SITCS

Implementing Cisco Threat Control Solutions

Version 1.0 **Lab Guide**

Part Number: 97-3339-01

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, In

https://t.me/learningnets

Table of Contents

Lab 1-1: Explore the Cisco ASA (CX) NGFW and PRSM ***L-5***

Visual Objective L-6
Required Resources L-6
Command List L-6
Job Aids L-7
Task 1: Verify the ASA (CX) NGFW Software Module Status L-11
Task 2: Shut Down and Uninstall the IPS Software Module (Perform only if CX is not Installed) L-13
Task 3: Install and Set Up the ASA (CX) NGFW Software Module (Perform only if CX is not Installed) L-14
Task 4: Explore the ASA (CX) NGFW CLI L-25
Task 5: Explore the On-Box PRSM GUI L-30
Task 6: Redirect Traffic from the ASA to ASA (CX) NGFW L-39
Task 7: Explore the System Predefined Default ASA (CX) NGFW Policy Objects L-42
Task 8: Configure ASA (CX) NGFW Policy Objects L-44

Lab 1-2: Configure Cisco ASA (CX) NGFW Access Policy ***L-47***

Visual Objective L-48
Required Resources L-48
Command List L-48
Job Aids L-48
Task 1: Configure the ASA CX Access Policy to Deny Access to Unacceptable Websites L-52
Task 2: Configure the ASA CX Access Policy to Deny Any Executable File Download L-57
Task 3: Configure an ASA CX Access Policy to Deny Access to Any Websites with a Bad Reputation L-63
Task 4: Optional Challenge Lab Task: Configure ASA CX Access Policies L-67

Lab 1-3: Configure Cisco ASA (CX) NGFW Identity Policy ***L-73***

Visual Objective L-74
Required Resources L-74
Command List L-74
Job Aids L-74
Task 1: Configure an ASA CX Identity Policy Using Active Authentication L-78
Task 2: Configure an ASA CX Identity Policy Using Passive Authentication L-95
Task 3: Configure an ASA CX Access Policy Using an Identity Object per the Given Requirements L-101

Lab 1-4: Configure Cisco ASA (CX) NGFW Decryption Policy ***L-107***

Visual Objective L-108
Required Resources L-108
Command List L-108
Job Aids L-108
Task 1: Enable Cisco ASA (CX) NGFW Decryption L-112

https://t.me/learningnets

Task 2: Configure a Cisco ASA (CX) NGFW Decryption Policy per Security Requirements L-113

Lab 2-1: Configure Cisco Web Security Appliance Explicit Proxy and User Authentication L-123

Visual Objective L-124
Required Resources L-124
Job Aids L-124
Task 1: Verify Basic Cisco WSA Settings L-128
Task 2: Implement the Cisco WSA in Explicit Proxy Mode L-135
Task 3: Implement User Authentication with Active Directory using Basic Authentication L-137
Task 4: Implement User Authentication using Transparent User Identification L-146

Lab 2-2: Configure Cisco Web Security Appliance Acceptable Use Controls L-153

Visual Objective L-154
Required Resources L-154
Job Aids L-154
Task 1: Implement the Cisco WSA in Transparent Proxy Mode L-158
Task 2: Configure the Access Policy L-164
Task 3: Configure URL Filtering for the Access Policy L-166
Task 4: Configure Application Visibility Control for the Access Policy L-176

Lab 3-1: Configure Cisco Cloud Web Security Connector on ISR G2 and on AnyConnect L-181

Visual Objective L-182
Required Resources L-182
Command List L-182
Job Aids L-183
Task 1: Enable the CWS Connector on the Partner ISR G2 Router L-187
Task 2: Enable the CWS Connector on the AnyConnect Secure Mobility Client L-194

Lab 4-1: Configure Cisco Email Security Appliance Basic Policies L-207

Visual Objective L-209
Required Resources L-209
Job Aids L-209
Task 1: Verify the Initial Email Exchange Without the Cisco ESA L-213
Task 2: Deploy the Cisco ESA Mail Proxy L-215
Task 3: Integrate the Cisco ESA with LDAP and Enable LDAP Accept Query L-233
Task 4: Configure Incoming Content Filters and Mail Policies L-242
Task 5: Configure Outbound Data Loss Prevention L-249

Lab 5-1: Configure Cisco ASA IPS Software Module L-267

Visual Objective L-268
Required Resources L-268
Command List L-268
Job Aids L-268

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

Task 1: Install the Cisco ASA IPS Software Module and Configure the Basic IPS Settings L-272
Task 2: Verify the IPS Operations L-279
Task 3: Tune Existing Signature L-285
Task 4: Create Custom Signature L-292

Lab Answer Keys ***L-299***

Lab 1-1: Explore the Cisco ASA (CX) NGFW and PRSM L-299
Lab 1-2: Configure Cisco ASA (CX) NGFW Access Policy L-303
Lab 1-3: Configure Cisco ASA (CX) NGFW Identity Policy L-304
Lab 1-4: Configure Cisco ASA (CX) NGFW Decryption Policy L-304
Lab 2-1: Configure Cisco Web Security Appliance Explicit Proxy and User Authentication L-305
Lab 2-2: Configure Cisco Web Security Appliance Acceptable Use Controls L-305
Lab 3-1: Configure Cisco Cloud Web Security Connector on ISR G2 and on AnyConnect L-305
Lab 4-1: Configure Cisco Email Security Appliance Basic Policies L-306
Lab 5-1: Configure Cisco ASA IPS Software Module L-306

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

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

Lab 1-1: Explore the Cisco ASA (CX) NGFW and PRSM

Activity Objective

To address the highly dynamic Web 2.0 applications and the bring-your-own-devices phenomenon in the workplace, and to pro-actively protect against new and emerging Web 2.0 threats, the CSO decides to implement the Cisco Adaptive Security Appliances Next Generation Firewall to address these needs by adding next-generation context aware capabilities including Broad Application Visibility and Control and Web Security to the existing Cisco ASA 5500-X. You will start testing the Cisco ASA NGFW on the Secure-X test lab by exploring the ASA NFGW CLI and Cisco Prime Security Manager GUI then later on, you will also implement a few access, identity and decryption test policies.

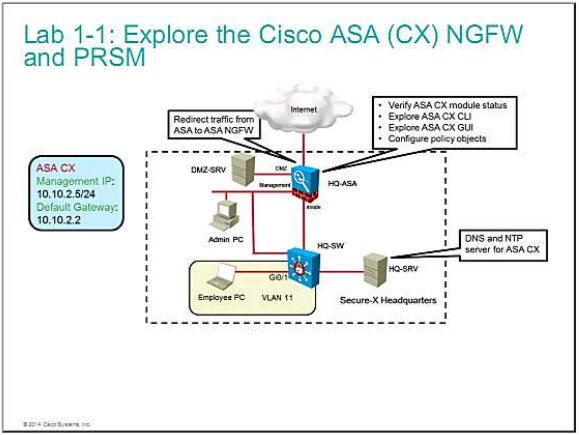
Upon completing this activity, you will be able to meet these objectives:

- Verify the Cisco ASA (CX) NGFW status
- Explore the Cisco ASA (CX) NGFW CLI
- Explore the on-box PRSM GUI
- Examine the default (implicit) Cisco ASA (CX) NGFW policies
- Redirect traffic from the Cisco ASA to the Cisco ASA (CX) NGFW
- Examine some of the system predefined default Cisco ASA (CX) NGFW policy objects
- Configure Cisco ASA (CX) NGFW policy objects
- Test basic Cisco ASA (CX) NGFW functionality

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. Refer to this list if you need configuration command assistance during the lab activity.

Commands

Command	Description
show module cxsc details	Displays the Cisco ASA (CX) NGFW module status
session cxsc console	Starts a session into the Cisco ASA (CX) NGFW console from the Cisco ASA CLI
?	Seeks help information from the CLI
config ?	Displays the CLI configuration options (NTP, time, time zone, and so on)
show ?	Seeks help information on the available CLI **show** commands
show services status	Displays the status of processes
ping	Performs a ping test from the CLI

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

Command	Description
system ?	Displays the Cisco ASA (CX) NGFW **system** command options (upgrade and install)
show interfaces	Displays the interface status
show routes	Displays the configured routes
nslookup domain-name	Tests the DNS operations
show time	Displays the current time and time zone
policy-map asacx_policy	Configures a policy map
class class-default	References the default class within the policy map
cxsc fail-close auth-proxy	Enables traffic to be redirected to the Cisco ASA (CX) NGFW and enables fail-closed and authentication proxy (for active authentication)
service-policy asacx_policy interface inside	Applies the policy map to an interface

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 asacx-5500x-boot-9.1.2-42.img asacx-sys-9.1.2-42.pkg
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
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**
ASA CX	**admin**	**Admin123**
AD Server (installed on HQ-SRV)	**Administrator**	**Ci5coAdmin**
ScanSafe portal (https://scancenter.scansafe.com)	**ccnpsec.scansafe@yahoo.com**	**C!sco!23**

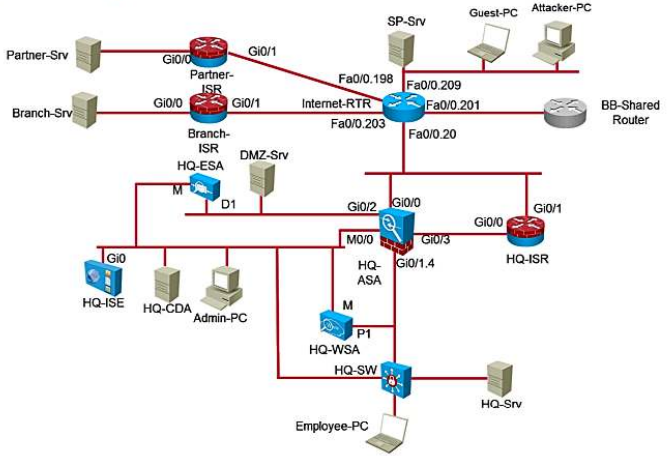
Employee PC is joined to the Active Directory domain.

AD User	AD password	AD Group	Email address in AD properties
it1	**cisco**	IT	**it1@secure-x.public**

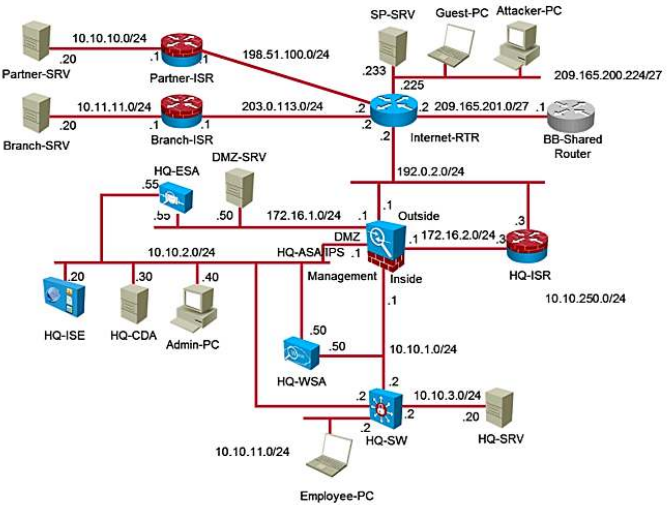
https://t.me/learningnets

Topology and IP Addressing

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



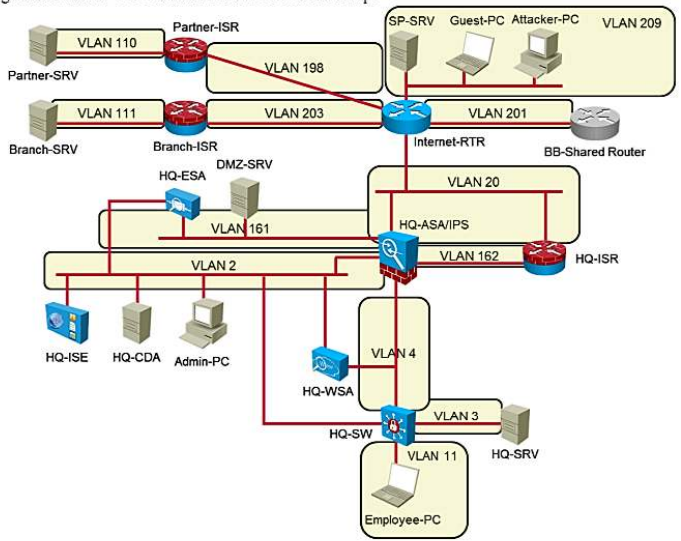
The figure shows the IP addresses that are used in this lab setup.



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

VLAN Setup

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



Task 1: Verify the ASA (CX) NGFW Software Module Status

In this task, you will verify if the ASA (CX) NGFW software module has already been installed on your assigned HQ-ASA.

Activity Procedure

Complete the following step:

Step 1

Connect to the HQ-ASA CLI and examine the module status using **show module** command.

```
HQ-ASA# show module
Mod  Card Type                                    Model              Serial No.
---- -------------------------------------------- ------------------ -----------
   0 ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC ASA5515            FCH1709J7WQ
 ips Unknown                                      N/A                FCH1709J7WQ
cxsc ASA CX5515 Security Appliance                ASA CX5515         FCH1709J7WQ
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 4c4e.35ea.8d5c to 4c4e.35ea.8d63  1.0          2.1(9)8      9.1(1)4
 ips 4c4e.35ea.8d5a to 4c4e.35ea.8d5a  N/A          N/A
cxsc 4c4e.35ea.8d5a to 4c4e.35ea.8d5a  N/A          N/A          9.1.2
Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- ------------------------
 ips Unknown                        No Image Present Not Applicable
cxsc ASA CX                         Up               9.1.2
Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
 ips Unresponsive       Not Applicable
cxsc Up                 Up
Mod  License Name   License Status  Time Remaining
---- -------------- --------------- ---------------
 ips IPS Module     Enabled         259 days
HQ-ASA#
```

The ASA (CX) NGFW module should be in the up state and running the 9.1.2 software version.

If you see the IPS module is up instead of the ASA (CX) NGFW module, continue to the tasks 2 and 3 to shut down and uninstall the IPS module then install and setup the ASA (CX) NGFW module. The ASA (CX) NGFW module installation and setup process will take about 30 minutes to complete.

If you see ASA CX module installed, you can skip lab tasks 2 and 3.

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

Step 2

Connect to the ASA (CX) NGFW console CLI if the ASA (CX) NGFW module is in the up state.

Log in to the ASA (CX) NGFW console CLI using **admin** as the username and **Admin123** as the password. Use the **show versio**n ASA (CX) NGFW CLI command to verify the software version is 9.1.2 (42).

```
HQ-ASA# session cxsc console
Opening console session with module cxsc.
Connected to module cxsc. Escape character sequence is 'CTRL-^X'.
Cisco ASA CX 9.1.2
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
You can access the Web UI from your browser using the following URL(s):
https://10.10.2.5/
https://[fe80::4e4e:35ff:feea:8d5a]/
asacx login: admin
Password: Admin123
            Cisco Prime Security Manager 9.1.2 (42) for asacx firewall
                Type ? for list of commands
asacx> show version
Cisco ASA CX Platform 9.1.2 (42)
Cisco Prime Security Manager 9.1.2 (42) for asacx firewall
asacx>
```

To return to the ASA CLI from the ASA (CX) NGFW CLI, press **Ctrl-Shift-6** two times and press **x** to disable the session to the ASA (CX) NGFW module. You should get access back to the ASA CLI.

When connected to the Cisco ASA CLI through the term server, enter **Control-Shift-6** once and then **x** will return to the term server console.

Task 2: Shut Down and Uninstall the IPS Software Module (Perform only if CX is not Installed)

In this lab task, you will shut down and uninstall the IPS module.

Activity Procedure

Complete these steps:

https://t.me/learningnets

Step 1

From the ASA CLI, use the **sw-module module ips shutdown** command to shut down the IPS module. The IPS module takes about 1 minute to go from the **Shutting Down** state to the **Down** state.

```
HQ-ASA# sw-module module ips shutdown
Shutdown module ips? [confirm]
Shutdown issued for module ips.
```

You can use the **show module ips** command (not shown) to verify that the Cisco IPS module has been shut down.

Step 2

Use the ASA CLI to uninstall the IPS module after the IPS module is shut down. Use the **sw-module module ips uninstall** command.

```
HQ-ASA# sw-module module ips uninstall
Module ips will be uninstalled. This will completely remove the disk image associated
with the sw-module including any configuration that existed within it.
Uninstall module ips? [confirm]
Uninstall issued for module ips.
```

Step 3

Reload the ASA using **reload** command after the IPS module has been uninstalled.

Task 3: Install and Set Up the ASA (CX) NGFW Software Module (Perform only if CX is not Installed)

In this lab task, you will install and set up the Cisco ASA (CX) NGFW software module.

Activity Procedure

Complete these steps:

Step 1

Configure the ASA (CX) NGFW boot image location as shown below (the filename is case-sensitive).

```
HQ-ASA# sw-module module cxsc recover configure image disk1:/asacx-5500x-
boot-9.1.2-42.img
```


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

Step 2

Boot the ASA (CX) NGFW boot image using **sw-module module cxsc recover boot** command. Confirm the prompt to recover the CXSC module. The ASA (CX) NGFW boot image will take about 10 minutes to load after you confirm the prompt

```
HQ-ASA# sw-module module cxsc recover boot
Module cxsc will be recovered. This may erase all configuration and all data
on that device and attempt to download/install a new image for it. This may take
several minutes.
Recover module cxsc? [confirm]
Recover issued for module cxsc.
```

Use the **show module cxsc** command from the ASA CLI to check the status. The status should be **Recover**, and the status will stay at the **Recover** state even after the ASA (CX) NGFW boot image has been successfully loaded.

The **show module cxsc log console** command can be used to check the ASA (CX) NGFW logs.

Wait for about 10 minutes then continue to the next step to log into the ASA (CX) NGFW console. Once you can console into the ASA (CX) NGFW, it means the ASA (CX) NGFW boot image has been successfully loaded.

Step 3

From the ASA CLI, establish a session into the ASA (CX) NGFW console. Log in to the ASA (CX) NGFW console using the default **admin** username with the default **Admin123** password.

```
HQ-ASA# session cxsc console
Opening console session with module cxsc.
Connected to module cxsc. Escape character sequence is 'CTRL-^X'.
Cisco ASA CX Boot Image 9.1.2
asacx login:admin
Password: Admin123
          Cisco ASA CX Boot 9.1.2 (42)
          Type ? for list of commands
asacx-boot>
```

Step 4

Use the **partition** command to partition the ASA SSD from the ASA (CX) NGFW CLI. Enter "**y**" when prompted **Are you sure you want to proceed?** This partition will take several minutes to complete.

NOTE: you must perform the step to partition the SSD. Otherwise when you try to install the ASA (CX) NGFW image package file in a later step the installation will fail and your ASA (CX) NGFW CLI will lock up. You will then have to reboot the ASA and reload the ASA (CX) NGFW boot image to start again.

```
asacx-boot> partition
Disk /dev/sda doesn't contain a valid partition table
Disk /dev/vda doesn't contain a valid partition table
  WARNING: You are about to erase all policy configurations and data.
  You cannot undo this action.
Are you sure you want to proceed? [y/n]:y
sfdisk: ERROR: sector 0 does not have an msdos signature
 /dev/sda: unrecognized partition table type
No partitions found
sfdisk: ERROR: sector 0 does not have an msdos signature
 /dev/vda: unrecognized partition table type
No partitions found
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  Volume group "vg" not found
  Skipping volume group vg
  No volume groups found
  Volume group "vg" not found
Disk /dev/sda doesn't contain a valid partition table
Disk /dev/vda doesn't contain a valid partition table
ROOTFS_SIZE >>>  120*1024*1024*1024/100
1288490188
        EUSB_BOOT_SIZE:  610469
      EUSB_ROOTFS_SIZE:  2506140
EUSB_ROOTFS_SECOND_SIZE:  2506140
Disk /dev/sda: 391 cylinders, 255 heads, 63 sectors/track
```


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

```
sfdisk: ERROR: sector 0 does not have an msdos signature
 /dev/sda: unrecognized partition table type
Old situation:
No partitions found
New situation:
Units = sectors of 512 bytes, counting from 0
   Device Boot    Start       End   #sectors  Id  System
/dev/sda1   *          1    610469     610469  83  Linux
/dev/sda2        610470   3116609    2506140  83  Linux
/dev/sda3       3116610   5622749    2506140  83  Linux
/dev/sda4       5622750   6281414     658665  83  Linux
Successfully wrote the new partition table
<output omitted>
asacx-boot>
```

Step 5

Set up the ASA (CX) NGFW for basic network connectivity. Use the **setup** command to run the setup dialog to configure the basic network settings as follows:

```
asacx-boot> setup
               Welcome to Cisco Prime Security Manager Setup
                         [hit Ctrl-C to abort]
                      Default values are inside []
Enter a hostname [asacx]: <Enter>
asacx
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n)
[N]: N
Enter an IPv4 address [192.168.8.8]: 10.10.2.5
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 10.10.2.2
Do you want to configure static IPv6 address on management interface?(y/n) [N]: N
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address: 10.10.3.20
Do you want to configure Secondary DNS Server?(y/n) [N]: N
Do you want to configure Local Domain Name?(y/n) [N]: N
Do you want to configure Search domains?(y/n) [N]: N
Do you want to enable the NTP service? [Y]: Y
Enter the NTP servers separated by commas: 10.10.3.20
Please review the final configuration:
Hostname:                   asacx
Management Interface Configuration
IPv4 Configuration:         static
        IP Address:         10.10.2.5
        Netmask:            255.255.255.0
        Gateway:            10.10.2.2
IPv6 Configuration:         Stateless autoconfiguration
DNS Configuration:
        DNS Server:
                            10.10.3.20
NTP configuration:
        10.10.3.20
CAUTION:
You have selected IPv6 stateless autoconfiguration, which assigns a global address
based on network prefix and a device identifier. Although this address is unlikely
to change, if it does change, the system will stop functioning correctly.
We suggest you use static addressing instead.
Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Done.
Press ENTER to continue...<Enter>
asacx-boot>
```


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

Step 6

Use the ASA (CX) NGFW CLI to ping the Admin PC (**10.10.2.40**) to test connectivity. Use the key sequence Ctrl-C to stop the pings. The Admin PC is the FTP server which will be used for installing the ASA (CX) NGFW system package file.

```
asacx-boot> ping 10.10.2.40
PING 10.10.2.40 (10.10.2.40): 56 data bytes
64 bytes from 10.10.2.40: seq=0 ttl=128 time=0.858 ms
64 bytes from 10.10.2.40: seq=1 ttl=128 time=0.848 ms
<control+c>
--- 10.10.2.40 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.848/0.853/0.858 ms
asacx-boot>
```

Step 7

Install the ASA (CX) NGFW system package file from the FTP server.

Ensure the Admin-PC image has the **asacx-sys-9.1.2-42.pkg** file in the DVD Drive (D:), CX directory.

From the ASA (CX) NGFW CLI, use the **system install FTP://10.10.2.40/cdromFiles/CX/asacx-sys-9.1.2-42.pkg** command to install the ASA (CX) NGFW system package from the 10.10.2.40 FTP server. The ASA (CX) NGFW package filename is **asacx-sys-9.1.2-42.pkg**.

Wait a few minutes for the package to download and extract, then type **Y** when prompted to continue with the upgrade.

Wait several minutes for the upgrade process to finish.

When the installation is done, press **Enter** at the prompt to reboot the ASA (CX) NGFW.

When the ASA (CX) NGFW reboots, you will be automatically returned to the ASA CLI. The ASA (CX) NGFW takes about 10 minutes to reboot.

```
asacx-boot> system install FTP://10.10.2.40/asacx-sys-9.1.2-42.pkg
Verifying
Downloading .....
Extracting.......
<output omitted>
Package Detail
        Description:                 Cisco ASA-CX 9.1.2-42 System Upgrade
        Requires reboot:             Yes
NOTE: If this device is being managed by a PRSM server, you must also apply the same
upgrade package to the PRSM server or you will not be able to deploy configurations
from the PRSM server to this device.
Do you want to continue with upgrade? [y]:Y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.
Upgrading
Starting upgrade process ...
Populating new system image...
Copying over new application components.....
Cleaning up old application components.....
Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
Broadcast message from root (ttyS1) (Thu Nov 14 23:05:00 2013):
The system is going down for reboot NOW!
Remote closed console session. Escape character sequence is 'CTRL-^X'.
Console session with module cxsc terminated.
HQ-ASA#
```


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

Step 8

From the ASA CLI, establish a session back into ASA (CX) NGFW. When the ASA (CX) NGFW finishes booting, log in to ASA (CX) NGFW as **admin** using the **Admin123** password.

```
HQ-ASA# session cxsc console
Opening console session with module cxsc.
Connected to module cxsc. Escape character sequence is 'CTRL-^X'.
Cisco ASA CX 9.1.2
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
You can access the Web UI from your browser using the following URL(s):
https://192.168.1.5/
https://[fe80::206:f6ff:fee6:9340]/
asacx login:admin
Password: Admin123
            Cisco Prime Security Manager 9.1.2 (21) for asacx firewall
                  Type ? for list of commands
asacx>
```


https://t.me/learningnets

Step 9

Use the **config timezone** ASA (CX) NGFW CLI command to set the time zone. The lab in this example is in California in the United States.

```
asacx> config timezone
The current time zone is:
UTC
  1. [Africa]          2. [America]         3. [Antarctica]      4. [Arctic]
  5. [Asia]            6. [Atlantic]        7. [Australia]       8. [Brazil]
  9. [Canada]         10. [Chile]          11. [Etc]            12. [Europe]
 13. [Indian]         14. [Mexico]         15. [Mideast]        16. [Pacific]
 17. [US]             18. CET              19. CST6CDT          20. Cuba
 21. EET              22. EST              23. EST5EDT          24. Egypt
 25. Eire             26. Factory          27. GB               28. GB-Eire
 29. GMT              30. GMT+0            31. GMT-0            32. GMT0
 33. Greenwich        34. HST              35. Hongkong         36. Iceland
 37. Iran             38. Israel           39. Jamaica          40. Japan
 41. Kwajalein        42. Libya            43. MET              44. MST
 45. MST7MDT          46. NZ               47. NZ-CHAT          48. Navajo
 49. PRC              50. PST8PDT          51. Poland           52. Portugal
 53. ROC              54. ROK              55. Singapore        56. Turkey
 57. UCT              58. UTC              59. Universal        60. W-SU
 61. WET              62. Zulu
Please enter your choice [Enter 'b' to go back]: 17
  1. Alaska           2. Aleutian          3. Arizona           4. Central
  5. East-Indiana     6. Eastern           7. Hawaii            8. Indiana-Starke
  9. Michigan        10. Mountain         11. Pacific          12. Samoa
Please enter your choice [Enter 'b' to go back]: 11
You have chosen the Pacific time zone.
Changing the time zone requires a process manager restart.
Do you want to restart the process manager now? [Y]: Y
The time zone has been changed to:
PST
Restarting process manager....
```

Step 10

Use the **show time** command to show the current time. If the time is not correct, correct it using the **config time** command.

```
asacx>show time
Tue Nov 26 05:14:25 PST 2013
asacx>config time
Enter the date and time [11/14/2013 18:09:17]: 11/14/2013 23:18:30
Thu Nov 14 23:18:00 PDT 2013
23:18:30
asacx>
```


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

Step 11

Use the **show ntp** command to verify the NTP status.

```
asacx> show ntp
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 hq-srv.secure-x 64.103.34.15     2 u   13   64   17    1.033  26374.8   9.386
asacx>
```

Step 12

Verify access to the on-box PRSM.

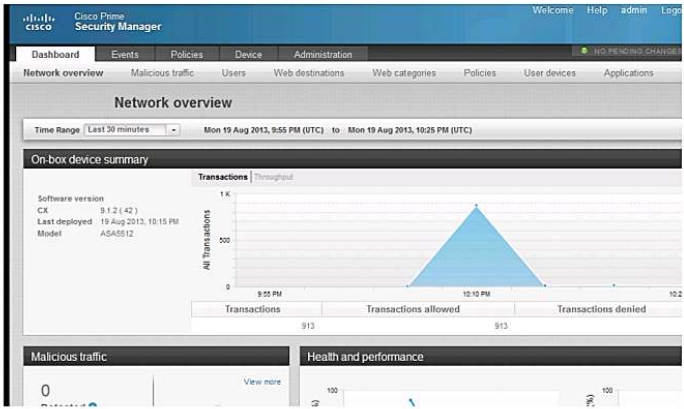
From the Admin-PC, use https to access the IP address 10.10.2.5 (the on-box PRSM GUI) and log in as **admin** using the **Admin123** password.

Accept the certificate warning.

You should see the on-box PRSM Welcome pop-up windows. Click **Skip**.

You should now be at the **PRSM Dashboard > Network Overview** page.

Verify that the CX software version is **9.1.2 (42)**.



Step 13

Install the AVC and Web Security subscription-based license on the ASA (CX) NGFW.

From the PRSM, go to **Administration > Licenses**.

Choose **I want to ... Upload license file**.

Click inside the **Drag files or click this area to upload** box.

Browse to the D: drive (DVD Drive) to locate the AVC and Web Security license file.

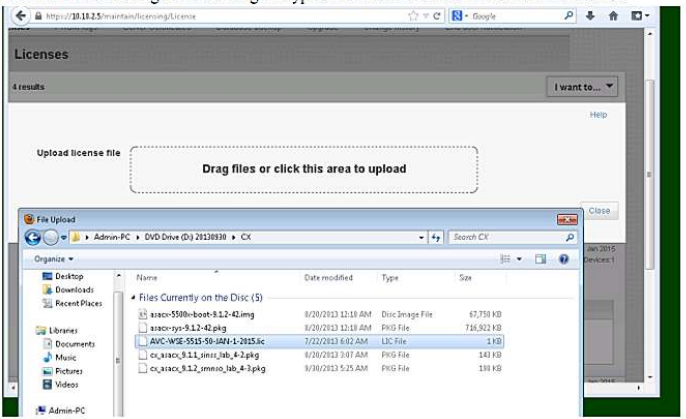
Choose the license file (for example, AVC-WSE-5515-50-JAN-1-2015.lic) and click **Open** to install the license file.

The folder location and the exact license filename may differ. If you do not see a license file, ask for help to identify the license file location and filename.

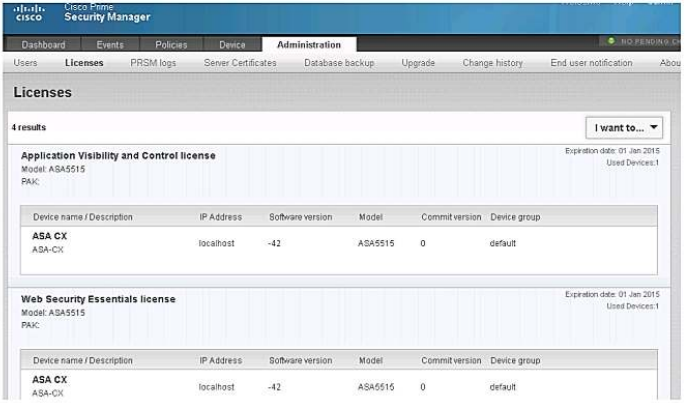
Click **Close** to return to the license list.

Verify the expiration date of the licenses.

In the lab, you may not have the K9 license available to be installed. When the ASA (CX) NGFW performs decryption, it will still work without strong encryption requirements on the destination secured Web server but it will not be able to negotiate a strong encryption method like AES without the K9 license.



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



Activity Verification

You have completed this task when you attain this result:

You have installed and setup the Cisco ASA (CX) NGFW module.

Task 4: Explore the ASA (CX) NGFW CLI

In this lab task, you will explore the Cisco ASA (CX) NGFW CLI.

Activity Procedure

Complete the following steps to explore the Cisco ASA (CX) NGFW CLI:

https://t.me/learningnets

Step 1

Display the Cisco ASA (CX) NGFW module details status from the ASA CLI using the **show module cxsc details** command from the Cisco ASA CLI.

```
HQ-ASA# show module cxsc details
Getting details from the Service Module, please wait...
Card Type:          ASA CX5515 Security Appliance
Model:              ASA CX5515
Hardware version:   N/A
Serial Number:      FCH1710J2Q7
Firmware version:   N/A
Software version:   9.1.2
MAC Address Range:  4c4e.35ea.eabe to 4c4e.35ea.eabe
App. name:          ASA CX
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       9.1.2
Data Plane Status:  Up
Status:             Up
Mgmt IP addr:       10.10.2.5
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       10.10.2.2
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

Step 2

Start a session into the Cisco ASA (CX) NGFW console using the **session cxsc console** command from the Cisco ASA CLI. If prompted for login credentials, log in to the Cisco ASA (CX) NGFW CLI using the **admin** username with the **Admin123** password.

```
HQ-ASA# session cxsc console
Opening console session with module cxsc.
Connected to module cxsc. Escape character sequence is 'CTRL-^X'.
Cisco ASA (CX) NGFW 9.1.2
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
You can access the Web UI from your browser using the following URL(s):
https://192.168.1.5/
https://[fe80::206:f6ff:fee6:969b]/
asacx login:admin
Password:Admin123
            Cisco Prime Security Manager 9.1.2 (21) for P13ASACX firewall
                 Type ? for list of commands
asacx>
```


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

Step 3

Explore the help facility in the Cisco ASA (CX) NGFW CLI. Use the **?** command to display the list of available CLI commands.

```
asacx> ?
    show            => Display system information. Enter show ? for options
    clear           => Clear system information. Enter clear ? for options
    config          => Configure the system. Enter config ? for options
    system          => Control system operation
    setup           => System Setup Wizard
    support         => Support information for TAC
    delete          => Delete files
    ping            => Ping a host to check reachability
    nslookup        => Look up an IP address or host name with the DNS servers
    traceroute      => Trace the route to a remote host
    services        => Control services on the box
    exit            => Exit the session
    help            => Get help on command syntax
```

Step 4

Verify the Cisco ASA (CX) NGFW processes status using **show services status** command. All of the processes should be up.

```
asacx> show services status
============================================================
Process           | PID   | Up    | Up Time
============================================================
AD Interface      | 2639  | True  | 20:02:37
Message Nameserver| 2379  | True  | 20:03:30
HTTP Auth Daemon  | 2451  | True  | 20:03:29
PDTS              | 2430  | True  | 20:03:30
HTTP Inspector    | 2546  | True  | 20:03:01
HTTP Server       | 3983  | True  | 17:23:10
Data Plane        | 2628  | True  | 20:02:42
Management Plane  | 2473  | True  | 20:03:14
HPM Monitor       | 2644  | True  | 20:02:36
Updater           | 2788  | True  | 20:01:40
Card Manager      | 2296  | True  | 20:03:30
ARP Daemon        | 2446  | True  | 20:03:29
Event Server      | 3972  | True  | 17:23:10
TLS Proxy         | 2551  | True  | 20:03:01
============================================================
```

Step 5

Explore the **services** command for starting and stopping the CX services. Use the **services?** command.

What are the two available options?

---

https://t.me/learningnets

Step 6

Verify the Cisco ASA (CX) NGFW interface status using the **show interfaces** command.

```
asacx> show interfaces
cplane    Link encap:Ethernet  HWaddr 00:00:00:03:00:01
          inet addr:127.0.3.1  Bcast:127.0.255.255  Mask:255.255.0.0
          inet6 addr: fe80::200:ff:fe03:1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:226050 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64652 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14473780 (13.8 MiB)  TX bytes:7893976 (7.5 MiB)
eth0      Link encap:Ethernet  HWaddr 4C:4E:35:EA:8D:5A
          inet addr:10.10.2.5  Bcast:10.10.2.255  Mask:255.255.255.0
          inet6 addr: fe80::4e4e:35ff:feea:8d5a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1078214 errors:0 dropped:0 overruns:0 frame:0
          TX packets:287613 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1544024747 (1.4 GiB)  TX bytes:31027930 (29.5 MiB)
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:84249 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84249 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5801375 (5.5 MiB)  TX bytes:5801375 (5.5 MiB)
```

Step 7

Verify the Cisco ASA (CX) NGFW configured default gateway using the **show route** command. The default gateway should be 10.10.2.2 (the HQ-SW).

```
asacx> show route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.2.0       0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.255.0.0     U     0      0        0 cplane
0.0.0.0         10.10.2.2       0.0.0.0         UG    0      0        0 eth0
Kernel IPv6 routing table
Destination                    Next Hop         Flags Metric Ref    Use Iface
::1/128                        ::               U     0      4        3 lo
fe80::200:ff:fe03:1/128        ::               U     0      0        1 lo
fe80::4e4e:35ff:feea:8d5a/128  ::               U     0      0        1 lo
fe80::/64                      ::               U     256    0        0 cplane
fe80::/64                      ::               U     256    0        0 eth0
ff00::/8                       ::               U     256    0        0 cplane
ff00::/8                       ::               U     256    0        0 eth0
```


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

Step 8

Verify the Cisco ASA (CX) NGFW DNS operations using the **nslookup www.cisco.com** command. In the lab setup, the HQ-SRV (**10.10.3.20**) is the Active Directory, DNS and NTP server in the lab.

```
asacx> nslookup www.cisco.com
Server:    10.10.3.20
Address 1: 10.10.3.20 hq-srv.secure-x.local
Name:      www.cisco.com
Address 1: 23.1.128.170 a23-1-128-170.deploy.static.akamaitechnologies.com
Address 2: 2a02:26f0:18:19f::90
Address 3: 2a02:26f0:18:19e::90
```

Step 9

Verify the current time and time zone. The time zone should be already configured to be PST.

```
asacx> show time
Thu Nov 14 14:29:31 PST 2013
```

Step 10

Verify the NTP server using the **show ntp** command. Your Cisco ASA (CX) NGFW should have been preconfigured with the HQ-SRV (**10.10.3.20**) as the NTP server.

```
asacx> show ntp
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*hq-srv.secure-x 64.103.34.15     2 u   33   64  377    0.811  105.108  11.540
```

Step 11

Use the **config** command to display the various configuration options.

```
asacx> config ?
    timezone          => Configure time zone
    passwd            => Change the admin user password
    time              => Configure date and time
    ntp               => Configure NTP servers
    mgmt-interface    => Configure mgmt-interface specific options
    reset             => Reset the database to factory defaults
    backup            => Backup of the current DB snapshot is taken
    restore           => Current DB is replaced by prev snapshot of backed up DB
    advanced          => Advanced configuration options
    cert-reset        => Overwrite the management certificate with a new self-signed
certificate
```

The **config** command is used to configure options such as the time zone, time, NTP server, and so on. It can also be used to set the admin user password. In this lab step, you will not need to use the **config** command to accomplish any required configurations. Just use the **config ?** command to view all of the available configuration options.

Step 12

Use the **system** command to view all of the options that are available to manage the ASA (CX) NGFW .

