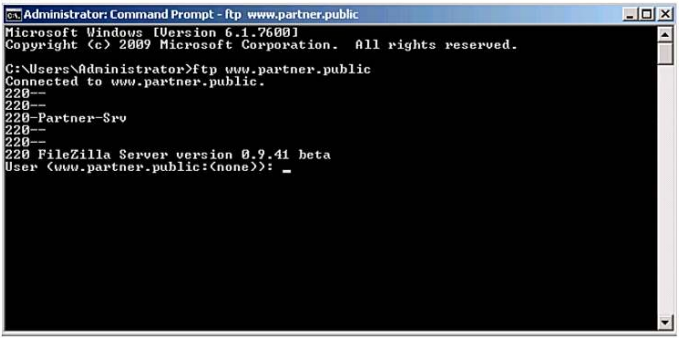

https://t.me/learningnets

Step 5

Access the SP-SRV to test connectivity from the OUTSIDE zone to the INSIDE zone. Open Internet Explorer and navigate to **http://www.partner.public**. This is the DNS record for the translated IP address (198.51.100.20) of the Partner-SRV. You should be successful.

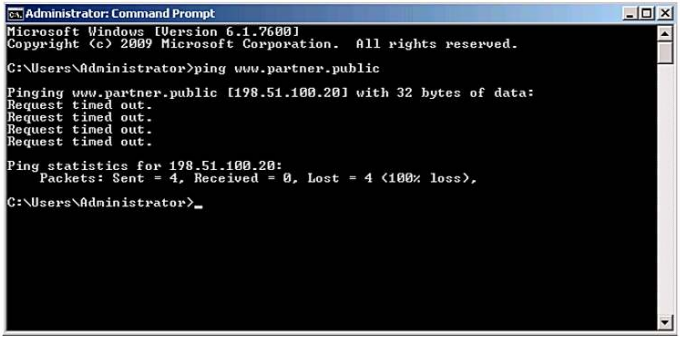


On the SP-SRV, open a command prompt and connect to **www.partner.public** using FTP. You should be successful.



On the SP-SRV, open a command prompt and ping **www.partner.public**. You should not be successful, as ICMP packets are dropped as the result of the drop action in the default-class traffic class.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



Step 6

Return to the Partner-ISR console and observe logging messages about dropped ICMP sessions.

```
*Jan 22 11:41:31.309: %FW-6-DROP_PKT: Dropping icmp session 209.165.200.233:0
10.10.10.20:0 on zone-pair OUT-TO-IN class class-default due to  DROP action found in
policy-map with ip ident 0
```


https://t.me/learningnets

Step 7

On the Partner-ISR console, display the policy map along with its class maps, and display session statistics. You should see a number of packets matching the **OUT-TO-PARTNER-SRV-HTTP-TRAFFIC**, **OUT-TO-PARTNER-SRV-FTP-TRAFFIC**, and **OUT-TO-PARTNER-SRV-DNS-TRAFFIC** class maps in the **OUT-TO-IN-POLICY** policy. You should also see packets matching the class-default class and being dropped.

```
Partner-ISR# show policy-map type inspect zone-pair
<output omitted>
policy exists on zp OUT-TO-IN
  Zone-pair: OUT-TO-IN
  Service-policy inspect : OUT-TO-IN-POLICY
    Class-map: OUT-TO-PARTNER-SRV-HTTP-TRAFFIC (match-all)
      Match: protocol http
      Match: access-group name OUT-TO-PARTNER-SRV-ACL
    Inspect
         Packet inspection statistics [process switch:fast switch]
         tcp packets: [0:75]

         Session creations since subsystem startup or last reset 5
         Current session counts (estab/half-open/terminating) [0:0:0]
         Maxever session counts (estab/half-open/terminating) [2:1:0]
         Last session created 01:28:00
         Last statistic reset never
         Last session creation rate 0
         Maxever session creation rate 3
         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: OUT-TO-PARTNER-SRV-FTP-TRAFFIC (match-all)
      Match: protocol ftp
      Match: access-group name OUT-TO-PARTNER-SRV-ACL
    Inspect
         Packet inspection statistics [process switch:fast switch]
         tcp packets: [32:0]
         Session creations since subsystem startup or last reset 2
         Current session counts (estab/half-open/terminating) [0:0:0]
         Maxever session counts (estab/half-open/terminating) [2:1:0]
         Last session created 00:06:02
         Last statistic reset never
         Last session creation rate 0
         Maxever session creation rate 2
         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: OUT-TO-PARTNER-SRV-DNS-TRAFFIC (match-all)
      Match: protocol dns
      Match: access-group name OUT-TO-PARTNER-SRV-ACL
    Inspect
         Packet inspection statistics [process switch:fast switch]
         udp packets: [12:0]
         Session creations since subsystem startup or last reset 6
         Current session counts (estab/half-open/terminating) [0:0:0]
         Maxever session counts (estab/half-open/terminating) [2:1:0]
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
        Last session created 00:06:15
        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
    Class-map: class-default (match-any)
      Match: any
      Drop
        14 packets, 572 bytes
```

Activity Verification

No verification is needed in this task.

Task 3: Configure Access Control Between the VPN and INSIDE Zones

In this task, you will configure access control between the VPN and INSIDE zones. Proceed to this task only if you correctly configured Twice NAT on the HQ-ASA for the overlapping IP addresses in the Secure-X headquarters VLAN 10 and Partner network. Identity-based access rules on the **HQ-ASA** should also be configured correctly to allow traffic from the SECURE-X\it1 domain user to the Partner-SRV. These configuration tasks should have be done in previous labs.

Activity Procedure

Complete the following steps:

Step 1

On the Partner-ISR router, configure the access policy using the Zone-based Policy Firewall configuration language that will allow 10.0.0.0/8 network in the VPN zone to access 10.0.0.0/8 network in the INSIDE zone, using any protocol (all IP traffic).