```
asacx> system ?
    reload            => Reload the system
    shutdown          => Shut down the system. Manual restart will be required
    upgrade           => Upgrade the system software
    revert            => Revert to the last version of the OS or application
```

Step 13

Return to the Cisco ASA console from the Cisco ASA (CX) NGFW console:

To return to the ASA CLI from the ASA (CX) NGFW CLI, press **Ctrl-Shift-6** two times and press **x** to disable the session to the ASA (CX) NGFW module. You should get access back to the ASA CLI.

When connected to the Cisco ASA CLI through the term server, enter **Control-Shift-6** once and then **x** will return to the term server console.

Task 5: Explore the On-Box PRSM GUI

In this lab task, you will explore the on-box PRSM GUI.

Activity Procedure

Complete the following steps to explore the on-box PRSM GUI:

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

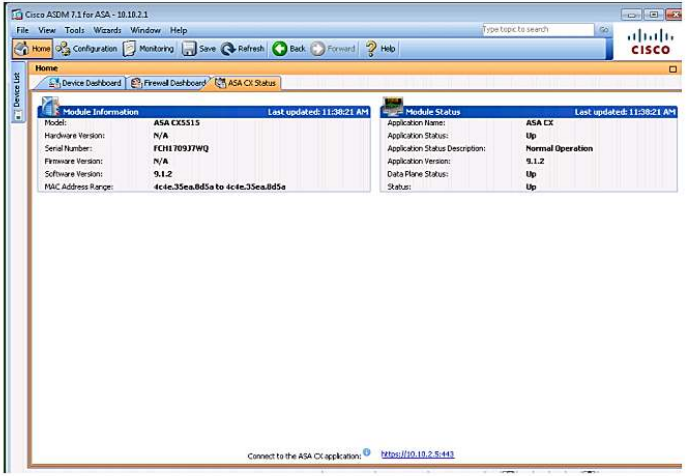
Step 1

Access the on-box PRSM GUI from the ASDM:

A) Access and log in to the Admin PC using the username **student** and password **Ci5coAdmin**

B) Use the ASDM launcher to connect to the Cisco ASA to IP address **10.10.2.1** using username **admin** and password **Ci5coAdmin**.

C) From the ASDM Home page, click on the **ASA CX Status** tab, click the **https://10.10.2.5:443** link on the bottom of the page to access the on-box PRSM GUI.



NOTE: The Google Chrome Frame plug-in for Internet Explorer is required for Internet Explorer to work with the PRSM GUI. Use Mozilla Firefox to perform all of the PRSM lab tasks.

Step 2

Access the on-box PRSM GUI using a web browser:

A) Open Mozilla Firefox and browse to **https://10.10.2.5** directly.

B) The PRSM is using its self-signed certificate, so accept the certificate security warnings to continue.

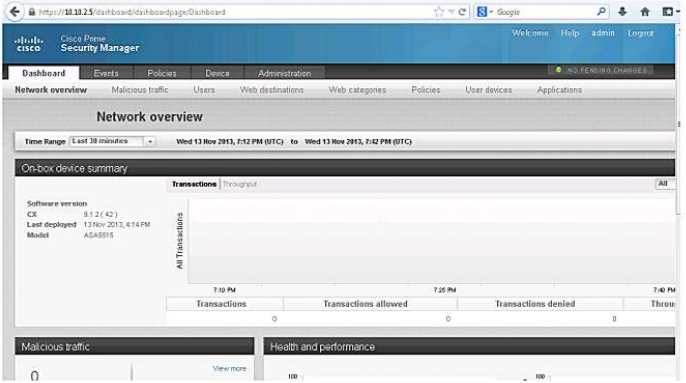
C) Log in to the PRSM using the **admin** username with the **Admin123** password.

In this lab, you will only use the on-box PRSM and not the off-box PRSM because the next version of the off-box PRSM will use a new policy model, and the way the ASA and ASA CX devices will be imported and managed by the off-box PRSM will change from the current 9.1.2 version of the off-box PRSM.

https://t.me/learningnets

Step 3

Which screen is displayed when you first log in to the PRSM? And what is the CX software version?



Step 4

What are the main menu options that are available in the PRSM besides the Dashboard option?

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

Step 5

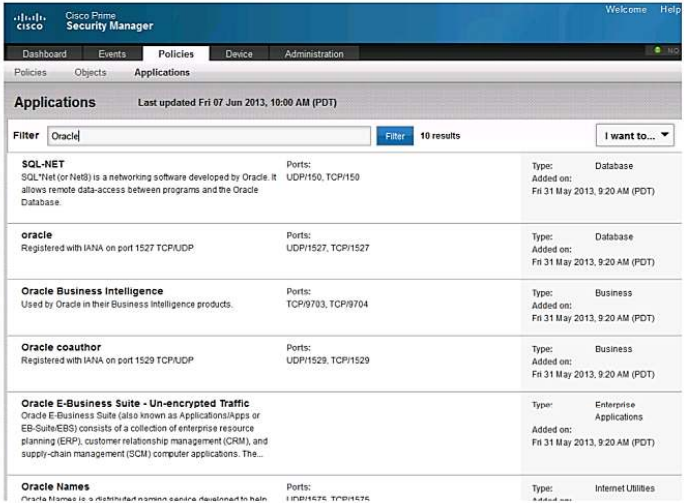
Select the **Policies** menu option. What are the available submenu options under the Policies menu options?

Step 6

Explore the PRSM display filter function.:

A) Access the **Policies > Applications** page. This page list all of the Cisco ASA (CX) NGFW-supported applications.

B) Many of the PRSM GUI screens have the display Filter option to filter the displayed information. From the **Policies > Applications** page, use the **Filter** option by typing **oracle** in the field to only display the different Oracle applications.



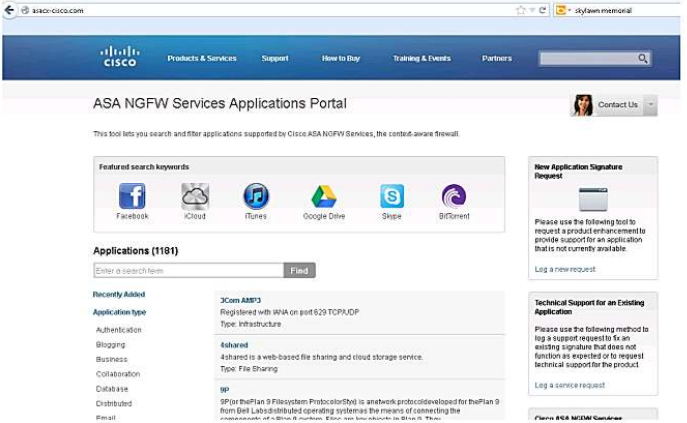
Step 7

Explore the latest applications that are supported by the Cisco ASA (CX) NGFW using the Cisco ASA NGFW Services Applications Portal:

A) From the Admin PC, browse to http://asacx-cisco.com.

B) Find some of the application types that are supported by the Cisco ASA (CX) NGFW such as Authentication, Blogging, Business, Collaboration, Database, Webmail, and so on.

C) Find the Google+ applications that are supported by the Cisco ASA (CX) NGFW such as Google+ Chat, Google+ Games, Google+ General, Google+ Location Tagging, Google+ Photos, and Google+ Videos.



Step 8

Return to the PRSM GUI. Verify the PRSM logging levels by accessing the **Administration > PRSM logs** screen.

What is the default logging level for the management plane, viewing events, HTTP inspection engine, data plane syslog and TLS decryption engine?

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

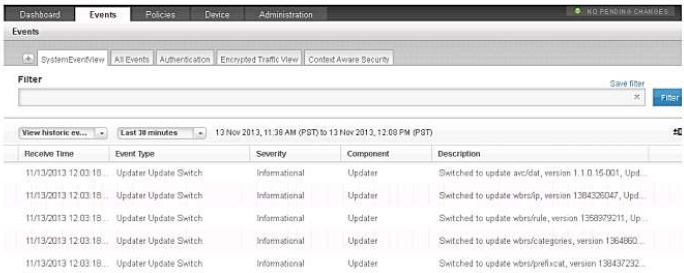
Step 9

View events from the **PRSM Event Viewer** by accessing the **Events** screen and choose the **SystemEventView** tab:

A) Set the Event Viewer to view the historic event from the **last 30 minutes**.

B) Locate the **Updater Update Switch** events, which are triggered each time the Cisco ASA (CX) NGFW checks the Cisco SIO for the application signature updates.

How often does the Cisco ASA (CX) NGFW check the Cisco SIO for application signature updates by default?



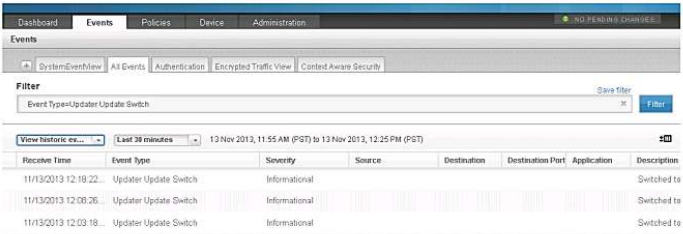
© 2014 Cisco Systems, In
https://t.me/learningnets

Step 10

The PRSM GUI has a display filter feature for filtering the output on some of the PRSM GUI screens. Like for the PRSM Event Viewer, you can use the filter to only display certain events you are interested in:

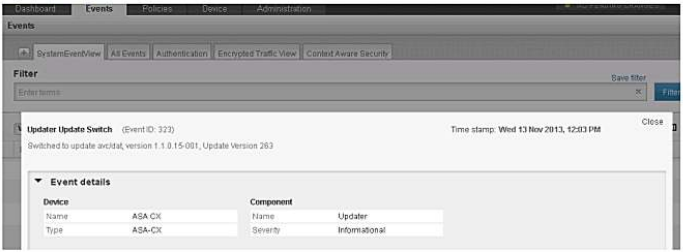
For example, to filter the display to only show the Updater Update Switch events, from the PRSM Event Viewer, under the Filter box, you can either manually type in **Event Type=Updater Update Switch** or you can just click on one of the **Updater Update Switch** events under the **Event Type** column to automatically create a filter. Then to filter the output, click the blue **Filter** box on the right.

You can also filter using on multiple criteria, like **Event Type=Updater Update Switch** and **Severity=Informational** and etc.



Step 11

Navigate to **Events** screen and choose the **SystemEventView** tab and hover your cursor over one of the **Updater Update Switch** events. When the **View details** button appears, click the **View Details** button to view the event details.



Close the **View details** window.

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

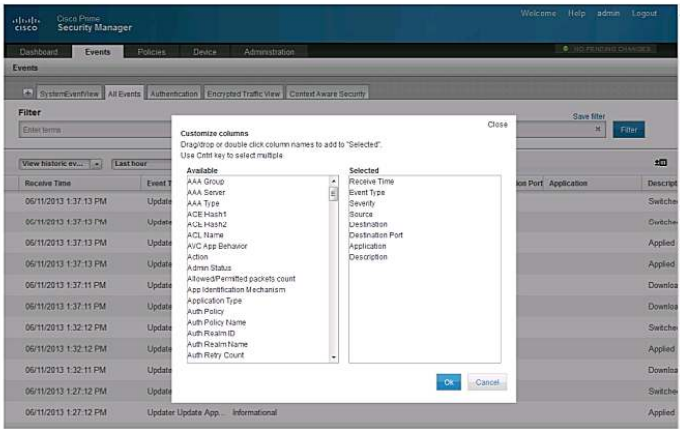
Step 12

Customize the PRSM Event Viewer display columns. Click the **Add/Remove Customize columns** button (to the far right of the screen above the Description column):

When you customized the display columns of a view, a copy of the view will be automatically created with the customized display columns.

A) Examine all of the Available and Selected column options to be displayed.

B) Close the **Customize Columns** window.



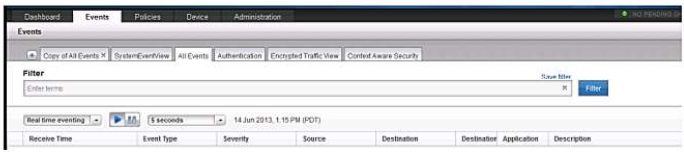
Step 13

Display the **Real Time Events** from the PRSM Event Viewer. Set the **Event Viewer** to view the real-time eventing and observe any real-time events:

The real-time display will refresh every 5 seconds by default.

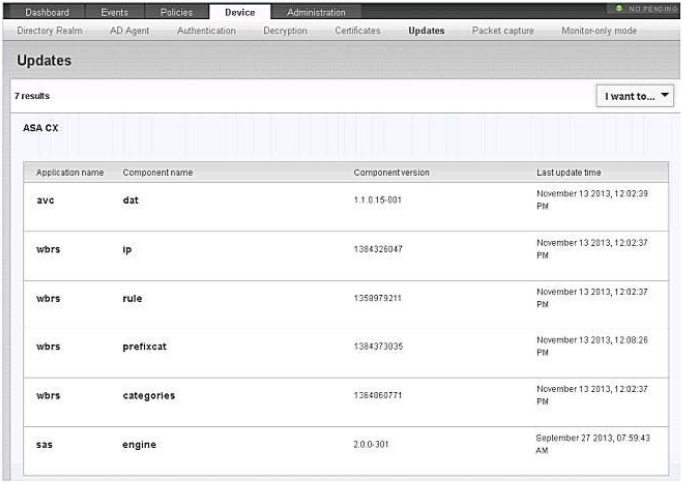
The PRSM Event Viewer has different predefined views (tabs).

For example, instead of viewing **SystemEventView**, you can select the **All Events** tab to show all of the events.



Step 14

Verify the Cisco ASA (CX) NGFW application components version. Navigate to **Device > Updates** screen to verify the Cisco ASA (CX) NGFW application components version.



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

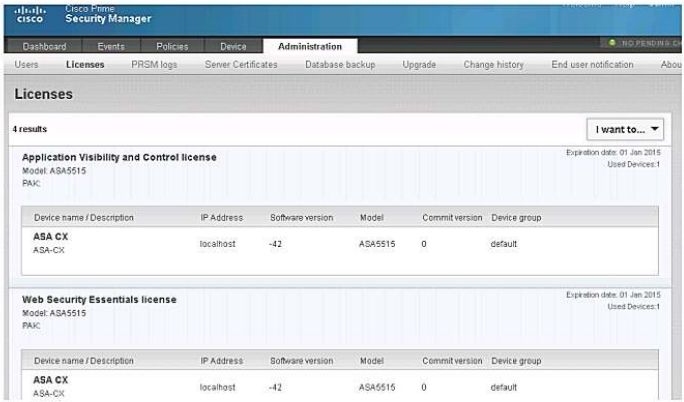
Step 15

Verify the installed Cisco ASA (CX) NGFW licenses by navigating to the **Administration > Licenses** page:

Verify the Application Visibility and Control and the Web Security Essential license has not expired.

The K9 license may not be available in the lab, if the K9 license is not available, the decryption operations (later configured in the decryption lab) will only work if the destination web server does not require a strong encryption method like AES.

Note that the software version that is shown on the Licenses page is the software version that was running when the license was installed.



Task 6: Redirect Traffic from the ASA to ASA (CX) NGFW

In this lab task, you will configure the Cisco ASA to redirect traffic to the Cisco ASA (CX) NGFW.

Activity Procedure

Complete the following steps to configure the Cisco ASA to redirect traffic to the Cisco ASA (CX) NGFW.

https://t.me/learningnets

Step 1

From the Cisco ASA CLI, configure the Cisco ASA to redirect all traffic from the inside interface to the Cisco ASA (CX) NGFW in the following manner:

A) If the Cisco ASA (CX) NGFW fails, the Cisco ASA should drop all of the traffic that would otherwise be redirected to the Cisco ASA (CX) NGFW.

B) Also enable the authentication proxy that is required to use active authentication in the identity policies on the Cisco ASA (CX) NGFW.

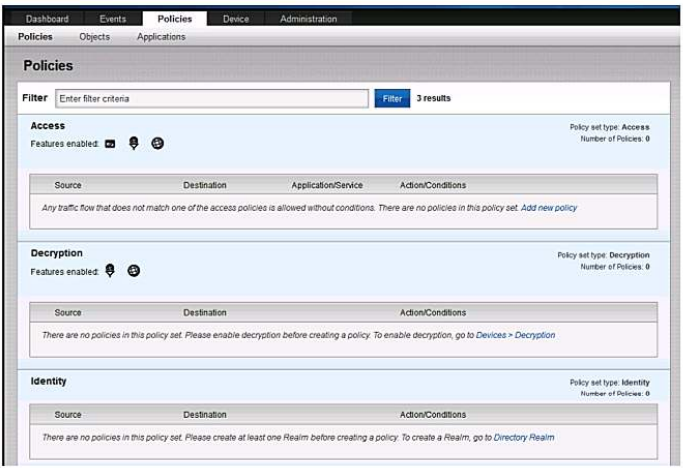
Note	To return back to the ASA console from CX console, press **<Ctrl, Shift, 6>**, **<Ctrl, Shift, 6>** and then **x**.