Create an access list that will match all IP traffic from the 10.0.0.0/8 network to 10.0.0.0/8 network . Use **VPN-TO-IN-ACL** as the name of the ACL.

Create a class map that will match the **VPN-TO-IN-ACL** access list AND HTTP protocol. Use **VPN-TO-IN-TRAFFIC** as the name of the class map.

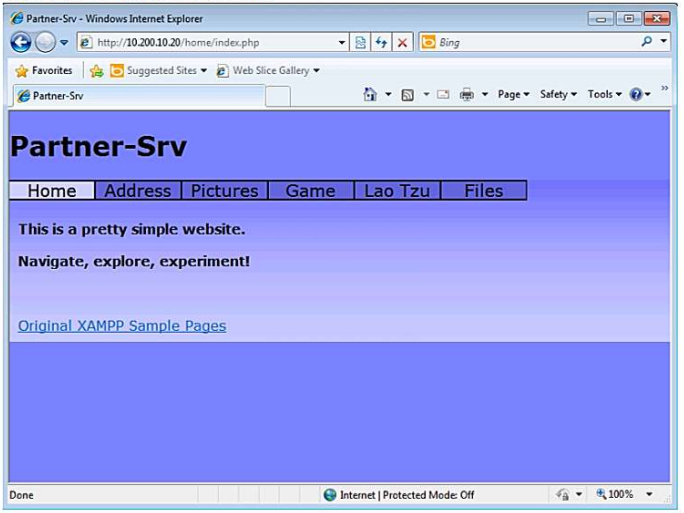
Create a policy map, that will refer to the **VPN-TO-IN-TRAFFIC** class map and apply inspect action to it. Use **VPN-TO-IN-POLICY** as the name of the policy map.

Apply the **VPN-TO-IN-POLICY** policy map to the VPN to INSIDE zone pair.

https://t.me/learningnets

Step 2

Access the Employee PC to test connectivity from the VPN zone to the INSIDE zone. Make sure that you are logged into the PC as the SECURE-X\it1 domain user. Open Internet Explorer and navigate to the translated IP address of the Partner-SRV at 10.200.10.20. Recall that this is how the inside VLAN 10 sees the Partner-SRV. You should be successful.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

Return to the Partner-ISR console and display the policy map along with its class maps, and display session statistics. You should see a number of packets matching the **VPN-TO-IN-TRAFFIC** class map in the **VPN-TO-IN-POLICY** policy.

```
Partner-ISR# show policy-map type inspect zone-pair
<output omitted>
policy exists on zp VPN-TO-IN
  Zone-pair: VPN-TO-IN
  Service-policy inspect : VPN-TO-IN-POLICY
    Class-map: VPN-TO-IN-TRAFFIC (match-all)
      Match: protocol http
      Match: access-group name VPN-TO-IN-ACL
    Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [0:45]
        Session creations since subsystem startup or last reset 2
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [2:1:0]
        Last session created 01:19:04
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 2
        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: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

Activity Verification

No verification is needed in this task.

Task 4: Configure Access Control for Management Traffic Between the SELF and OUTSIDE Zones

In this task, you will configure access control between the INSIDE and SELF zones. You will configure the Partner-ISR router to allow only ICMP and SSH access from the INSIDE zone to the router's control and management plane.

Activity Procedure

Complete the following steps:

https://t.me/learningnets

Step 1

On the Partner-ISR router, configure the access policy using the Zone-based Policy Firewall configuration language that will allow the Partner-SRV host (10.10.10.20) in the INSIDE zone to ping the Partner-ISR and connect to it using SSH. All other attempts should be logged and denied.

Create an access list that will match the following traffic. Use **IN-TO-SELF-ACL** as the name of the ACL.

- ICMP traffic from the Partner-SRV to any host
- SSH traffic from the Partner-SRV to any host

Create a class map that will match the **IN-TO-SELF-ACL** access list. Use **IN-TO-SELF-TRAFFIC** as the name of the class map.

Create a policy map, that will refer to the **IN-TO-SELF-TRAFFIC** class map and apply inspect action to it. Use **IN-TO-SELF-POLICY** as the name of the policy map.

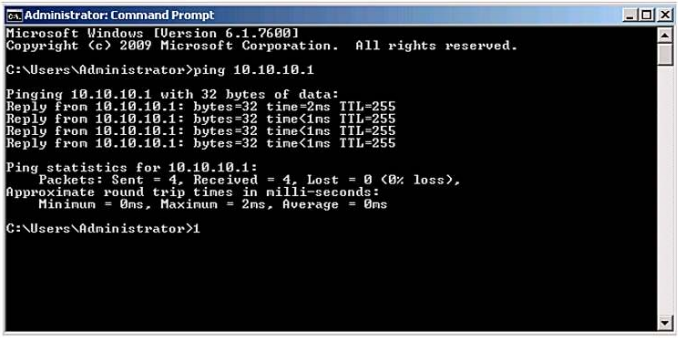
Inside the policy map, refer to the **class-default** class map and apply drop and log action to it.

Apply the **IN-TO-SELF-POLICY** policy map to the INSIDE to SELF zone pair.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

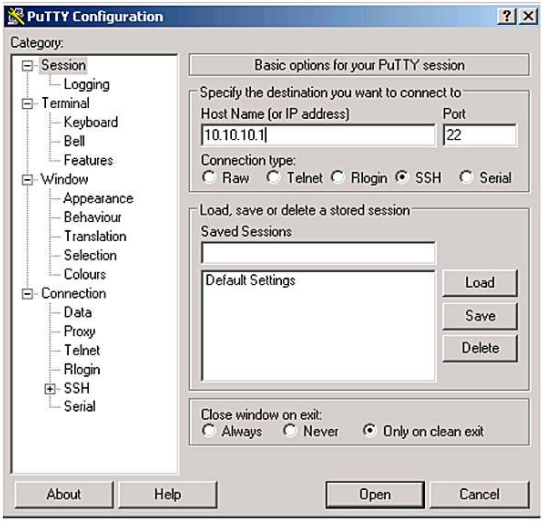
Step 2

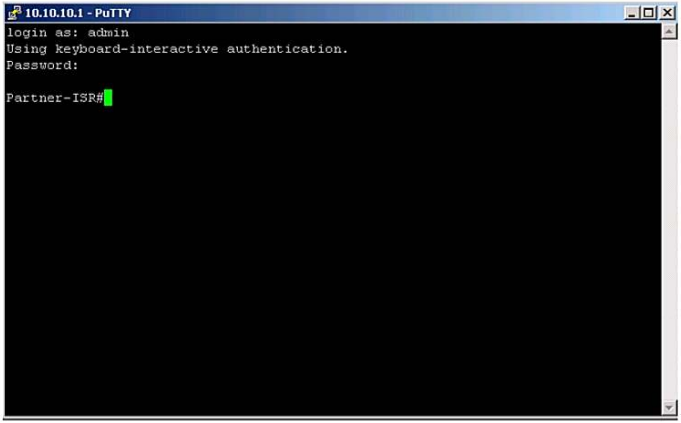
Return to the Partner-SRV to test connectivity from the INSIDE zone to the SELF zone. Open a command prompt and ping the Partner-ISR router at 10.10.10.1. You should be successful.



On the Partner-SRV, open the Putty and connect to the Partner-ISR at 10.10.10.1 using SSH. Log in using **admin** as the username and **Ci5coAdmin** as the password. You should be successful. If the attempt is not successful, return to the Partner-ISR console and create an RSA pair key using the **crypto key generate rsa modulus 1024** command.

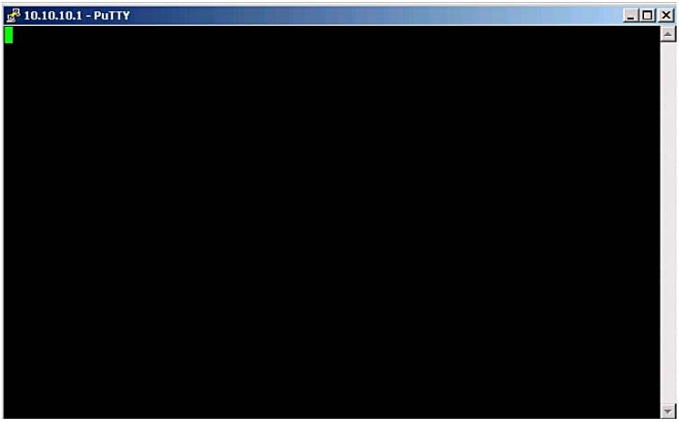
https://t.me/learningnets





On the Partner-SRV, open the Putty again and connect to the Partner-ISR at 10.10.10.1 using Telnet. You should not be successful as Telnet packets are dropped as the result of the drop action in the default-class traffic class.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



Step 3

Return to the Partner-ISR console and observe logging messages about dropped TCP Telnet sessions.