```
policy-map asacx_policy
 class class-default
  cxsc fail-close auth-proxy
!
service-policy asacx_policy interface inside
```

Step 2

From the Admin PC, access the PRSM GUI, **Policies > Policies** page.

What is the default (implicit) access, decryption, and identity policy?



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

Step 3

From the Admin PC trigger some outbound HTTP traffic to test outbound HTTP connectivity.

A) Use browser that is still opened to the Cisco ASA (CX) NGFW Applications portal site (http://asacx-cisco.com), browse around the Cisco ASA (CX) NGFW Applications portal.

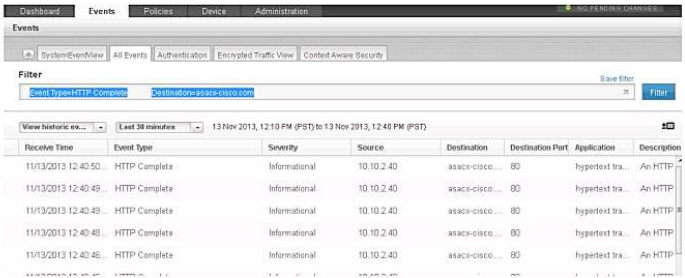
B) From the PRSM GUI, navigate to the **Events** screen. Choose the **All Events** tab.

C) Set the **Event Viewer** to view the historic event from the last 30 minutes.

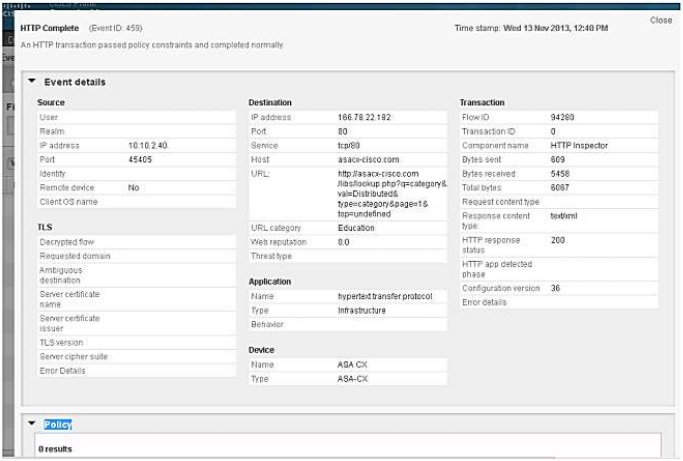
D) Filter the output to only display with **Event Type=HTTP** Complete and **Destination=asacx-cisco.com**.

E) To get more detailed information about the HTTP Complete event, hover your cursor over the event and click **View Details**.

F) View the details about the **HTTP Complete** event. Observe the time stamp, source IP address, port, destination IP address, URL, URL category, web reputation, and so on.



https://t.me/learningnets



Task 7: Explore the System Predefined Default ASA (CX) NGFW Policy Objects

In this lab task, you will explore some of the system predefined objects that cannot be modified.

Activity Procedure

Complete the following steps:

Step 1

From the Admin-PC, access the PRSM GUI, **Policies > Objects** page. From the list of the objects that are shown, which is listed by alphabetical order, locate the **All Remote Devices** object.

Why are you not able to edit or delete the All Remote Devices object?

Step 2

From the **Policies > Objects** page, use the **Filter** option to display the Apple-iPad object.

Which type of object is the Apple-iPad object? Is it a system predefined object?

---

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

Step 3

From the **Policies > Objects** page, use the **Filter** option to display the Default Reputation Profile.

TIP: If your filter does not work, make sure that you enter **Default Reputation Profile** in the **Filter** box without any extra spaces after the word "Profile."

Which type of object is the Default Reputation Profile? What is the reputation score range of the Default Reputation Profile?

Step 4

From the **Policies > Objects** page, use the **Filter** option to display all of the ICMP-related objects.

What is the name of the service group object that matches ICMP Type 8 (echo request)?

Step 5

From the **Policies > Objects** page, use the **Filter** option to display all of the Identity objects.

What are the two system predefined Identity objects?

Step 6

From the **Policies > Objects** page, use the **Filter** option to only display the **tcp-smtp** object. View the **tcp-smtp** object details.

Which service matches the **tcp-smtp** service group object?

Step 7

From the **Policies > Objects** page, use the **Filter** option to display the **tcp-udp-domain** object.

Which services match the **tcp-udp-domain** service group object?

Task 8: Configure ASA (CX) NGFW Policy Objects

In this lab task, you will configure two new Cisco ASA (CX) NGFW policy objects.

Activity Procedure

Complete the following steps to configure two new Cisco ASA (CX) NGFW policy objects.

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

Step 1

Create a new CX network group object to match the DMZ network. You may use this object in the access policy lab optional challenge lab task. Choose **Policies > Objects > I Want To** and then choose **Add CX Network group**. Enter the following object parameters:

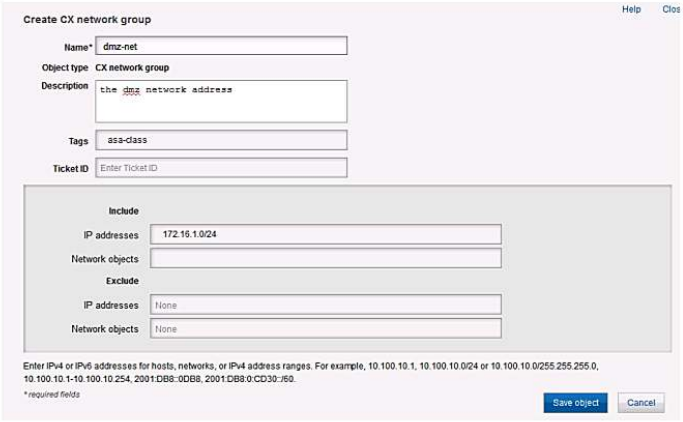
Name: **dmz-net**

Description: **the dmz network address**

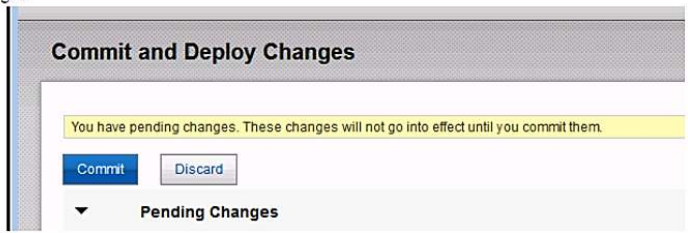
Tags: **asa-class**

Include IP address: **172.16.1.0/24**

Exclude: **None**



Click the **Save Object** button and navigate to CHANGES PENDING in the upper right corner of the screen to open the **Commit and Deploy Changes** page and then click **Commit** to commit the configuration changes.



https://t.me/learningnets

Step 2

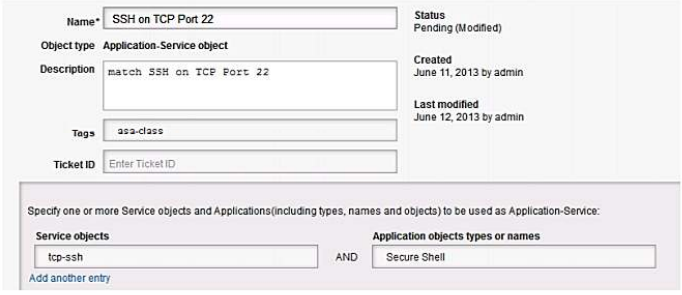
Create a new application-service object to only match SSH traffic on TCP port 22. You may use this object in the access policy lab optional challenge lab task. For example, if the SSH traffic is using a nonstandard port such as TCP 222, the SSH traffic will not match this application-service object. The Cisco ASA (CX) NGFW can match traffic based on the application signature and not just based on the protocol and port that it is using.

Choose **Policies > Objects** and then choose **I Want To > Add Application-Service object**. Enter the following object parameters:

Name: **SSH on TCP Port 22**

Description: **match SSH on TCP port 22**

Tags: **asa-class**



Click the **Save Object** button and navigate to **CHANGES PENDING** in the upper right corner of the screen to open the **Commit and Deploy Changes** page and then click **Commit** to commit the configuration changes.

Step 3

Perform a search using the tags. From the **Policies > Objects** screen, filter the display using "**asa-class.**"



You should see the two objects that you created, both of which have the "**asa-class**" tags.

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

Lab 1-2: Configure Cisco ASA (CX) NGFW Access Policy

Activity Objective

In this lab activity, you will configure and verify Cisco Adaptive Security Appliances Context Aware Next Generation Firewall access policies per given security requirements. For instance, you will create an access policy to block access to web sites belonging to the Gambling, Job Search or Shopping URL categories.

After completing this activity, you will be able to:

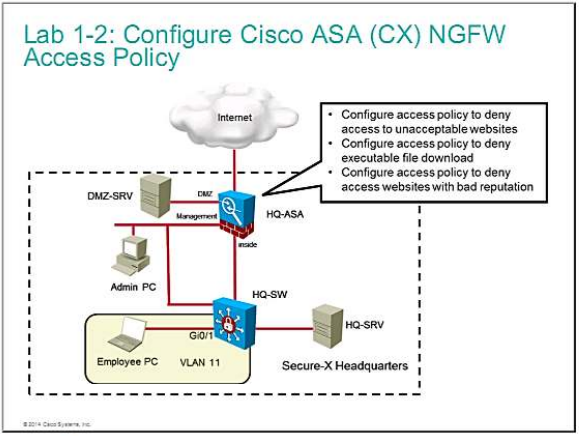
Upon completing this activity, you will be able to meet this objective:

Configure and verify Cisco ASA (CX) NGFW access policies per the given security requirements

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

No commands are used in this activity.

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 asacx-5500x-boot-9.1.2-42.img asacx-sys-9.1.2-42.pkg
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
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**
ASA CX	**admin**	**Admin123**
AD Server (installed on HQ-SRV)	**Administrator**	**Ci5coAdmin**
ScanSafe portal (https://scancenter.scansafe.com)	**ccnpsec.scansafe@yahoo.com**	**C!sco!23**

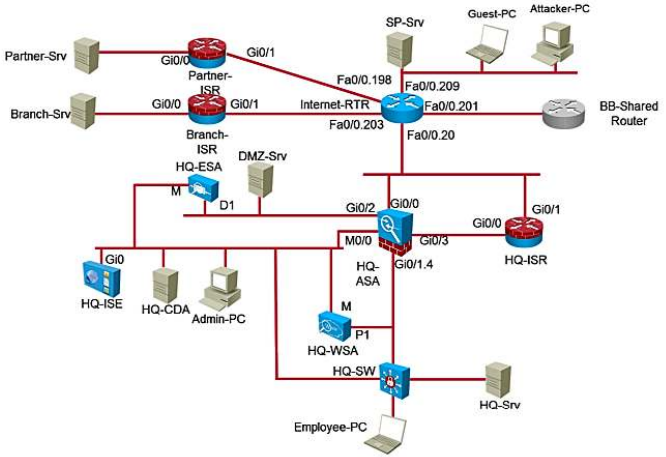
Employee PC is joined to the Active Directory domain.

AD User	AD password	AD Group	Email address in AD properties
it1	**cisco**	IT	**it1@secure-x.public**

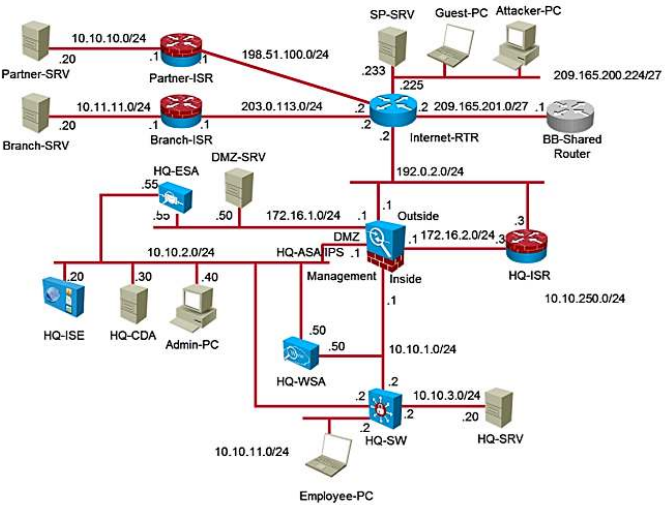
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

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

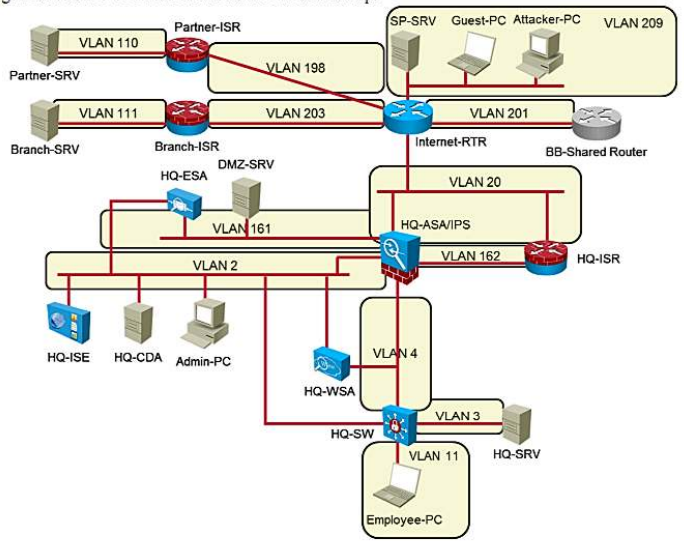


The figure shows the IP addresses that are used in this lab setup.



VLAN Setup

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



Task 1: Configure the ASA CX Access Policy to Deny Access to Unacceptable Websites

In this lab task, you will configure and verify a Cisco ASA CX access policy to deny access to unacceptable websites based on the given security requirements. You will create access policy to block URL object, which consists of URL categories Gambling, Job Search and Shopping.

Activity Procedure

Complete the following steps to configure and verify a Cisco ASA CX access policy to deny access to unacceptable websites:

Step 1

From your Employee PC browser, browse to the following websites: www.cisco.com, www.yahoo.com, www.amazon.com, www.monster.com, and www.poker.com. These should all be successful.

Step 2

From the Admin PC browser navigate to **https://10.10.2.5** (the on-box PRSM GUI) and log in as **admin** using the **Admin123** password.

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

Step 3

Configure a URL object to match the unacceptable websites. From the CX management GUI, navigate to the **Policies > Objects** screen. Configure a URL object to match all of the unacceptable websites that will be used in the new access policy. Choose **Add URL object** from the **I want to** drop-down menu. Create a new URL object using the following object parameters:

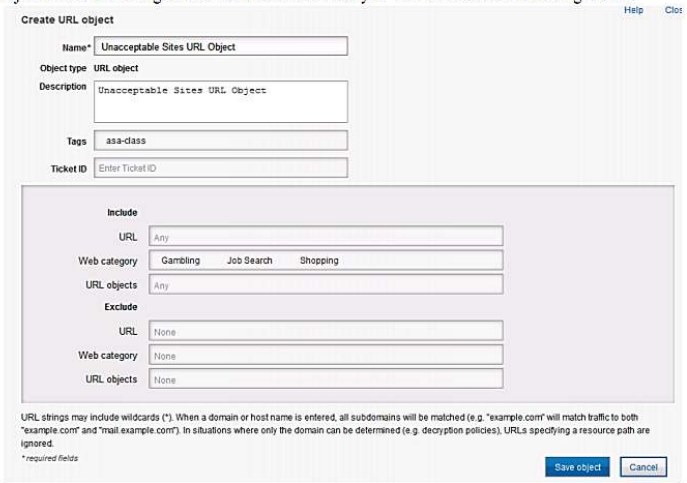
Name: **Unacceptable Sites URL Object**

Description: **Unacceptable Sites URL Object**

Tags: **asa-class**

Include > Web Category: **Gambling**, **Job Search**, and **Shopping**

Click the **Save object** button. The gold clock icon on the right of the **Policies > Objects** screen next to the new object means the changes have not been committed yet. You will commit the changes later.





https://t.me/learningnets

Step 4

Configure an access policy to deny access to the unacceptable websites. From the CX management GUI, navigate to the **Policies**. Hover your mouse over the access policy set. The **Add new policy** link will appear. Click this link. Create a new access policy using the following policy parameters:

Policy Name: **Block Unacceptable Sites**

Use the default settings of **Enable Policy On, Eventing On**, and **Capture Packets Off**

Policy Action: **Deny**

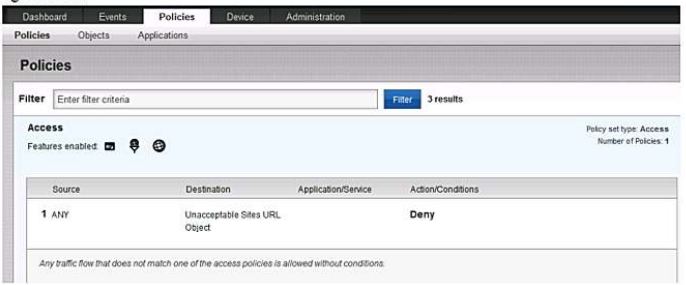
Source: Use the default of **Any**

Destination: Select the **Unacceptable Sites URL object** that you created in the previous step

Application/Service: Use the default of **Any**



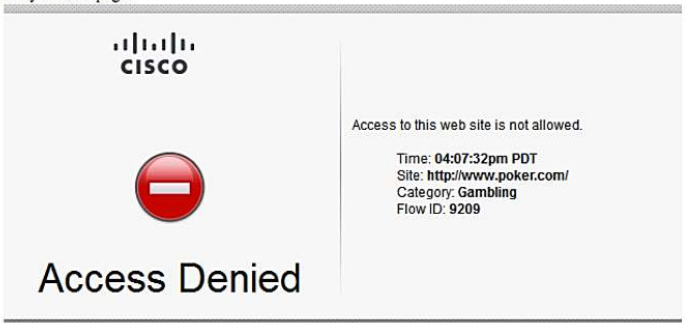
Save the policy and commit all of your configurations changes by clicking the **gold clock** icon and then clicking **Commit**.



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

Step 5

Test the access policy by browsing to a gambling-type website. From your Employee PC browser, try to browse to http://www.poker.com. This site should be blocked by the Cisco ASA CX because this is a gambling-type website. If it is not blocked, try to refresh your browser so that it is not showing the previously cached page.



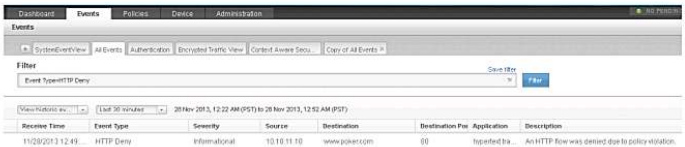
Step 6

Examine the **HTTP Deny** events using the **Events Viewer**:

A) From the CX management GUI, navigate to the **Events** screen.

B) Choose the **All Events** tab. View the historic events from the last hour.

C) Filter the display by using **Event Type=HTTP Deny**.

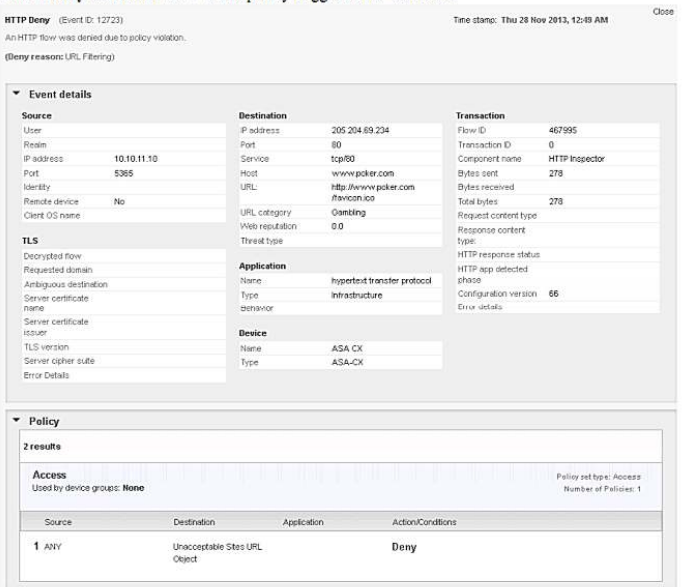


You should see the **HTTP Deny** event at the http://www.poker.com destination with a description of an HTTP flow that was denied because of a policy violation.

https://t.me/learningnets

Step 7

Examine the **HTTP Deny** event details using the **Events Viewer**. To get more detailed information about the HTTP Deny event, hover your cursor over this event and click **View details**. Examine the source IP address and port, destination IP address, Flow ID, Device Name and Type. From the ***Event details*** screen, expand the **Policy** section to view which policy triggered the violation.



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

Step 8

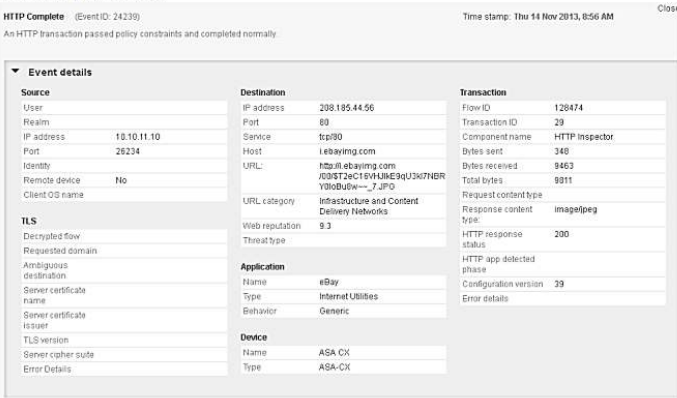
Test the access policy by browsing to other websites:

A) From your Employee PC browser, try to browse to http://www.amazon. This site should be blocked by the Cisco ASA CX because this is a shopping-type website. If it is not blocked, try to refresh your browser so that it is not showing the previously cached page.

B) From your Employee PC browser, try to browse to http://www.monster.com. This site should be blocked by the Cisco ASA CX because this is a job search-type website. If it is not blocked, try to refresh your browser so that it is not showing the previously cached page.

C) From your Employee PC browser, try to browse to http://www.cisco.com or https://www.yahoo.com and so on. These sites should be successful because these are not gambling, shopping, or job search-type websites. Also try to go to shopping from Yahoo, it should be blocked.

D) From your Employee PC browser, try to browse to http://www.ebay.com. Is this successfully? From the event viewer, look for the event details about the HTTP event to ebay and examine what is the URL category for ebay.



Task 2: Configure the ASA CX Access Policy to Deny Any Executable File Download

In this lab task, you will configure and verify a Cisco ASA (CX) NGFW access policy to deny any executable file download. You will try to download executable file from DMZ Server to Employee PC, and this attempt will fail due to access policy violation.

Activity Procedure

Complete the following steps to configure and verify a Cisco ASA (CX) NGFW access policy to deny any executable file download:

Step 1

Configure a file filtering profile by navigating to the **Policies > Objects** screen and choose **Add File Filtering Profile** from the **I Want To** drop-down menu. Create a new file filtering profile using the following parameters:

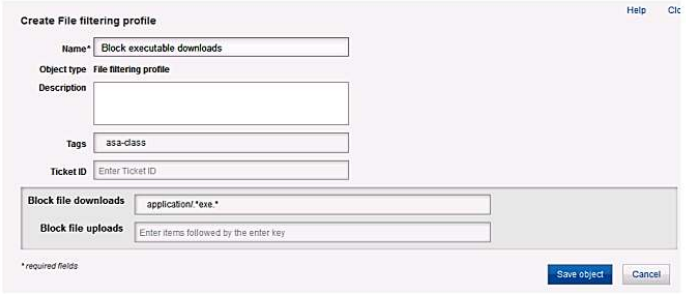
Name: **Block executable downloads**

Description: **Block executable downloads**

Tags: **asa-class**

Under Block file downloads, type **application/.*exe.***

CAUTION: Do not select "application/*" because this will also block the needed signature update downloads from the Cisco SIO.



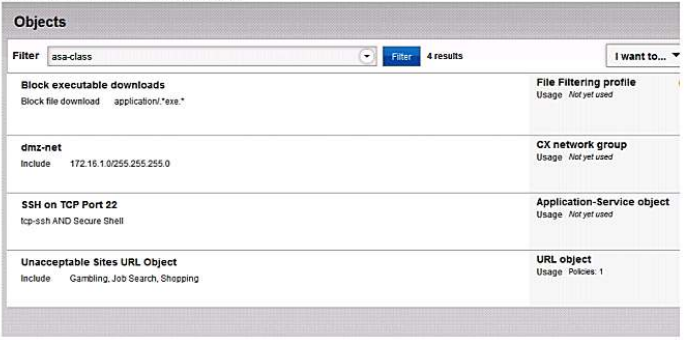
Click the **Save Object** button and commit your configuration changes.

NOTE: File filtering and web reputation profiles do not apply to non-HTTP traffic.

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

Step 2

From the **Policies > Objects** screen, enter **asa-class** in the **Filter** field and click the **Filter** button to display all of the objects with the **asa-class** tag.



You should see all of the objects that you created so far. Notice the **Usage** should indicate **Not Yet Used** for the Block Executable Downloads, dmz-net, and SSH on TCP Port 22 objects. And the **Unacceptable Sites URL Object Usage** should indicate that it is used in one policy.

https://t.me/learningnets

Step 3

Configure an access policy to deny any executable file download.

From the **Policies > Policies** screen, hover your cursor over the first access policy and click the **Add Above** link.

Create a new access policy using the following parameters:

Policy Name: **Filter Executable Downloads**

Use the default settings of **Enable Policy On, Eventing On, and Capture Packets Off**

Policy Action: **Allow**

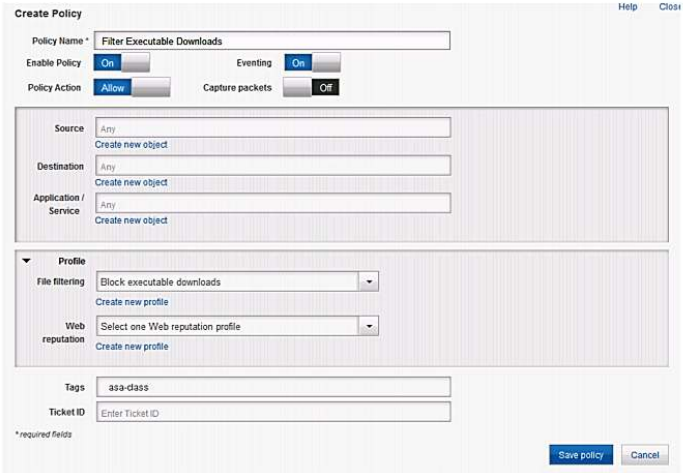
Use the default settings of **Source, Destination, and Application/Service = Any**

Click the word **Profile** to expand the profile section.

For File filtering, choose **Block Executable Downloads**

Try to change the Policy Action to **Deny**. You should notice that the Profile section disappears because you cannot use the Deny policy action when you are using profiles. Profiles are used to conditional allow certain access.

Change the **Policy Action** back to **Allow**.



Click the **Save Policy** button and commit your configuration changes.

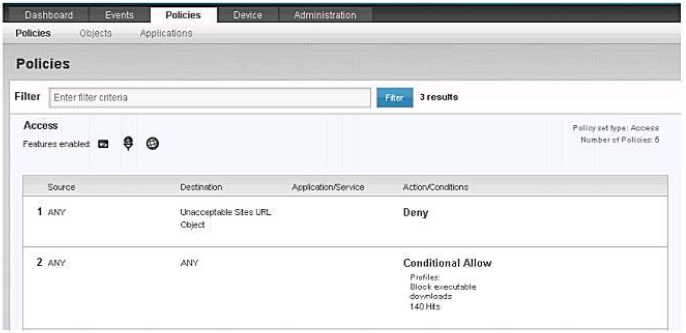
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 4

Verify the order of the two access policies. From the **Policies > Policies** screen, review the two access policies that you created. The order of the policies matters, and the policies are matched top down. Similar to ACL configurations, the more specific policies should be at the top, so perform these actions:

A) Move the unacceptable websites access policy up so that it is the first access policy (as shown in the figure below) by using **Move Up** or **Move Down** buttons to reorder the policies.

B) Commit your configuration changes.

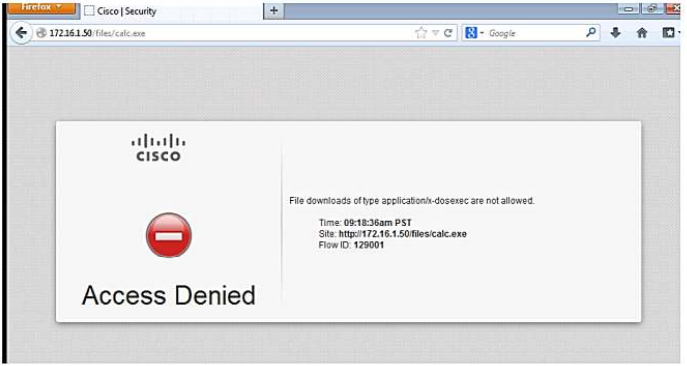


Step 5

Test the access policy:

A) From your Employee PC browser, browse to the DMZ Server (**http://172.16.1.50** or **http://dmz.secure-x.local**).

B) From the DMZ server home web page, click the **Files** tab. Click on the **Windows Calculator Program (.exe)** link to try to download it.



This should fail because the Cisco ASA (CX) NGFW access policy is blocking all executable downloads.

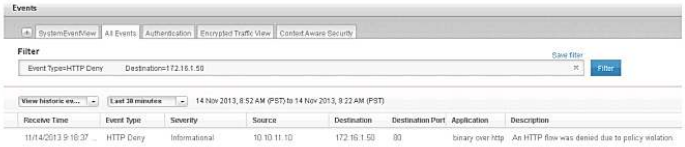
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 6

From the PRSM GUI, navigate to the **Events** screen. Choose the **All Events** tab. View the historic events from the past hour:

A) Filter the display using **Event Type=HTTP Deny** and **Destination=172.16.1.50**

B) A way to select the filter instead of manually typing it in is to find one of the **HTTP Deny** events to the **172.16.1.50** Destination, click **HTTP Deny** under the **Event Type** column, click **172.16.1.50** under the **Destination** column, this will automatically fill in the filtering conditions in the filter box, then click the **Filter** button.



You should see the **HTTP Deny** event at the **172.16.1.50** destination with a description that HTTP flow was denied due to policy violation.

Task 3: Configure an ASA CX Access Policy to Deny Access to Any Websites with a Bad Reputation

In this lab task, you will configure and verify a Cisco ASA (CX) NGFW access policy to deny access to any websites with a bad reputation.

Activity Procedure

Complete the following steps to configure and verify a Cisco ASA (CX) NGFW access policy to deny access to any websites with a bad reputation:

https://t.me/learningnets

Step 1

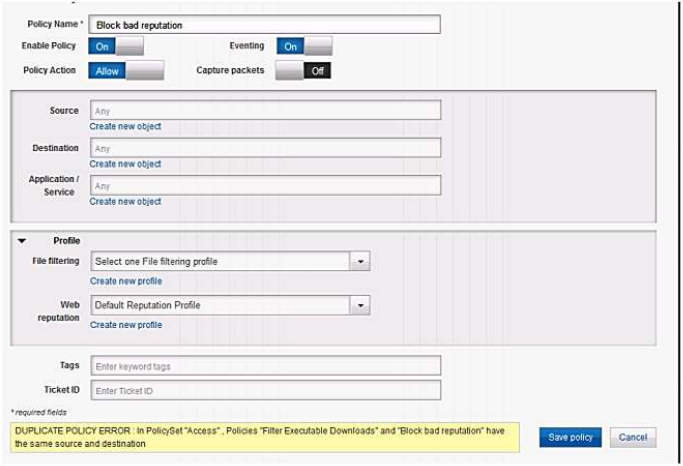
Try to add another access policy with the same source and destination and application or service as an existing access policy that denies all executable file downloads. From the **Policies > Policies** screen, hover your cursor over the first access policy and click the **Add Above** link. Try to configure a new access policy using the following parameters:

Policy Name: **Block Bad Reputation**

Leave all other fields as the default

Click the word **Profile** to expand the profile section.

For Web reputation, choose **Default Reputation Profile**.



Click the **Save Policy** button. You should receive the error **"DUPLICATE POLICY ERROR: In PolicySet 'Access.'" The Filter Executable Downloads and Block Bad Reputation policies have the same source and destination.**

It is not possible for two access polices to have the same source and destination as well as the same application or service. Click the **Cancel** button.

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

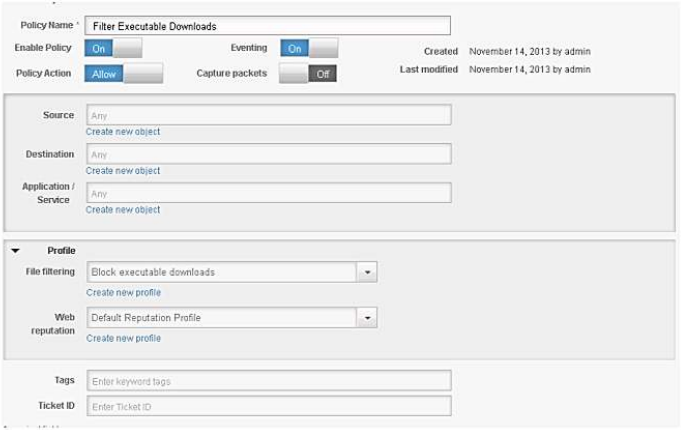
Step 2

Edit the previous access policy that denies all executable file downloads. From the **Policies > Policies** screen, hover your cursor over the second access policy that denies all executable file downloads and click the **Edit Policy** link:

Click the word **Profile** to expand the profile section.

For **File filtering**, confirm that it is set to **Block Executable Downloads**.

For **Web reputation**, choose **Default Reputation Profile,** which has a default score range of -10 to -6.



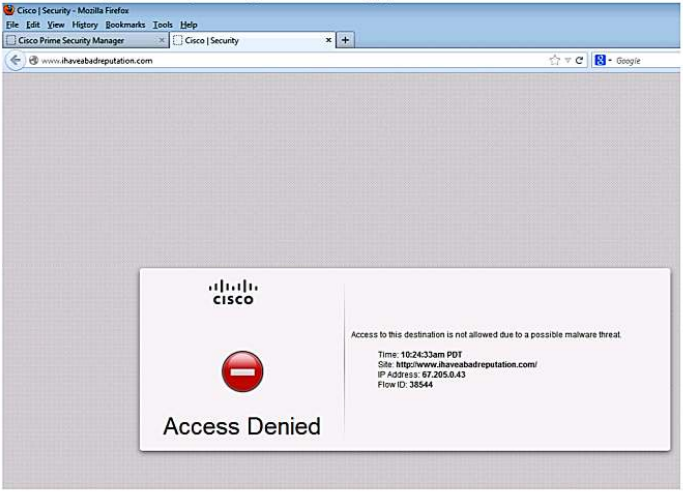
Click the **Save policy** button and commit your configuration changes.

https://t.me/learningnets

Step 3

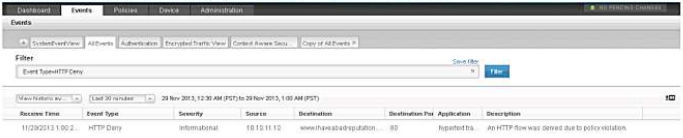
Test the access policy by browsing to http://www.ihaveabadreputation.com from your Employee PC browser. This should be blocked by the access policy because this site has a low reputation score. If the www.ihaveabadreputation.com website is not available anymore, ask your instructor for another site that has a low reputation score.

NOTE: File filtering and web reputation profiles do not apply to non-HTTP traffic.



Step 4

From the PRSM GUI, navigate to the **Events** screen. Choose the **All Events** tab. View the historic events from the last hour. Filter the display using **Event Type=HTTP Deny**.



You should see the HTTP Deny event to the www.ihaveabadreputation.com destination with a description of An HTTP flow that was denied due to policy violation.

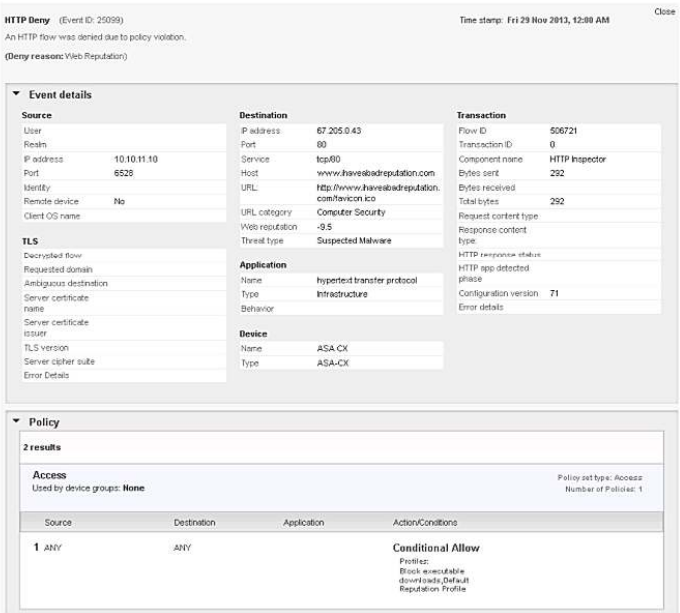
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 5

To get more detailed information about the HTTP Deny event, hover your cursor over the event and click **View Details:**

Examine the source IP address and port, destination IP address, URL category, Web reputation score, and Device Name and Type.

From the Event details screen, expand the **Policy** section to view which policy triggered the violation.



Task 4: Optional Challenge Lab Task: Configure ASA CX Access Policies

In this optional challenge lab task, you will configure and verify Cisco ASA (CX) NGFW access policies to allow SSH traffic only on TCP port 22 to any destinations on the DMZ network.. The solution is shown in the Lab Answer Key.

Activity Procedure

Complete the following steps to configure and verify Cisco ASA (CX) NGFW access policies to allow SSH traffic only on TCP port 22 to any destinations on the DMZ network:

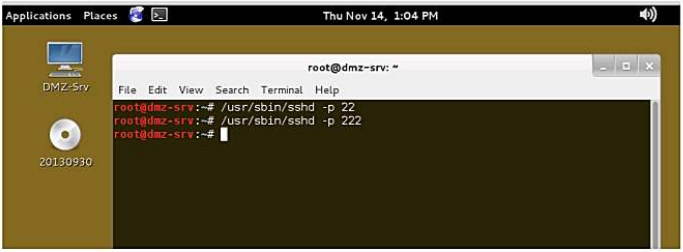
https://t.me/learningnets

Step 1

You will first need to access the console to the DMZ Server (Linix) to enable SSH server services on it:

A) Access the DMZ Server and open the Linux command prompt window.

B) Use the **/usr/sbin/sshd –p 22** and the **/usr/sbin/sshd –p 222** commands to enable SSH server on ports 22 and 222.



Step 2

Configure the Cisco ASA (CX) NGFW to permit SSH traffic only on TCP port 22 to any destinations on the DMZ network. Configure two access policies to accomplish this task:

A) The first access policy to allow SSH traffic on TCP port 22 to any destinations on the DMZ network. In the access policy you will create, you can use the two policy objects created in the previous lab.

B) The second access policy to deny all SSH traffic based on the SSH application signature. The Cisco ASA (CX) NGFW can match traffic based on the application signature and not just based on the protocol and port that it is using.

A solution to this optional challenge lab task is provided in the lab solution.

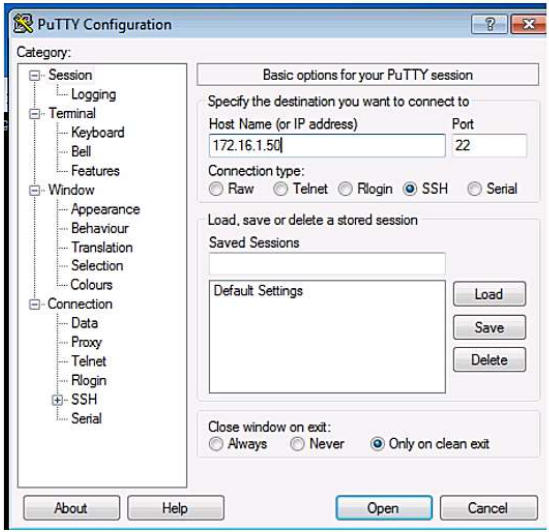
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

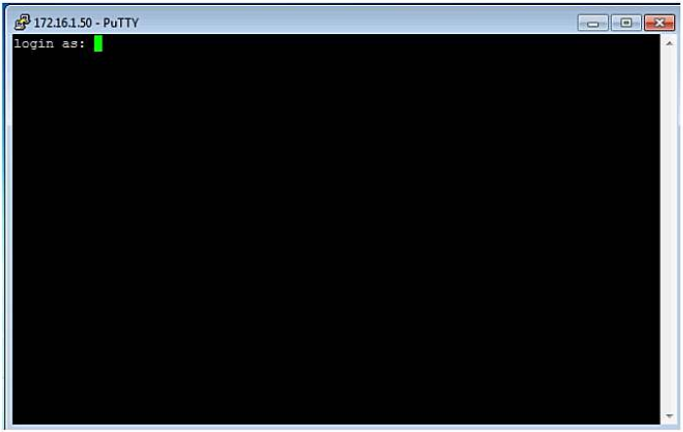
Step 3

Test your access policies as follows:

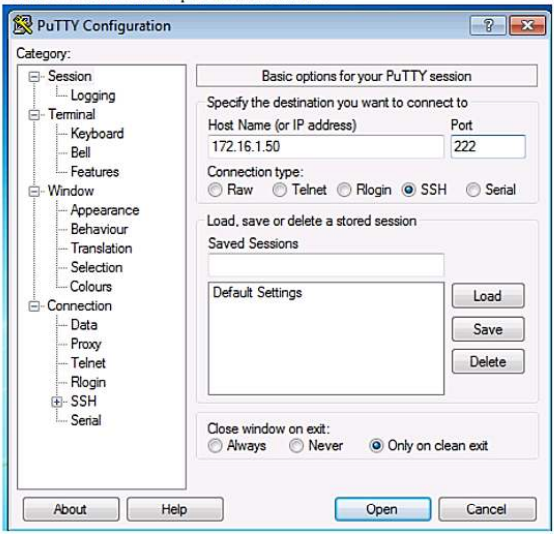
A) From the Employee-PC, use PuTTY and SSH to the DMZ Server (172.16.1.50) on port 22. This should be successful.

B) From the Employee-PC, use PuTTY and SSH to the DMZ Server (172.16.1.50) on port 222. This should not be successful.

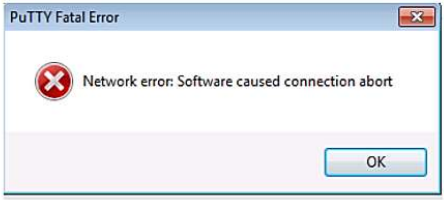




You should see that SSH connection on port 22 is successful.



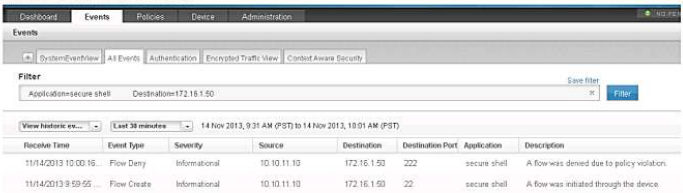
https://t.me/learningnets
© 2014 Cisco Systems, Inc.



You should see that SSH connection on port 222 is not successful.

Step 4

Examine the events in the PRSM event viewer using the **Application=secure shell** and **Destination=172.16.1.50** filters.

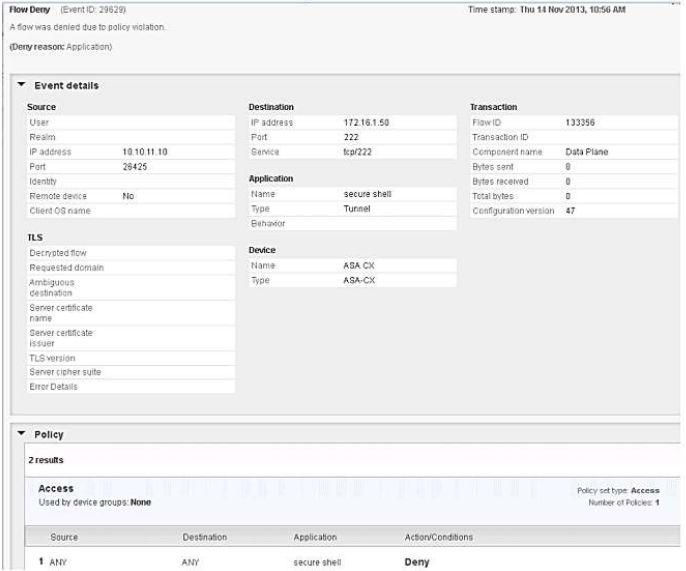


You should see a corresponding Flow Deny and Flow Create events in the PRSM Event Viewer.

https://t.me/learningnets

Step 5

View the details information about the **Flow Deny** event and examine the access policy that was matched.



You should see details about denied flow to DMZ server on TCP port 222.

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

Lab 1-3: Configure Cisco ASA (CX) NGFW Identity Policy

Activity Objective

In this lab activity, you will configure and verify a Cisco Adaptive Security Appliances Context Aware Next Generation Firewall identity policy per given requirements. Fisrt you will configure identity policy using active authentication and afther that you will change the setting of identity policy to passive authentication. You will also configure access policy, which will use identity object in its definition.

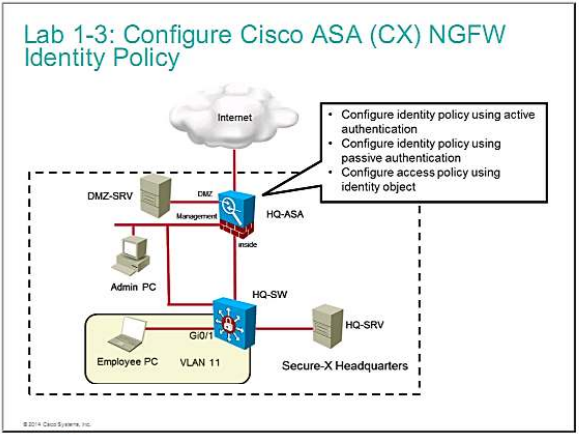
Upon completing this activity, you will be able to meet these objectives:

- Configure and verify Cisco ASA (CX) NGFW identity policies using active authentication
- Configure and verify Cisco ASA (CX) NGFW identity policies using passive authentication
- Configure and verify Cisco ASA (CX) NGFW identity-based access policies

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 following table describes the commands that are used in this activity. Refer to this list if you need configuration command assistance during the lab activity.

Commands

Command	Description
show opdata adisessions	Displays the content of the Cisco ASA (CX) NGFW ADI session directory
clear opdata adisessions	Clears the Cisco ASA (CX) NGFW ADI session directory

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 asacx-5500x-boot-9.1.2-42.img asacx-sys-9.1.2-42.pkg
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
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**
ASA CX	**admin**	**Admin123**
AD Server (installed on HQ-SRV)	**Administrator**	**Ci5coAdmin**
ScanSafe portal (https://scancenter.scansafe.com)	**ccnpsec.scansafe@yahoo.com**	**C!sco!23**

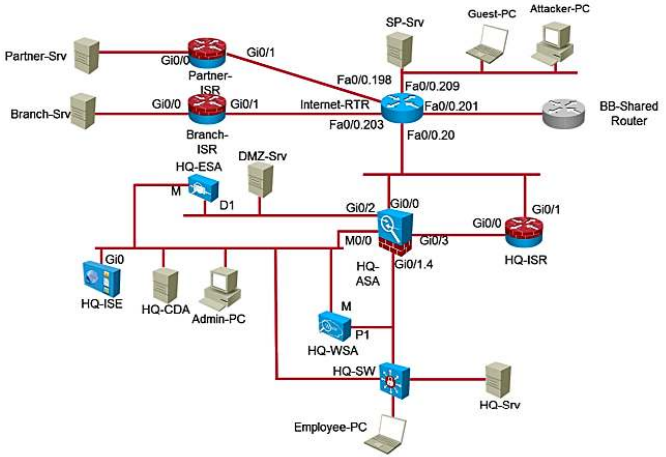
Employee PC is joined to the Active Directory domain.

AD User	AD password	AD Group	Email address in AD properties
it1	**cisco**	IT	**it1@secure-x.public**

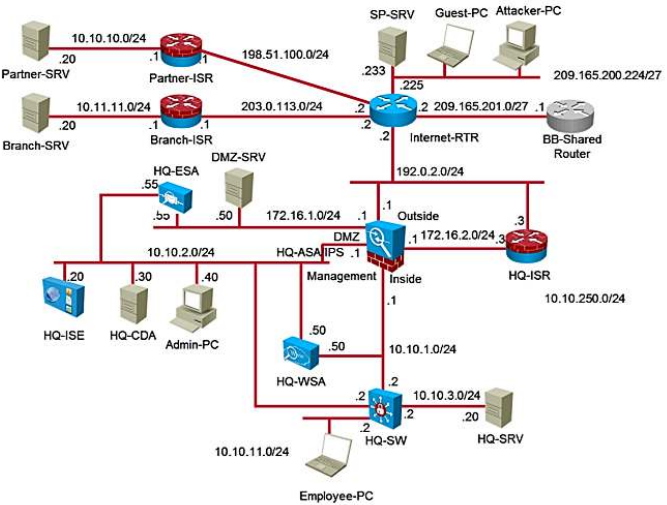
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

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



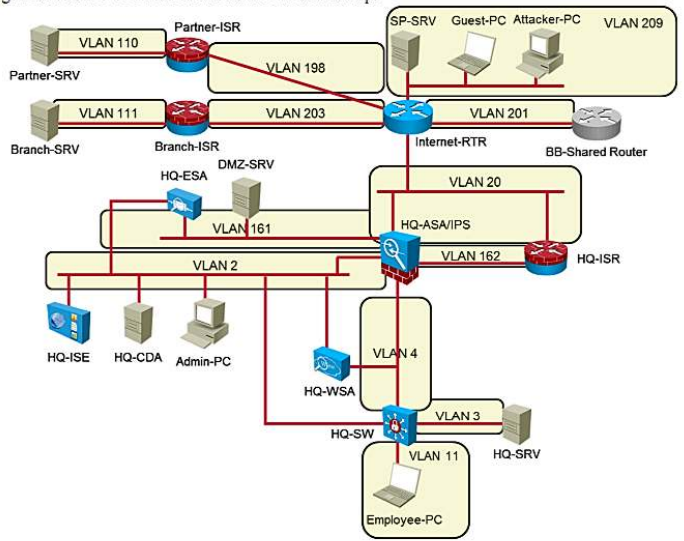
The figure shows the IP addresses that are used in this lab setup.



https://t.me/learningnets

VLAN Setup

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



Task 1: Configure an ASA CX Identity Policy Using Active Authentication

In this lab task, you will configure and verify a Cisco ASA (CX) NGFW identity policy using active authentication. You will define a realm in the Cisco ASA (CX) NGFW and then create an Active Directory server in the realm. After that you will try to access web sites from Employee PC and you will get prompted for domain username and password.

Activity Procedure

Complete the following steps to configure and verify a Cisco ASA (CX) NGFW identity policy using active authentication:

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

Step 1

From the AdminPC, access the PRSM GUI (https://10.10.2.5) and log in using **admin** username and **Admin123** password. Navigate to the **Devices > Directory Realm** screen. Choose **Add Realm** from the **I want to** drop-down menu.

NOTE: Within the Cisco ASA (CX) NGFW, a realm is a logical group of a common type of directory servers (think of it as an AAA server group in the Cisco ASA). The directory servers are defined within a realm in the Cisco ASA (CX) NGFW. You will first define a realm in the Cisco ASA (CX) NGFW and then define an Active Directory server in the realm.

Add a realm using the following parameters:

Name: **Secure-X Realm**

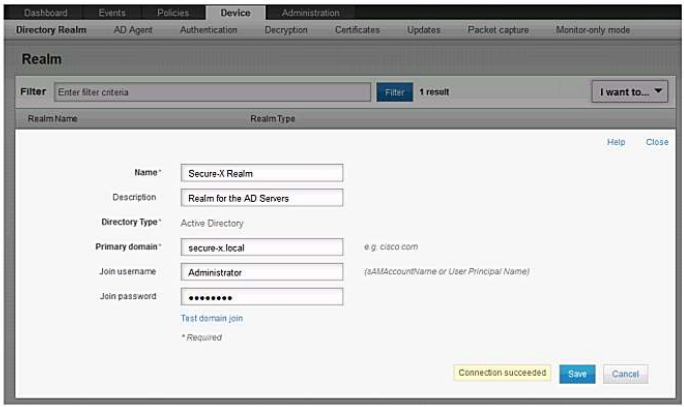
Description: **Realm for the AD Servers**

Directory type: **Active Directory**

Primary domain: **secure-x.local**

Join username: **Administrator**
The Cisco ASA (CX) NGFW will need to join the Active Directory domain using this username.

Join password: **Ci5coAdmin**



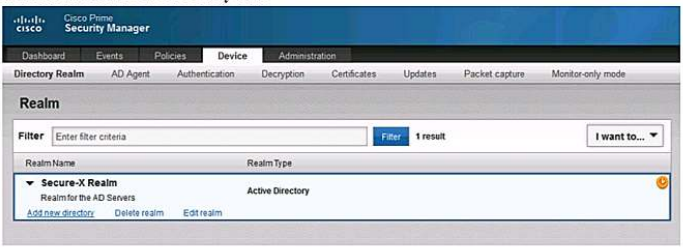
Click **Test Domain Join** to test connectivity to the Active Directory server. You should see that test succeeded.

Click the **Save** button.

https://t.me/learningnets

Step 2

Add an Active Directory server in the authentication realm. Hover your cursor over the **Secure-X Realm** box and click the **Add New Directory** link.



Add a new directory under the realm using the following parameters:

Directory hostname/IP: **hq-srv.secure-x.local**

Port: **389** (default)

Active Directory login name: **Administrator@secure-x.local**

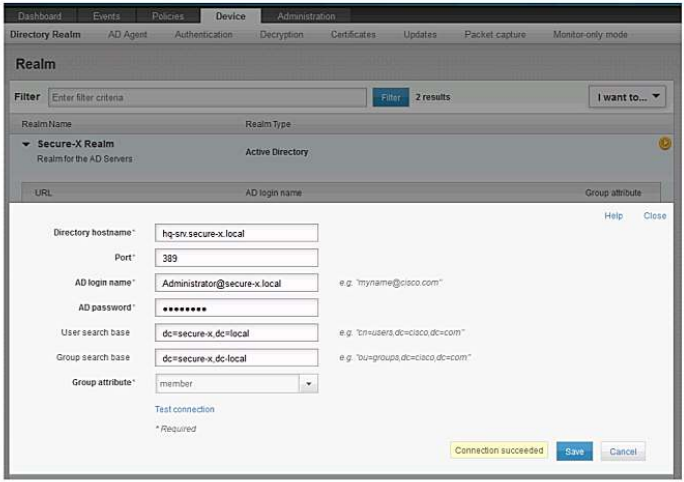
Active Directory password: **Ci5coAdmin**

For User search base, enter **dc=secure-x,dc=local**

For Group search base, enter **dc=secure-x,dc=local**

Group attribute: **member** (default)

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

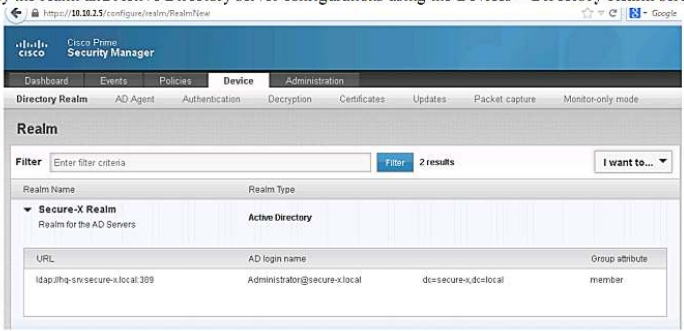


Click the **Save** button and **Test Connection** to test connectivity to the Active Directory server.

Commit your changes.

Step 3

Verify the realm and Active Directory server configurations using the **Devices > Directory Realm** screen.



https://t.me/learningnets

Step 4

Access the Employee PC command line prompt, use the **ipconfig** command to determine the IP address of the Employee PC. The Employee-PC is using DHCP to obtain its IP address from the subnet 10.10.11.0/24.

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

Step 5

Configure an authentication policy using active authentication to only authenticate the traffic source from the Employee PC IP address. Navigate to the **Policies > Policies** screen. Hover your cursor over the Identity policy set and click the **Add New Policy** link.

NOTE: To implement user-based access or decryption policies, the identity of the user that is associated with a traffic flow must be known. This requires the user to provide identification when connecting to the network. Using active authentication, the user HTTP and HTTPS traffic is redirected by the Cisco ASA (CX) NGFW to the Cisco ASA, and the Cisco ASA will prompt the user to enter his or her username and password.

Add a new identity policy using the following parameters:

Policy Name: **Enforce Active Authentication**

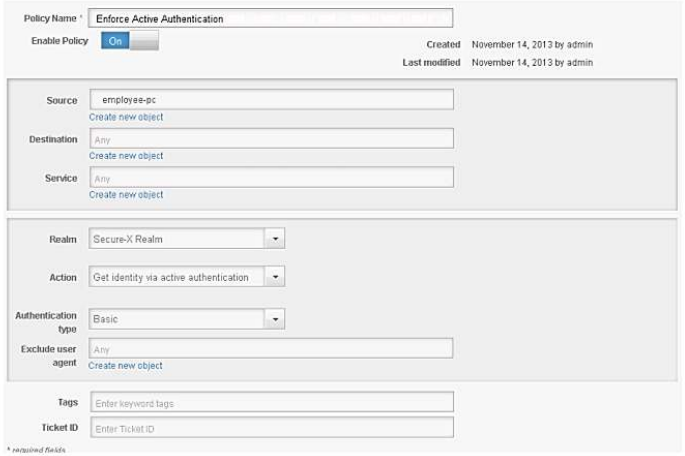
For Source, click **Create New Object** under the Source field and create a new **CX Network Group Object** to match the Employee-PC IP address (10.10.11.10 in this example, your Employee PC IP address may be different).

For Realm, select the **Secure-X Realm**

For Action, select **Get Identity Via Active Authentication** (default setting).

For Authentication type, select **Basic** (default setting).

Review all other default identity policy settings, but leave them as they are.



Click the **Save Policy** button. Commit your configuration changes.

https://t.me/learningnets

Step 6

Verify the resulting identity policy. Navigate to **Policies > Policies** screen.



Step 7

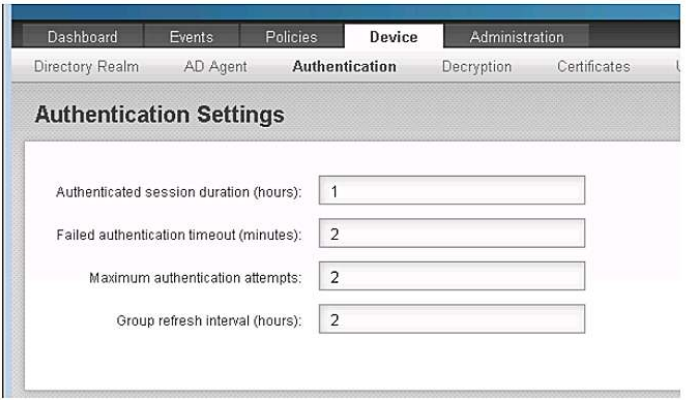
Configure the Authentication Settings by navigating to the **Device > Authentication** screen. For this lab testing environment, set the Authentication Settings to the following:

Authenticated session duration: 1 hour

Failed authentication timeout: 2 minutes

Maximum authentication attempts: 2

Group refresh interval: 2 hours



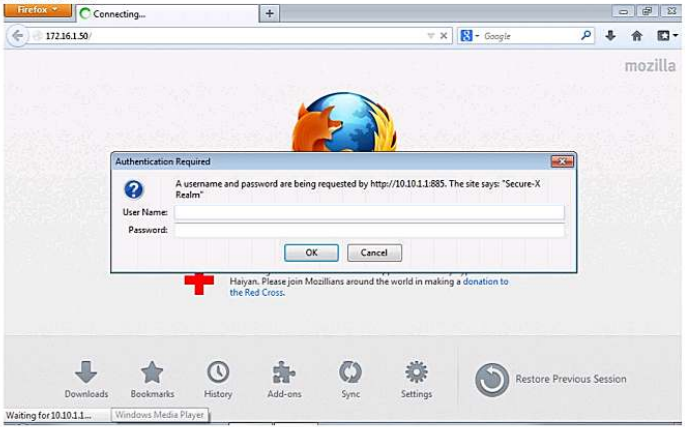
Click the **Save** button. Commit your configuration changes.

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

Step 8

Test the active authentication policy and try to authenticate using a bad password for the **secure-x\it1** user. From the Employee PC (**secure-x\it1** username, password **cisco**), open Firefox and try to browse to the DMZ server (http://172.16.1.50 or http://dmz.secure-x.local). You should receive a pop-up window requesting a username and password from the Cisco ASA IP address 10.10.1.1 and port 885. The default authentication proxy TCP port is 885. If users must be prompted for authentication credentials using active authentication, then they are prompted through this port.

NOTE: When using Active Directory, the username must include the domain name in the DOMAIN \username format.



Step 9

Try to authenticate as the **secure-x\it1** user with bad password of **wrongpassword** again. After the third login attempt with the bad password, the message **"Retry limit exceeded"** should be displayed very briefly before being directed to the DMZ server web page.



The failed authentication timeout value (which you set to 2 minutes) determines the length of time, in minutes, before the user at this IP address is again prompted to authenticate. During this time, all traffic from the IP address is evaluated based on the IP address alone, and no user or user group-based access or decryption policies are applied to the traffic. Thus, during this failed timeout period, the user traffic may be allowed or denied differently as if the user had successfully authenticated.

Before the failed authentication timeout of 2 minutes times out, you should be able to browse around the DMZ server web site.

Step 10

Users who fail active authentication are represented by the IP address in the PRSM User Dashboard. If you access the PRSM GUI before the 2 minutes fail active authentication timeout interval, you should be able to navigate to the PRSM **Dashboard > Users** screen. You should see the **Secure-X Realm\10.10.11.10** user name.



You should see the **Secure-X Realm\10.10.11.10** user name.

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

Step 11

Access the Cisco ASA CLI and console into the Cisco ASA (CX) NGFW CLI. Display the contents of the Cisco ASA (CX) NGFW ADI session database using the **show opdata adisession** Cisco ASA (CX) NGFW CLI command.

NOTE: If a user fails to correctly authenticate during active authentication and exceeds the maximum number of authentication attempts, the IP address for the user is considered to have failed authentication and will be presented using the **Unknown** Identity Type. Users who fail active authentication are represented as **ANONYMOUS** user in the ADI session directory.

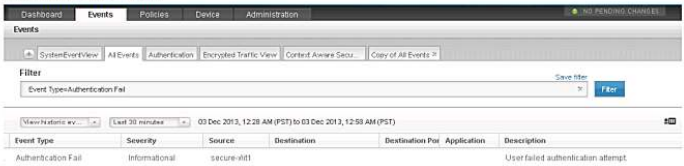
```
asacx> show opdata adisessions
Vdi Session Directory:
============================
total_sessions: 1
contained_op_data {
realm: "Secure-X Realm"
username: "ANONYMOUS"
ip: "10.10.11.10"
identity_type: IDENTITY_FAILED_AUTH
auth_type: AUTH_TYPE_BASIC
```

You should see the **ANONYMOUS** user in the **Secure-X Realm** who failed the active authentication.

Press **Ctrl-C** to exit the **show opdata adisessions** command.

Step 12

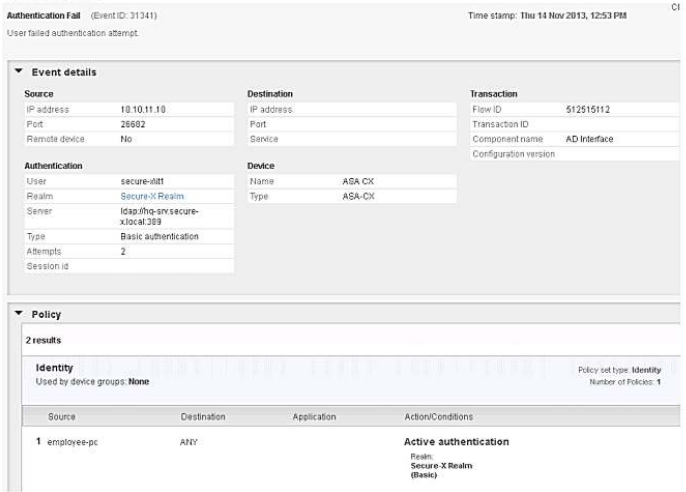
From the PRSM GUI, navigate to the **Events > Events** screen. Filter the display using **Event Type=Authentication Fail**.



You should see the **Authentication Fail** event.

Step 13

To get more detailed information about the Authentication Fail event, hover your cursor over the event and click **View Details**.



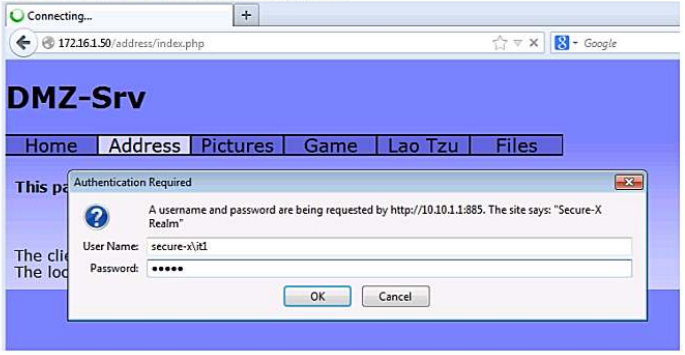
Examine the source IP address, User, Realm, Server and authentication type.

From the Event details screen, expand the **Policy** section to view which policy triggered the Authentication Fail event.

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

Step 14

Test the active authentication policy and log in using a valid login credential. From the Employee PC, open Firefox and try to browse to **http://172.16.1.50** or **http://dmz.secure-x.local**. You should get a popup window for entering the username and password if it has been more than 2 minutes since the last time that you passed the maximum authentication attempts limit.



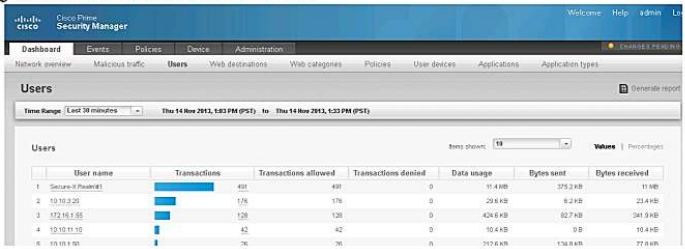
This time, authenticate as the **secure-x\it1** user with a valid password of **cisco**. The authentication should be successful and you should be redirected to the DMZ server web page.

Step 15

From the Employee PC Firefox browser, browse to different websites such as https://www.google.si, https://www.yahoo.com, and so on. You should not be asked to authenticate again because the user-to-IP mappings are cached in the ADI session directory.

Step 16

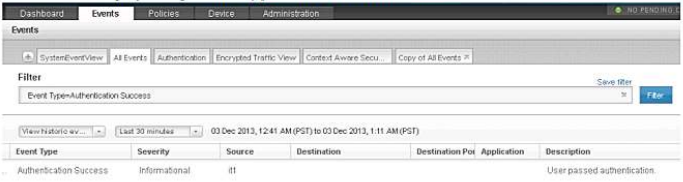
Navigate to the PRSM **Dashboard > Users** screen.



You should see the **Secure-X Realm\it1** user name.

Step 17

From the PRSM GUI, navigate to the **Events > Events** screen. View the historic events from the past 30 minutes. Filter the display using **Event Type=Authentication Success**.

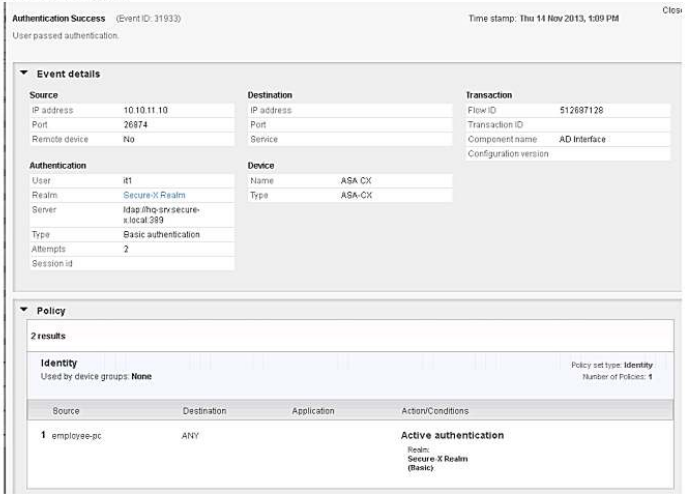


You should see the Authentication Success event.

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

Step 18

To get more detailed information about the Authentication Success event, hover your cursor over the event and click **View Details**.



Examine the source IP address, User, Realm, Server, Authentication Type, and Device Name and Type.

From the Event details screen, expand the **Policy** section to view which policy triggered the Authentication Success event.

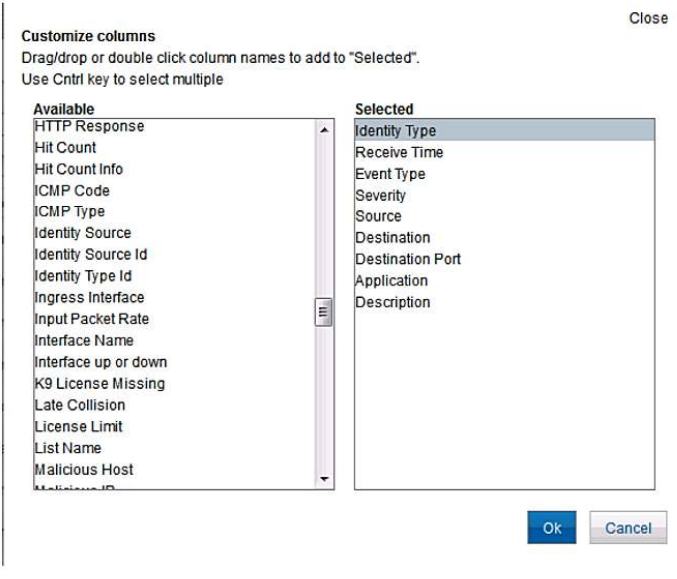
Step 19

From the **Events > Events** screen, choose the All Events tab. View the historic events from the last hour. The columns to be displayed in the event viewer can be customized by clicking the small icon to the far right of View the historic events row. Click this icon to bring up a small screen to select the columns to be displayed in the event viewer.

A) Drag and drop the **Identity Type** column name from **Available** to **Selected**.

B) Move the **Identity Type** to the top in the **Selected** side.

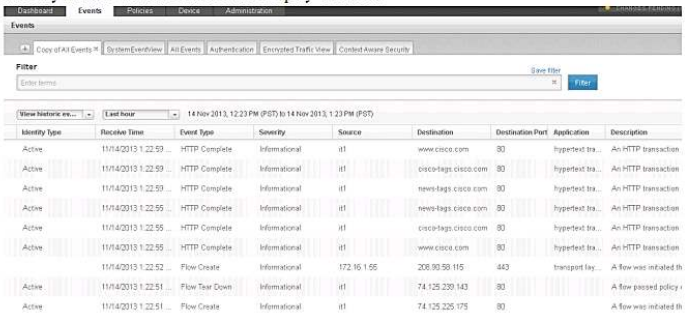
C) Click **OK**.



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

Step 20

When you customized the display columns of the **All Events** view, a **Copy of All Events** view will be automatically created with the customized display columns.



From the All Events display output, you should see different event types in the Event Types column. And in the Identity Type column, you should see **Active** for users who successfully authenticated.

To filter the All Events display output to only see the events that are related to the Active users, you can filter the All Events display using a filter of **Identity Type=Active**.

Remove the filter of **Identity Type=Active**. Then apply another filter of **Identity Type=Unknown** to only see the events that are related to the Unknown users.



https://t.me/learningnets

Step 21

Use the **show opdata adisessions** Cisco ASA (CX) NGFW CLI command to verify Active Authentication Operations. Access the Cisco ASA (CX) NGFW CLI and enter the **show opdata adisessions** command.

```
asacx> sh opdata adisessions
Vdi Session Directory:
============================
total_sessions: 1
contained_op_data {
realm: "Secure-X Realm"
username: "it1"
ip: "10.10.11.10"
identity_type: IDENTITY_ACTIVE
auth_type: AUTH_TYPE_BASIC
```

The output should include information about the **it1** user in the **Secure-X Realm** which passed the active authentication.

Press **Ctrl-C** to exit the **show opdata adisessions** command.

Step 22

Use the **clear opdata adisessions** Cisco ASA (CX) NGFW CLI command to clear the Cisco ASA (CX) NGFW Authentication Directory Interface session directory.

```
asacx>clear opdata adisessions
Cleared sessions
Press Enter to continue, 'CTRL + C' to exit
Cleared sessions
Exiting!!
```

Press **Ctrl-C** to exit the **clear opdata adisessions** command.

Step 23

From the Employee-PC, open Firefox and browse to http://www.cisco.com. You should be asked to authenticate again and receive a pop-up window for entering the username and password:

A) Enter a valid Active Directory username of **secure-x\it1** and password of **cisco**. The authentication should be successful.

B) Close Firefox and log off from the Employee PC.

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

Task 2: Configure an ASA CX Identity Policy Using Passive Authentication

In this lab task, you will configure and verify a Cisco ASA (CX) NGFW identity policy using passive authentication. You will configure the communication between Cisco CDA and ASA CX NGFW. Cisco CDA (which was pre-configured for communication with Active Directory Server) will pass the IP-to-identity mapping to the CX, so you will not prompted for username and password when browsing the Internet pages. This is called passive authentication.

Activity Procedure

Complete the following steps to configure and verify a Cisco ASA (CX) NGFW identity policy using passive authentication:

Step 1

Access the Cisco CDA GUI (https://cda.secure-x.local) from the Admin PC. Accept security warning messages and log in to the Cisco CDA GUI using the **admin** username with the **Ci5coAdmin** password.

https://t.me/learningnets

Step 2

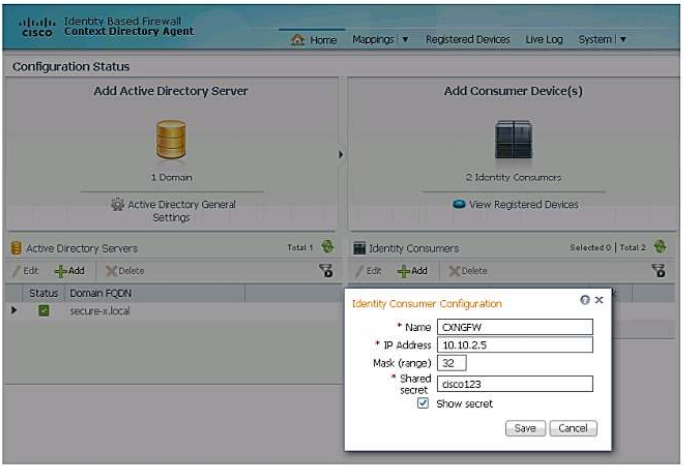
Add the Cisco ASA (CX) NGFW as a consumer device in the Cisco CDA. The Cisco CDA has already been pre-configured to communicate with the AD server. In this lab step, you will just need to add the Cisco ASA (CX) NGFW as another consumer device in the Cisco CDA. Add the Cisco ASA (CX) NGFW as a consumer device using the following parameters:

Name: **CXNGFW**

IP Address: **10.10.2.5**

Mask: **32**

Shared secret: **cisco123**



Click **Save**.

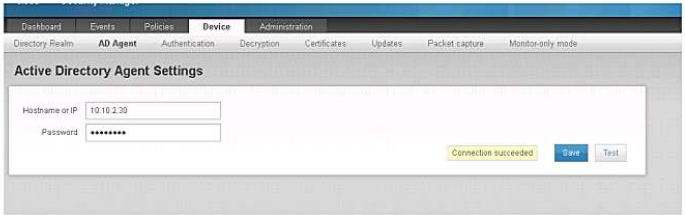
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 3

Return to the PRSM GUI (https://10.10.2.5) on the Admin PC, and navigate to the **Device > AD Agent** screen to add the Cisco CDA in the ASA CX. Add the Cisco CDA using the following parameters:

A) For Hostname or IP, enter **10.10.2.30**.

B) For Password, enter **cisco123**.



Click **Test**. The test should be successful.

Click **Save** and commit your changes.

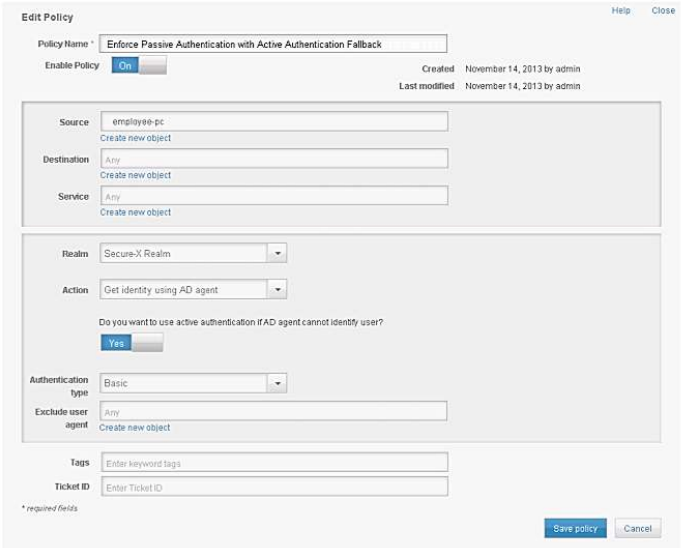
Step 4

Modify the existing identity policy to use passive authentication first. From the PRSM GUI, navigate to the **Policies > Policies** screen and scroll down to the **Identity** section. Hover your cursor over the **Enforce Active Authentication** identity policy that you created in the previous lab task and click **Edit Policy:**

Change the policy name to **Enforce Passive Authentication with Active Authentication Fallback**.

Change the action to **Get Identity Using AD Agent**.

Choose **Yes** for Do you want to use active authentication if AD agent cannot identify user?



Click the **Save Policy** button and commit your configuration changes.

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

Step 5

Test the passive authentication operations:

Restart the Employee PC.

Log in to the Employee PC as the **it1** Active Directory user in the **secure-x** domain with the **cisco** password.

From the Employee PC, open Firefox and browse to www.yahoo.com. You should not be asked to actively authenticate.

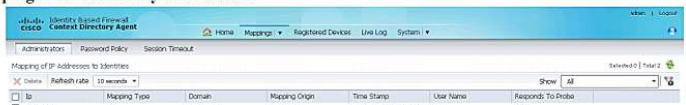
NOTE: If passive authentication is not working, access the Cisco CDA GUI and verify the User to IP Mappings. If the Cisco CDA does not contain the **it1** Active Directory User to IP mapping, check to see if the clock is correct on the Cisco CDA and check the NTP status. If the time is off between the Cisco CDA and the AD Server, the Cisco CDA may not be getting the User to IP Mappings from the AD server.

NOTE: If passive authentication is still not working and you are still getting the active authentication login popup, restart the Employee PC but do not log into it yet, then use the CX CLI **service stop** and **service start** commands to stop and start the CX services then log in to the Employee PC as the **it1** Active Directory user in the **secure-x** domain with the **cisco** password.

```
asacx> services stop
asacx> services start
```

Step 6

Return to the Admin PC and access the Cisco CDA GUI. Verify the IP to Identity Mappings from the **Mappings > IP to Identity** CDA screen.



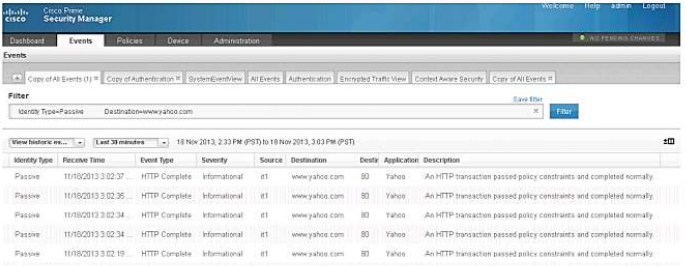
You should see the mapping between domain user **it1** and IP address of the Employee PC (**10.10.11.10** in this example).

Step 7

Examine the PRSM Events Viewer for the Passive Authentication related events:

A) From the PRSM GUI, navigate to the **Events > Events** screen. Choose the **Copy of All Events** view created from an earlier lab step. The **Copy of All Events** view should have the **Identity Type** column display added. View the historic events from the past 30 minutes.

B) Filter the display using **Identity Type=Passive** and **Destination=www.yahoo.com**.



Step 8

From the PRSM GUI, navigate to the **Events > Events** screen. Choose the **Authentication** view. View the historic events from the past 30 minutes.



You should see the **Redirect Authentication** events.

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

Step 9

Display the content of the Cisco ASA (CX) NGFW ADI session database using the **show opdata adisession** Cisco ASA (CX) NGFW CLI command.

```
asacx> show opdata adisessions
Vdi Session Directory:
============================
total_sessions: 1
contained_op_data {
realm: "Secure-X Realm"
username: "it1"
ip: "10.10.11.10"
identity_type: IDENTITY_PASSIVE
auth_type: AUTH_TYPE_NEGOTIATE
}
```

The output should include information about the **it1** user in the **Secure-X Realm** who has been authenticated passively using the Cisco CDA. Press **Ctrl-C** to exit the **show opdata adisessions** command.

Task 3: Configure an ASA CX Access Policy Using an Identity Object per the Given Requirements

In this lab task, you will configure and verify a Cisco ASA (CX) NGFW access policy using an identity object per the given requirements. You will create access policy, which will refer to the identity object, which represents Active Directory Group **IT.** Active Directory user **it1** is part of Active Directory group **IT.** You will also verify that web transactions are matched against newly created access policy.

Activity Procedure

Complete the following steps to configure and verify a Cisco ASA (CX) NGFW access policy using an identity object per the given requirements:

Step 1

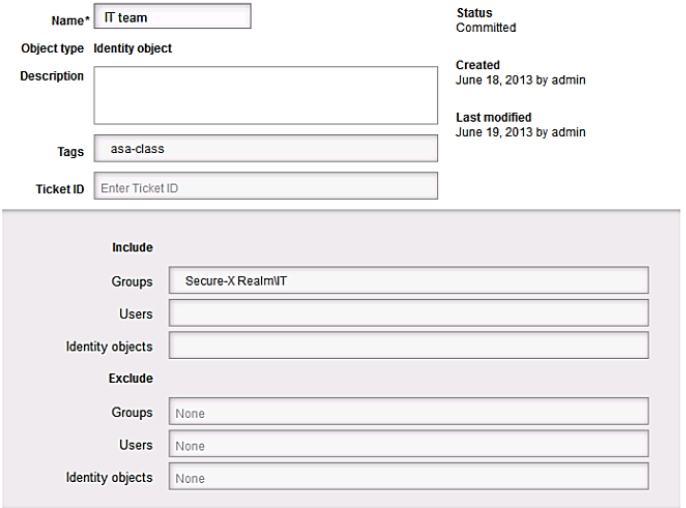
Return to Admin PC and from the PRSM GUI , navigate to the **Policies > Objects** screen to choose **Add Identity Object** from the **I want to** drop-down menu. Create identity object with these parameters:

Name: **IT team**

Tags: **asa-class**

Under Include for Group, enter **Secure-X Realm\IT**

Leave all of the other fields as the default



Click the **Save Object** button.

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

Step 2

In this lab step, you will configure an access policy to allow all of the users in the **IT** Active Directory group to download executable files but deny all of the users in the IT Active Directory group to access any websites with a bad reputation. Navigate to the **Policies > Policies** screen. Hover your cursor over the Access policy set and click the Add New Policy link. Configure an identity-based access policy with these parameters:

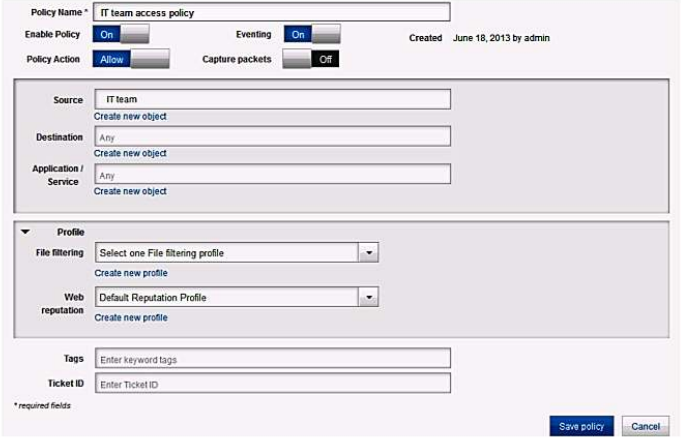
A) Policy Name: **IT team access policy**

B) For Source, select the **IT Team** identity object you created in the previous step

C) Click the word **Profile** to open the profile selection

D) For File filtering, do not select a profile

E) For Web reputation, select the **Default Reputation Profile**

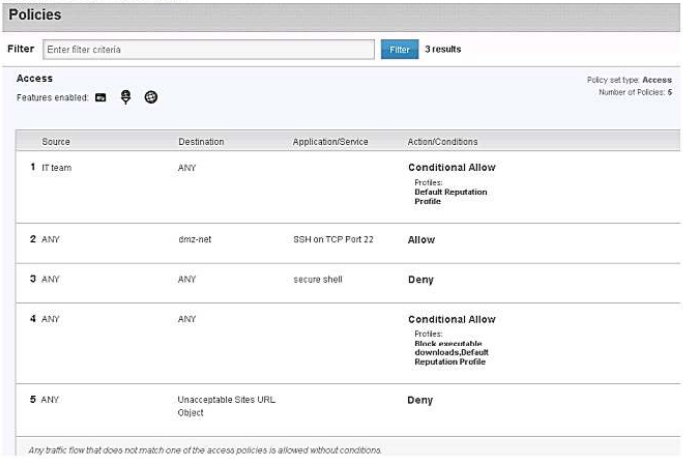


Click the **Save Policy** button and commit your configuration changes.

https://t.me/learningnets

Step 3

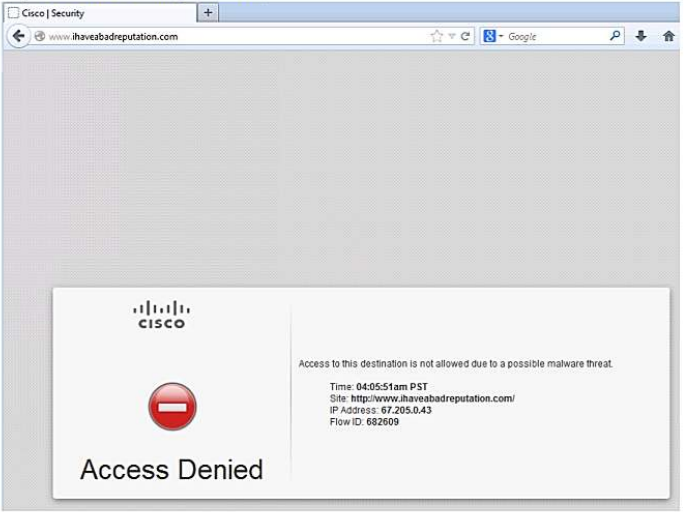
Navigate to the **Policies > Policies** screen. Move this access policy to be the first policy in the access policy set if it is not already at the top.



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

Step 4

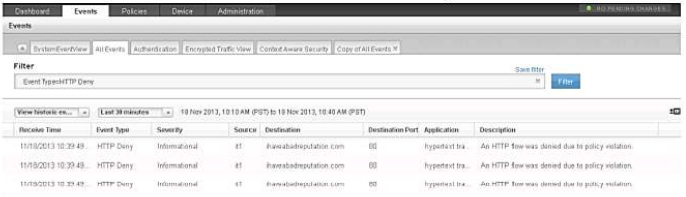
If you are not already logged in to the **Employee PC** as the **it1** secure-x domain user, log out then log in as the **it1** secure-x domain user with the **cisco** password. Test the access policy from the Employee PC by browsing to www.ihaveabadreputation.com.



This site should be blocked by the IT team access policy because this site has a low reputation score.

Step 5

Access the PRSM **Event Viewer > All Events** and use a filter to only show the **Event Type=HTTP Deny**.

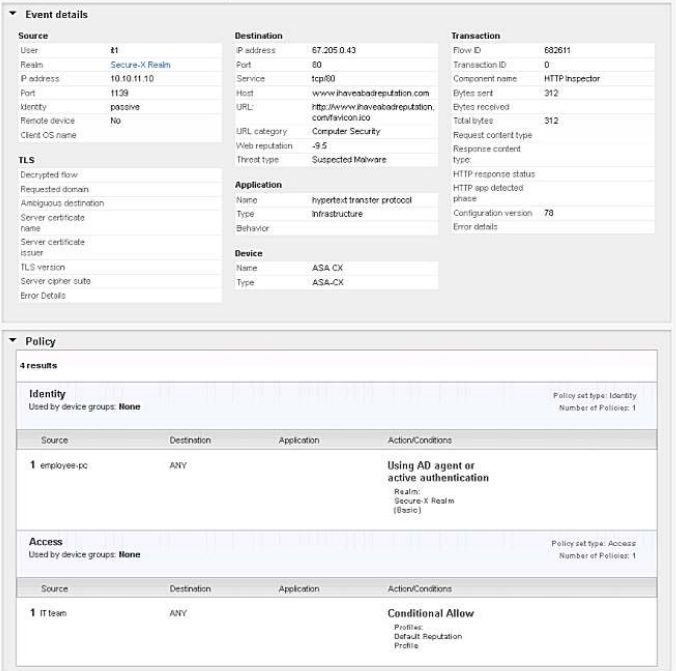


You should see the corresponding **HTTP Deny** Event with the **it1** user as the Source.

https://t.me/learningnets

Step 6

Hover the mouse over the **HTTP Deny** event and click **View Details**.



Expand the **Policy** section to confirm that HTTP transaction was matched against access policy you created earlier in this lab (with **IT team** identity object as source).

Step 7

Test the access policy from **Employee PC** again:

A) Use Firefox and browse to the DMZ Server (http://172.16.1.50 or http://dmz.secure-x.local):

B) From the DMZ server home web page, click the **Files** tab. Click on the **Windows Calculator Program (.exe)** link to try to download it. This should be successful as allowed by the **IT team** access policy.

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

Lab 1-4: Configure Cisco ASA (CX) NGFW Decryption Policy

Activity Objective

In this lab activity, you will configure and verify Cisco Adaptive Security Appliances Context Aware Next Generation Firewall decryption policy. First you will enable decryption feature globally and create self-signed certificate. After that you will configure and verify decryption policy, which will decrypt traffic for all URL categories except Finance.

After completing this activity, you will be able to:

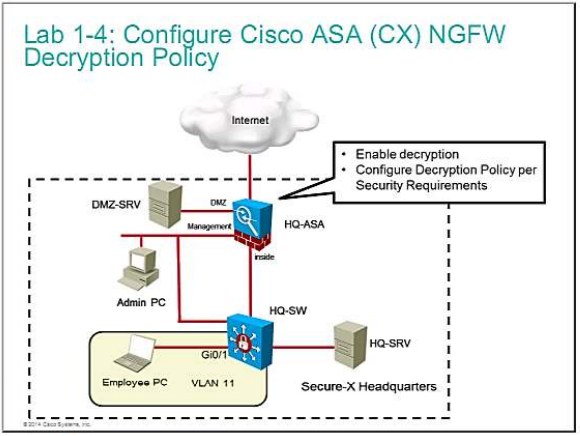
Upon completing this activity, you will be able to meet this objective:

Configure and verify decryption policy based on given security policy requirements

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

No commands are used in this activity.

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 asacx-5500x-boot-9.1.2-42.img asacx-sys-9.1.2-42.pkg
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
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**
ASA CX	**admin**	**Admin123**
AD Server (installed on HQ-SRV)	**Administrator**	**Ci5coAdmin**
ScanSafe portal (https://scancenter.scansafe.com)	**ccnpsec.scansafe@yahoo.com**	**C!sco!23**

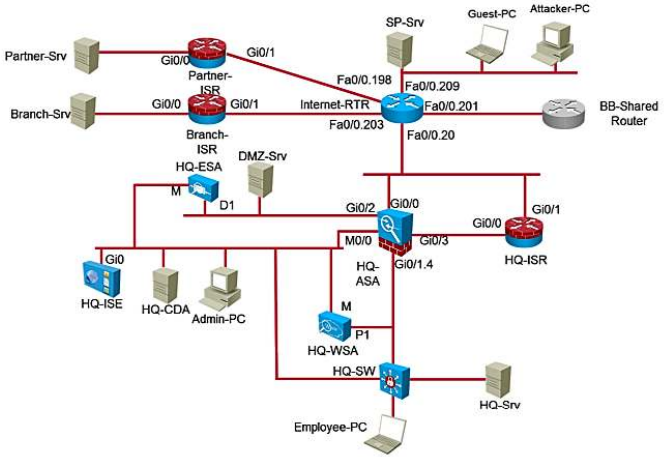
Employee PC is joined to the Active Directory domain.

AD User	AD password	AD Group	Email address in AD properties
it1	**cisco**	IT	**it1@secure-x.public**

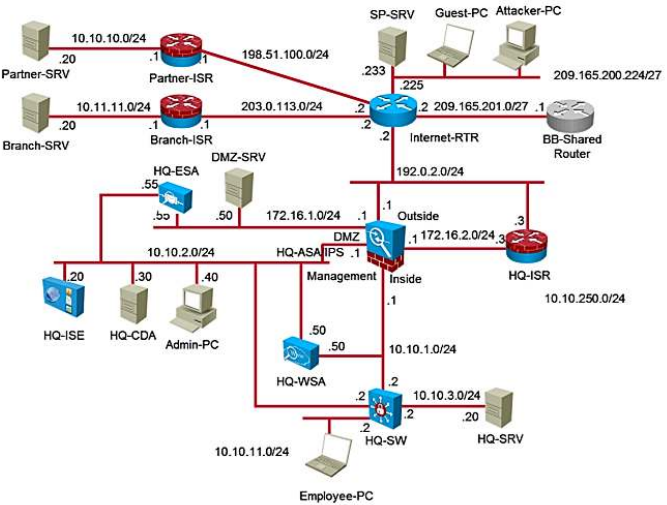
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

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

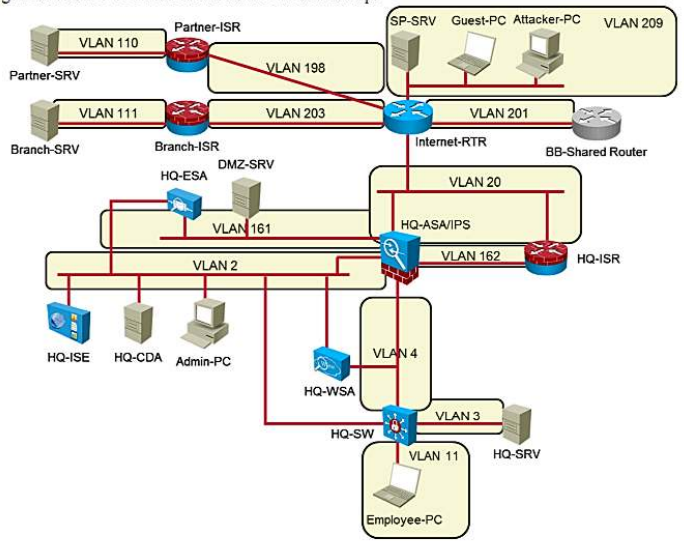


The figure shows the IP addresses that are used in this lab setup.



VLAN Setup

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



Task 1: Enable Cisco ASA (CX) NGFW Decryption

In this lab task, you will enable Cisco ASA (CX) NGFW decryption and generate a self-signed certificate.

Activity Procedure

Complete the following steps to enable Cisco ASA (CX) NGFW decryption and generate a self-signed certificate.

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

Step 1

From the AdminPC, access the PRSM GUI (https://10.10.2.5) and log in using **admin** username and **Admin123** password. Navigate to the **Device > Decryption** screen to enable the TLS/SSL proxy on the Cisco ASA (CX) NGFW and generate a self-signed certificate. Set the certificate fields as follows:

Set Enable Decryption Policies to **On**.

Set the Certificate Initialization method to **Generate**.

Common name: **asacx.secure-x.local**

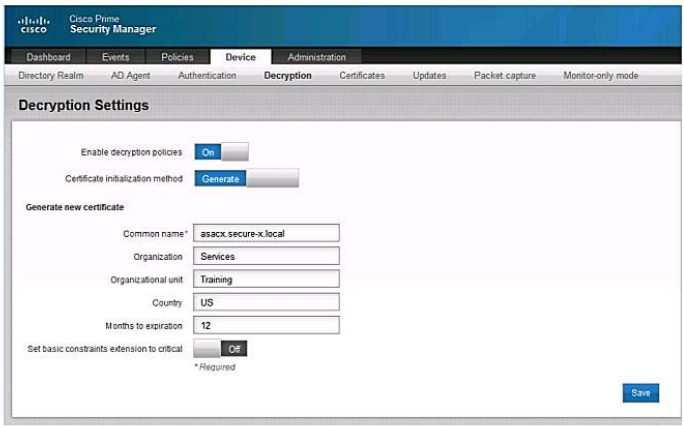
Organization: **Services**

Organization unit: **Training**

Country: **US**

Months to expiration: **12**

Set basic constraints to critical: **Off**



Click the **Save** button. Commit your configuration changes.

Task 2: Configure a Cisco ASA (CX) NGFW Decryption Policy per Security Requirements

In this lab task, you will configure and verify a Cisco ASA (CX) NGFW decryption policy per the given security requirements. You will configure decryption policy, which will decrypt traffic for all URL categories except **Finance**.

Activity Procedure

Complete the following steps to configure and verify a Cisco ASA (CX) NGFW decryption policy per the given security requirements:

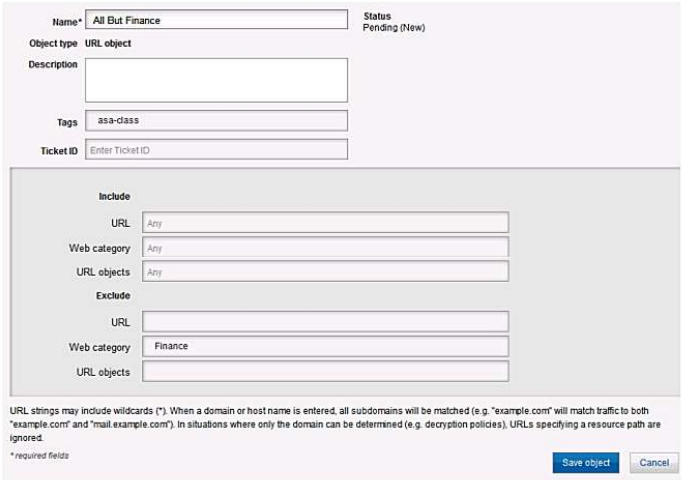
Step 1

Create a URL object that matches all web categories except the Finance web category. From the PRSM GUI, choose **Policies > Objects**. Choose **Add URL object** from the **I want to** drop-down list to create URL object with following parameters:

Name: **All But Finance**.

Tags: **asa-class**.

Under **Exclude**, for the Web category choose **Finance**.



Click the **Save Object** button and commit your configuration changes.

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

Step 2

Configure a decryption policy to decrypt all HTTPS traffic sourced from the Employee-PC IP address to all destinations except for financial-type websites. From the PRSM GUI, choose **Policies > Policies**. Hover your cursor over the Decryption policy set, and then click the **Add New Policy** link. Create decryption policy with following parameters:

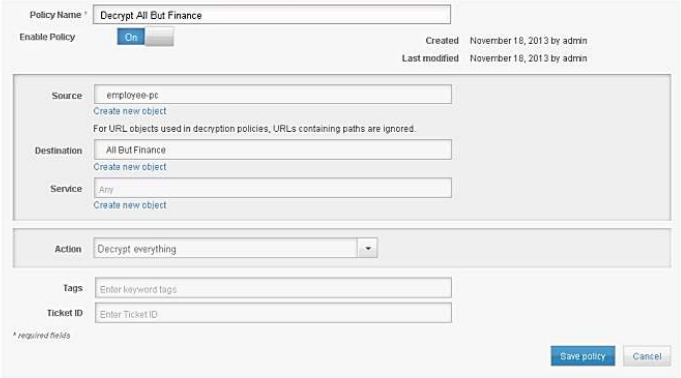
Policy Name: **Decrypt All But Finance**

For the source, choose the **CX Network Group** object to match the Employee-PC IP address. You should have already created a CX Network Group object to match the Employee-PC IP address in the Identity Policy lab.

For Destination, choose the **All But Finance URL** object.

For Action, choose **Decrypt Everything**.

Leave all other fields at their default settings.



Click the **Save Policy** button and commit your configuration changes.

Step 3

Restart the Employee PC and log in as the **it1 secure-x** domain user with the **cisco** password.

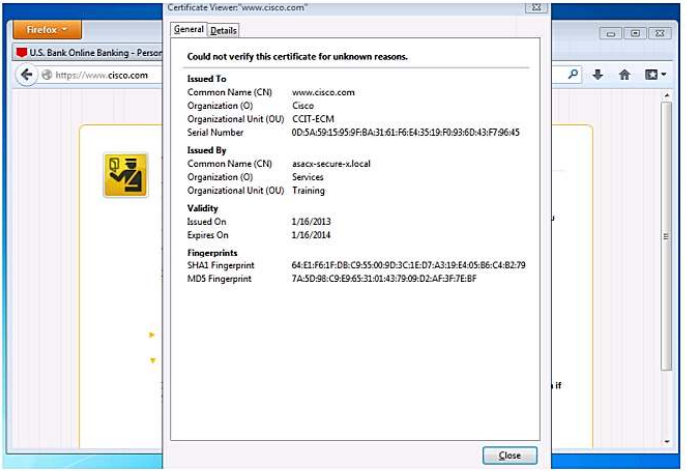
https://t.me/learningnets

Step 4

From the Employee PC, use Firefox and browse to https://www.cisco.com (nonfinancial-type secured website) to test the decryption policy. Since we have not exported and imported the ASA CX self-signed certificate to the Employee PC, you should get a certificate warning. Follow these instructions:

A) View the certificate

B) Accept the certificate warning



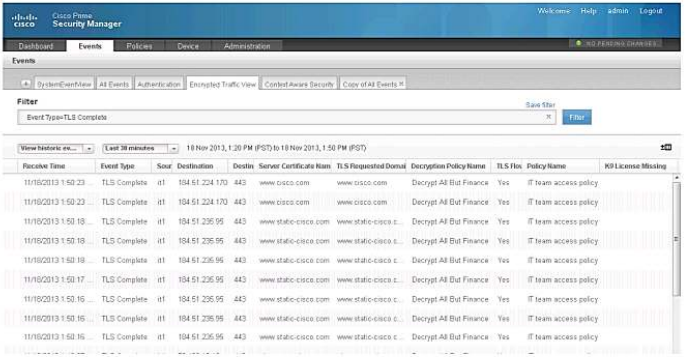
You should see the certificate issued to https://www.cisco.com was issued by **asacx-secure-x.local.** The Cisco ASA (CX) NGFW should be performing decryption, because https://www.cisco.com is not a financial-type website. The Cisco ASA (CX) NGFW should be acting as the "man in the middle" between the client browser and the destination web server.

NOTE: Without the K9 license installed on the Cisco ASA (CX) NGFW, web sites requiring strong encryption like using AES will not be supported.

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

Step 5

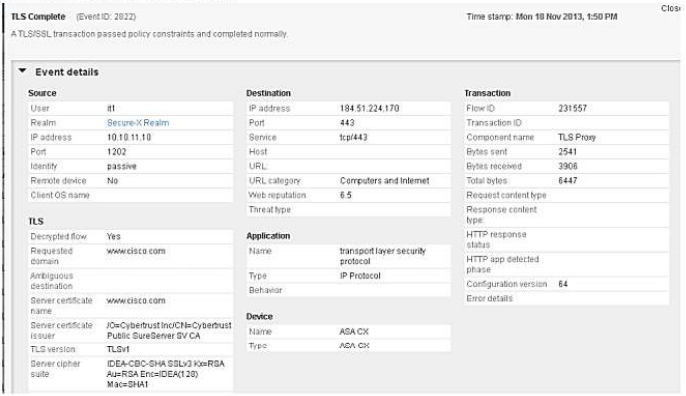
Return to the Admin PC. From the PRSM GUI, choose **Events > Events**. Choose the **Encrypted Traffic View** tab. View the historic events from the past 30 minutes. Filter the display using **Event Type=TLS Complete**.



https://t.me/learningnets

Step 6

To get more detail information about the **TLS Complete** event from the preceding step, hover your cursor over that event and click **View Details**.

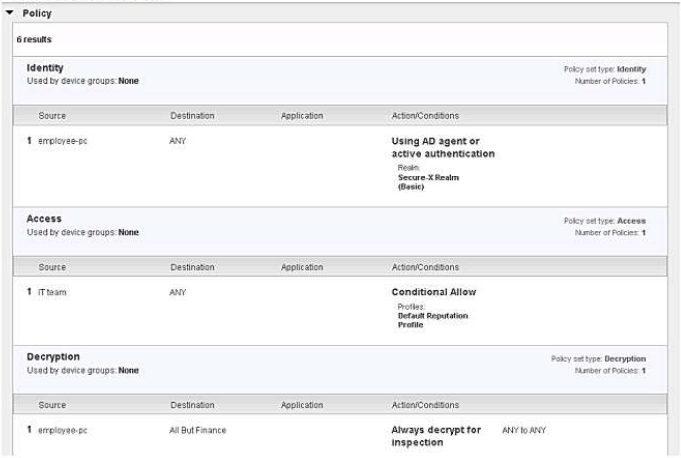


Examine the source IP address and port, Identity type, TLS version, Server cipher suite, destination IP address and port, and the URL category. You should also see **Yes** for **TLS Decrypted flow** because the flow to https://www.cisco.com should have been decrypted since https://www.cisco.com is not a financial-type website.

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

Step 7

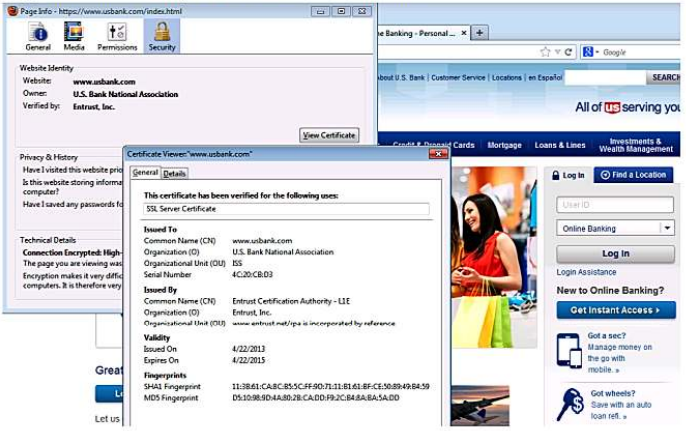
Expand the **Policy** section od **TLS complete** detailed window to see the matched identity policy, access policy and decryption policy.



You should see matched decryption policy you created earlier.

Step 8

From the Employee PC, use Firefox and browse to https://www.usbank.com (financial-type secured website) to test the decryption policy. Right-click somewhere in the web page that is not an image. Choose **View Page Info**. Click **Security** and then click **View Certificate.**



You should see the certificate that was issued to https://www.usbank.com and that was issued by a trusted public CA (such as Entrust Certificate Authority).The certificate your browser received should be the certificate from https://www.usbank.com.

The Cisco ASA (CX) NGFW should not be performing any decryption because this is a financial-type website.

Step 9

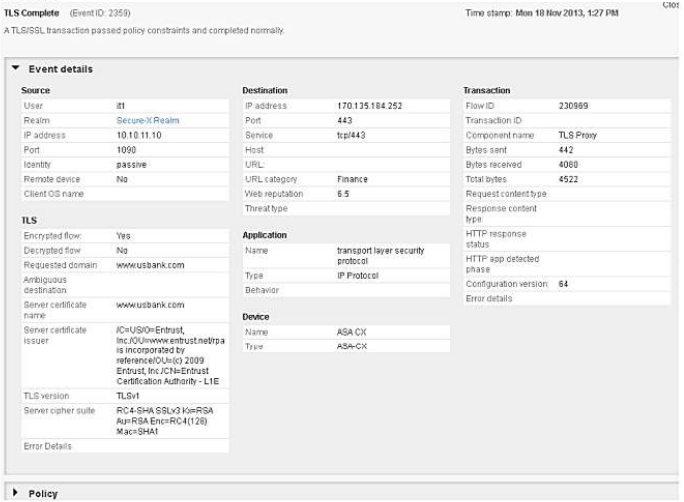
Return to the Admin PC. From the PRSM GUI, choose **Events > Events**. Choose the **Encrypted Traffic View** tab. View the historic events from the past 30 minutes. Filter the display using **Event Type=TLS Complete** and **Server Certificate Name=www.usbank.com**



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

Step 10

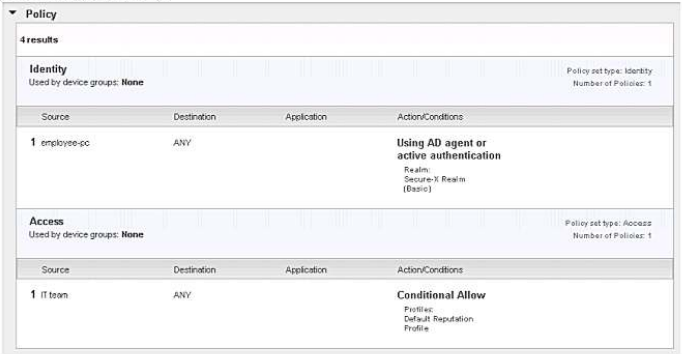
To get more detail information about the **TLS Complete** event, hover your cursor over the event and click **View Details**.



Examine the source IP address and port, identity type, TLS version, Server cipher suite, destination IP address and port, and the URL category. You should also see **No** for **TLS Decrypted flow** since the flow to https://www.usbank.com should not have been decrypted. It is a financial-type website.

Step 11

Expand the **Policy** section of **TLS complete** detailed window to see the matched identity policy, access policy and decryption policy.



You should see that there is no match against decryption policy as you are accessing financial-type website.

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

Lab 2-1: Configure Cisco Web Security Appliance Explicit Proxy and User Authentication

Activity Objective

Lab Scenario: The CSO is looking into deploying a Web security solution to provide outbound Web usage controls at some of the branch offices. The CSO asked the network security team to test a solution using the Cisco WSA in some of the branch offices with an existing Cisco ASA 5510 (instead of upgrading the Cisco 5510 to the Cisco 5500-X with the NFGW services). You will test the Cisco WSA on the Secure-X test lab using a virtual WSA for testing purposes.

In this lab exercise, you will deploy the Cisco Web Security Appliance to secure the Web-related connectivity. To prepare the Cisco Web Security Appliance for management access and configure basic settings, the system setup wizard has been used to bootstrap the Cisco Web Security Appliance by your instructor. You will first deploy the web proxy in the explicit proxy mode. Further, you will control web access by enforcing client authentication.

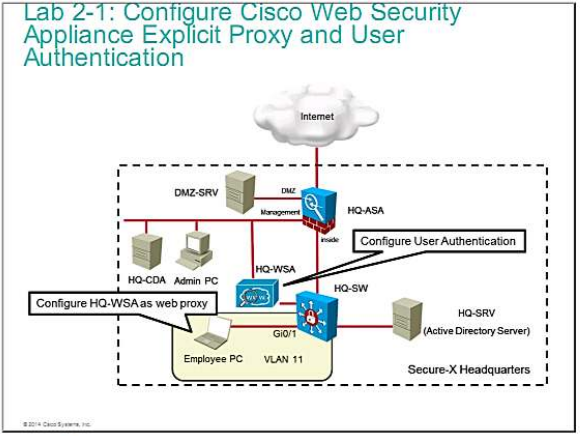
In this activity, you will implement the Cisco Web Security Appliance. Upon completing this activity, you will be able to meet these objectives:

- Deploy the Cisco WSA in Explicit Proxy Mode
- Implement User Authentication using Basic Authentication
- Implement Transparent User Authentication

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

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
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.

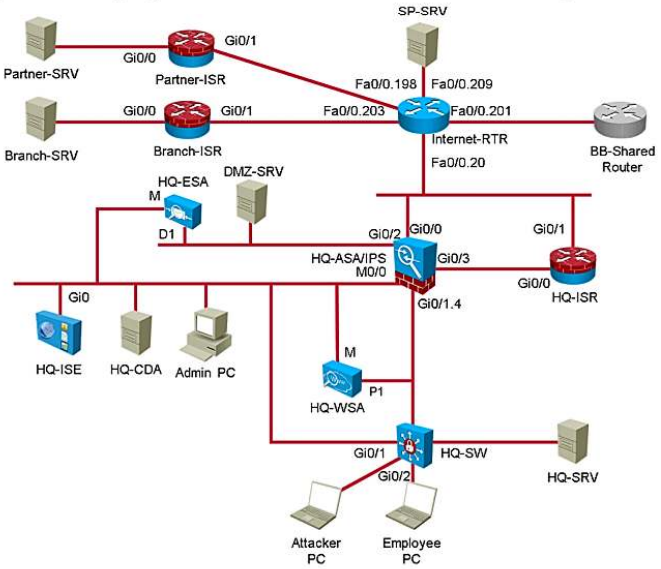
Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

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**
ASA CX	**admin**	**Admin123**
AD Server (installed on HQ-SRV)	**Administrator**	**Ci5coAdmin**

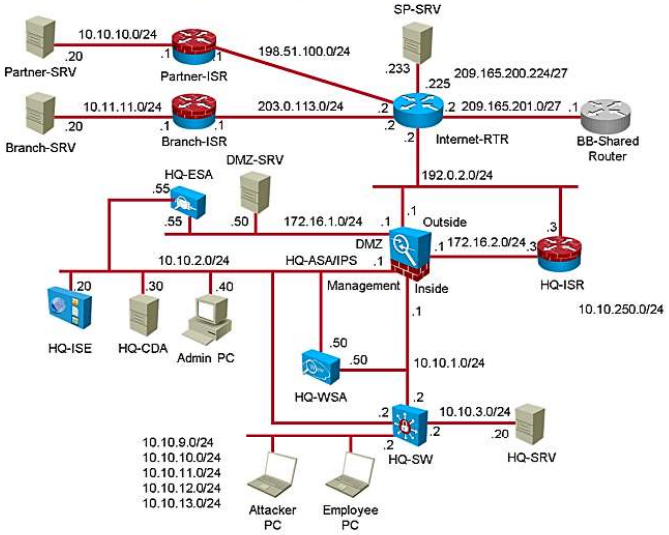
Topology and IP Addressing

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



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

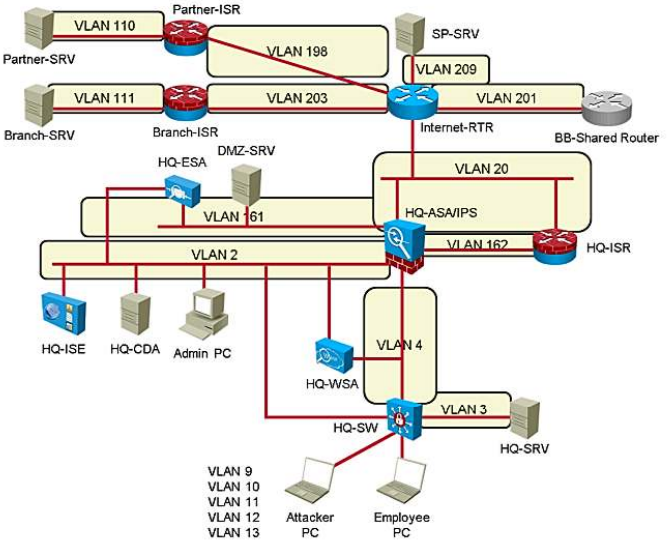
The figure shows the IP addresses that are used in this lab setup.



https://t.me/learningnets

VLAN Setup

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



Task 1: Verify Basic Cisco WSA Settings

In this lab task, you will verify the basic Cisco WSA settings. HQ-WSA has been pre-configured with basic settings, which will guarantee you IP connectivity.

Note The Cisco WSA has been deployed by your instructor using the system setup wizard for explicit proxy mode with the default settings that has been slightly modified to enable management access. In this task you will connect to the Cisco WSA GUI using HTTPS and CLI (via SSH). You will also make sure that the Cisco WSA has the required feature keys.

Activity Procedure

Complete the following steps:

Step 1

Connect to the console of the HQ-ASA. Remove the policy map and service policy that was used to redirect traffic to ASA CX module.