```
*Jan 22 13:20:12.373: %FW-6-DROP_PKT: Dropping tcp session 10.10.10.20:4709
10.10.10.1:23 on zone-pair IN-TO-SELF class class-default due to  DROP action found
in policy-map with ip ident 0
```


https://t.me/learningnets

Step 4

On the Partner-ISR console, display the policy map along with its class maps, and display session statistics. You should see a number of packets matching the **IN-TO-SELF-TRAFFIC** class map in the **IN-TO-SELF-POLICY** policy. You should also see packets matching the class-default class and being dropped.

```
Partner-ISR# show policy-map type inspect zone-pair
policy exists on zp IN-TO-SELF
  Zone-pair: IN-TO-SELF
  Service-policy inspect : IN-TO-SELF-POLICY
    Class-map: IN-TO-SELF-TRAFFIC (match-all)
      Match: access-group name IN-TO-SELF-ACL
    Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [40:42]
        icmp packets: [4:4]
        Session creations since subsystem startup or last reset 3
        Current session counts (estab/half-open/terminating) [1:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 00:05:27
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 2
        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: class-default (match-any)
      Match: any
      Drop
        17 packets, 3075 bytes
```

Activity Verification

No verification is needed in this task.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lab 5-2: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies

Activity Objective

The partner company of the Secure-X company has a network topology as shown in the figure. The partner company has the Cisco IOS router that has been configured by you with NAT and basic Zone-based Policy Firewall configuration to provide secure connectivity over the router.
The partner network wants to have additional insight into HTTP traffic that traverses the router and goes to the internal web server.

You are the network security engineer for the Secure-X network. The CSO of the Secure-X network tasked you to help the partner company to configure advanced Zone-based Policy Firewall access policies on their Cisco IOS Software router. You will configure the router to detect HTTP protocol conformance violations and attempts to download executable files from the internal web server.

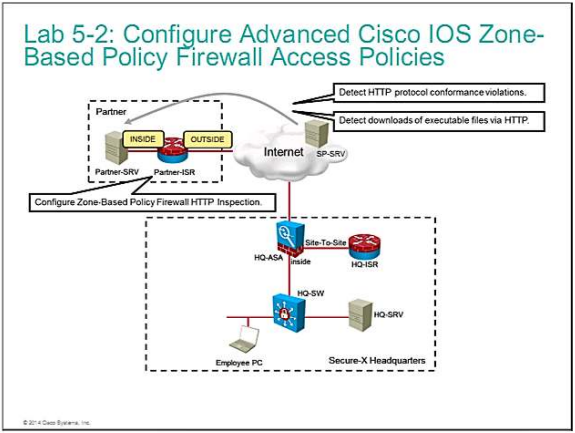
In this activity you will configure advanced Cisco IOS Zone-Based Policy Firewall access policies:

- Configure HTTP Application-Layer Inspection

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

A PC with Internet connectivity

Command List

The table describes the Cisco IOS commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco IOS Commands

Command	Description
class-map type inspect *protocol-name* {**match-any** | **match-all**} *class-map-name*	Creates a Layer 7 (application-specific) inspect-type class map
class type inspect *class-map-name*	Specifies the traffic (class) on which an action is to be performed in policy map configuration mode
log	Specifies the log action in a Layer 7 inspect-type policy map
match request arg regex *regular_expression*	Configures a match statement to match a regular expression map in the arguments field of the HTTP request