```
no service-policy asacx_policy interface inside
no policy-map asacx_policy
```


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

Step 2

Test Web Connectivity without the Cisco WSA proxy. Connect to the Employee PC, log in as the **it1** secure-x domain user with the **cisco** password. Open **Internet Explorer**, and check Internet connectivity by going to http://www.cisco.com. The connection should succeed.

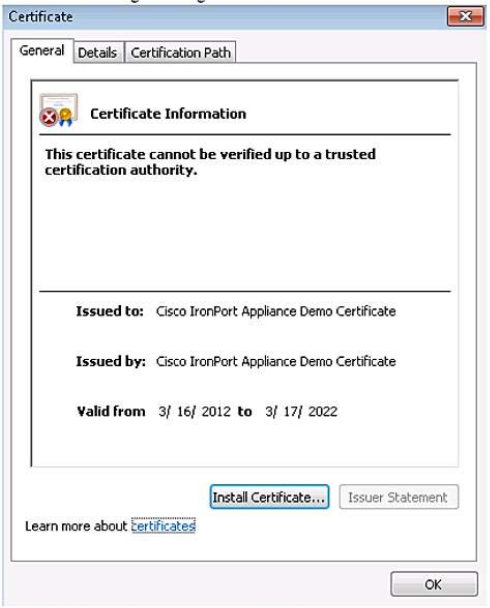
https://t.me/learningnets

Step 3

Connect to the Admin PC (**student**/**Ci5coAdmin**) and start the Cisco WSA management GUI.

A) Open **Internet Explorer**, and connect to the Cisco WSA management GUI (https://wsa-mgmt.secure-x.local).

B) If presented with a certificate warning, accept the certificate security warning. The Cisco WSA has not been enrolled to the PKI and is using a self signed certificate.

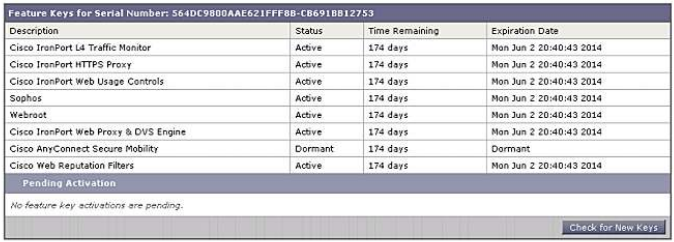


C) Log in to the Cisco WSA GUI as the **admin** user with the **Ci5coAdmin** password.

D) Choose **System Administration > Feature Keys**. You should see the various activated features.

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

Feature Keys



Feature Keys for Serial Number: S64DC9800AAE621FFF8B-CB691BB12753

Description	Status	Time Remaining	Expiration Date
Cisco IronPort L4 Traffic Monitor	Active	174 days	Mon Jun 2 20:40:43 2014
Cisco IronPort HTTPS Proxy	Active	174 days	Mon Jun 2 20:40:43 2014
Cisco IronPort Web Usage Controls	Active	174 days	Mon Jun 2 20:40:43 2014
Sophos	Active	174 days	Mon Jun 2 20:40:43 2014
Webroot	Active	174 days	Mon Jun 2 20:40:43 2014
Cisco IronPort Web Proxy & DVS Engine	Active	174 days	Mon Jun 2 20:40:43 2014
Cisco AnyConnect Secure Mobility	Dormant	174 days	Dormant
Cisco Web Reputation Filters	Active	174 days	Mon Jun 2 20:40:43 2014

Pending Activation

No feature key activations are pending.

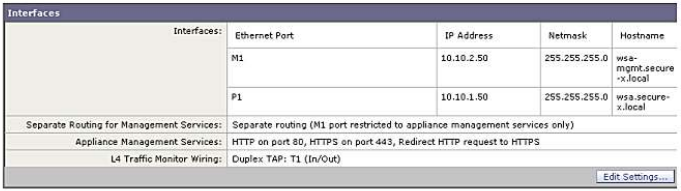
Check for New Keys

Step 4

In the Cisco WSA GUI, review the settings that have been applied with the system setup wizard by your instructor.

A) Choose **Network > Interfaces**. Examine the IP addresses and hostnames of the management (M1) and data (P1) interfaces.

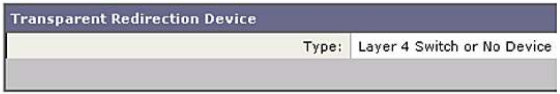
Interfaces



You should see that HQ-WSA uses two different interfaces, one for management traffic (M1) and one for data traffic (P1).

B) Choose **Network > Transparent Redirection**. For explicit proxy operations, it should be set to **Layer 4 Switch or No Device**.

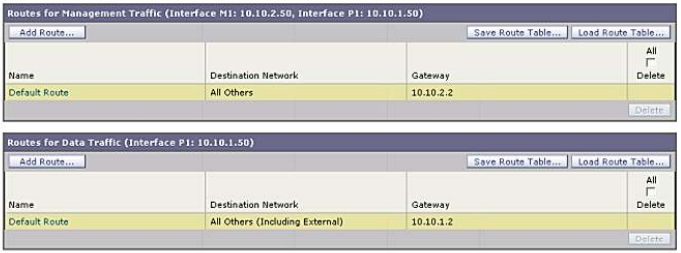
Transparent Redirection



You should see that transparent redirection (WCCP) is not configured.

C) Choose **Network > Routes**. Examine the default gateways for both interfaces.

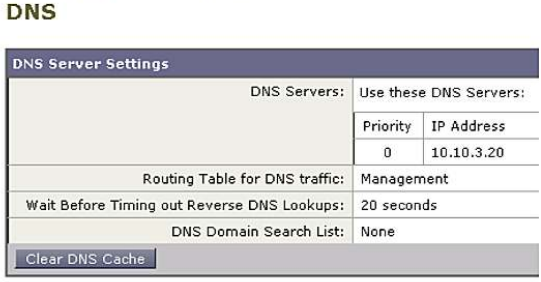
Routes



You should see that default gateways for management and data traffic point to the corresponding **vlan** interfaces on the HQ-SW where the management interface default gateway should be 10.10.2.2 and the data interface default gateway should be 10.10.1.2.

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

D) Choose **Network > DNS** to verify DNS settings.

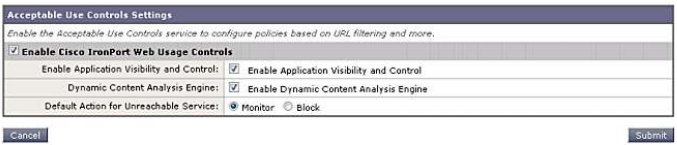


The DNS server should be set to the HQ-srv IP address (10.10.3.20). The default setting is to use the management routing table for DNS traffic.

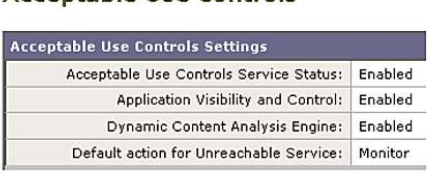
E) Choose **Security Services > Policy Service > Acceptable Use Controls**. If any settings of **Acceptable Use Controls** are not enabled in your pod, click **Edit Global Settings.**



F) Enable **Web Usage Controls**, **Application Visibility and Control** and **Dynamic Content Analysis Engine**.



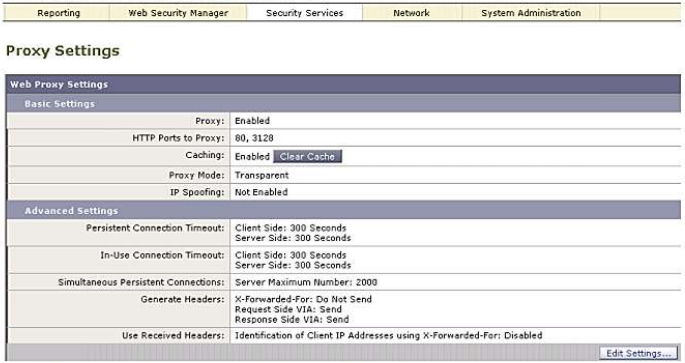
Click **Submit** then **Commit** the changes.



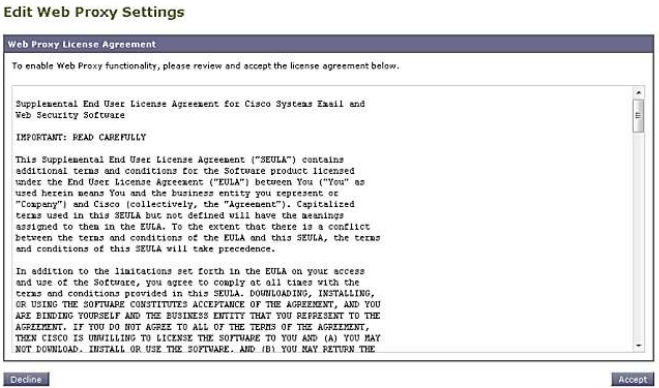
https://t.me/learningnets

Note In the lower part of the **Security Services > Policy Service > Acceptable Use Controls** page, you can see the current version information of the individual controls. If you are using the learning@cisco lab, due to the internal demo Cisco WSA license installed, you may see the new updates failing.

G) Choose **Security Services > Web Proxy** and examine the web proxy ports. You should see the default ports 80 and 3128. Click the **Edit Settings** button.



H) **Accept** the Web Proxy license agreement and **Commit** the changes.



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

Step 5

Verify Cisco WSA Basic Network Connectivities. From the Admin PC, connect to the Cisco WSA CLI (wsa-mgmt.secure-x.local) via SSH using Putty. Log in as **admin** with password **Ci5coAdmin**.

A) Test the name resolution using **nslookup** tool:

```
wsa.secure-x.local> nslookup
Please enter the host or IP address to resolve.
[]> cisco.com
Choose the query type:
1. A       the host's Internet address
2. CNAME   the canonical name for an alias
3. MX      the mail exchanger
4. NS      the name server for the named zone
5. PTR     the hostname if the query is an Internet address,
 otherwise the pointer to other information
6. SOA     the domain's "start-of-authority" information
7. TXT     the text information
[1]> 1
A=72.163.4.161 TTL=21h 48m 32s
```

You should see that **cisco.com** is resolved into IP address.

B) Test Internet connectivity using the ping utility from data interface.

```
wsa.secure-x.local> ping
Which interface do you want to send the pings from?
1. Auto
2. Management (10.10.2.50/24: wsa-mgmt.secure-x.local)
3. P1 (10.10.1.50/24: wsa.secure-x.local)
[1]> 3
Please enter the host you wish to ping.
[]> cisco.com
Press Ctrl-C to stop.
PING cisco.com (72.163.4.161) from 10.10.1.50: 56 data bytes
36 bytes from l3-sw.secure-x.local (10.10.1.2): Redirect Network(New addr:
10.10.1.1)
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 928f   0 0000  40  01 8f9a 10.10.1.50  72.163.4.161
64 bytes from 72.163.4.161: icmp_seq=0 ttl=241 time=50.793 ms
```

Test should be successful. Interrupt the ping using the **Ctrl-C** key combination.

Task 2: Implement the Cisco WSA in Explicit Proxy Mode

In this lab task, you will deploy the Cisco WSA in the explicit proxy mode. You will manually configure the web browser to send traffic to HQ-WSA web proxy.

Activity Procedure

Complete the following steps:

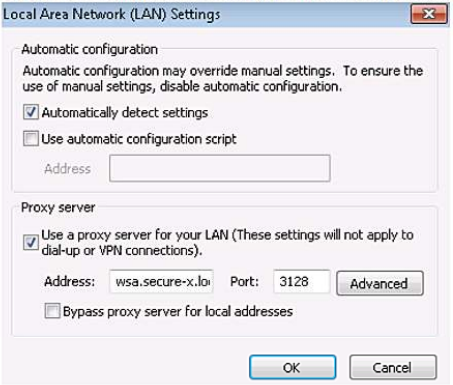
https://t.me/learningnets

Step 1

On the Employee PC, configure the proxy server in **Internet Explorer**.

A) Choose **Tools > Internet Options > Connections**. Click **LAN Settings**.

B) Set the proxy server for the LAN with the Address and port **3128**. Confirm the changes.



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

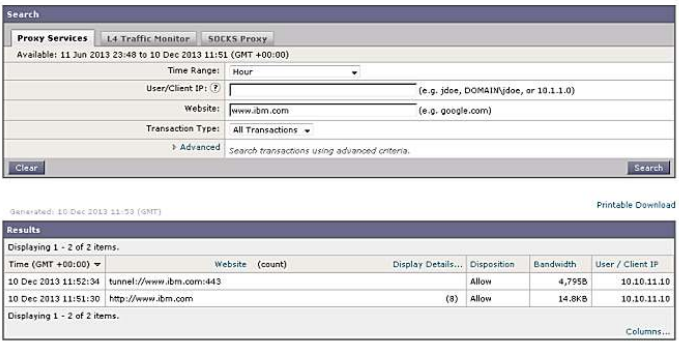
Step 2

Verify the explicit web proxy operation.

A) Open another tab in **Internet Explorer**, or close and launch the browser again. Connect to www.ibm.com. The connection should work. If it fails, make sure the Acceptable Use Control feature is enabled and the Web Proxy license agreement has been accepted (both should have be completed in the earlier steps).

B) From the Admin PC, access the Cisco WSA GUI, choose **Reporting > Reporting Services > Web Tracking**. Make sure that the **Proxy Services** tab is selected and search all events for accessing **www.ibm.com** website within the last hour.

Web Tracking



You should see the access attempts to http://www.ibm.com which was sourced from IP address of Employee PC (**10.10.11.10** in this example).

C) Generate more access attempts by connecting from the Employee PC to several sites, for example, www.cisco.com, www.microsoft.com.

D) Choose **Reporting > Reporting Services > Web Tracking** and search for all events again. You should see the accessed to the different websites.

Task 3: Implement User Authentication with Active Directory using Basic Authentication

In this lab task, you will configure an identity in the Cisco WSA to use the basic authentication method to actively authenticate the users against the Active Directory. You will test authentication by browsing to various websites from the Employee PC, where you will get prompted by the Cisco WSA to enter the log in credentials to be authenticated.

Activity Procedure

Complete the following steps to add a new identity which will require authentication:

https://t.me/learningnets

Step 1

Verify if the Cisco WSA Active Directory account already exist.

Connect to HQ-srv (**administrator/Ci5coAdmin**) and choose **Start > Administrative Tools > Active Directory Users and Computers**. Go to the **DomainComputers** directory of the **secure-x.local** domain. Verify that there is no computer account for the Cisco WSA. It will be created when you configure the authentication realm on the Cisco WSA. If the account for the Cisco WSA is already there, delete it.

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

Step 2

Configure a NTLM authentication realm to support the AD server.

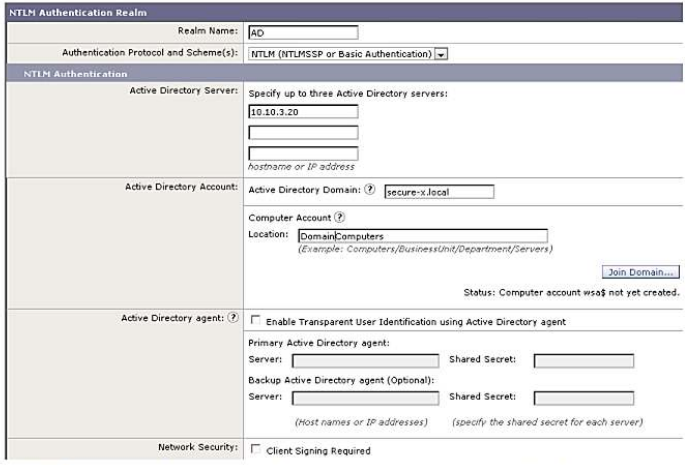
An authentication realm is a set of authentication servers (or a single server) supporting a single authentication protocol.

A) In the Cisco WSA GUI, choose **Network > Authentication**. In the **Authentication Realms** area, click **Add Realm**.

B) Create an authentication realm named **AD** with these settings:

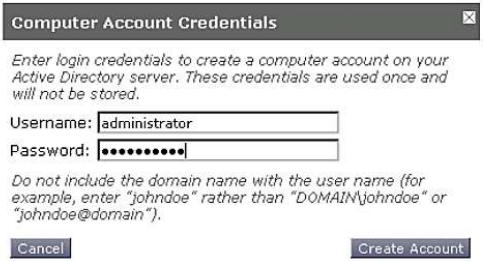
- Authentication protocol: **NTLM (NTLMSSP or Basic Authentication)**
- Active Directory server: **10.10.3.20**
- Active Directory domain: **secure-x.local**
- Computer Account location: **DomainComputers**

Add Realm

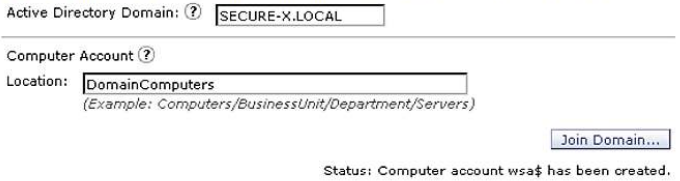


- Click the **Join Domain** button and enter the domain administrator credentials (**administrator**/**Ci5coAdmin**). Click **Create Account.**

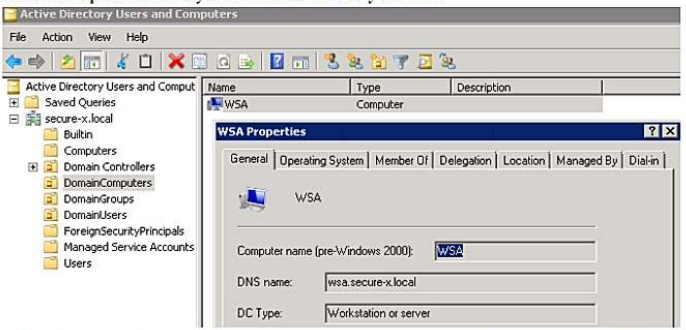
https://t.me/learningnets



- Verify the joining status. You should see that the wsa computer account has been created.



- On the HQ-srv, verify that the computer account for the Cisco WSA has been created in the **DomainComputers** directory of the **Active Directory** structure.



C) Go back to the Cisco WSA GUI, to the configuration of the authentication realm, **AD**. Click the **Start Test** button. The test should be successful.

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



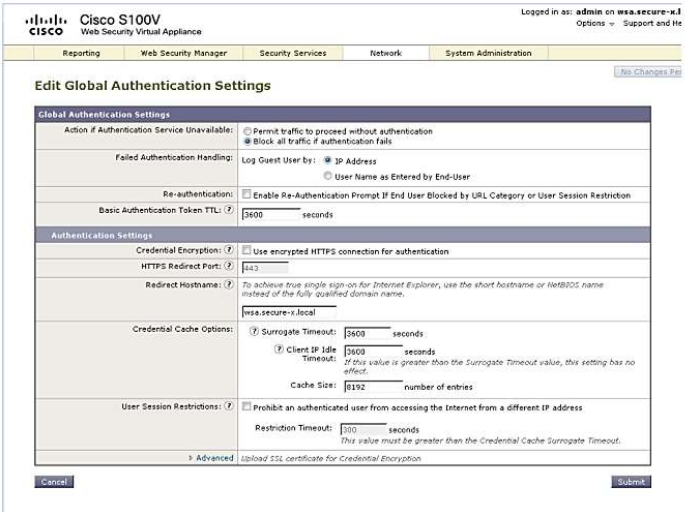
D) **Submit** then **Commit** the changes. You may get a warning message. In the Confirm window, ignore the warning and click **Submit**.

Step 3

Examine the default global authentication settings. Choose **Network > Authentication**. Click the **Edit Global Settings...**

A) Examine the default action if an authentication server is unavailable if the network connection is broken or if the authentication server is experiencing a problem.

B) Examine the default time that user credentials are stored in the cache before revalidating them with the authentication server (Basic Authentication Token TTL).



https://t.me/learningnets

Step 4

Configure a new Identity named **IT group** which will be required to use **Basic** authentication. With **Basic** authentication, the Cisco WSA will pop up a log in box when the user opens the Web browser. The passwords are sent unencrypted.

The IT group users will be identified based on the IP subnet and by the HTTP or HTTPS protocol. The IT group users should get a DHCP IP address in the 10.10.11.0/24 subnet.

You will also reference this **IT group** Identity in a later lab when you will configure an access policy for the **IT group**.

Configure new identity with these settings:

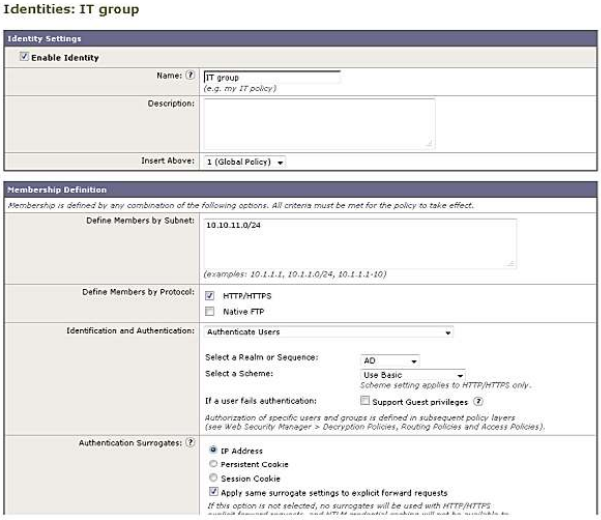
A) Choose **Web Security Manager > Authentication > Identities**. Click the **Add Identity** link.
   - The **Enable Identity** box should be checked by default.
   - Enter **IT group** as the name.
   - Under the **Membership Definition > Define Members by Subnet**:

     Enter **10.10.11.0/24** as the subnet.
   - Under the **Membership Definition > Define Members by Protocol**:

     Leave the **HTTP/HTTPS** box checked.

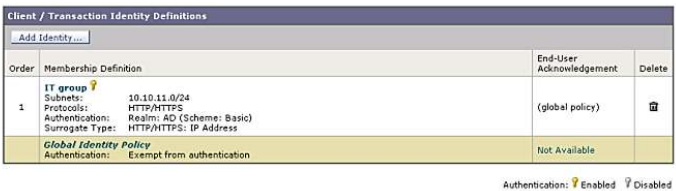
B) Under the **Membership Definition > Identification and Authentication**:
   - Choose **Authenticate Users** from the drop down menu.
   - **Realm: AD**.
   - **Scheme: Use Basic**.
   - Leave other settings at their default values.
   - Click **Submit** then **Commit** the changes.

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



Step 5

Choose **Web Security Manager > Authentication > Identities** to verify the newly created **IT group** identity.



https://t.me/learningnets

Step 6

On the Employee PC, close the Internet Explorer web browser if it is opened. Open the Internet Explorer again and try to browse to **www.cisco.com**, you should be prompted for authentication. Authenticate as the domain user **secure-x\it1** with the password of **cisco**.



After successful authentication, you should be able to browse Internet websites.

Step 7

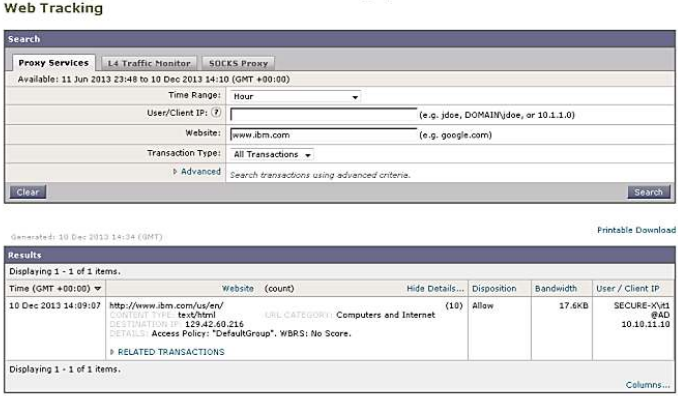
Open another tab in Internet Explorer and connect to www.ibm.com. The attempt should be successful since you have been successfully authenticated already.

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

Step 8

From the Admin PC, access the Cisco WSA GUI, choose **Reporting > Reporting Services > Web Tracking**. Make sure that the **Proxy Services** tab is selected and search all events for accessing www.ibm.com website within the last hour.

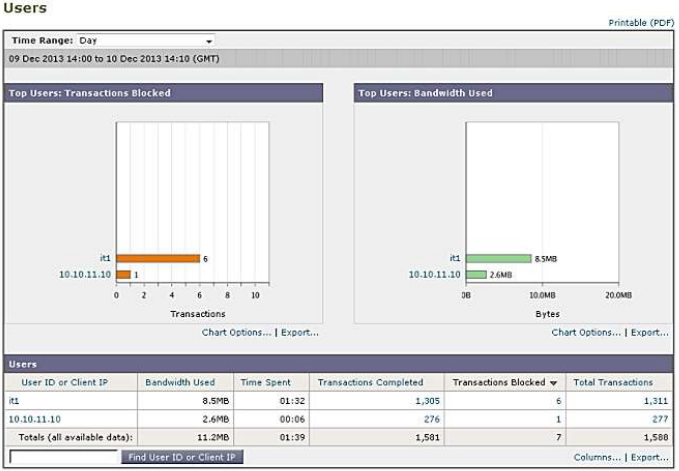
Click the **Display Details** button. You should see web transaction to **www.ibm.com** performed by **SECURE-X\it1 @AD** user with the IP address of the Employee PC.



https://t.me/learningnets

Step 9

Test how user authentication reflects the Cisco WSA reporting. Choose **Reporting > Users.** You should see per-user statistics.



You should see per user-statistics (the **it1** user in this case) when authentication is successful.

Task 4: Implement User Authentication using Transparent User Identification

In this lab task, you will change the settings on the Cisco WSA to use transparent user identification with the Cisco CDA so the users will not get prompted to enter their log in credentials to be authenticated.

Activity Procedure

Complete the following steps to enable transparent user identification:

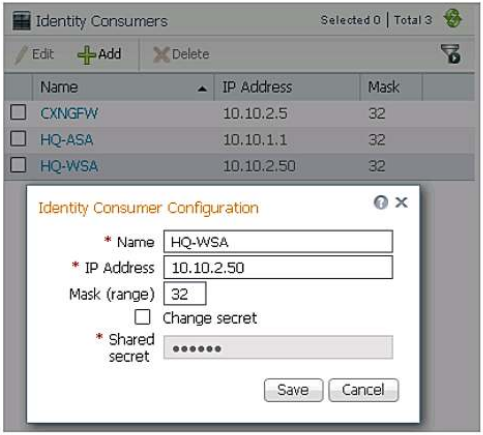
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 1

Verify the HQ-WSA has been added in the Cisco CDA as a consumer device. The HQ-CDA should already been pre-configured to communicate with the HQ-WSA using a shared secret of **cisco:**

A) From the Admin PC, use the Firefox browser to the access the CDA GUI (https://cda.secure-x.local). Log in to the CDA as the **admin** user with the **Ci5coAdmin** password

B) In the **Home** page, **Identity Consumers** section, click on **HQ-WSA** to verify the Cisco WSA consumer device configurations. The IP address should be **10.10.2.50**, mask should be **32** and the shared secret which is masked out should be configured as **cisco** already.



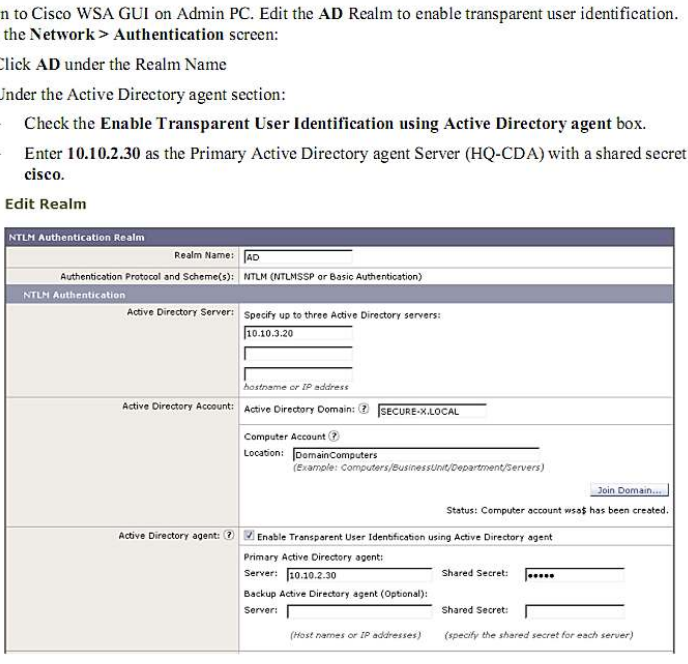
Step 2

Return to Cisco WSA GUI on Admin PC. Edit the **AD** Realm to enable transparent user identification. From the **Network > Authentication** screen:

A) Click **AD** under the Realm Name

B) Under the Active Directory agent section:

- Check the **Enable Transparent User Identification using Active Directory agent** box.
- Enter **10.10.2.30** as the Primary Active Directory agent Server (HQ-CDA) with a shared secret of **cisco**.

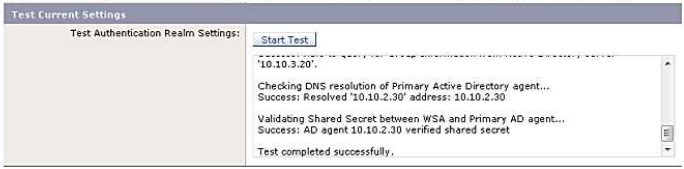


Click **Submit** then **Commit** the changes.

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

Step 3

Go back to the Cisco WSA GUI **Network > Authentication** screen and edit settings for **AD** realm. Click the **Start Test** button to test the connectivity to the AD server and to the AD Agent (HQ-CDA).



You should see that test included the verification of communication between the HQ-WSA and HQ-CDA. The test should be successful.

https://t.me/learningnets

Step 4

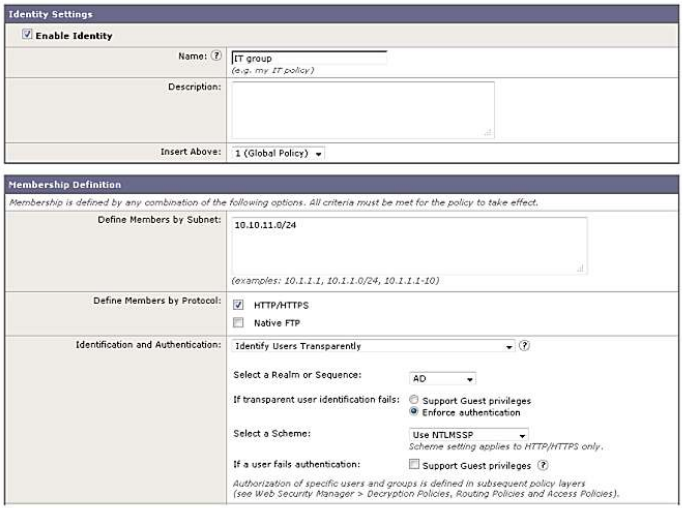
Edit the **IT group** Identity to use transparent user identification and if transparent user identification fails, enforce authentication:

A) Choose **Web Security Manager > Authentication > Identities**. Click the **IT group** Identity link.

B) Under the **Membership Definition > Identification and Authentication**:

- Choose **Identify Users Transparently** from the drop down menu.
- Realm: **AD**.
- If transparent user identification fails: select **Enforce Authentication**.
- Scheme: **Use NTLMSSP**.
- Leave all other fields as the default.
- Click **Submit** then **Commit** the changes.

Identities: IT group

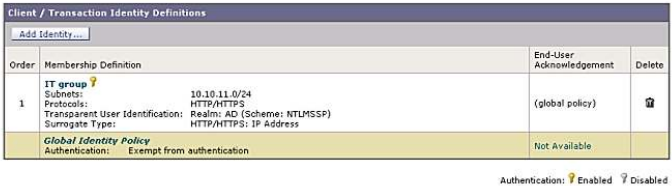


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 5

Choose **Web Security Manager > Authentication > Identities** to verify changed settings for the **IT group** identity.

Identities



You should see that transparent user identification is configured for the **IT group** identity.

Step 6

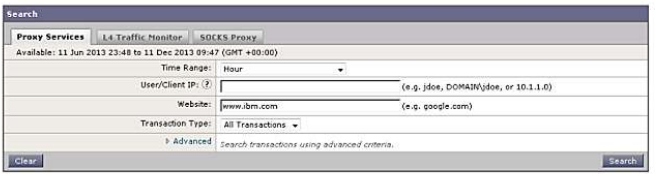
Restart the Employee PC. Log in as **it1** user in the **secure-x** domain and **cisco** password. Open Internet Explorer and connect to www.ibm.com. This should be successfully and you should not get the pop up window for entering the user credential to be authenticated.

Step 7

From the Admin PC, access the Cisco WSA GUI, choose **Reporting > Reporting Services > Web Tracking**. Make sure that the **Proxy Services** tab is selected and search all events for accessing www.ibm.com website within the last hour.

Click the **Display Details** button. You should see web transaction to www.ibm.com performed by **SECURE-X\it1** @AD user (which was **Identified Transparently**) with the Employee PC IP address.

Web Tracking

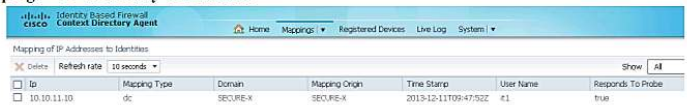




https://t.me/learningnets

Step 8

Return to the Admin PC and access the HQ-CDA GUI. Verify the IP to Identity Mappings from the **Mappings > IP to Identity** CDA screen.



You should see the mapping between domain user **it1** and IP address of the Employee PC (10.10.11.10 in this example).

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

Lab 2-2: Configure Cisco Web Security Appliance Acceptable Use Controls

Activity Objective

In this lab exercise, you will deploy Acceptable Use Controls in the Cisco WSA. Firstly, you will convert the explicit web proxy mode to transparent web proxy mode. After that, you will deploy URL filtering using predefined and custom URL categories. You will also deploy Application Visibility and Control (AVC) to block access to all Facebook applications.

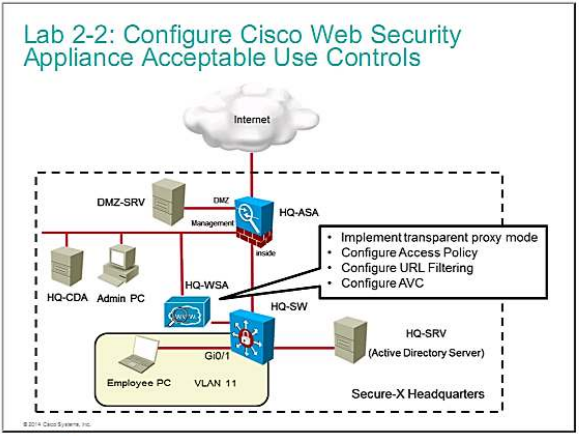
Upon completing this activity, you will be able to meet these objectives:

- Implement the Cisco WSA in transparent proxy mode
- Configure an Access Policy for the IT Group
- Enable custom URL Filtering using predefined and custom URL categories for the IT Group
- Enable AVC - Blocking Facebook for the IT Group

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

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 asacx-5500x-boot-9.1.2-42.img asacx-sys-9.1.2-42.pkg
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
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**
ASA CX	**admin**	**Admin123**
AD Server (installed on HQ-SRV)	**Administrator**	**Ci5coAdmin**
ScanSafe portal (https://scancenter.scansafe.com)	**ccnpsec.scansafe@yahoo.com**	**C!sco!23**

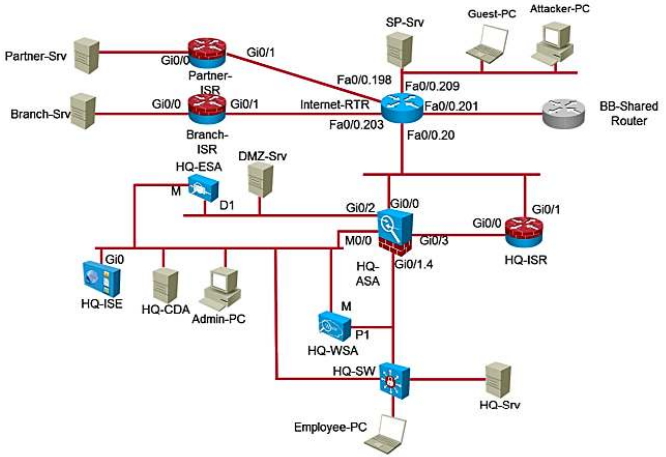
Employee PC is joined to the Active Directory domain.

AD User	AD password	AD Group	Email address in AD properties
it1	**cisco**	IT	**it1@secure-x.public**

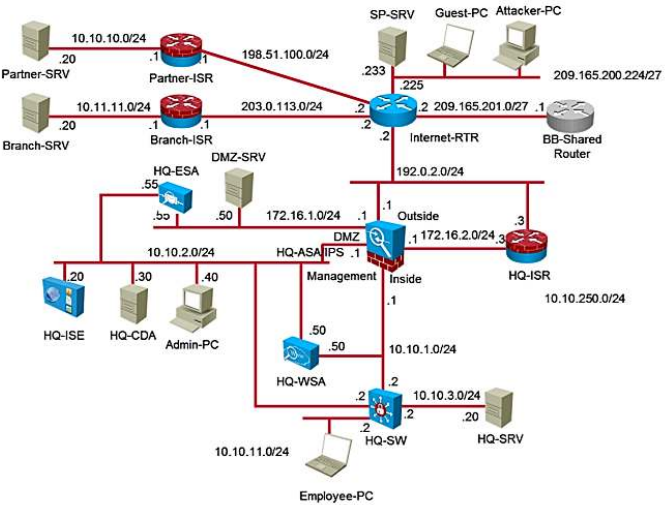
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

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

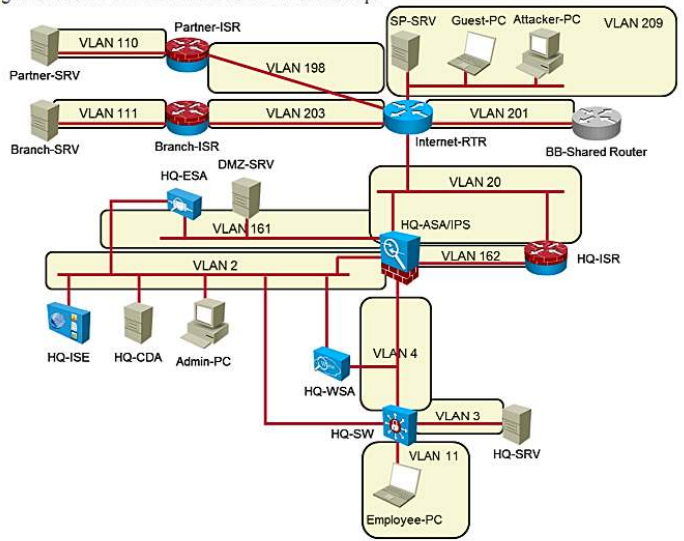


The figure shows the IP addresses that are used in this lab setup.



VLAN Setup

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



Task 1: Implement the Cisco WSA in Transparent Proxy Mode

In this lab task, you will convert the explicit web proxy mode to transparent web proxy mode. The transparent web proxy mode does not require any proxy settings in the web browsers. WCCP will be implemented on the Cisco WSA and the Cisco ASA security appliance. The Cisco ASA will intercept web traffic arriving on the inside interface and redirect to the WSA for inspection.

Activity Procedure

Complete the following steps:

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

Step 1

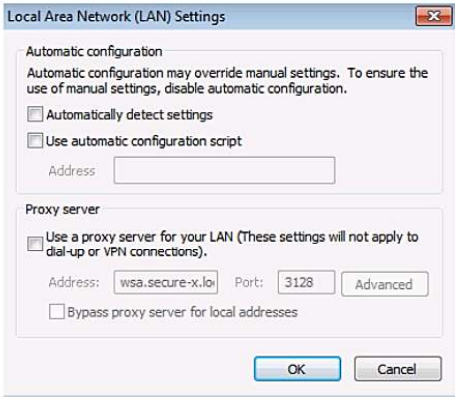
On the Employee PC log in as **secure-x** domain suer **it1** with password **cisco** and remove the proxy server configuration in **Internet Explorer**.

A) Choose **Tools > Internet Options > Connections**. Click **LAN Settings**.

B) Uncheck the **Automaticallly detect settings** checkbox

C) Uncheck the **Use a proxy server for your LAN** checkbox

D) Click **OK**.



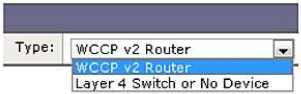
https://t.me/learningnets

Step 2

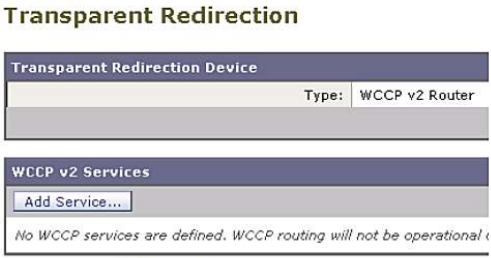
Configure WCCP on the Cisco WSA:

A) In the Cisco WSA GUI, choose **Network > Transparent Redirection** and edit the existing device (Layer 4 switch or no device.)

B) Choose the **WCCPv2 Router** and click **Submit**.



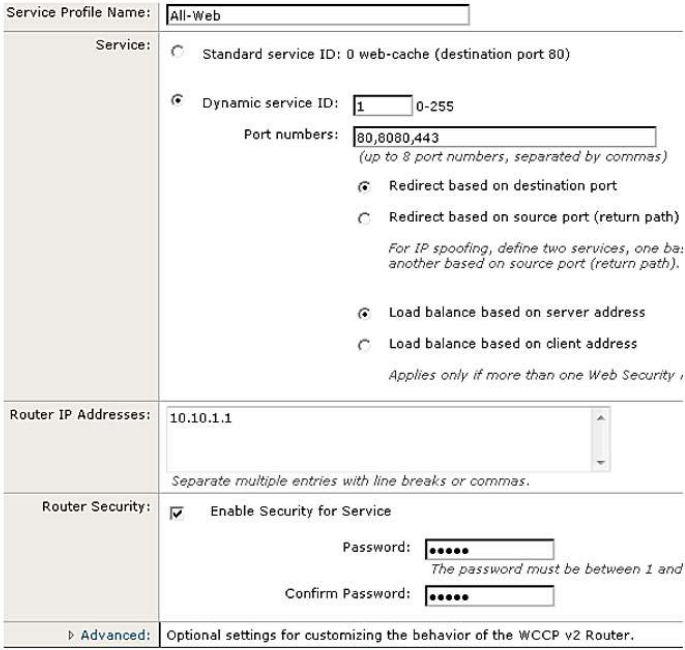
C) Click the **Add Service** button.



D) Create a service profile named **All-Web** with these settings:

- **Dynamic service ID: 1**
- **Port numbers: 80,8080,443**
- **Redirect Based on Destination Port:** enabled (checked)
- **Load Balance Based on Server Address:** enabled (checked)
- **Router IP address: 10.10.1.1** (ASA inside address)
- Enable router security using password **cisco**.

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



- Examine the **Advanced** settings but do not change their default values.
- Click **Submit**.

E) **Commit** the changes.

https://t.me/learningnets

Step 3

Configure WCCP on the Cisco ASA security appliance:

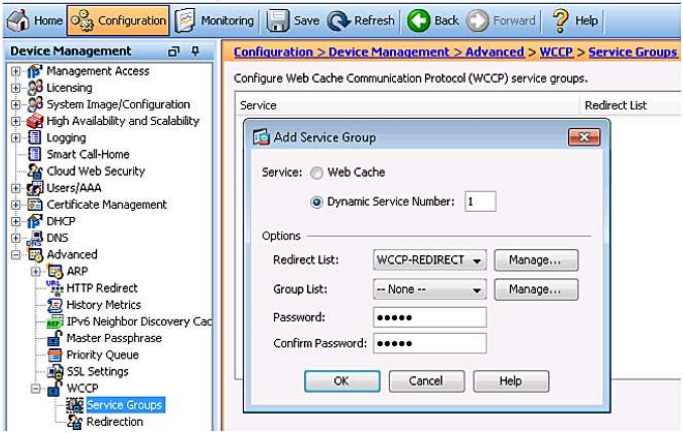
A) Launch the **Cisco ASDM-IDM Launcher** on the desktop of the Admin PC. Log in as **admin** with password **Ci5coAdmin**. Choose **Configuration > Firewall > Advanced > ACL Manager**.

B) Configure access list named **WCCP-REDIRECT**, which denies traffic from management network (10.10.2.0/24) to any destination on web ports 80,443,8080 while permits traffic from any source to any destination on web ports 80,443,8080. You can use this ACL for WCCP redirection.



C) Choose **Configuration > Device Management > Advanced > WCCP > Service Groups** and click **Add**.

D) Create a service group with the dynamic service number **1** that was previously configured on the Cisco WSA, set the Redirect List to **WCCP-REDIRECT**, and the Password identical with the one on configured the Cisco WSA (**cisco**).

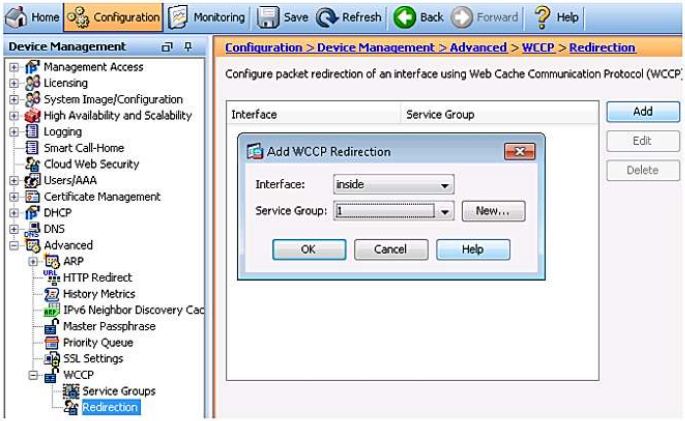


E) Click **OK**.

F) Choose **Configuration > Device Management > Advanced > WCCP > Redirection** and click **Add**.

G) Create a redirection for the inside interface with Service Group 1. This way all traffic arriving on HQ-ASA inside interface will be transparently redirected to HQ-WSA web proxy.

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



H) Click **OK** and apply the changes.

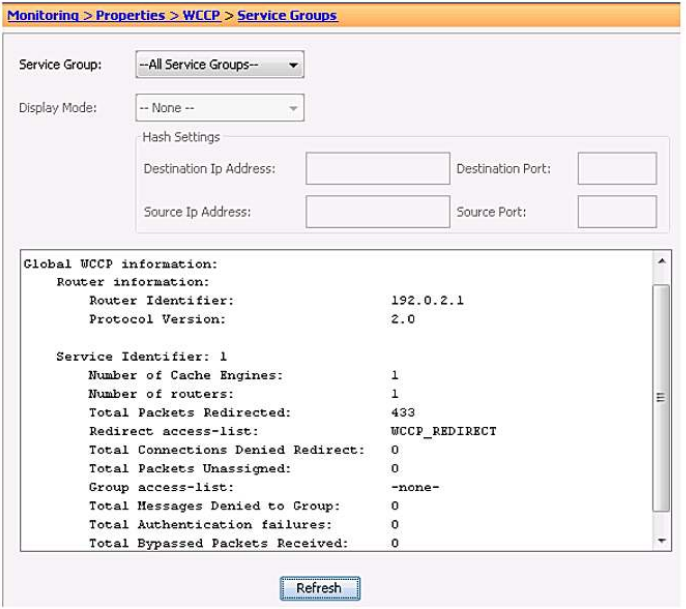
https://t.me/learningnets

Step 4

Verify the operation of WCCP:

A) Open Internet Explorer on Employee PC, and connect to www.ibm.com. The connection should work.

B) Launch to the Cisco ASDM GUI on the Admin PC. Choose **Monitoring > Properties > WCCP > Service Groups** screen to verify operation of WCCP.



You should see non-zero value for the **Total Packets Redirected** counter. The counter should increase as you initiate web traffic from the Employee PC.

Task 2: Configure the Access Policy

In this lab task, you will configure an access policy for the IT Group. You will tie identity you created early for IT group to the newly created access policy. You will also tie **IT** AD group (to which belongs domain user **secure-x\it1**) to newly created access policy.

Activity Procedure

Complete the following steps:

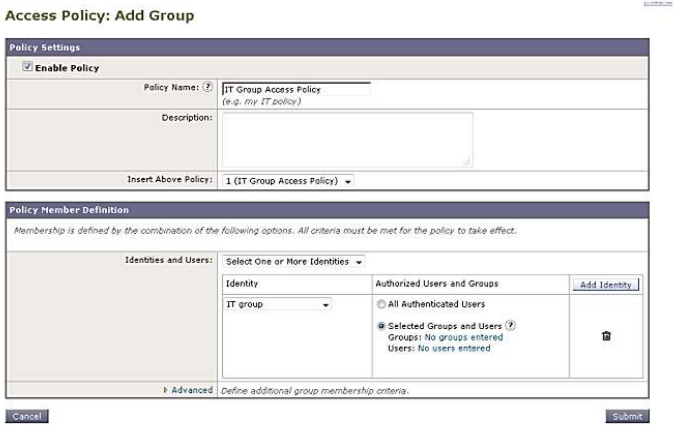
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 1

Configure an access policy for the IT Group:

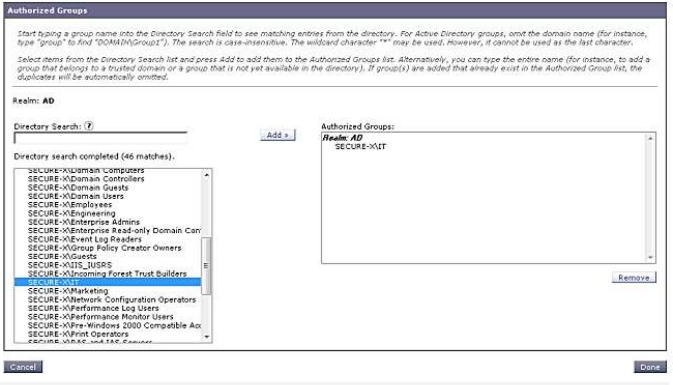
A) From the Admin PC Cisco WSA GUI, navigate to **Web Security Manager > Access Policies** and click **Add Policy...** and use these parameters:

- Use the **Policy Name** of **IT Group Access Policy**.
- Under **Policy Member Definition > Identities and Users**, choose **Select One or More Identities** from the drop down box.
- Under **Identity**, choose Select **IT group** from the drop down box. Recall the **IT group** identity was created in the previous lab.



B) Under **Authorized Users and Groups**, choose **Select Groups and Users**. Click on the **No groups entered** link next to Groups:

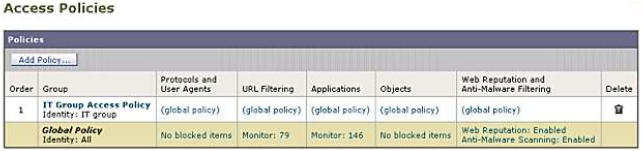
- Under **Directory search completed**, choose the **SECURE-X\IT** group from the drop down box.
- Click **Add** to add the **SECURE-X\IT** group to the **Authorized Groups**.
- Click **Done**.



C) Click **Submit** and then **Commit** the changes.

Step 2

Navigate to **Web Security Manager > Access Policies** to verify newly created access policy. By default, the new **IT Group Access Policy** will use the global policy for each of the policy setting like Protocols and User Agents, URL Filtering, Applications and etc.... In the next two tasks, you will edit the **IT Group Access Policy** to use a custom URL Filtering settings and a custom Applications settings (AVC).



Task 3: Configure URL Filtering for the Access Policy

In this task, you will deploy URL filtering using predefined and custom URL categories. You will augment the explicit proxy mode by URL filtering policies. The Cisco WSA comes with a wide range of Cisco designed filters. You will enable three predefined filter categories: Advertisements, Fashion, and Web-Based Email. You will also configure custom filters to deny access to the lab DMZ web server.

Activity Procedure

Complete the following steps:

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

Step 1

Configure URL filtering for IT Group Access Policy:

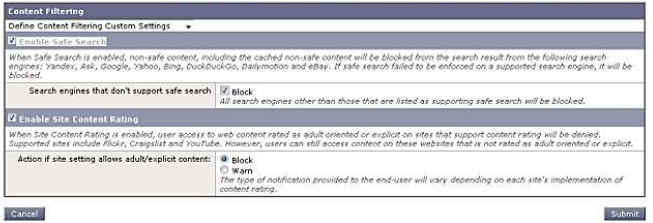
A) In the Cisco WSA GUI on Admin PC, choose **Web Security Manager > Web Policies > Access Policies**. Click the **(global policy)** link under **URL Filtering** for the **IT Group Access Policy**.



B) Block three predefined categories: **Advertisements**, **Fashion**, and **Web-Based Email**. Partial screen shot blocking **Advertisements** URL category is shown below. You should also block **Fashion** and **Web-Based Email** URL categories.



C) Scroll down to the **Content Filtering** section. Select **Define Content Filtering Custom Settings** from the drop down menu. Check the **Enable Safe Search** and **Enable Site Content Rating** check boxes.

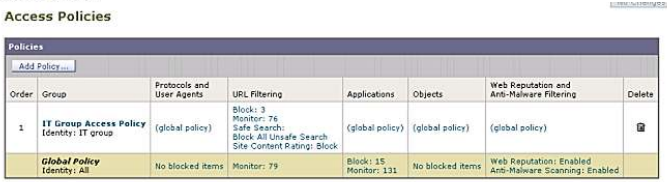


D) Click **Submit** then **Commit** the changes.

https://t.me/learningnets

Step 2

Navigate to **Web Security Manager > Access Policies** to verify changed settings for URL filtering of IT Group access policy.



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

Step 3

Test the URL filtering based on the predefined URL categories using **Policy Trace** tool, which simulates client requests as if they were made by the end users. Cisco WSA evaluates the request against all committed policies and calculates other attributes, such as the web reputation score.

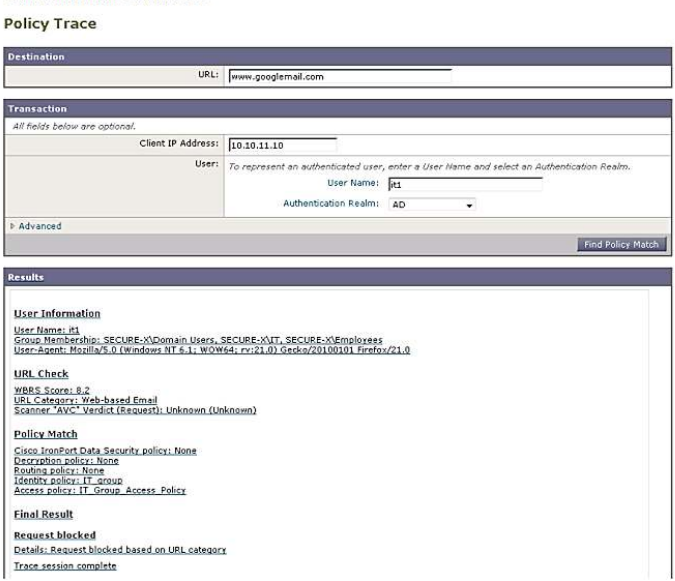
A) In the Cisco WSA GUI on Admin PC, choose **System Administration > Policy Trace.** Use these parameters:

URL: www.googlemail.com

Client IP Address: 10.10.11.10

User Name: it1

Authentication Realm: AD



You should see that test transaction to http://googlemail.com, is matched against **IT group** identity and **IT Group Aceess Policy.** Request is blocked based on URL category, because **IT Group Access Policy** blocks **web-based email** URL category.

https://t.me/learningnets

Step 4

Test the URL filtering based on the predefined URL categories:

A) From the Employee PC logged in as the **it1** user in the **secure-x** domain with the **cisco** password, open a browser and connect via HTTP to http://fashion.net. The access should be blocked because the web category **Fashion** is blocked:



Date: Sun, 09 Feb 2014 15:52:58 GMT
Username:
Source IP: 10.10.11.10
URL: GET http://fashion.net/
Category: Fashion
Reason: BLOCK-WEBCAT
Notification: WEBCAT

B) From the Employee PC, connect via HTTP to http://googlemail.com. The access should be blocked because the web category **Web-based Email** is blocked:



Date: Sun, 09 Feb 2014 15:52:12 GMT
Username:
Source IP: 10.10.11.10
URL: GET http://googlemail.com/
Category: Web-based Email
Reason: BLOCK-WEBCAT
Notification: WEBCAT

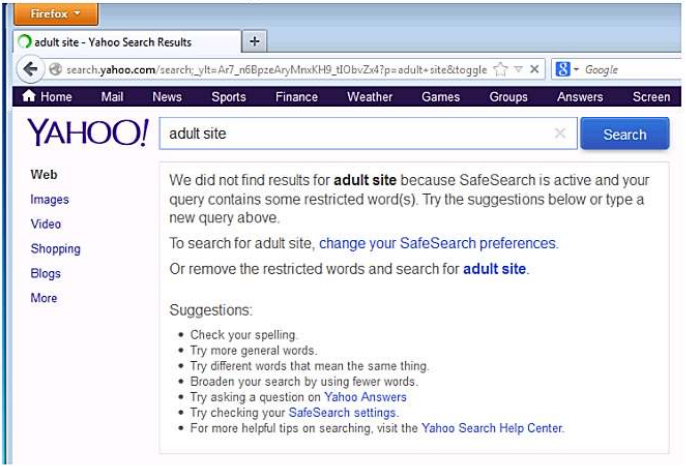
C) From the Employee PC logged in as the **it1** user in the **secure-x** domain with the **cisco** password. Use **Internet Explorer** to connect via HTTP to http://youtube.com. Only the advertising content part of the YouTube web page should be blocked:

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





D) From the Employee PC, connect via HTTP to the http://www.yahoo.com/. This should be successful. Try to search for "**adult site**" in Yahoo, this will fail because Safe Search is enabled.

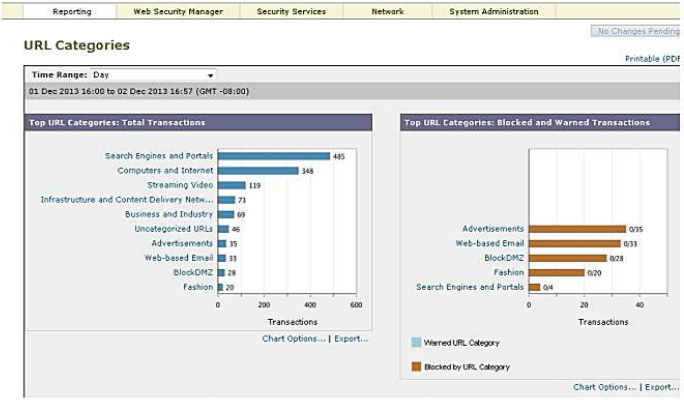


https://t.me/learningnets

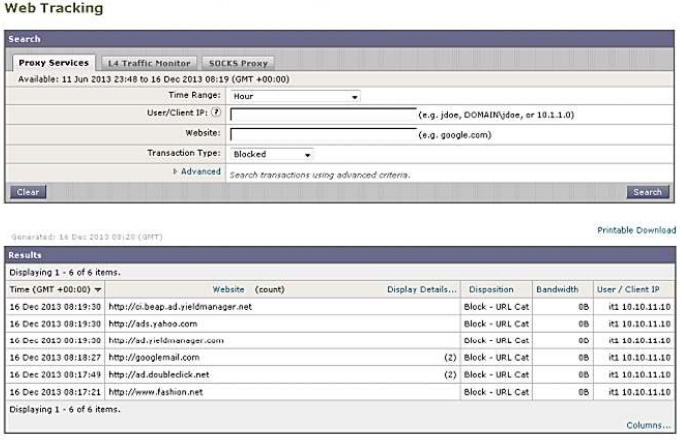
Step 5

Verify blocked transactions in reports and web tracking messages:

A) From the Admin PC Cisco WSA GUI, choose **Reporting > URL Categories**. In the **Top URL Catagories: Blocked and Warned Transactions** chart, you should see the blocked transactions for the different categories being blocked.



B) Choose **Reporting > Reporting Services > Web Tracking**. In the **Proxy Services** tab, choose **Blocked** from the **Transaction Type** drop-down box and search for the latest events. You should see blocked access attempts to the different blocked websites.



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

Step 6

From the Employee PC, connect via HTTP to the lab DMZ server (http://dmz.secure-x.local). This should be successful.



Note	In the next step, you will deploy custom filters based on regular expressions to block access to the lab DMZ server (http://dmz.secure-x.local).

https://t.me/learningnets

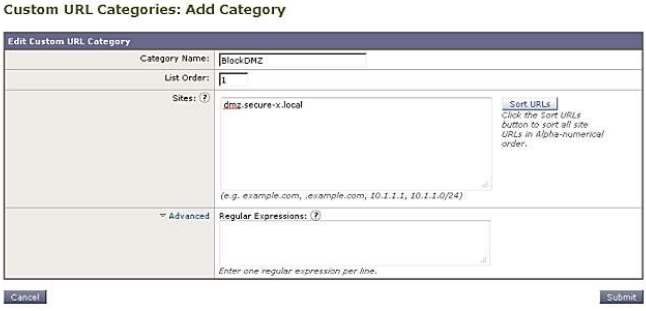
Step 7

Create custom URL category that will be used to block access to the DMZ server:

A) From the Admin PC Cisco WSA GUI, choose **Web Security Manager > Custom Policy Elements > Custom URL Categories**. Click the **Add Custom Category** button.



B) Create a custom URL category (named **BlockDMZ**). It should match the site dmz.secure-x.local.



Click **Submit** then **Commit** the changes.

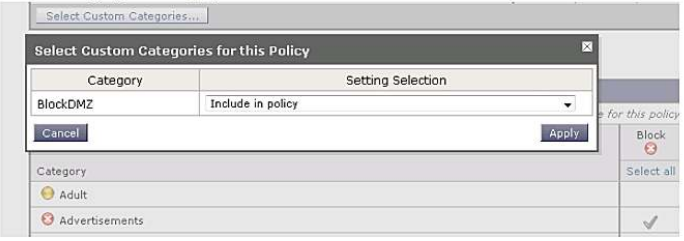
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 8

Configure the access policy to filter based on the custom categories:

A) From the Admin PC Cisco WSA GUI, choose **Web Security Manager > Web Policies > Access Policies**. Click the link under **URL Filtering** for the **IT Group Access Policy**.

B) Click the **Select Custom Categories** button. Choose the **Include in Policy** option for the custom **BlockDMZ** category. Click **Apply**.



C) Choose the **Block** action for the custom **BlockDMZ** category.



D) Click **Submit** then **Commit** the changes.

https://t.me/learningnets

Step 9

From the Employee PC, try to connect via HTTP to http://dmz.secure-x.local. This should fail as a result of the custom category block.





Date: Mon, 16 Dec 2013 08:45:58 GMT
Username: SECURE-X\it1@AD
Source IP: 10.10.11.10
URL: GET http://dmz.secure-x.local/home/index.php
Category: BlockDMZ
Reason: BLOCK-DEST
Notification: BLOCK_DEST

Task 4: Configure Application Visibility Control for the Access Policy

In this lab task, you will deploy Application Visibility and Control (AVC) to block access to all Facebook applications.

Activity Procedure

Complete the following steps:

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

Step 1

Configure Application Visibility and Control (AVC) settings for IT Group Access Policy:

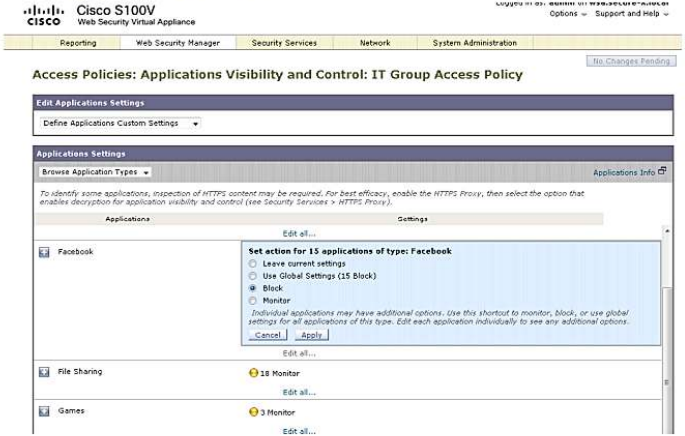
A) From the Admin PC Cisco WSA GUI, navigate to **Web Security Manager > Access Policies**

B) Click the **(global policy)** link under **Applications** for the **IT Group Access Policy**

C) Under **Edit Applications Settings**, select **Define Applications Custom Settings** from the drop down box to configure a custom settings (instead of using the global settings).

D) Under **Applications Settings**, look for **Facebook**, click **Edit all**, select **Block**, then click **Apply**.

E) Click **Submit** then **Commit** the changes.



Step 2

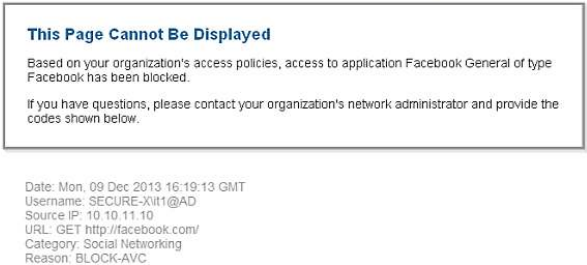
Navigate to **Web Security Manager > Access Policies** to verify the changed **Applications** settings for the IT Group Access Policy.



https://t.me/learningnets

Step 3

From the browser on the Employee PC, try to connect via HTTP to http://www.facebook.com.



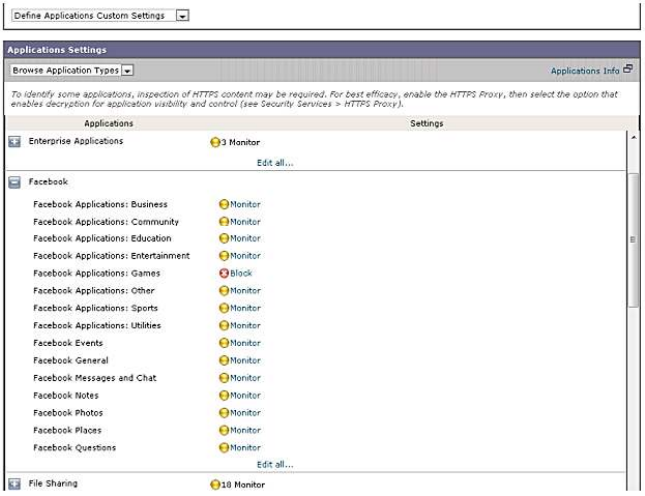
This should fail, because of application visibility setting for IT Group Access Policy is blocking all Facebook applications.

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

Step 4

You can edit the rule for each of the individual Facebook applications by clicking on the + box to the left of the word Facebook under **Applications Settings**, such as only blocking **Games** and monitoring all the other Facebook applications.

NOTE: In this lab step, we will not test the different Facebook applications since you may not wish to log in to Facebook from our lab PC using your Facebook account. Also by default, many of the Facebook transactions use HTTPS but we will not enable the Cisco WSA to perform decryption for the purpose of this class.



https://t.me/learningnets

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

Lab 3-1: Configure Cisco Cloud Web Security Connector on ISR G2 and on AnyConnect

Activity Objective

Lab Scenario: The CSO asked the network security team to test using a cloud based Web security solution in some of the smaller branch offices with an Integrated Services Router G2. The CSO also wants to examine the AnyConnect CWS connector to implement Web security for remote user's using a cloud based solution.

In this lab exercise, using the Secure-X test lab, you will test the Cisco ISR G2 CWS Connector using the Partner ISR G2 router which will represent the branch office and then test the Cisco AnyConnect CWS Connector on the Guest PC which will represent the mobile user.

In this lab exercise, you will not be configuring the Web Filtering rule in the Cisco ScanCenter portal. The Web Filtering rule will be pre-configured by your instructor, you will just access the Cisco ScanCenter as a read only administrator to verify the pre-configured Web filtering rule.

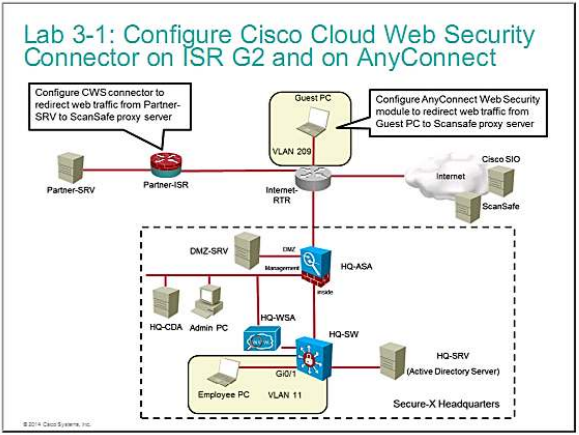
Upon completing this activity, you will be able to meet these objectives:

- Configure and verify the CWS connector on the Cisco ISR G2 router
- Access the Cisco ScanCenter as a read only administrator to verify the pre-configured web filtering rule
- Configure and verify the Web Security module on the Cisco AnyConnect Secure Mobility Client

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.

IOS Commands

Commands	Description
content-scan out	Enables content scanning on the interface.
license 0 *license_key*	Configures the license key that the ISR G2 sends to the Cloud Web Security proxy servers to indicate from which organization the request comes. The license is a 16 byte hexadecimal key. The license key you specify here is generated from the Cisco ScanCenter. Value **0** used for prefix means indicates the license is unencrypted.
logging	Enables IOS syslogs for content scan feature.
parameter-map type content-scan global	Enters the configuration mode for configuring parameters for the Web Security feature on the ISR G2.

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

Commands	Description
server scansafe primary name proxy1753.scansafe.net port http 8080 https 8080	Configures the primary Cloud Web Security proxy servers as well as ports to use for redirecting HTTP and HTTPS requests. By default, Cloud Web Security uses port 8080 for both HTTP and HTTPS traffic, but you can choose to use different ports for each request type.
server scansafe secondary name proxy1363.scansafe.net port http 8080 https 8080	Configures the secondary Cloud Web Security proxy servers as well as ports to use for redirecting HTTP and HTTPS requests. By default, Cloud Web Security uses port 8080 for both HTTP and HTTPS traffic, but you can choose to use different ports for each request type.
server scansafe on-failure *block-all | allow-all*	Determines how to handle client traffic when the ISR G2 cannot reach either configured Cloud Web Security proxy servers. You can block or allow all client web traffic. Default is block.
show content-scan summary	Dsplays generic ScanSafe related details, like active/ standby ScanSafe information.
show content-scan statistics	Displays content scanning process statistics.
show show content-scan session history *number_of_sessions*	Displays the history of content scanning process sessions.
source interface GigabitEthernet0/1	Configures the interface the ISR G2 uses to originate all packets it sends to the CWS proxy servers. The interface configured here should match one that is associated with the egress interface on which **content-scan** is configured.

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 asacx-5500x-boot-9.1.2-42.img asacx-sys-9.1.2-42.pkg
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
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**
ASA CX	**admin**	**Admin123**
AD Server (installed on HQ-SRV)	**Administrator**	**Ci5coAdmin**
ScanSafe portal (https://scancenter.scansafe.com)	**ccnpsec.scansafe@yahoo.com**	**C!sco!23**

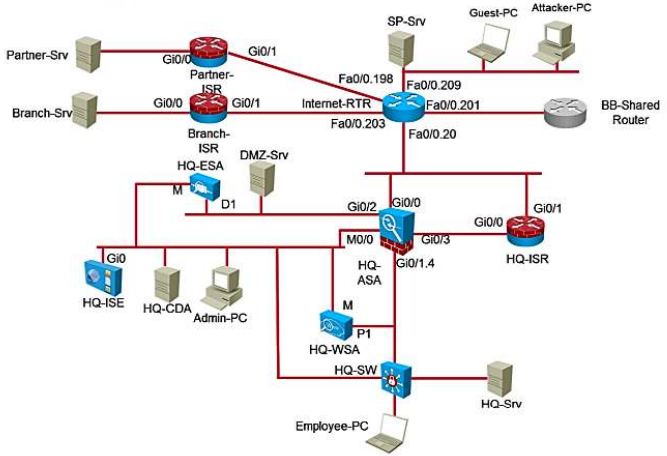
Employee PC is joined to the Active Directory domain.

AD User	AD password	AD Group	Email address in AD properties
it1	**cisco**	IT	**it1@secure-x.public**

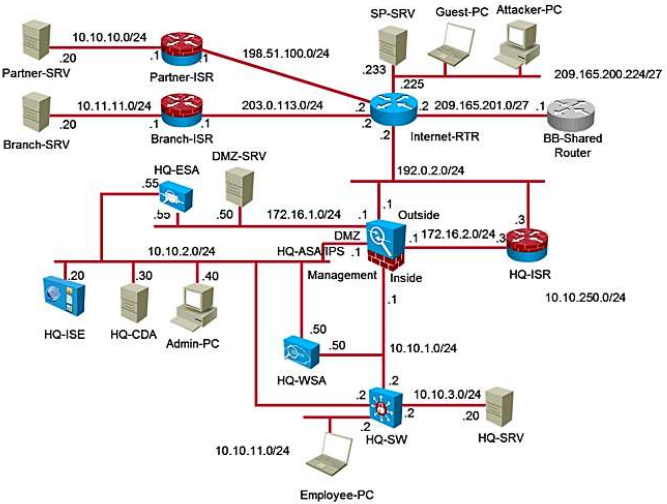
https://t.me/learningnets

Topology and IP Addressing

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



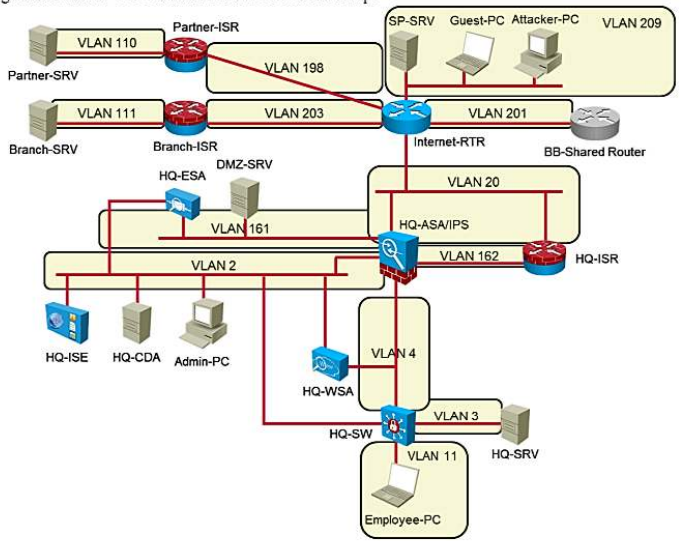
The figure shows the IP addresses that are used in this lab setup.



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

VLAN Setup

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



Task 1: Enable the CWS Connector on the Partner ISR G2 Router

In this task you will configure CWS connector on Partner-ISR router and thus redirect web traffic originated from Partner-SRV to ScanSafe proxy servers.

Activity Procedure

Complete the following steps to verify basic network connectivity:

Step 1

Access the console of Partner-ISR router and set the SP-Srv (IP address 209.165.200.233) as DNS server. Also make sure that **ip domain-lookup** feature is enabled.