match req-resp protocol-violation	Configures a match statement to match HTTP protocol violations
parameter-map type *regex parameter-map-name*	Configures a parameter map type to match a specific traffic pattern

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command	Description
pattern *regular_expression*	Specifies the regular expression that will match data inside the parameter map configuration mode
policy-map type inspect *policy-map-name*	Creates a Layer 3 and Layer 4 inspect-type policy map
policy-map type inspect *protocol-name policy-map-name*	Creates a Layer 7 inspect-type policy map
service-policy type inspect *policy-map-name*	Attaches a firewall policy map to a zone pair in zone-pair configuration mode
show class-map type inspect http	Displays the configured class map of type inspect HTTP
show policy-map type inspect http	Displays the configured policy map of type inspect HTTP

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2.0
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

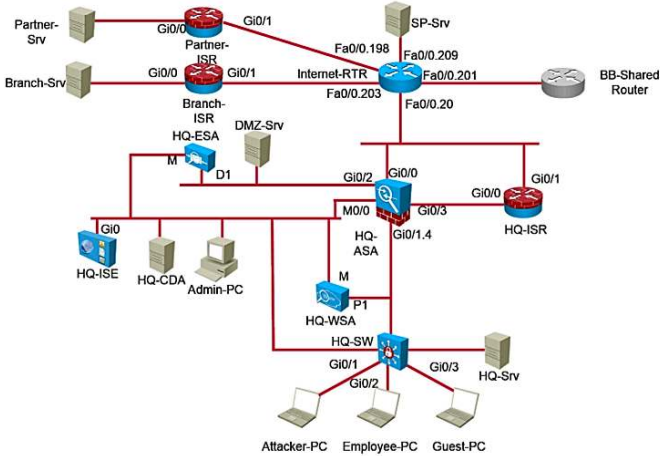
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

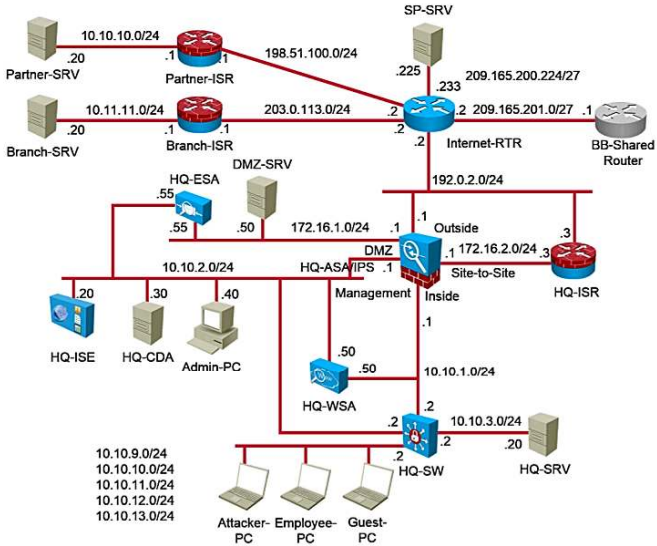
Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



https://t.me/learningnets

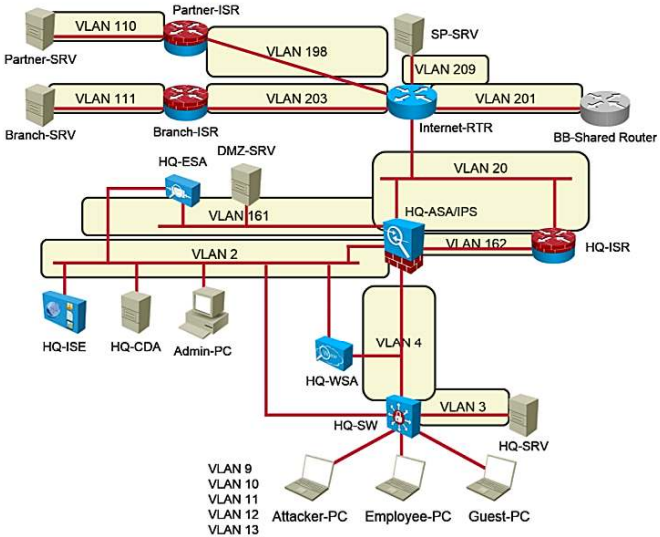
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure HTTP Application-Layer Inspection

In this task, you will configure HTTP protocol inspection. You will configure the Partner-ISR router to detect HTTP protocol conformance violations and downloads of executable files via HTTP for traffic, which goes from the OUTSIDE zone to the Partner-SRV in the INSIDE zone.

Activity Procedure

Complete the following steps:

Step 1

Access the Partner-ISR router console.

https://t.me/learningnets

Step 2

On the Partner-ISR router, first create a parameter map of type regex. Use **EXE_REGEX** as the name of the map. Then create a regular expression for argument matching. The regular expression should match any executable (*.EXE) file, regardless of the case. The regular expression should look like **.+\.[eE][xX][eE]**. The .+ part of the regex matches any string with one or more characters, \. part of the regex matches . (dot), and [eE][xX][eE] part of the regex matches exe file extension, regardless of the case.

Step 3

On the Partner-ISR router, configure a class map of type inspect HTTP. Use **BAD_HTTP_TRAFFIC** as the name of the class. The class map should match the following:

Match the previously configured **EXE_REGEX** regular expression map in the URI field of the HTTP request.

Match protocol violation in the HTTP requests or responses.

The class map should match any of the conditions.

Step 4

On the Partner-ISR router, configure a policy map of type inspect HTTP. Use **HTTP_POLICY** as the name of the policy map. Inside the policy map match the previously configured **BAD_HTTP_TRAFFIC** class map. Set the action to **log**.

Step 5

Apply the **HTTP_POLICY** policy map to the existing **OUT-TO-PARTNER-SRV-HTTP-TRAFFIC** class in the existing **OUT-TO-IN-POLICY** policy map as the service policy.

Step 6

On the Partner-ISR console, display the configured class map of type inspect HTTP.

```
Partner-ISR# show class-map type inspect http
 Class Map type inspect http match-any BAD_HTTP_TRAFFIC (id 1)
   Match  req-resp protocol-violation
   Match  request uri regex EXE_REGEX
```

Step 7

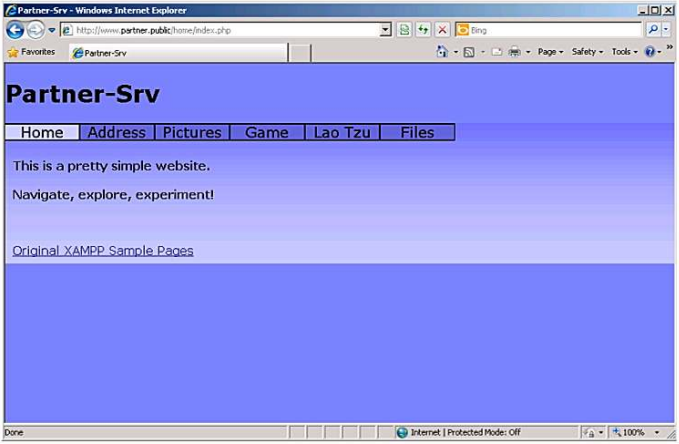
On the Partner-ISR console, display the configured policy map of type inspect HTTP.

```
Partner-ISR# show policy-map type inspect http
  Policy Map type inspect http HTTP_POLICY
    Class BAD_HTTP_TRAFFIC
      Log
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

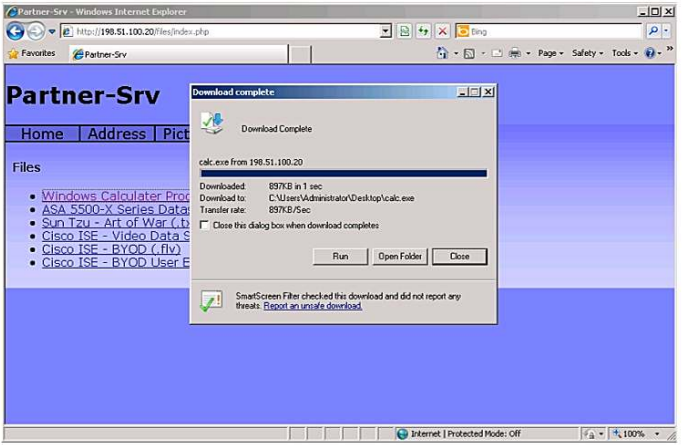
Step 8

Access the SP-SRV to test HTTP application inspection from hosts in the OUTSIDE zone to the Partner-SRV in the INSIDE zone. Open Internet Explorer and navigate to **http://www.partner.public**. You should be successful.



On the menu in the web page, navigate to the **Files** link and download the **Windows Calculator Program (.exe)**. You should be successful

https://t.me/learningnets



Step 9

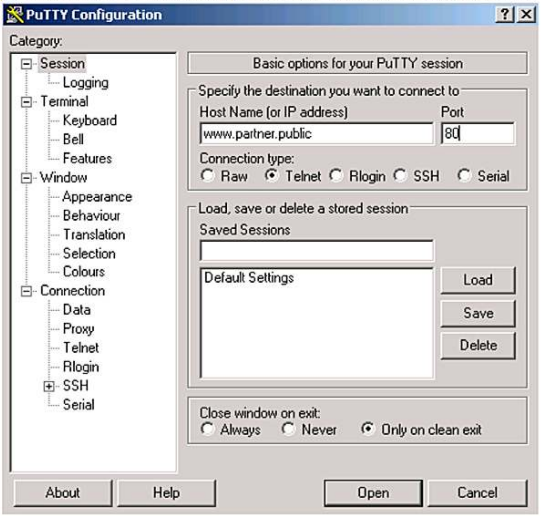
Return to the Partner-ISR console. Observe the logging message, indicating the matched regular expression in the HTTP request.

```
*Jan 27 08:51:53.458: %APPFW-4-HTTP_URI_REGEX_MATCHED: URI regex (.+\.[eE][xX][eE])
matched - session 209.165.200.233:1141 10.10.10.20:80 on zone-pair OUT-TO-IN class
OUT-TO-PARTNER-SRV-HTTP-TRAFFIC appl-class BAD_HTTP_TRAFFIC
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 10

Return to the SP-SRV and simulate an abnormal HTTP session by opening the PuTTY and starting a nonconforming HTTP session by connecting via Telnet to port 80 on the Partner-SRV (**www.partner.public**). Enter any character and press **Enter**. The session should disconnect.



Step 11

Return to the Partner-ISR console. Observe the logging message, indicating HTTP protocol violation.