```
Partner-ISR(config)# ip domain-lookup
Partner-ISR(config)# ip name-server 209.165.200.233
```


https://t.me/learningnets

Step 2

Verify the Partner-ISR has Internet connectivity by pinging www.cisco.com.

```
Partner-ISR# ping www.cisco.com
Translating "www.cisco.com"...domain server (209.165.200.233) [OK]
Translating "www.cisco.com"...domain server (209.165.200.233) [OK]
Translating "www.cisco.com"...domain server (209.165.200.233) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.199.112.170, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
```

Step 3

Log in to the Partner-Srv PC using **admin** username and **Ci5coAdmin** password. Open a browser on the Partner Server PC and browse to http://www.cisco.com and to http://www.poker.com, the traffic should be permitted.

Step 4

From the Partner-Srv PC, browse to http://whoami.scansafe.net, to verify if the web traffic is being redirected to CWS proxy server.



User is not currently using the service

You should see the web traffic is currently not being redirected to CWS proxy server.

Step 5

Configure the CWS connector on the Partner-ISR router using these parameters:

Primary Proxy Server = proxy1753.scansafe.net

Secondary Proxy Server = proxy1363.scansafe.net

HTTP port = 8080

HTTPS port = 8080

License Key = To be provided by your instructor

Internet Facing Egress Interface = GigabitEthernet 0/1

Block all web traffic if CWS proxy servers are not accessible

Enable syslogs for content scan

You can verify if your configuration is correct by checking the Lab Answer Keys in the back of the lab guide.

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

Step 6

Enable content scanning on **GigabitEthernet 0/1** Partner-ISR interface.

You can verify if your configuration is correct by checking the Lab Answer Keys in the back of the lab guide.

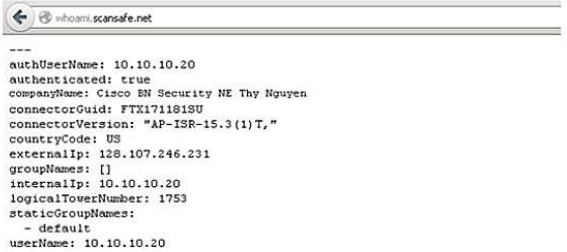
Step 7

On Partner-ISR router verify the reachability of the primary and secondary CWS proxy servers

```
Partner-ISR# show content-scan summary
Primary: 72.37.244.203 (Up)*
Secondary: 70.39.231.99 (Up)
Interfaces: GigabitEthernet0/1
```

Step 8

From the Partner-Srv PC, browse to http://whoami.scansafe.net, to verify if the web traffic is being redirected to CWS proxy server.



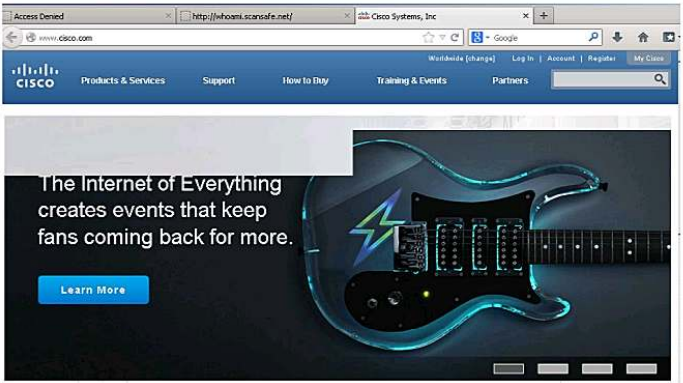
You should see that web traffic is being redirected to CWS proxy server. You will also see an internal IP address of 10.10.10.20 which is the SP-Srv IP address, the company name and etc.... Since we have not enabled user authentication to send the user identity to CWS, the username shown is also the internal IP address of 10.10.10.20.

https://t.me/learningnets

Step 9

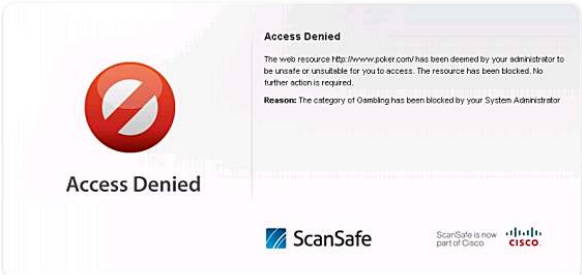
From the Partner-Srv PC, use the web browser to test access to different websites:

Browse to http://www.cisco.com and verify the traffic is being allowed by CWS.



Try to browse to http://www.poker.com and verify the traffic is being blocked by CWS.





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

Step 10

Use the **show content-scan** CLI command options to verify the CWS connector operations:

Use the **show content-scan statistics** command to displayed the CWS connector scanning statistics.

```
Partner-ISR# show content-scan statistics
Current HTTP sessions: 22
Current HTTPS sessions: 0
Total HTTP sessions: 29
Total HTTPS sessions: 1
White-listed sessions: 0
Time of last reset: 00:01:03
-----------------------------------
Details:
Max Concurrent Active Sessions: 24
Connection Rate in last minute:
    Redirected
        HTTP: 28
        HTTPS: 1
    White-listed
        IP-Based: 0
        User/User-group: 0
        Header-Based: 0
Max Connection Rate per minute:
    Redirected
        HTTP: 28
        HTTPS: 1
    White-listed
        IP-Based: 0
        User/User-group: 0
        Header-Based: 0
```

You should see non-zero number for total HTTP sessions counter.

Use the **show content-scan session history 50** command to display the last 50 HTTP and HTTPS sessions information.

```
Partner-ISR# show content-scan session history 25
Protocol          Source          Destination     Bytes     URI              Time
HTTPS 10.10.10.20 74.125.239.47   (3032:984)                                 04:35:16
HTTP 10.10.10.20  74.125.239.155  (0:0)                                      00:00:46
HTTP 10.10.10.20  66.235.138.217  (0:0)                                      00:00:46
HTTP 10.10.10.20  199.7.55.72     (0:0)                                      00:00:47
HTTP 10.10.10.20  74.125.239.156  (0:0)                                      00:00:46
HTTP 10.10.10.20 205.204.69.234   (440:630)             www.poker.com        00:00:42
HTTP 10.10.10.20  23.199.59.95    (0:0)                                      00:00:47
HTTP 10.10.10.20  23.199.59.95    (0:0)                                      00:00:47
HTTP 10.10.10.20  23.199.59.95    (0:0)                                      00:00:47
HTTP 10.10.10.20  23.199.59.95    (0:0)                                      00:00:47
HTTP 10.10.10.20  173.37.144.208  (0:0)                                      00:00:47
HTTPS 10.10.10.20 173.37.144.208  (505:4388)                                 00:00:47
HTTP 10.10.10.20  72.163.10.14    (2441:1887)       news-tags.cisco.com      00:00:46
HTTP 10.10.10.20  72.163.10.14    (1403:1887)       news-tags.cisco.com      00:00:46
HTTPS 10.10.10.20 80.254.145.88   (551:1493)                                 00:00:57
HTTP 10.10.10.20  80.254.145.88   (306:561)         whoami.scansafe.net      00:00:52
HTTP 10.10.10.20  80.254.145.88   (306:561)         whoami.scansafe.net      00:00:52
HTTP 10.10.10.20  80.254.145.88   (295:561)         whoami.scansafe.net      00:00:52
```


https://t.me/learningnets

```
HTTPS 10.10.10.20 80.254.145.88   (853:1943)                    00:00:57
HTTPS 10.10.10.20 80.254.145.88   (810:2083)                    00:00:58
<output omitted>
```

You should see HTTP sessions to www.poker.com, cisco and whoami.scansafe.net

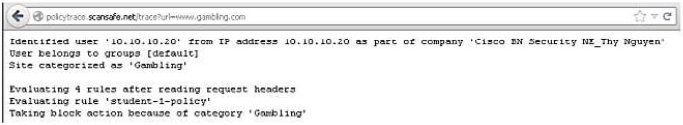
Step 11

On the Partner-Srv PC web browser, use Policy Trace to verify if web transaction to www.gambling.com will be blocked:

A) Browse to policytrace.scansafe.net

B) Enter **www.gambling.com** into **Enter URL** field and click **GO**





You should see that web transaction is not allowed as the web filtering policy pre-configured in the Cisco ScanCenter by your instructor blocks the **Gambling** URL category. You should see that rule responsible for blocking this web transaction is **student-1-policy**.

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

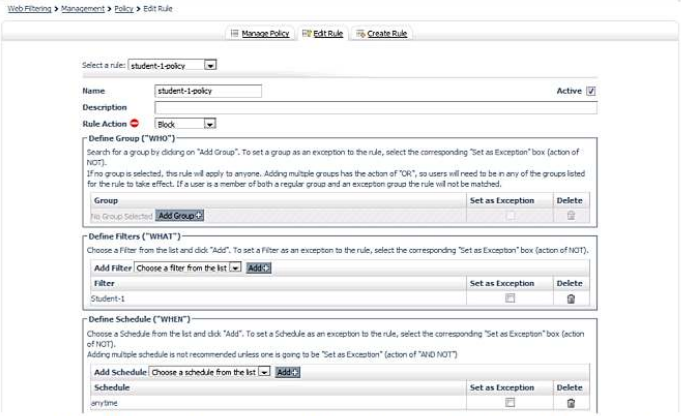
Step 12

From the Partner-Srv PC, log in to the Cisco ScanCenter portal at https://scancenter.scansafe.com using username **ccnpsec.scansafe@yahoo.com** and password **C!sco!23.** This user account has full read only access in the Cisco ScanCenter.

A) Navigate to **Web Filtering > Management > Policy** and locate the **student-1-policy** rule within the Company Policy. Click on this rule.

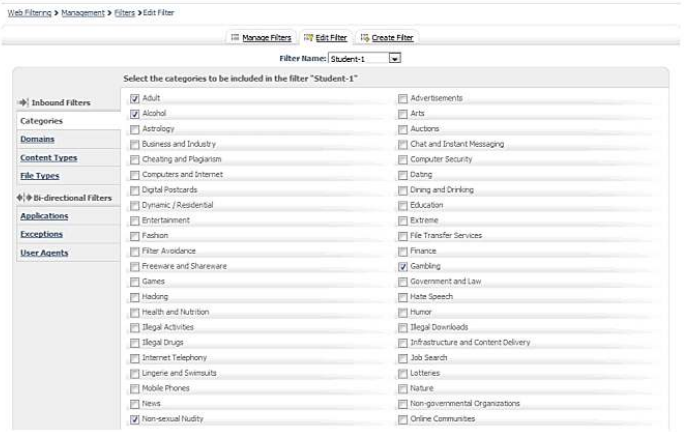


B) Verify that the **student-1-policy** rule has the block rule action and is using the **Student-1** filter which defines which web transactions will be blocked.



C) Navigate to **Web Filtering > Management > Filters** and locate the **Student-1** filter. Click on this filter and confirm that the **Gambling** URL category is checked along with some other categories such as **Adult** and etc..

https://t.me/learningnets



Task 2: Enable the CWS Connector on the AnyConnect Secure Mobility Client

In this lab task performed on Guest PC, you will enable the AnyConnect Web Security Module (with the VPN module also enabled) using the standalone Web Security Profile Editor. You will create the required AnyConnect Web Security Module XML profile using the Web Security Profile Editor and verify the AnyConnect Web Security Module operations by browsing to different websites

Activity Procedure

Complete the following steps:

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

Step 1

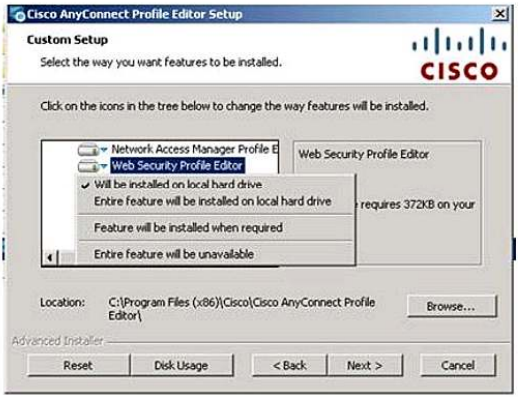
From the Guest-PC **D:\AnyConnect** folder, double-click on the **anyconnect-profileeditor-win-3.1.04059-k9.exe** to launch the standalone profiler editor installation wizard.

A) Click **Next**, accept the license agreement.

B) Choose the **Custom** setup type then click **Next**.

C) Choose **Web Security Profile Editor** from the list of available features, select **Will be installed on local hard drive** then click **Next.** Click **Install** to complete installation. Uncheck "View readme file" and click **Finish** to exit installation wizard.

D) Click **Install** to complete installation. Uncheck "**View readme file**" and click **Finish** to exit installation wizard.



Step 2

On the Guest-PC, launch the standalone Web Security Profile Editor using **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.

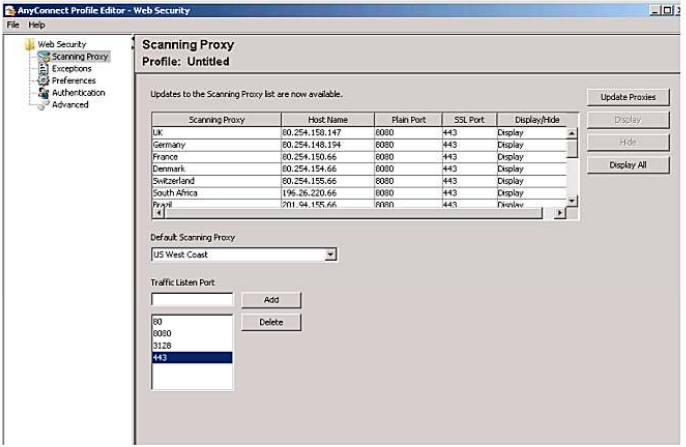
https://t.me/learningnets

Step 3

In the **WebSecurity > Scanning Proxy** page:

Add the **443** port to the list of the Traffic Listen Port so HTTPS traffic will also be redirected to CWS

In the **Default Scanning Proxy** drop down box, use the **US West Coast** option.



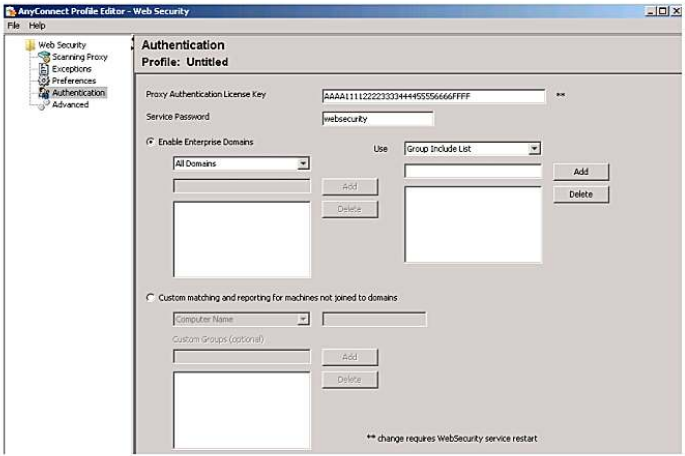
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 4

In the **WebSecurity > Authentication** page:

Enter the Proxy Authorization License Key, which will be provided by your instructor. Note that license key in the figure is not valid one.

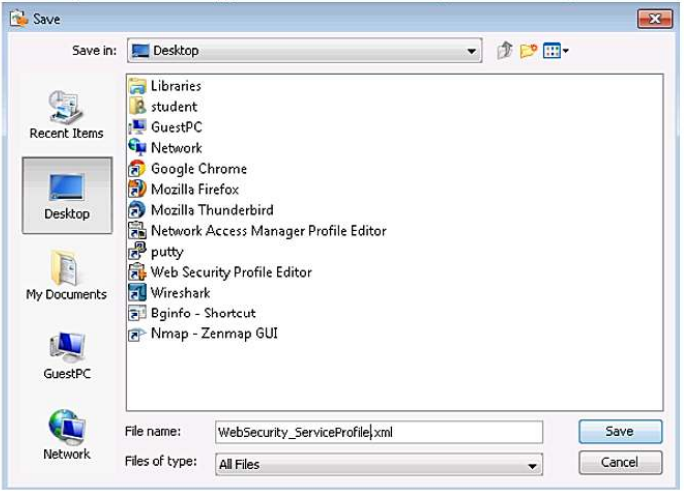
Leave the default **Service Password** as **websecurity**. This password is only required when using the **acwebsecagent -disablesvc** CLI command to disable the Web Security agent. You should not need to use this CLI command in this lab task.



Step 5

From the **File** menu of Web Security Profile Editor, select **Save As:**

A) Enter **WebSecurity_ServiceProfile.xml** as the filename and save it to the **Desktop** folder. NOTE: You must use the specific **WebSecurity_ServiceProfile.xml** filename (not case sensitive).



B) The pop-up window will appear, notifying you that obfuscated profile with **.wso** extension will be created in the same folder you are trying to save **.xml** file. You will need to copy **WebSecurity_ServiceProfile.wso** to the proper directory later after installing AnyConnect Web Security Module. Click **Done**.



C) Exit the Web Security Profile Editor.

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

Step 6

Access the Guest PC, and click the **Setup.exe** file in the **D:\AnyConnect\anyConnect-win-3.1.04059-pre-deploy-k9** folder to start Cisco AnyConnect Secure Mobility Client Install Selector:

A) Check the **AnyConnect VPN** and **AnyConnect Web Security** checkboxes and click **Install Selected**.



B) Click **OK** to confirm the installation and **Accept** to accept license agreement and complete the installation.

https://t.me/learningnets

Step 7

Launch the AnyConnect Secure Mobility client using **Start > Programs > Cisco > Cisco AnyConnect Secure Mobility Client**.

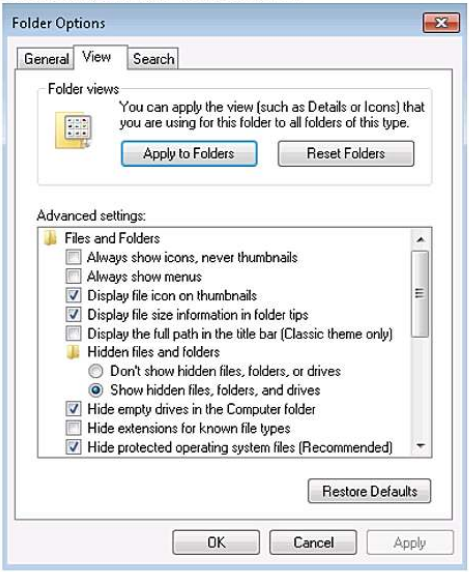


You should see that there is no license key for Web Security module at the moment, because you have not copied the **.wso** profile file to the proper directory.

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

Step 8

On the Guest PC, open **Windows Explorer** and click **Organize>Folder and search options.** Select **View** tab and check **Show hidden files, folders, or drives** checkbox.



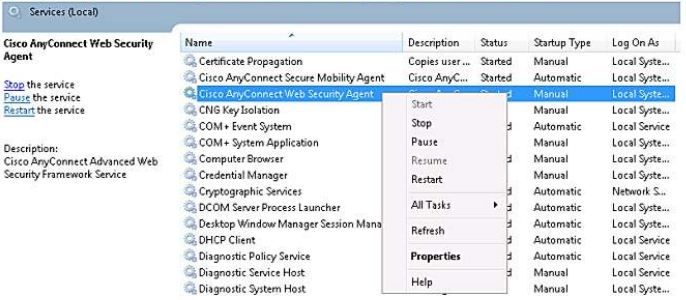
Step 9

On the Guest PC copy the **WebSecurity_ServiceProfile.wso** file from the **Desktop** folder to the **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security** folder.

https://t.me/learningnets

Step 10

On Guest PC exit the Cisco AnyConnect Secure Mobility Client and restart the **Cisco AnyConnect Web Security Agent** service. Use the **services.msc** windows CLI command to launch the Windows Services manager, right click on **Cisco AnyConnect Web Security Agent** and select **Restart**.



Step 11

Launch the AnyConnect Secure Mobility client using **Start > Programs > Cisco > Cisco AnyConnect Secure Mobility Client**.



You should see that Web Security module is enabled and working. In this lab task, you will not configure and test the AnyConnect VPN operations, you will only test the AnyConnect Web Security operations.

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

Step 12

Open a web browser on the Guest PC and verify operation of Cisco AnyConnect Web Security Module:

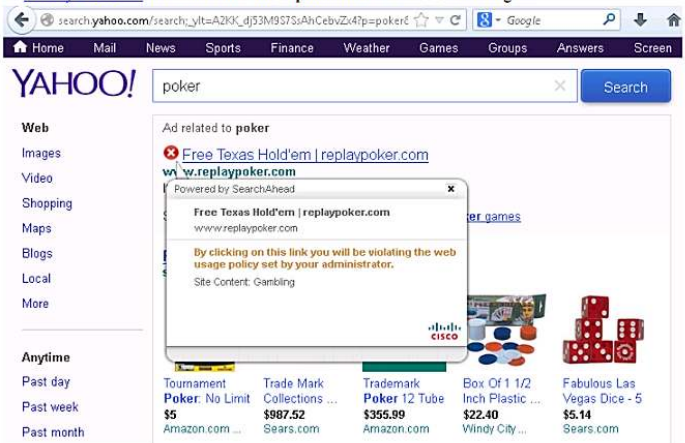
A) From the browser, go to http://whoami.scansafe.net to verify the web traffic is being redirected to Scansafe.

whoami.scansafe.net