```
*Jan 27 09:14:01.698: %APPFW-4-HTTP_PROTOCOL_VIOLATION: HTTP protocol violation (0)
detected - session 209.165.200.233:1144 10.10.10.20:80 on zone-pair OUT-TO-IN class
OUT-TO-PARTNER-SRV-HTTP-TRAFFIC appl-class BAD_HTTP_TRAFFIC
```

Activity Verification

No verification is needed in this task.

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab Answer Keys

Lab 2-1: Configure Control and Management Plane Security Controls

Task 1: Configure Management Plane Security Controls on Cisco IOS Software

Step 2

Enter the following command on the HQ-ISR router:

```
HQ-ISR(config)# ip domain name secure-x.local
```

Step 3

Enter the following command on the HQ-ISR router:

```
HQ-ISR(config)# crypto key generate rsa modulus 2048
```

Step 4

Enter the following command on the HQ-ISR router:

```
HQ-ISR(config)# ip ssh version 2
```

Step 5

Enter the following command on the HQ-ISR router:

https://t.me/learningnets

```
HQ-ISR(config)# username admin privilege 15 secret Ci5coAdmin
```

Step 6

Enter the following command on the HQ-ISR router:

```
HQ-ISR(config)#line vty 0 1114
HQ-ISR(config-line)#transport input ssh
HQ-ISR(config-line)#login local
```

Step 10

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)#snmp-server contact Admin
HQ-ISR(config)#snmp-server location Secure-X HQ
```

Step 11

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# snmp-server group SECURE-X v3 priv
```

Step 12

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# snmp-server user admin SECURE-X v3 auth sha Ci5coAdmin priv aes 128
Ci5coAdmin
```

Step 13

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# snmp-server host 10.10.2.40 version 3 priv admin
HQ-ISR(config)# snmp-server enable traps
```

Step 21

Enter the following commands on the HQ-ISR router:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
HQ-ISR(config)#ip access-list extended SNMP_MGMT
HQ-ISR(config-ext-nacl)#permit udp any any eq snmp
HQ-ISR(config)#ip access-list extended SSH_MGMT
HQ-ISR(config-ext-nacl)#permit tcp any any eq 22
```

Step 22

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# class-map SSH_MGMT
HQ-ISR(config-cmap)# match access-group name SSH_MGMT
HQ-ISR(config)# class-map SNMP_MGMT
HQ-ISR(config-cmap)# match access-group SNMP_MGMT
```

Step 23

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config) #policy-map CPPR
HQ-ISR(config-pmap)# class SSH_MGMT
HQ-ISR(config-pmap-c)# police rate 64000 bps burst 1500 bytes conform-action transmit
exceed-action drop violate-action drop
HQ-ISR(config-pmap)# class SNMP_MGMT
HQ-ISR(config-pmap-c)# police rate 64000 bps burst 1500 bytes conform-action transmit
exceed-action drop violate-action drop
HQ-ISR(config-pmap)# class class-default
HQ-ISR(config-pmap-c)# police rate 128000 bps burst 1500 bytes conform-action
transmit exceed-action drop violate-action drop
```

Step 24

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)#control-plane host
HQ-ISR(config-cp-host)#service-policy input CPPR
```

Task 2: Configure Management Plane Security Controls on Cisco ASA

Step 2

Enter the following commands on the HQ-ASA:

```
HQ-ASA(config)# http server enable
HQ-ASA(config)# http 10.10.2.40 255.255.255.255 management
```


https://t.me/learningnets

Task 3: Configure Management Access AAA on Cisco IOS Software

Step 2

Enter the following command on the HQ-ISR router:

```
HQ-ISR(config)# aaa new-model
```

Step 3

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# radius server MY-RADIUS
HQ-ISR(config-radius-server)# address ipv4 10.10.2.20 auth-port 1645 acct-port 1646
HQ-ISR(config-radius-server)# key cisco
```

Step 4

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# aaa authentication login MGMT_ACCESS group radius local
```

Step 5

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# aaa authorization exec MGMT_ACCESS group radius local
```

Step 6

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# aaa accounting exec MGMT_ACCESS start-stop group radius
```

Step 7

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# line vty 0 1114
HQ-ISR(config-line)# login authentication MGMT_ACCESS
HQ-ISR(config-line)# authorization exec MGMT_ACCESS
HQ-ISR(config-line)# accounting exec MGMT_ACCESS
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lab 2-2: Configure Traffic Telemetry Methods

Task 1: Configure Traffic Telemetry Methods on Cisco IOS Software

Step 2

Enter the following command on the HQ-ISR router:

```
HQ-ISR(config)# clock timezone PT -8 0
```

Step 3

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# ntp authentication-key 1 md5 Ci5coAdmin
HQ-ISR(config)# ntp authenticate
HQ-ISR(config)# ntp trusted-key 1
HQ-ISR(config)# ntp server 192.0.2.2 key 1
```

Step 6

Enter the following command on the HQ-ISR router:

```
HQ-ISR(config)# logging on
```

Step 7

Enter the following command on the HQ-ISR router:

```
HQ-ISR(config)# logging buffered debugging
HQ-ISR(config)# logging trap debugging
HQ-ISR(config)# logging host 10.10.2.40
```

Step 12

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# flow exporter MY_EXPORTER
HQ-ISR(config-flow-exporter)# destination 10.10.2.40
HQ-ISR(config-flow-exporter)# transport udp 9996
HQ-ISR(config-flow-exporter)# export-protocol netflow-v9
```


https://t.me/learningnets

Step 13

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# flow monitor MY_MONITOR
HQ-ISR(config-flow-monitor)# exporter MY_EXPORTER
HQ-ISR(config-flow-monitor)# record netflow ipv4 original-output
```

Step 14

Enter the following commands on the HQ-ISR router:

```
HQ-ISR(config)# interface GigabitEthernet0/0
HQ-ISR(config-if)# ip flow monitor MY_MONITOR output
```

Lab 2-3: Configure Layer 2 Data Plane Security Controls

Task 1: Configure DHCP Snooping

Step 16

Enter the following command on the HQ-SW switch:

```
HQ-SW(config)# ip dhcp snooping
```

Step 17

Enter the following command on the HQ-SW switch:

```
HQ-SW(config)# ip dhcp snooping database flash:/dhcp-snooping.db
```

Step 18

Enter the following commands on the HQ-SW switch:

```
HQ-SW(config)# interface GigabitEthernet0/4
HQ-SW(config-if)# ip dhcp snooping trust
```

Step 19

Enter the following command on the HQ-SW switch:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
HQ-SW(config)# ip dhcp snooping vlan 9
```

Step 20

Enter the following commands on the HQ-SW switch:

```
HQ-SW(config)# interface range GigabitEthernet 0/1 - 3
HQ-SW(config-if-range)# ip dhcp snooping limit rate 10
HQ-SW(config-if-range)# switchport port-security
HQ-SW(config-if-range)# switchport port-security maximum 2
```

Step 28

Enter the following command on the HQ-SW switch:

```
HQ-SW(config)# interface GigabitEthernet0/3
HQ-SW(config-if)# shutdown
HQ-SW(config-if)# no shutdown
```

Task 2: Configure ARP Inspection

Step 10

Enter the following command on the HQ-SW switch:

```
HQ-SW(config)# ip arp inspection vlan 9
```

Lab 2-4: Configure Layer 3 Data Plane Security Controls

Task 1: Configure uRPF on the Cisco IOS Router

Step 4

Enter the following command on the Branch-ISR router:

```
Branch-ISR(config)# interface GigabitEthernet0/0
Branch-ISR(config-if)# ip verify unicast source reachable-via rx
!
Branch-ISR(config)# interface GigabitEthernet0/1
Branch-ISR(config-if)# ip verify unicast source reachable-via rx allow-default
```


https://t.me/learningnets

Task 3: Configure IP Source Guard on the Cisco IOS Catalyst Switch

Step 4

Enter the following commands on the HQ-SW switch:

```
HQ-SW(config)# interface range GigabitEthernet0/1 - 3
HQ-SW(config-if-range)# ip verify source
```

Step 7

Enter the following commands on the HQ-SW switch:

```
HQ-SW(config)# interface range GigabitEthernet0/1 - 3
HQ-SW(config-if-range)# ip verify source port-security
```

Lab 3-1: Configure Cisco ASA NAT

Task 1: Configure Static NAT

Step 1

There are no solutions for this lab.

Lab 3-2: Configure Cisco IOS Software NAT

Task 1: Configure Static NAT

Step 2

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# interface GigabitEthernet0/1
Partner-ISR(config-if)# ip nat outside
```

Step 3

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# interface GigabitEthernet0/0
Partner-ISR(config-if)# ip nat inside
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 4

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# ip nat inside source static 10.10.10.20 198.51.100.20
```

Task 2: Configure Dynamic NAT

Step 2

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# ip access-list standard NAT
Partner-ISR(config-std-nacl)# permit 10.10.10.0 0.0.0.255
```

Step 3

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# ip nat pool POOL 198.51.100.100 198.51.100.100 netmask
255.255.255.0
```

Step 4

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# ip nat inside source list NAT pool POOL overload
```

Lab 4-1: Configure Basic Cisco ASA Access Policies

Task 1: Configure Object Groups

Step 1

There are no solutions for this lab.

https://t.me/learningnets

Lab 4-2: Configure Advanced Cisco ASA Access Policies

Task 1: Tune OSI Layer 3-4 Stateful Inspection

Step 3

Observe enabled inspectors and populate the following table:

Protocol	Enabled
CTIQBE	No
Cloud Web Security	No
DCERPC	No
DNS	Yes
ESMTP	Yes
FTP	Yes
H.323 H.225	Yes
H.323 RAS	Yes
HTTP	No
ICMP	No
ICMP Error	No
ILS	No
IM	No
IP-Options	Yes
IPsec Pass-Thru	No
IPv6	No
MMP	No
MGCP	No
NETBIOS	Yes
PPTP	No
RSH	Yes
RTSP	Yes
SCCP (Skinny)	Yes
SIP	Yes
SNMP	No

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Protocol	Enabled
SQLNET	Yes
SUNRPC	Yes
TFTP	Yes
WAAS	No
XDMCP	Yes

Lab 4-3: Configure Cisco ASA Botnet Traffic Filter

Task 1: Configure the Botnet Traffic Filter using Dynamic Database

Step 1

There are no solutions for this lab.

Lab 4-4: Configure Cisco ASA Identity Firewall

Task 1: Configure Cisco CDA

Step 1

There are no solutions for this lab.

Lab 5-1: Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies

Task 1: Configure Security Zones

Step 2

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# zone security INSIDE
Partner-ISR(config)# zone security OUTSIDE
Partner-ISR(config)# zone security VPN
```

Step 3

Enter these commands on Partner-ISR:

https://t.me/learningnets

```
Partner-ISR(config)# interface GigabitEthernet0/1
Partner-ISR(config-if)# zone-member security OUTSIDE
Partner-ISR(config-if)# interface GigabitEthernet0/0
Partner-ISR(config-if)# zone-member security INSIDE
Partner-ISR(config)# interface Tunnel 0
Partner-ISR(config-if)# zone-member security VPN
```

Step 4

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# zone-pair security IN-TO-OUT source INSIDE destination OUTSIDE
Partner-ISR(config)# zone-pair security OUT-TO-IN source OUTSIDE destination INSIDE
Partner-ISR(config)# zone-pair security VPN-TO-IN source VPN destination INSIDE
```