```
---
authUserName: "WinNT://GUEST-PC\\student"
authenticated: true
companyName: Cisco BN Security NE_Thy Nguyen
connectorGuid: A53A0C972DF00D31B6ED90983672BB1A
connectorVersion: AP_AC3.1.04059
countryCode: US
externalIp: 128.107.246.231
groupNames:
  - "WinNT://GUEST-PC\\None"
internalIp: 209.165.200.241
logicalTowerNumber: 1742
staticGroupNames:
  - default
userName: "WinNT://GUEST-PC\\student"
```

Note that the internal IP address of **209.165.200.x** (Guest PC gets its IP address from DHCP server) reported by the AnyConnect Secure Mobility client to the Scansafe proxy server is the IP address of the Guest PC.

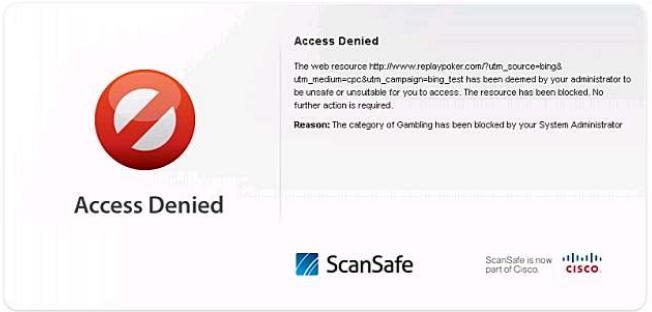
B) Go to www.yahoo.com and enter enter word **poker** in the Yahoo search engine.



You should see the warning that by clicking on some of the gambling category links you will be violating the web usage policy set by your administrator because the **SearchAhead** feature has been enabled on the Cisco ScanCenter by your instructor.

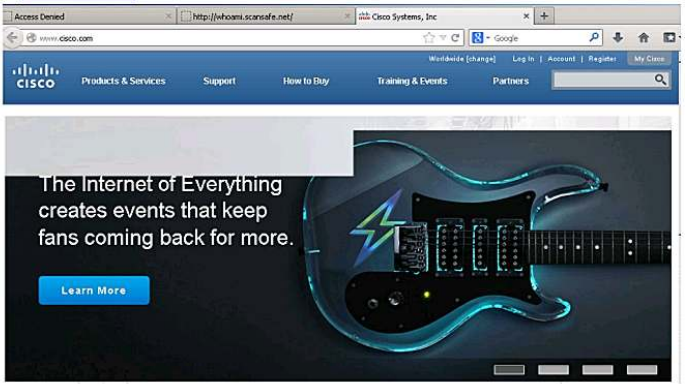
C) Click one of such links from yahoo search results.





You should not be able to visit web pages that belong to the **Gambling** category being blocked by CWS.

D) Go to www.cisco.com.



You should see the web transaction is allowed as CWS is not blocking the attempt.

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

Step 13

Click on the **Cisco AnyConnect Secure Mobility Client** icon in the system tray and click small **Settings** icon in the lower left corner. Navigate to **Web Security > Statistics**.



You should see non-zero number for filtered active and filtered total connections.

https://t.me/learningnets

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

Lab 4-1: Configure Cisco Email Security Appliance Basic Policies

Activity Objective

Lab scenario: the IT team managing the Email services is asking the network security team which you are a member of to deploy the Cisco Email Security Appliance and setup a basic email policy on it. Once the network security team has setup the Cisco Email Security Appliance with a basic email policy, the IT team will then fully configure the Cisco Email Security Appliance with all the remaining email security configurations and policies which are not the responsibility of the network security team.

In this exercise, as a member of the network security team, you will deploy the Cisco Email Security Appliance using a vESA in the secure-x test lab to test the email security infrastructure of a typical enterprise. The secure-x test lab environment includes two mail server domains: **secure-x.public** running on the HQ-srv, and **sp.public** running on the SP-srv. The network already has been set up by your instructor to enable email exchange between mail servers and bypass the vESA.

First you will verify the mail operation and examine the mail flows without the vESA. Then you will deploy the mail proxy and put the vESA in the path between the internal and external mail servers. The integration of the vESA with the Active Directory will allow the ESA to forward inbound email only to existing internal user accounts. You will implement incoming content filters that drop compressed attachments. The Data Loss Prevention policies will block the leakage of credit card information and sensitive network data documents. Throughout the deployment, you will use the vESA monitoring and message tracking capabilities to verify the email flow.

Upon completing this activity, you will be able to meet these objectives:

- Verify the initial email exchange without the ESA
- Deploy the ESA mail proxy
- Integrate the ESA with LDAP
- Configure incoming content filters and mail policies

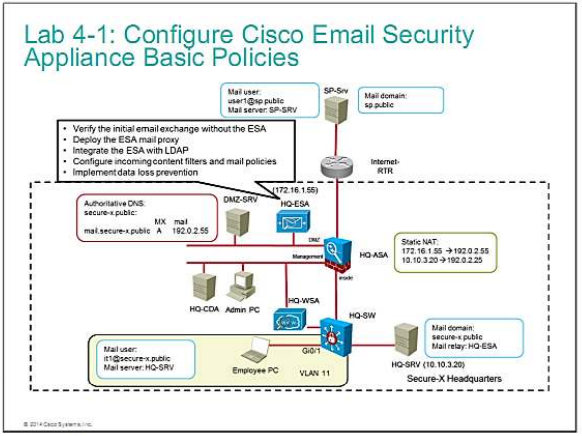
https://t.me/learningnets

Implement data loss prevention

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

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources and equipment are required to complete this activity:

- Cisco Email Security Appliance
- Three email servers and clients

Job Aids

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

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 asacx-5500x-boot-9.1.2-42.img asacx-sys-9.1.2-42.pkg
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
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**
ASA CX	**admin**	**Admin123**
AD Server (installed on HQ-SRV)	**Administrator**	**Ci5coAdmin**
ScanSafe portal (https://scancenter.scansafe.com)	**ccnpsec.scansafe@yahoo.com**	**C!sco!23**

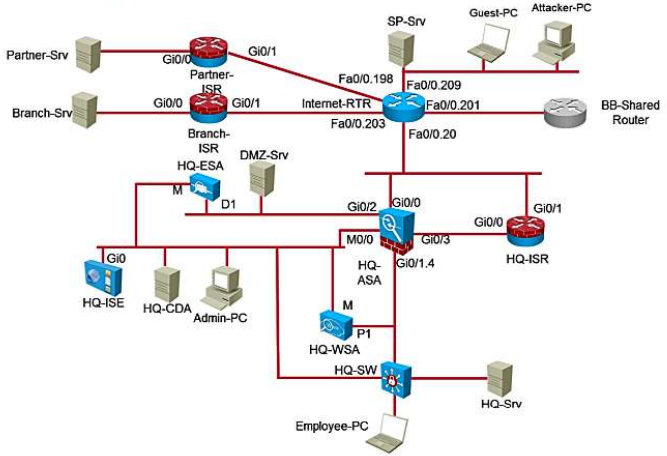
Employee PC is joined to the Active Directory domain.

AD User	AD password	AD Group	Email address in AD properties
it1	**cisco**	IT	**it1@secure-x.public**

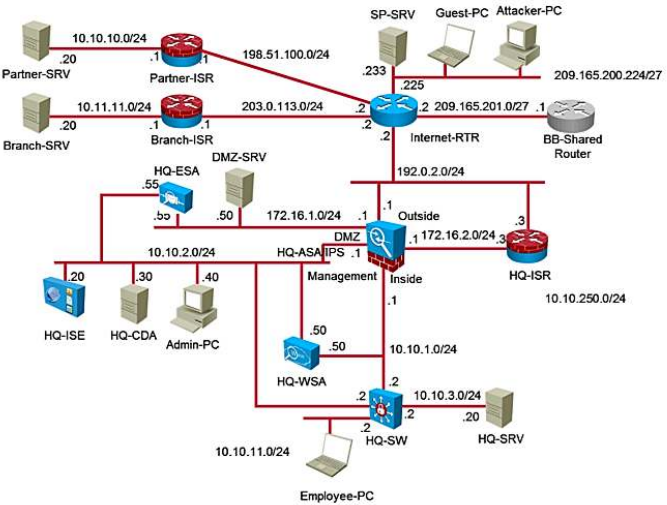
https://t.me/learningnets

Topology and IP Addressing

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



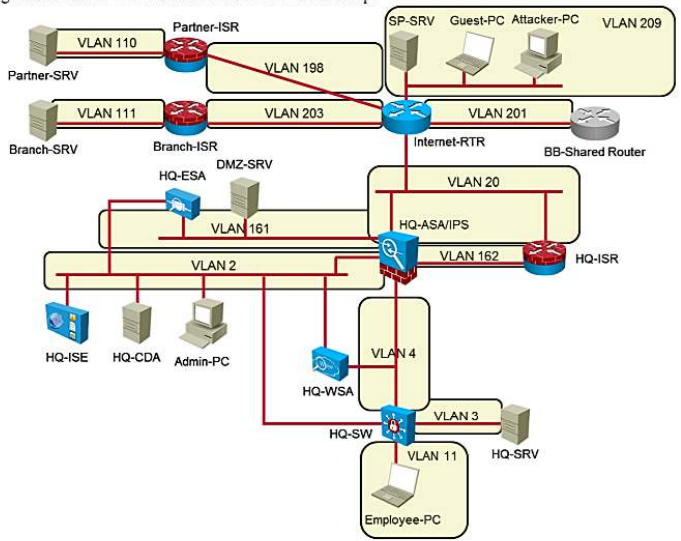
The figure shows the IP addresses that are used in this lab setup.



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

VLAN Setup

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



Task 1: Verify the Initial Email Exchange Without the Cisco ESA

In this task you will verify the initial email flow that bypasses the Cisco ESA.

Note	The environment includes two mail server domains: **secure-x.public** running on HQ-srv, and **sp.public** running on SP-srv. The network has been set up to enable email exchange between the two mail servers, and bypass the Cisco ESA. First you will verify the mail operation and examine the mail flows.

Activity Procedure

Complete the following steps:

https://t.me/learningnets

Step 1

Test the operation of the internal and external email servers:

A) Connect to the Employee PC (**student**/**Ci5coAdmin**), and start the **Mozilla Thunderbird** email client. The client should be preconfigured for IMAP/SMTP connectivity to the HQ-SRV (**hq-srv.secure-x.local**).

Note	The hMailServer on the HQ-SRV has been preconfigured with four email accounts: **it1@secure-x.public**, **marketing1@secure-x.public**, **engineer1@secure-x.public**, and **sales1@secure-x.public**. Each uses the password **cisco**.

Note	The Mozilla Thunderbird email client has been prepared for the **it1** user.

B) Send an email to yourself. This action will test the operation of the hMailServer that is running on the HQ-SRV. The email test should work.

C) Connect to the SP-SRV (log in as **administrator** with the password **Ci5coAdmin**), and start the **Mozilla Thunderbird** email client. The email client should be preconfigured for the user **user1@sp.public** of the hMailServer that is running on the SP-SRV (**sp-srv.sp.public**).

Note	The hMailServer on the SP-SRV has been preconfigured with the email account **user1@sp.public** and the password **cisco**.

D) Send an email to yourself (**user1@sp.public**). This action will test the operation of the hMailServer that is running on the SP-SRV. The email test should work.

Step 2

From the external email client (**user1@sp.public**) on SP-SRV, send an email to an internal user **it1@secure-x.public**. The email should arrive in the recipient inbox. Review the email delivery process:

A) The DNS database on the SP-SRV has a conditional forwarder for the **secure-x.public** domain set to the DMZ-SRV public address (192.0.2.50).

B) The HQ-ASA translates the DMZ-SRV local address (172.16.1.50) to the global address (192.0.2.50) and permits incoming DNS traffic bound to the DMZ-SRV.

C) The DMZ-SRV has in the DNS configuration for the **secure-x.public** domain an MX record (email), and an A record for email (192.0.2.25).

Note	You can verify the DNS database on DMZ-SRV by connecting to the DMZ server. The database is stored in the file **db.secure-x.public** in the **/etc/bind** directory.

D) The HQ-ASA translates the HQ-SRV local address (10.10.3.20) to the global address (192.0.2.25) and permits inbound SMTP.

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

Step 3

From the internal email client (for example, **it1@secure-x.public**), send an email to the external user (**user1@sp.public**). The email should arrive in the recipient inbox. Review the email delivery process:

A) The DNS server on the HQ-SRV has a forwarder set to the DMZ-SRV address (172.16.1.50).

B) The HQ-ASA permits outbound DNS (inside to DMZ).

C) The DMZ-SRV forwards requests for the sp.public domain to the SP-SRV.

D) The HQ-ASA permits outbound DNS (DMZ to outside).

E) The SP-SRV DNS database has an MX record (**sp-srv.sp.public**) and an A record for **sp-srv.sp.public** to its IP address (209.165.200.233).

Task 2: Deploy the Cisco ESA Mail Proxy

In this task you will deploy the Cisco ESA. The mail proxy will now be put in the path between the internal and external mail servers. You will ensure that the Cisco ESA has the required feature keys and use the system setup wizard to provision the Cisco ESA network settings. You will redirect the email flows to the Cisco ESA by changing the mail record in the DNS database on the DMZ server. At the end of this task, the Cisco ESA will be filtering emails exchanged between the internal and external servers using default policies.

Activity Procedure

Complete the following steps:

Step 1

Connect to the Admin PC (log in as **student** with the password **Ci5coAdmin**) and start the management GUI of the Cisco ESA:

A) Open Internet Explorer, and connect via HTTP or HTTPS to the Cisco ESA management IP address (**https://esa-mgmt.secure-x.local**).

B) Accept the security warning. The Cisco ESA has not been enrolled to the PKI.

C) Log in as **admin** with the password **Ci5coAdmin**.

D) In the Cisco ESA management GUI, go to **Network > IP Interfaces** and verify that the management interface has been preconfigured to the correct value (10.10.2.55/24). This setting enables your management session.

E) Go to **System Administration > Feature Keys**. You should see a number of feature keys that are required for implementing the email security policy in this environment.

Note	The next step walks you through the system setup wizard. Your Cisco ESA has been preconfigured with some network settings to enable initial management connectivity. You will revisit these network settings and configure additional details.

https://t.me/learningnets

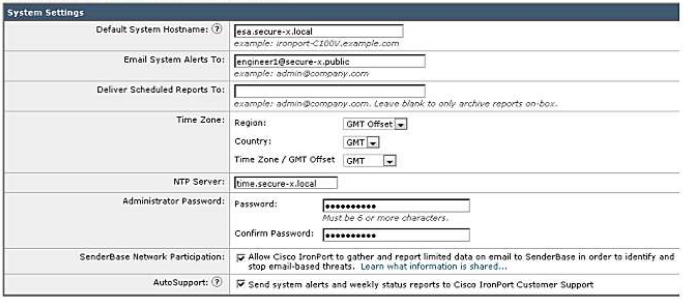
Step 2

Configure the Cisco ESA using the system setup wizard:

A) Go to **System Administration > System Setup > System Setup Wizard** and start the wizard.

B) In task 2 (System), in the first page revisit and configure the following settings:

- **Default System Hostname: esa.secure-x.local**
- **Email System Alerts To: engineer1@secure-x.public**
- **NTP Server: time.secure-x.local**
- **Administrator Password: Ci5coAdmin**



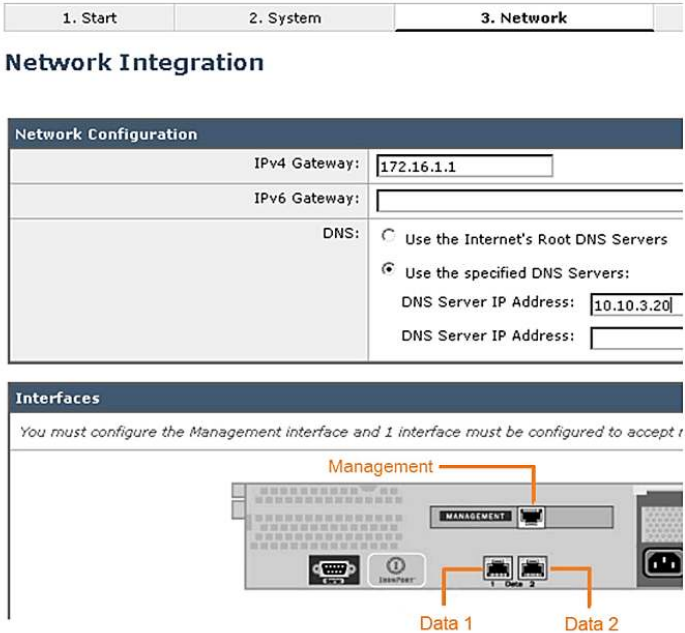
Note You may be prompted to reset the configuration if you already performed some configuration without committing it. In that case, click **Commit Configuration** in the upper-right corner and then choose **Abandon Configuration**.

- Click **Next**.

C) Configure the settings in the **Network Integration** page:

- Set the IPv4 default gateway to the IP address of the ASA DMZ interface (172.16.1.1).
- Set the DNS server to the HQ-SRV (10.10.3.20).

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



- Scroll down, check the **Enable Data 1 Interface** check box, and configure its settings (This will automatically setup one Listener on the **Data1** Interface):

  IPv4 Address / Netmask: 172.16.1.55/24

  Fully Qualified Hostname: mail.secure-x.public

  Accept Incoming Mail:

  - Enable the **Accept Mail on This Interface** check box
  - **Domain**: **secure-x.public**
  - **Destination**: **10.10.3.20**

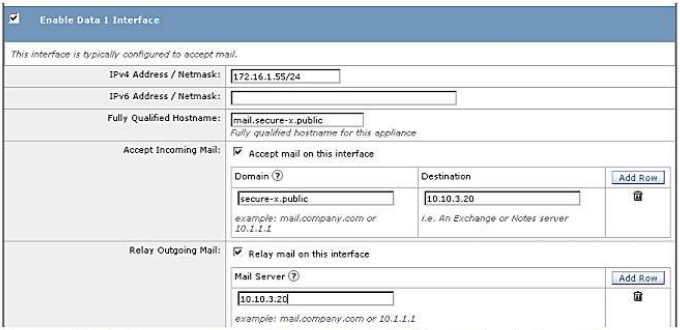
Note	This will automatically setup the RAT to accept email to **secure-x.public** domain and set the SMTP route for **secure-x.public** domain to SMTP server on HQ-SRV at **10.10.3.20.**

  Relay Outgoing Mail:

  - Enable the **Relay Mail on This Interface** check box
  - **Mail Server**: **10.10.3.20**

Note	This will automatically setup the **RELAYLIST** Sender Group in the HAT.

https://t.me/learningnets



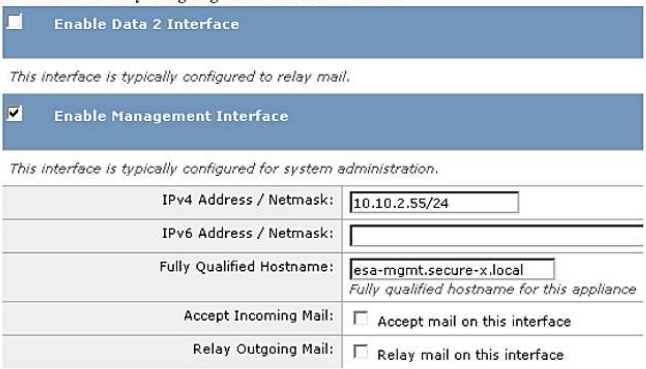
- Scroll down and check the **Enable Management Interface** check box and apply these settings:

  IPv4 Address / Netmask: 10.10.2.55/24

  Fully Qualified Hostname: esa-mgmt.secure-x.local

  Ensure that the **Accept Incoming Mail** check box is cleared

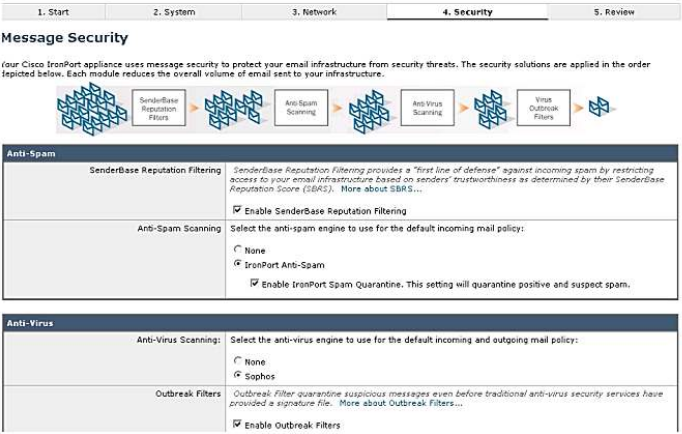
  Ensure that the **Relay Outgoing Mail** check box is cleared



- Click **Next**.

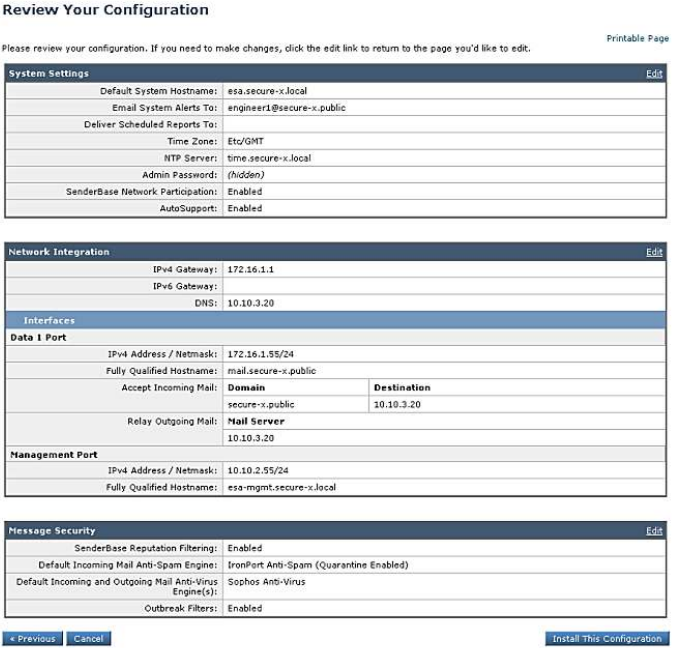
D) In the **Message Security** page, examine the antispam and antivirus settings. Leave them at their default values and click **Next**.

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



E) Review the configuration. Click the **Install This Configuration** button.

https://t.me/learningnets



Review Your Configuration

Printable Page

Please review your configuration. If you need to make changes, click the edit link to return to the page you'd like to edit.

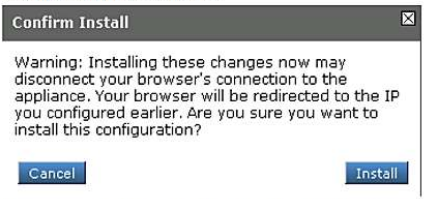
System Settings	Edit
Default System Hostname:	esa.secure-x.local
Email System Alerts To:	engineer1@secure-x.public
Deliver Scheduled Reports To:	
Time Zone:	Etc/GMT
NTP Server:	time.secure-x.local
Admin Password:	*(hidden)*
SenderBase Network Participation:	Enabled
AutoSupport:	Enabled

Network Integration	Edit	
IPv4 Gateway:	172.16.1.1	
IPv6 Gateway:		
DNS:	10.10.3.20	
Interfaces		
Data 1 Port		
IPv4 Address / Netmask:	172.16.1.55/24	
Fully Qualified Hostname:	mail.secure-x.public	
Accept Incoming Mail:	**Domain**	**Destination**
	secure-x.public	10.10.3.20
Relay Outgoing Mail:	**Mail Server**	
	10.10.3.20	
Management Port		
IPv4 Address / Netmask:	10.10.2.55/24	
Fully Qualified Hostname:	esa-mgmt.secure-x.local	

Message Security	Edit
SenderBase Reputation Filtering:	Enabled
Default Incoming Mail Anti-Spam Engine:	IronPort Anti-Spam (Quarantine Enabled)
Default Incoming and Outgoing Mail Anti-Virus Engine(s):	Sophos Anti-Virus
Outbreak Filters:	Enabled

« Previous | Cancel | Install This Configuration

F) Click the **Install** button on the confirmation window.



G) Open another tab in web browser and log in (**admin/Ci5coAdmin**) to HQ-ESA again. You will be redirected to **Active Directory Wizard**. Cancel the wizard by clicking the **Cancel** button. You will invoke Active Directory server in the next task.

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

Step 3

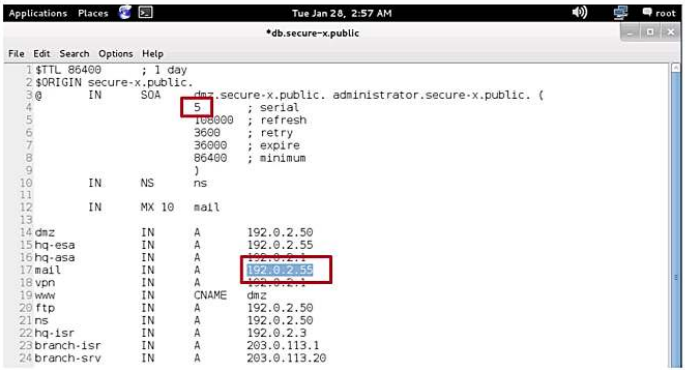
Change the public DNS data to enforce the inbound SMTP traffic to flow via the ESA:

A) Connect to the DMZ-SRV.

B) Double click the **DMZ-SRV** icon. Go to **File System**. Go to the **/etc/bind** and list the directory.

C) Edit the file **db.secure-x.public** by double-clicking the file: Change the A record "mail" from 192.0.2.25 to **192.0.2.55**. **Save** the changes.

- Change the A record **mail** from 192.0.2.25 to **192.0.2.55**. **Save** the changes.
- Increment serial number by one.



D) Restart the DNS Server by opening a command prompt on DMZ-SRV and entering the command: **/etc/init.d/bind9 restart**



Step 4

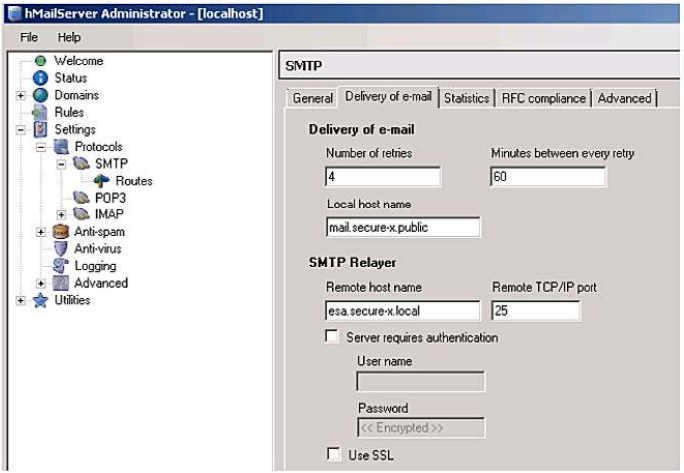
Configure the hMailServer that is running on the HQ-SRV to relay emails to the Cisco ESA:

A) Connect to the HQ-SRV (log in as **administrator** with the password **Ci5coAdmin**) and go to **Start > hMailServer Administrator**.

B) Click **Connect** if you see a page with the local host entry and the Administrator account. Enter the password **Ci5coAdmin**.

C) Go to **Settings > Protocols > SMTP**. Choose the **Delivery of E-mail** tab.

D) Set the SMTP relayer to **esa.secure-x.local** with port 25.



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

Step 5

Clear the DNS cache on SP-SRV:

A) Open the DNS Manager (**Start > Administrative Tools > DNS**), right-click SP-SRV and select **Clear Cache**.



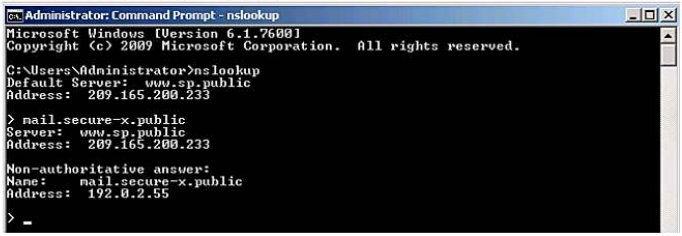
B) Open the command prompt and clear local DNS cache of SP-SRV by issuing the command **ipconfig /flushdns**.



Step 6

Verify that the network is prepared for Cisco ESA integration:

A) On the SP-SRV, open a command prompt, and resolve the name **mail.secure-x.public** by using the **nslookup** command. After the change on the DMZ-SRV, **mail.secure-x.public** should resolve to 192.0.2.55 (the Cisco ESA public address).



Note If the name resolution does not work, check the configuration on the DMZ-SRV. If it is correct, you may have to reload the DMZ-SRV first and then the SP-SRV.

B) On the ASA, use the **show xlate** CLI command to verify that that the local Cisco ESA address (172.16.1.55) is statically translated to the public address 192.0.2.55 and that inbound SMTP traffic is allowed to the Cisco ESA.

```
HQ-ASA#  show xlate
12 in use, 38 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
<...output omitted...>
NAT from inside:10.10.3.20 to outside:192.0.2.25
    flags s idle 1:06:34 timeout 0:00:00
NAT from DMZ:172.16.1.50 to outside:192.0.2.50
    flags s idle 0:03:32 timeout 0:00:00
NAT from DMZ:172.16.1.55 to outside:192.0.2.55
    flags s idle 0:00:06 timeout 0:00:00
<...output omitted...>
```

C) On the ASA, use the **show access-list FROM_DMZ** CLI command to verify that SMTP traffic is permitted from the Cisco ESA to the HQ-SRV.