Task 2: Configure Access Control Between the INSIDE and OUTSIDE Zones

Step 1

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# ip access-list extended IN-TO-OUT-ACL
Partner-ISR(config-ext-nacl)# permit ip any any
!
Partner-ISR(config-cmap)# class-map type inspect IN-TO-OUT-TRAFFIC
Partner-ISR(config-cmap)# match access-group name IN-TO-OUT-ACL
!
Partner-ISR(config)# policy-map type inspect IN-TO-OUT-POLICY
Partner-ISR(config-pmap)# class IN-TO-OUT-TRAFFIC
Partner-ISR(config-pmap-c)# inspect
!
Partner-ISR(config)# zone-pair security IN-TO-OUT source INSIDE destination OUTSIDE
Partner-ISR(config-sec-zone-pair)# service-policy type inspect IN-TO-OUT-POLICY
```

Step 2

Enter these commands on Partner-ISR:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
Partner-ISR(config)# ip access-list extended OUT-TO-PARTNER-SRV-ACL
Partner-ISR(config-ext-nacl)# permit ip any host 10.10.10.20
!
Partner-ISR(config)# class-map type inspect match-all OUT-TO-PARTNER-SRV-HTTP-
TRAFFIC
Partner-ISR(config-cmap)# match protocol http
Partner-ISR(config-cmap)# match access-group name OUT-TO-PARTNER-SRV-ACL
!
Partner-ISR(config)# class-map type inspect match-all OUT-TO-PARTNER-SRV-FTP-
TRAFFIC
Partner-ISR(config-cmap)# match protocol ftp
Partner-ISR(config-cmap)# match access-group name OUT-TO-PARTNER-SRV-ACL
!
Partner-ISR(config)# class-map type inspect match-all OUT-TO-PARTNER-SRV-DNS-
TRAFFIC
Partner-ISR(config-cmap)# match protocol dns
Partner-ISR(config-cmap)# match access-group name OUT-TO-PARTNER-SRV-ACL
!
Partner-ISR(config)# policy-map type inspect OUT-TO-IN-POLICY
Partner-ISR(config-pmap)# class OUT-TO-PARTNER-SRV-HTTP-TRAFFIC
Partner-ISR(config-pmap-c)# inspect
Partner-ISR(config-pmap)# class OUT-TO-PARTNER-SRV-FTP-TRAFFIC
Partner-ISR(config-pmap-c)# inspect
Partner-ISR(config-pmap)# class OUT-TO-PARTNER-SRV-DNS-TRAFFIC
Partner-ISR(config-pmap-c)# inspect
Partner-ISR(config-pmap)# class class-default
Partner-ISR(config-pmap-c)# drop log
!
Partner-ISR(config-pmap)# zone-pair security OUT-TO-IN source OUTSIDE destination
INSIDE
Partner-ISR(config-sec-zone-pair)# service-policy type inspect OUT-TO-IN-POLICY
```

Task 3: Configure Access Control Between the VPN and INSIDE Zones

Step 1

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# ip access-list extended VPN-TO-IN-ACL
Partner-ISR(config-ext-nacl)# permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
!
Partner-ISR(config)# class-map type inspect match-all VPN-TO-IN-TRAFFIC
Partner-ISR(config-cmap)# match protocol http
Partner-ISR(config-cmap)# match access-group name VPN-TO-IN-ACL
!
Partner-ISR(config)# policy-map type inspect VPN-TO-IN-POLICY
Partner-ISR(config-pmap)# class VPN-TO-IN-TRAFFIC
Partner-ISR(config-pmap-c)# inspect
!
Partner-ISR(config)# zone-pair security VPN-TO-IN source VPN destination INSIDE
Partner-ISR(config-sec-zone-pair)# service-policy type inspect VPN-TO-IN-POLICY
```


https://t.me/learningnets

Task 4: Configure Access Control for Management Traffic Between the SELF and OUTSIDE Zones

Step 1

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# ip access-list extended IN-TO-SELF-ACL
Partner-ISR(config-ext-nacl)# permit icmp host 10.10.10.20 any
Partner-ISR(config-ext-nacl)# permit tcp host 10.10.10.20 any eq 22
!
Partner-ISR(config)# class-map type inspect match-all IN-TO-SELF-TRAFFIC
Partner-ISR(config-cmap)# match access-group name IN-TO-SELF-ACL
!
Partner-ISR(config)# policy-map type inspect IN-TO-SELF-POLICY
Partner-ISR(config-pmap)# class type inspect IN-TO-SELF-TRAFFIC
Partner-ISR(config-pmap-c)# inspect
Partner-ISR(config-pmap)# class class-default
Partner-ISR(config-pmap-c)# drop log
!
Partner-ISR(config)# zone-pair security IN-TO-SELF source INSIDE destination self
Partner-ISR(config-sec-zone-pair)# service-policy type inspect IN-TO-SELF-POLICY
```

Lab 5-2: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies

Task 1: Configure HTTP Application-Layer Inspection

Step 2

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# parameter-map type regex EXE_REGEX
Partner-ISR(config-profile)# pattern .+\.[eE][xX][eE]
```

Step 3

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# class-map type inspect http match-any BAD_HTTP_TRAFFIC
Partner-ISR(config-cmap)# match request uri regex EXE_REGEX
Partner-ISR(config-cmap)# match req-resp protocol-violation
```

Step 4

Enter these commands on Partner-ISR:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
Partner-ISR(config)# policy-map type inspect http HTTP_POLICY
Partner-ISR(config-pmap)# class type inspect http BAD_HTTP_TRAFFIC
Partner-ISR(config-pmap-c)# log
```

Step 5

Enter these commands on Partner-ISR:

```
Partner-ISR(config)# policy-map type inspect OUT-TO-IN-POLICY
Partner-ISR(config-pmap)# class type inspect OUT-TO-PARTNER-SRV-HTTP-TRAFFIC
Partner-ISR(config-pmap-c)# service-policy http HTTP_POLICY
```


https://t.me/learningnets