```
HQ-ASA# show access-list FROM_DMZ
access-list FROM_DMZ; 9 elements; name hash: 0xf6b191e3
access-list FROM_DMZ line 1 extended permit object-group HQ_SERVICES object ESA
object MAIL (hitcnt=60) 0xccfd2dc3
  access-list FROM_DMZ line 1 extended permit tcp host 172.16.1.55 host 10.10.3.20
eq smtp (hitcnt=60) 0x91afad05
  access-list FROM_DMZ line 1 extended permit udp host 172.16.1.55 host 10.10.3.20
eq domain (hitcnt=551) 0x0fb3c514
  access-list FROM_DMZ line 1 extended permit tcp host 172.16.1.55 host 10.10.3.20
eq 3268 (hitcnt=575) 0x39fd56e5
  access-list FROM_DMZ line 1 extended permit icmp host 172.16.1.55 host 10.10.3.20
echo (hitcnt=0) 0xc9f52d9f
  access-list FROM_DMZ line 1 extended permit icmp host 172.16.1.55 host 10.10.3.20
echo-reply (hitcnt=0) 0x087983cf
```


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

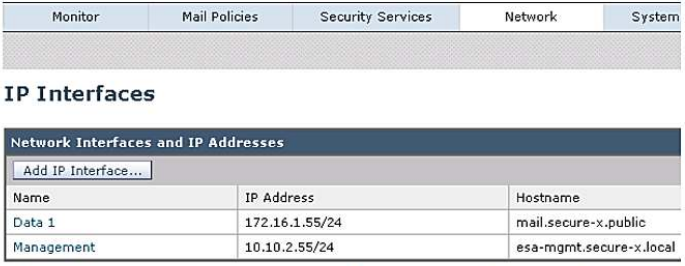
```
access-list FROM_DMZ line 2 extended deny ip any object-group INTERNAL_NETWORKS
(hitcnt=111810) 0xd81ec360
  access-list FROM_DMZ line 2 extended deny ip any 10.10.0.0 255.255.0.0
(hitcnt=111810) 0x877f2d31
  access-list FROM_DMZ line 2 extended deny ip any 172.16.2.0 255.255.255.0
(hitcnt=0) 0xa243e0cd
  access-list FROM_DMZ line 2 extended deny ip any 10.11.11.0 255.255.255.0
(hitcnt=0) 0x28fe244e
access-list FROM_DMZ line 3 extended permit ip any any (hitcnt=325622) 0xe0702b3c
```


https://t.me/learningnets

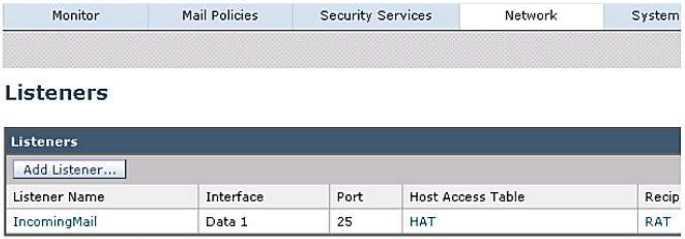
Step 7

Verify the configuration that was entered using the System Setup Wizard:

A) In the Cisco ESA GUI, go to **Network > IP Interfaces** and verify the configuration of the two Cisco ESA interfaces:



B) Go to **Network > Listeners**. The listener that is named IncomingMail should be enabled on the Data 1 interface with default HAT and RAT.



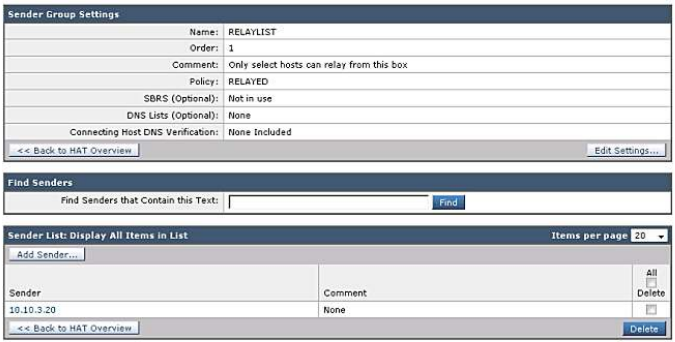
C) Go to **Network > SMTP Routes**. You should see that the route to **secure-x.public** points to the HQ-SRV (10.10.3.20). Incoming emails from SP-SRV to Employee PC will use this SMTP route.

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



D) Go to **Mail Policies > HAT Overview** and click on **RELAYLIST** sender group. You should see that emails sent from the HQ-SRV (10.10.3.20) will be relayed.

Sender Group: RELAYLIST - IncomingMail 172.16.1.55:25



E) Go to **Mail Policies > RAT**, where you will see that incoming emails to only **secure-x.public** domain are accepted.

Recipient Access Table Overview



F) Browse the remaining settings of your choice. The other settings should all use the default values.

https://t.me/learningnets

Step 8

From the external email client (**user1@sp.public**) on SP-SRV, send an email to an internal user **it1@secure-x.public.**

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

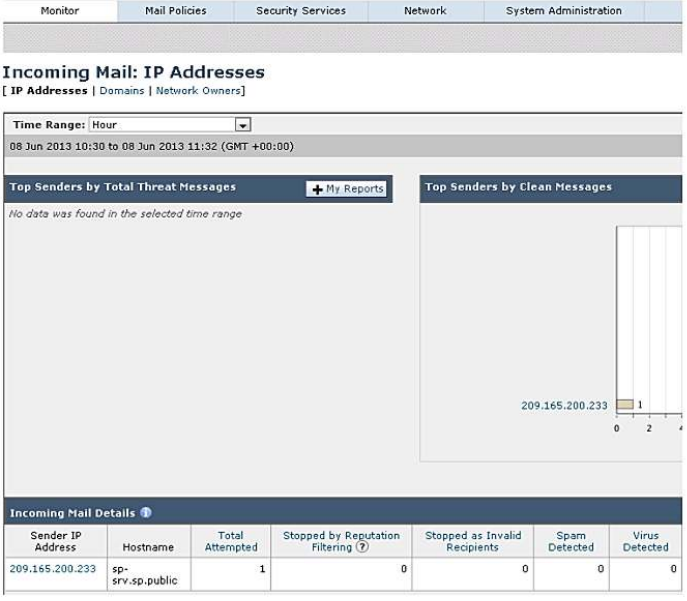
Step 9

Verify the incoming email delivery:

A) Check that the email arrived in the recipient inbox. If this fails, proceed with the following verification steps to determine the reason for the failure.

B) In the Cisco ESA GUI, go to **Monitor > Reports > Incoming Mail** and click **IP Addresses**. Information about the email is in the **Incoming Mail Details** section at the bottom of the page.

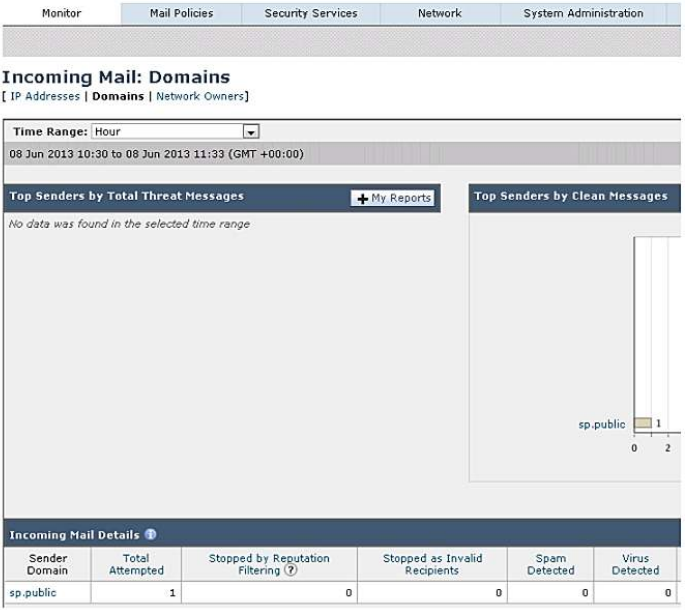
C) Use the **Time Range** drop down box to see the available settings, set the time range to **Hour**.



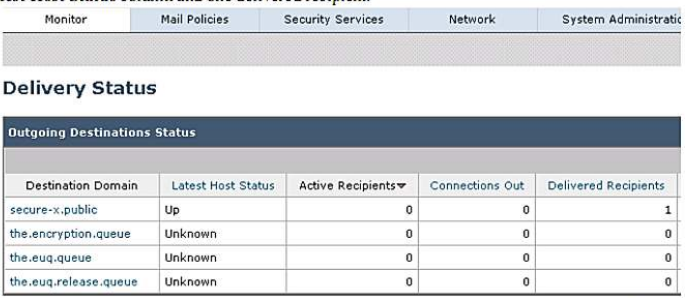
Note In general it will take some time for the events to show up in reports.

D) In the **Monitor > Reports > Incoming Mail** page, click **Domains**. Examine the information in the **Incoming Mail Details** section.

https://t.me/learningnets

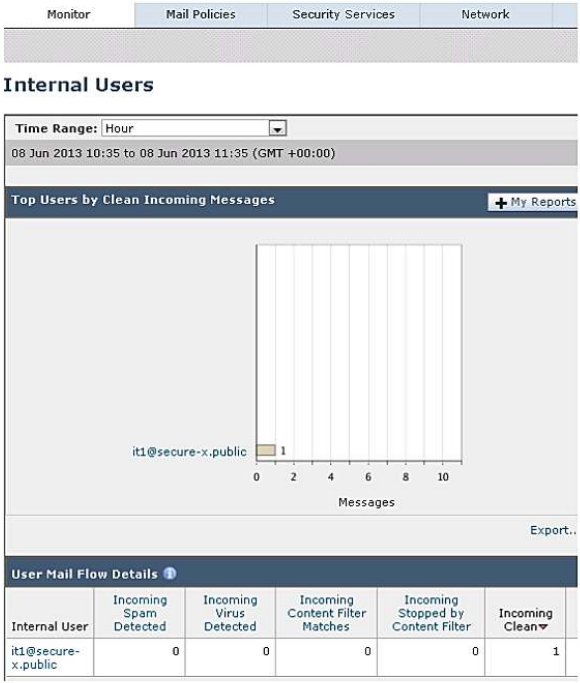


E) Go to **Monitor > Reports > Delivery Status**. The **secure-x.public** domain should have "Up" in the **Latest Host Status** column and one delivered recipient.



F) Go to **Monitor > Reports > Internal Users**. Examine the graph and the **User Mail Flow Details** section. You should see one clean mail sent to the internal recipient.

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



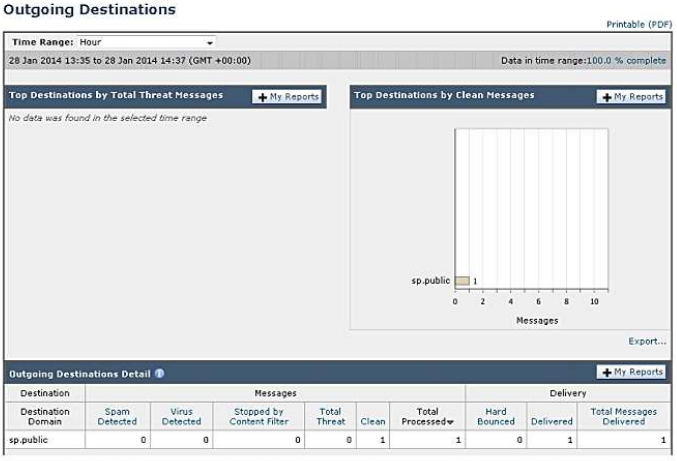
https://t.me/learningnets

Step 10

In the internal email client (**it1@secure-x.public**) on Employee PC, send an email to **user1@sp.public**. Verify the outgoing mail delivery:

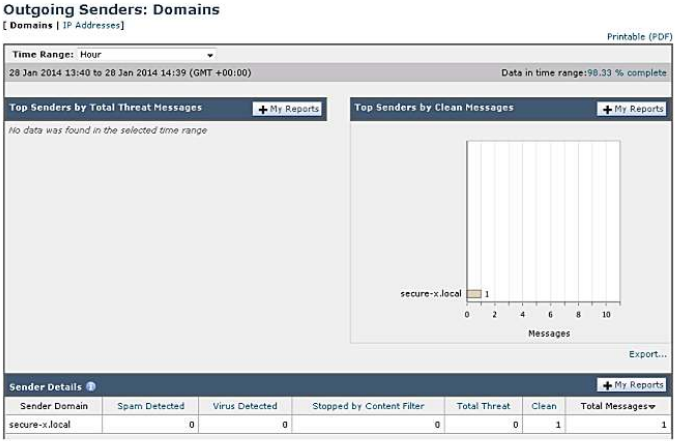
A) On the SP-SRV, check the inbox of **user1@sp.public**. The email should have arrived.

B) In the Cisco ESA GUI, go to **Monitor > Reports > Outgoing Destinations**. You should see information about outgoing emails.



C) In the Cisco ESA GUI, go to **Monitor > Reports > Outgoing Senders**. Examine the sender information that is displayed when you click the **Domains** and **IP Addresses** links at the top of the page.

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



Task 3: Integrate the Cisco ESA with LDAP and Enable LDAP Accept Query

In this task you will integrate the Cisco ESA with Microsoft Active Directory, which is a type of LDAP server. With this task completed, the Cisco ESA can check the recipient email addresses in Active Directory using LDAP Accept Query.

Note The integration of the Cisco ESA with the Active Directory using LDAP Accept Query will allow the Cisco ESA to forward inbound email only to existing internal user accounts. Without the integration, all mails to the internal mail domain would be delivered to the internal server. The server would then discard the mails for non-existing user accounts.

Activity Procedure

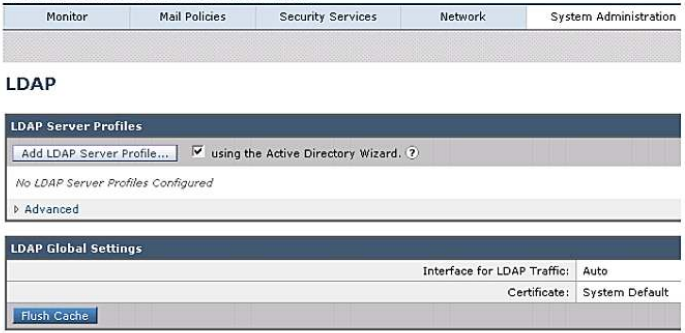
Complete the following steps:

https://t.me/learningnets

Step 1

Configure the Active Directory settings by using the Active Directory Wizard:

A) Go to **System Administration > LDAP**. Check the **Using the Active Directory Wizard** check box and click the **Add LDAP Server Profile** button.



B) Configure these settings in the **Active Directory Settings** table:

- **Profile name: AD**
- **Host Name: 10.10.3.20**
- **Port: 3268**
- **Credentials: secure-x\administrator** with the password **Ci5coAdmin**



C) Click **Next**. In the optional **Directory Lookup Test** page, click **Finish**. Do not perform test now, you will perform the test in the next step.

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


Test Directory Settings
Directory Lookup Test (optional)
Recipient Email Address:
Test Query
Enter an email address you know is in your Active Directory.
Connection Status:
« Previous
Cancel
Finish

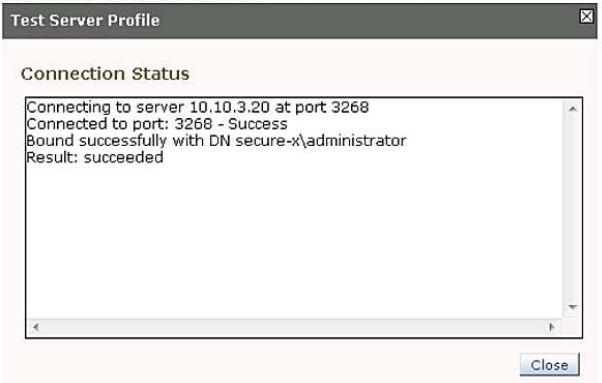
Step 2

Tune the LDAP server parameters and test the integration:

A) In the **System Administration > LDAP** menu, click the **AD** link. The **Edit LDAP Server Profile** page should open.

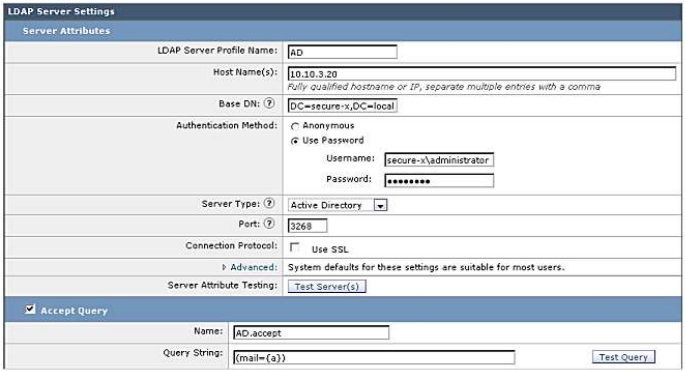


B) In the **Edit LDAP Server Profile** page, click the **Test Server(s)** button to test the connection to AD server on HQ-SRV. Test should be successful.

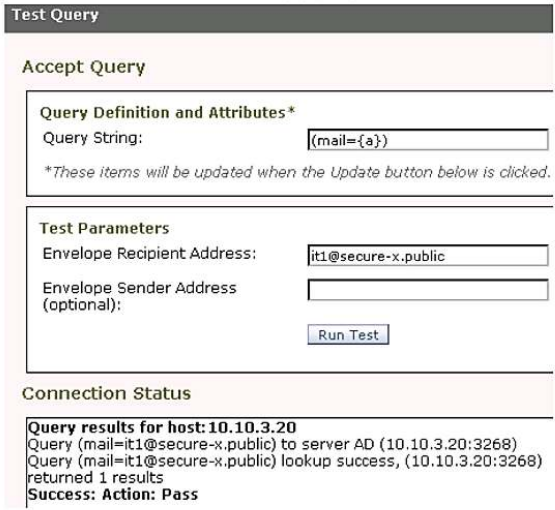


C) In the **Edit LDAP Server Profile** page, go to the **Accept Query** section and change the **Query String** to **(mail={a})**. Clear the **Group Query** check box.

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



D) Click the **Test Query** button in the **Accept Query** section. Enter **it1@secure-x.public** in the **Envelope Recipient Address** field and click **Run Test**. The test should succeed.



E) Click **Update** and then click **Submit**. Click the **Commit Changes** button at the top right.

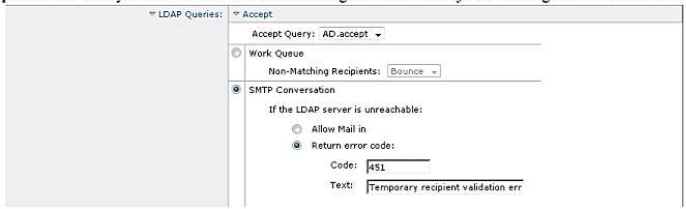
https://t.me/learningnets



F) Optionally, you can enter a comment and click the **Commit Changes** button.

Step 3

Navigate to **Network > Listeners** and click on the **IncomingMail** listener. Search for **LDAP Queries > Accept** section. Verify that e-mails sent to nonexisting users will be rejected during SMTP conversation.



Step 4

Enable message tracking on the Cisco ESA.

A) In the Cisco ESA GUI, go to **Security Services > Centralized Services > Message Tracking**. Click the **Enable** button.

B) Check the **Enable Message Tracking Service** check box. Click **Submit**.



C) Commit the changes.

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

Step 5

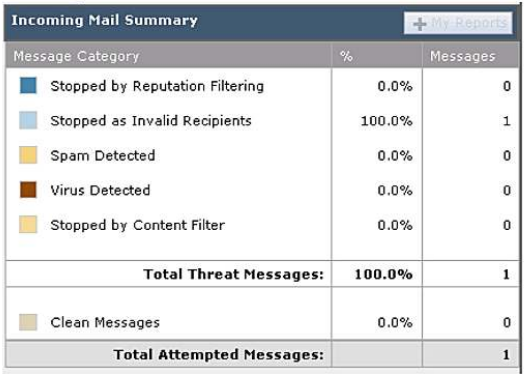
From the external email client (**user1@sp.public**) on SP-SRV, send an email to a nonexisting internal user (for example, **support1@secure-x.public**).

https://t.me/learningnets

Step 6

Examine the incoming mail process:

A) In the Cisco ESA GUI, go to **Monitor > Reports > Overview**. You should see an email within the **Stopped as Invalid Recipients** row.



Incoming Mail Summary — My Reports

Message Category	%	Messages
Stopped by Reputation Filtering	0.0%	0
Stopped as Invalid Recipients	100.0%	1
Spam Detected	0.0%	0
Virus Detected	0.0%	0
Stopped by Content Filter	0.0%	0
Total Threat Messages:	**100.0%**	**1**
Clean Messages	0.0%	0
Total Attempted Messages:		**1**

Note In general it will take some time for the events to show up in reports.

B) In the **Monitor > Reports > Incoming Mail** page, you should see more details about the email being stopped as invalid recipient.



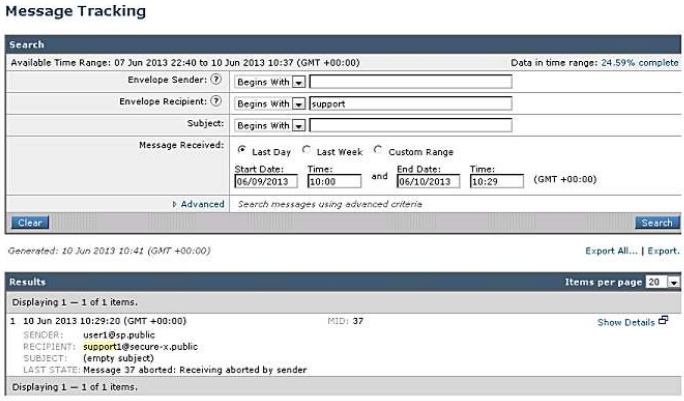
Incoming Mail Details — My Reports

Sender IP Address	Hostname	Total Attempted	Stopped by Reputation Filtering	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Clean
209.165.200.233	mail.sp.public	4	0	1	0	0	0	1	3

Columns... | Export...

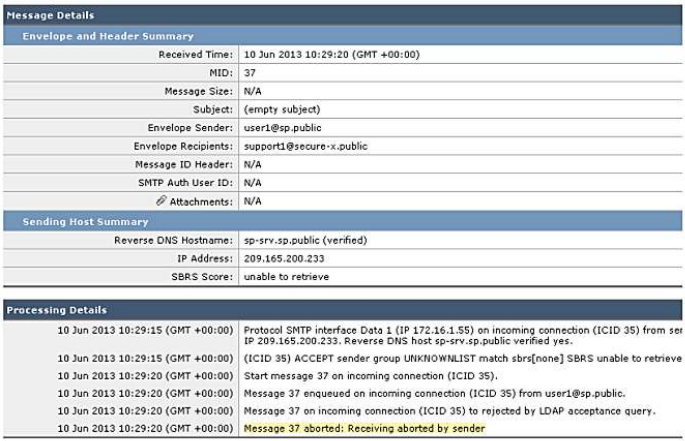
C) Go to **Monitor > Message Tracking**. In the **Envelope Recipient** search condition, set it to "**Begins with support**." Click the **Search** button. You should see similar results as shown below.

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



Note In general it will take some time for the events to show up message tracking.

D) Click the **Show Details** button. Examine the information. The LDAP acceptance query should reject the message.



Note If you did not configure the LDAP server integration, the email would be delivered to the destination server and the destination server would discard it.

https://t.me/learningnets

Task 4: Configure Incoming Content Filters and Mail Policies

In this task you will configure the incoming content filters and mail policies to block compressed attachments from untrusted sources. The content filters and mail policies should block compressed attachments sent from **sp.public** domain.

Activity Procedure

Complete the following steps:

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

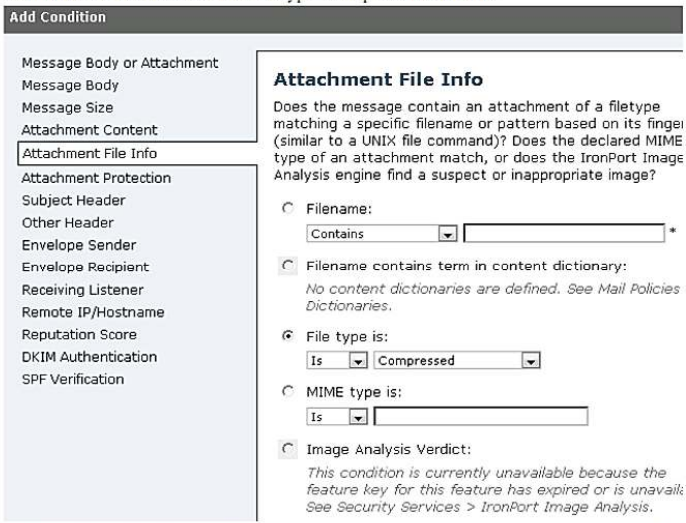
Step 1

Configure an incoming content filter that blocks compressed attachments.

A) Go to **Mail Policies > Email Security Manager > Incoming Content Filters** and click the **Add Filter** button.

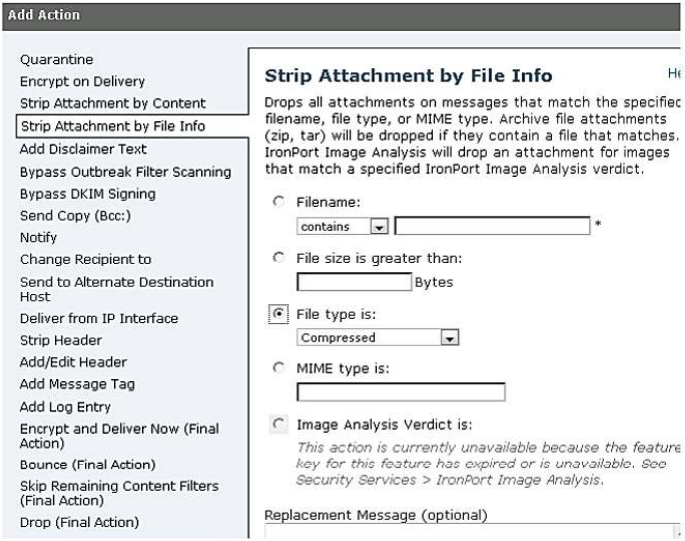
B) Create a filter named "**Drop-compressed-attachments**" with these settings:

- Add a condition by clicking the **Add Contdition** button. Choose **Attachment File Info**. Set the condition rule so that the attachment file type is compressed. Click **OK**.

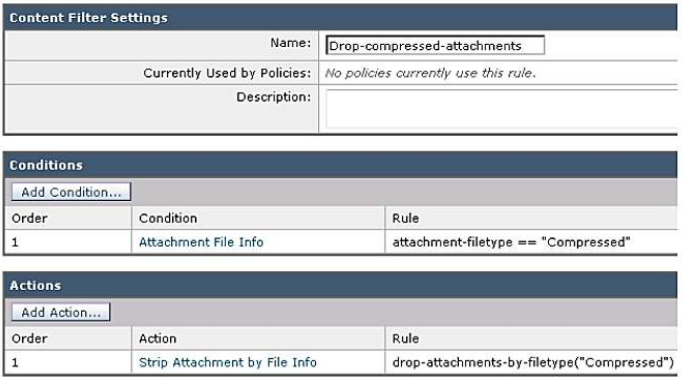


- Add an action by clicking the **Add Action** button. Choose **Strip Attachment by File Info**. Set the condition rule so that the attachment file type is compressed. Click **OK**.

https://t.me/learningnets



- Examine the incoming content filter configuration.



- **Submit** and **Commit** the configuration.

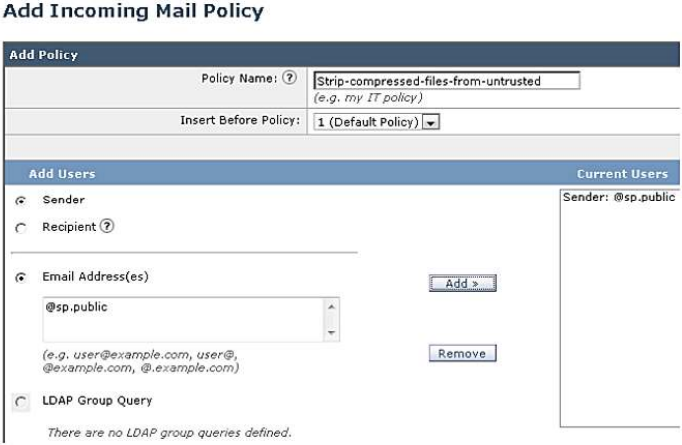
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 2

Create an incoming email policy that applies the content filter (**Drop-compressed-attachments**) when receiving emails from untrusted sources:

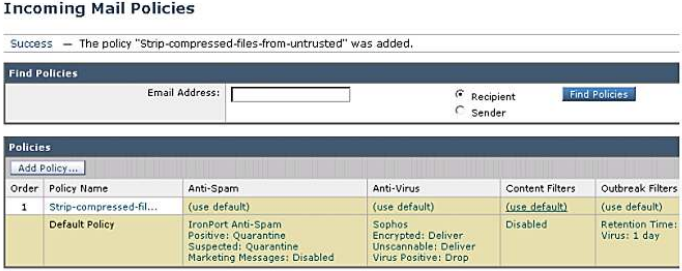
A) Go to **Mail Policies > Email Security Manager > Incoming Mail Policies**. Click the **Add Policy** button.

B) Create a policy named "**Strip-compressed-files-from-untrusted**" with these settings:
   - **Insert Before Policy: 1 (Default Policy)**
   - **Add Users > Sender > @sp.public**



   - **Submit** the configuration.

C) In the **Policies** table, click the **(use default)** link in the **Content Filters** column of the new policy row.

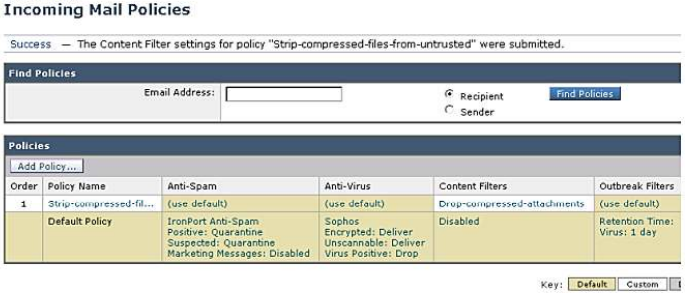


https://t.me/learningnets

D) In the **Mail Policies: Content Filters** page, choose **Enable Content Filters (Customize Settings)** from the drop-down list, and check the **Enable** check box for the filter that is named **Drop-compressed-attachments**.



E) Click **Submit**.



Step 3

Commit the changes.

Step 4

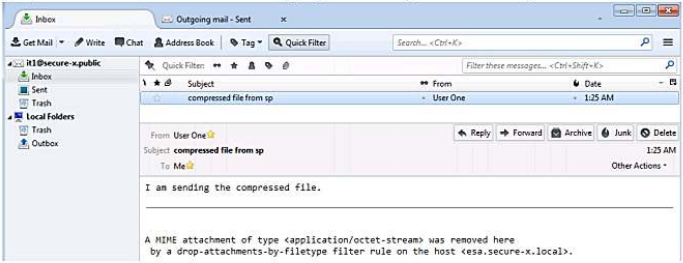
On the SP-SRV, use the 7-Zip program to compress a file **C:\ipconfig.txt**. Right-click on the file and click the **7-Zip > Add to "ipconfig.7z"**. Attach the compressed file in an email to the internal user **it1@secure-x.public**. Verify that the email is delivered to the recipient. Make sure that the compressed attachment is received.

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

Step 5

Verify the content filter operation:

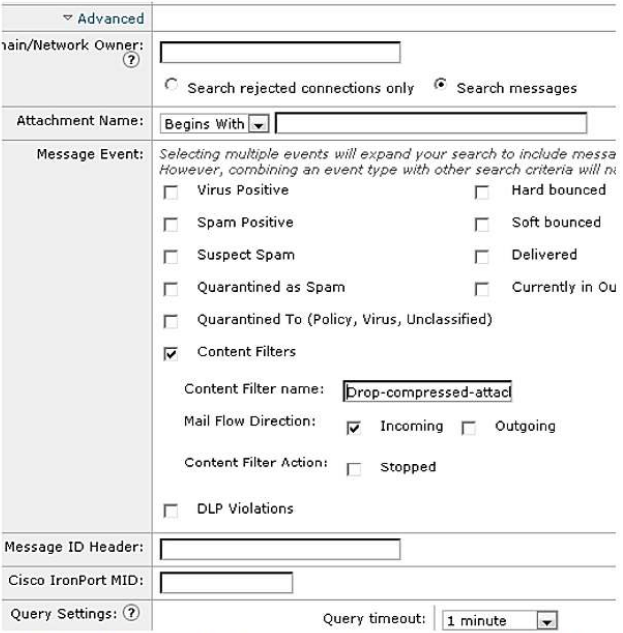
A) On Employee PC, verify that the email has arrived in the recipient inbox, that the attachment has been stripped, and that the Cisco ESA added an appropriate message within the body of the email.



Note	If the mail to the **it1@secure-x.public** user fails, make sure in the AD server profile, the LDAP Accept Query string has been set to **(mail={a})** from the previous task. If it is using the default LDAP Accept Query string, the LDAP lookup will fail.

B) In **Monitor > Message Tracking**, delete the **support** string in the **Envelope Recipient** field. Under Advanced, in the **Message Event** section, check the **Content Filters** check box. Enter **Drop-compressed-attachments** in the **Content Filter Name** field.

https://t.me/learningnets

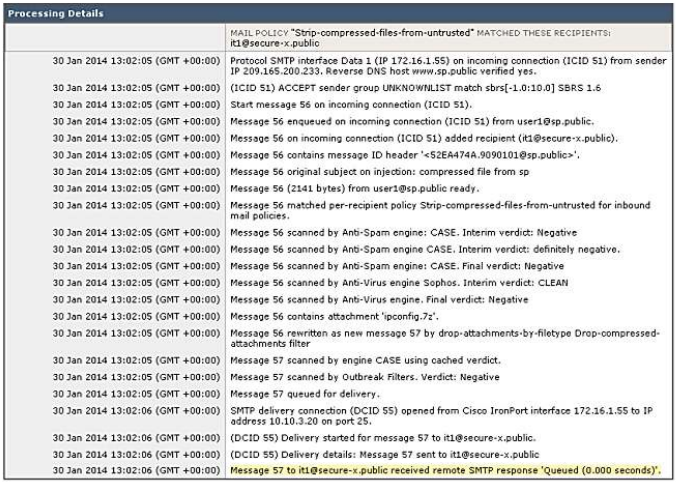


C) Click **Search**. Wait a while and refresh the page. You should see one message in the search result at the bottom of the page.



D) Click the **Show Details** button. Examine the information. You should see that a compressed attachment has been identified and stripped and that the message has been rewritten.

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



Processing Details	
	MAIL POLICY "Strip-compressed-files-from-untrusted" MATCHED THESE RECIPIENTS: it1@secure-x.public
30 Jan 2014 13:02:05 (GMT +00:00)	Protocol SMTP interface Data 1 (IP 172.16.1.55) on incoming connection (ICID 51) from sender IP 209.165.200.233. Reverse DNS host www.sp.public verified yes.
30 Jan 2014 13:02:05 (GMT +00:00)	(ICID 51) ACCEPT sender group UNKNOWNLIST match sbrs[-1.0:10.0] SBRS 1.6
30 Jan 2014 13:02:05 (GMT +00:00)	Start message 56 on incoming connection (ICID 51).
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 enqueued on incoming connection (ICID 51) from user1@sp.public.
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 on incoming connection (ICID 51) added recipient (it1@secure-x.public).
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 contains message ID header '<52EA474A.9090101@sp.public>'.
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 original subject on injection: compressed file from sp
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 (2141 bytes) from user1@sp.public ready.
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 matched per-recipient policy Strip-compressed-files-from-untrusted for inbound mail policies.
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 scanned by Anti-Spam engine: CASE. Final verdict: Negative
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 scanned by Anti-Virus engine. Final verdict: Negative
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 contains attachment 'ipconfig.7z'.
30 Jan 2014 13:02:05 (GMT +00:00)	Message 56 rewritten as new message 57 by drop-attachments-by-filetype Drop-compressed-attachments filter
30 Jan 2014 13:02:05 (GMT +00:00)	Message 57 scanned by engine CASE using cached verdict.
30 Jan 2014 13:02:05 (GMT +00:00)	Message 57 scanned by Outbreak Filters. Verdict: Negative
30 Jan 2014 13:02:05 (GMT +00:00)	Message 57 queued for delivery.
30 Jan 2014 13:02:06 (GMT +00:00)	SMTP delivery connection (DCID 55) opened from Cisco IronPort interface 172.16.1.55 to IP address 10.10.3.20 on port 25.
30 Jan 2014 13:02:06 (GMT +00:00)	(DCID 55) Delivery started for message 57 to it1@secure-x.public.
30 Jan 2014 13:02:06 (GMT +00:00)	(DCID 55) Delivery details: Message 57 sent to it1@secure-x.public
30 Jan 2014 13:02:06 (GMT +00:00)	Message 57 to it1@secure-x.public received remote SMTP response 'Queued (0.000 seconds)'.

Task 5: Configure Outbound Data Loss Prevention

In this task you will configure the outgoing mail policies for Data Loss Prevention. The Data Loss Prevention policies will block the leakage of credit card information and sensitive network data documents. Credit card information must not be sent to any external destinations. Network diagrams must not be sent to any external domains.

Activity Procedure

Complete the following steps:

https://t.me/learningnets

Step 1

Enable the **RSA Email DLP**:

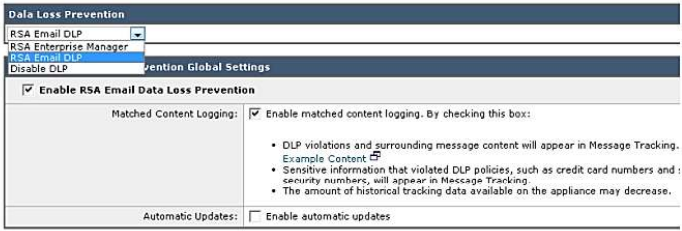
A) Go to **Security Services > Data Loss Prevention > RSA Email DLP**.

Note	Loading the DLP pages may take about 2 minutes per page.

B) You should see that DLP is disabled. Click the **Enable** button.

C) In the **Data Loss Prevention Global Settings** section, choose **RSA Email DLP** from the drop-down list, verify that the **Enable RSA Email Data Loss Prevention** check box is checked, and enable the **Matched Content Logging** setting. Click **Submit**.

Data Loss Prevention Global Settings



D) Verify that the DLP settings have been enabled successfully.

Data Loss Prevention Settings

Success — RSA DLP Policies are now available to this IronPort appliance.

- Configure policies in the DLP Policy Manager, then apply them to use the DLP Assessment Wizard to guide you.

RSA Email Data Loss Prevention Settings	
Data Loss Prevention:	Enabled
Matched Content Logging:	Enabled
Automatic Updates:	Disabled

Export DLP Configuration
For faster set up, export the existing Email DLP configuration then import it to the RSA Enter

Current DLP Version Files		
File Type	Last Update	Current Version
RSA DLP Engine	Never Updated	3.0.2.31
No updates in progress.		

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

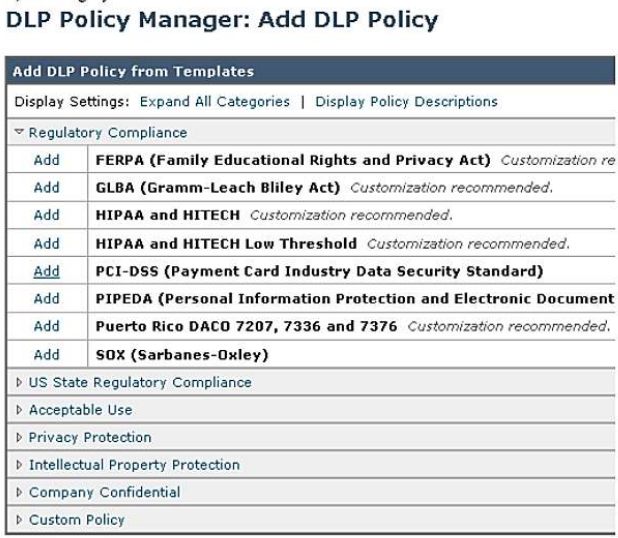
Step 2

Create a DLP policy that prevents credit card information from being leaked:

A) Go to **Mail Policies > DLP Policy Manager**. Click the **Add DLP Policy** button.



B) In the **Add DLP Policy from Templates** section, expand the **Regulatory Compliance** group. Examine the subcategories. Click the **Add** link next to the **PCI-DSS (Payment Card Industry Data Security Standard)** subcategory.



C) Leave the PCI-DSS policy settings at their default values and click **Submit**.

https://t.me/learningnets

Mail Policies: DLP: Policy: PCI-DSS (Payment Card Industry Data Sec

Policy: PCI-DSS (Payment Card Industry Data Security Standard)	
DLP Policy Name:	PCI-DSS (Payment Card Industry Data Security Standard)
Description:	Identifies documents and transmissions that contain credit cardholder data regulated by the Payment Card Industry Data Security Standard (PCI DSS) 2.0. The Standard is applicable
Content Matching Classifier:	Credit Card Number OR Credit Card Track Data
▷ Filter Senders and Recipients:	*Restrict this DLP policy by specific recipients and senders.*
▷ Filter Attachments:	*Restrict this DLP policy to detect specific attachment types.*
▷ Filter Message Tags:	*Restrict this DLP policy to detect message tags.*

Severity Settings	
Critical Severity Incident:	Default Action
High Severity Incident:	Inherit Action from Critical Severity Incident
Medium Severity Incident:	Inherit Action from High Severity Incident
Low Severity Incident:	Inherit Action from Medium Severity Incident
Severity Scale:	IGNORE: 0 - 9 / LOW: 10 - 34 / MEDIUM: 35 - 59 / HIGH: 60 - 89 / CRITICAL: 90 - 100

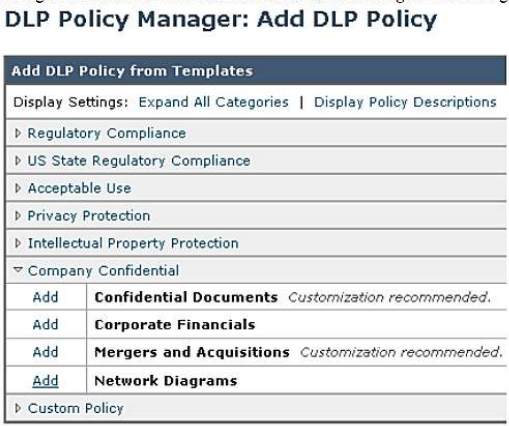
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 3

Create a DLP policy that prevents sensitive network information from being sent to untrusted domains.

A) Under **Mail Policies > DLP Policy Manager**, click the **Add DLP Policy** button.

B) In the **Add DLP Policy from Templates** section, expand the **Company Confidential** category. Examine the subcategories. Click the **Add** link next to the **Network Diagrams** subcategory.

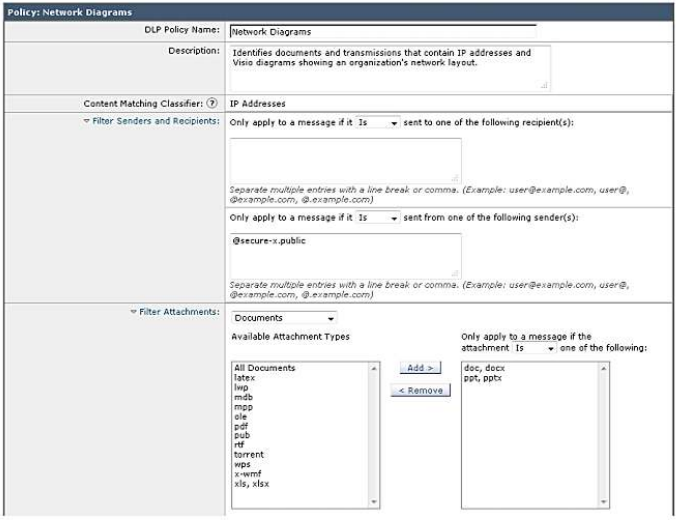


C) Click **Filter Senders and Receipients**. Customize the **Network Diagrams** policy with these rules:

- Apply to a message if it is sent from **@secure-x.public**.
- Apply to a message if an attachment has one of the following extensions: **.doc, .docx, .ppt, or .pptx.**

https://t.me/learningnets

Mail Policies: DLP: Policy: Network Diagrams



Note Choose **Documents** from the **Filter Attachments** drop-down list to select the **.doc, .docx, .ppt, and .pptx** file types.

- Leave the other settings at their default values and click **Submit**.

DLP Policy Manager

Success — Settings have been saved.

Active DLP Policies for Outgoing Mail

Add DLP Policy...

Order	DLP Policy
1	PCI-DSS (Payment Card Industry Data Security Standard)
2	Network Diagrams

Edit Policy Order...

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

Step 4

Change the default message action to drop.

A) Go to **Mail Policies > DLP Message Actions**. Click **Default Action**.

B) Verify that the **Drop** is selected in the **Message Action** drop-down list.

DLP Policy Manager: Edit Message Action



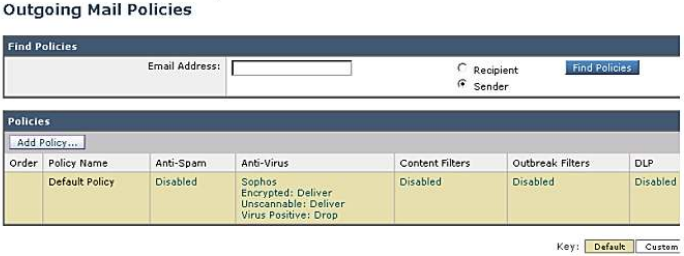
C) Click **Submit**.

https://t.me/learningnets

Step 5

Configure the outgoing policy for DLP:

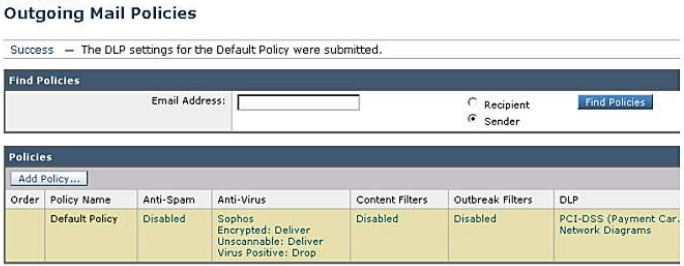
A) Go to **Mail Policies > Email Security Manager > Outgoing Mail Policies**. Click the link in the **DLP** column of the **Default Policy** entry.



B) Choose **Enable DLP (Customize Settings)** from the drop-down list, and enable both configured policies.



C) Click **Submit**.



Note Alternatively, you may add another outgoing mail policy, before the default policy, which would activate the DLP policies.

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

Step 6

Commit the changes.

https://t.me/learningnets

Step 7

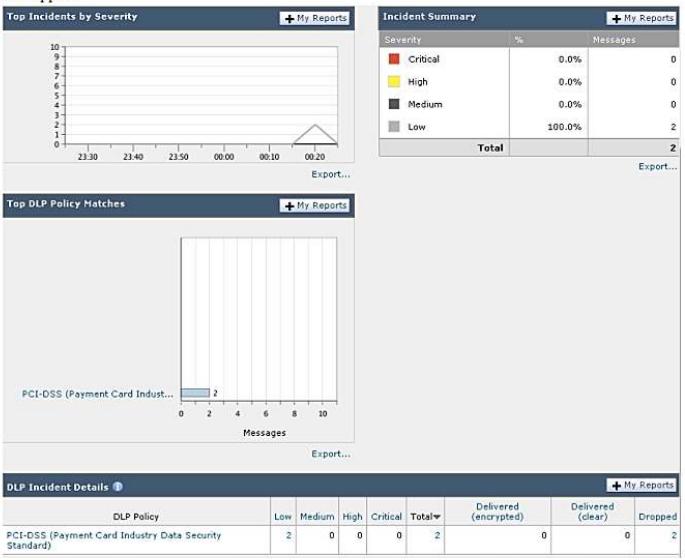
Verify that any credit card information is protected:

A) From the internal email client (for example, **it1@secure-x.public**), send emails that contain credit card information. Send the emails to **user1@sp.public** and to **partner1@partner.public**.

```
4999-9999-9999-9996 01/15
```

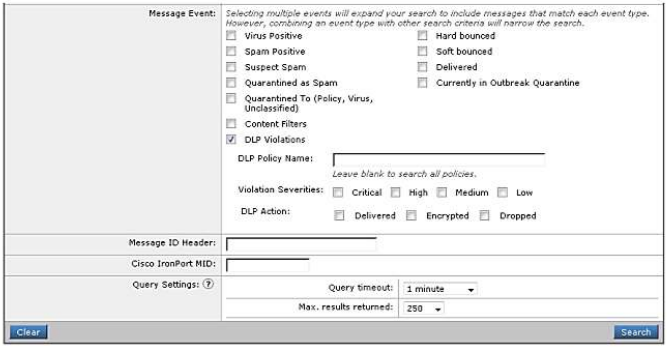
B) Verify that the emails do not reach their destinations.

C) Go to **Monitor > Reports > DLP Incidents**. Verify that the two breaches against the PCI-DSS (Payment Card Industry Data Security Standard) setting have been identified and that the emails have been dropped.



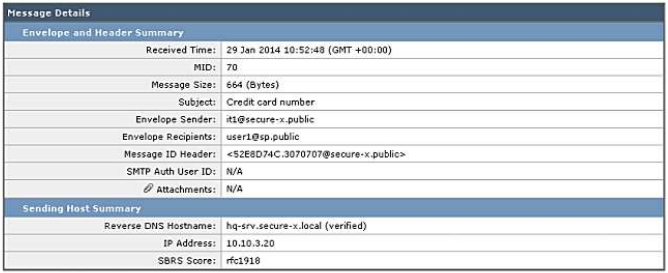
D) Go to **Monitor > Message Tracking**. Clear all previous selections and check the **DLP Violations** check box. Search for the appropriate messages. They should appear at the bottom of the page.

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



E) View the details by clicking **Show Details** button. You should see the following: "Message scanned by DLP engine. Violation severity: LOW (Risk Factor: 10). DLP match: PCI-DSS (Payment Card Industry Data Security Standard)."

https://t.me/learningnets



Message Details

Envelope and Header Summary	
Received Time:	29 Jan 2014 10:52:48 (GMT +00:00)
MID:	70
Message Size:	664 (Bytes)
Subject:	Credit card number
Envelope Sender:	it1@secure-x.public
Envelope Recipients:	user1@sp.public
Message ID Header:	<52E8D74C.3070707@secure-x.public>
SMTP Auth User ID:	N/A
Attachments:	N/A
Sending Host Summary	
Reverse DNS Hostname:	hq-srv.secure-x.local (verified)
IP Address:	10.10.3.20
SBRS Score:	rfc1918

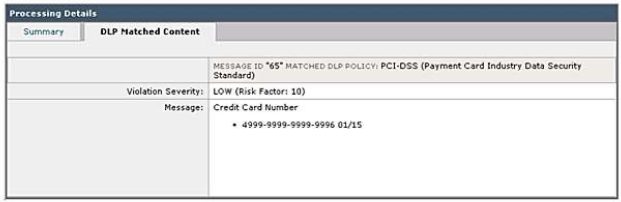
Processing Details

Summary | DLP Matched Content

	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: user1@sp.public
29 Jan 2014 10:52:48 (GMT +00:00)	Protocol SMTP interface Data 1 (IP 172.16.1.55) on incoming connection (ICID 65) from sender IP 10.10.3.20. Reverse DNS host hq-srv.secure-x.local verified yes.
29 Jan 2014 10:52:48 (GMT +00:00)	(ICID 65) RELAY sender group RELAYLIST match 10.10.3.20 SBRS rfc1918
29 Jan 2014 10:52:48 (GMT +00:00)	Start message 70 on incoming connection (ICID 65).
29 Jan 2014 10:52:48 (GMT +00:00)	Message 70 enqueued on incoming connection (ICID 65) from it1@secure-x.public.
29 Jan 2014 10:52:48 (GMT +00:00)	Message 70 on incoming connection (ICID 65) added recipient (user1@sp.public).
29 Jan 2014 10:52:48 (GMT +00:00)	Message 70 contains message ID header '<52E8D74C.3070707@secure-x.public>'.
29 Jan 2014 10:52:48 (GMT +00:00)	Message 70 original subject on injection: Credit card number
29 Jan 2014 10:52:48 (GMT +00:00)	Message 70 (664 bytes) from it1@secure-x.public ready.
29 Jan 2014 10:52:48 (GMT +00:00)	Message 70 matched per-recipient policy DEFAULT for outbound mail policies.
29 Jan 2014 10:52:48 (GMT +00:00)	Message 70 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
29 Jan 2014 10:52:48 (GMT +00:00)	Message 70 scanned by Anti-Virus engine. Final verdict: Negative
29 Jan 2014 10:52:48 (GMT +00:00)	Message 70 scanned by DLP engine. Violation severity: LOW (Risk Factor: 10). DLP policy match: PCI-DSS (Payment Card Industry Data Security Standard)
29 Jan 2014 10:52:48 (GMT +00:00)	Message 70 aborted: Dropped by DLP

F) In the **Processing Details** section, choose the **DLP Matched Content** tab. View the content that matches the DLP policy.

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



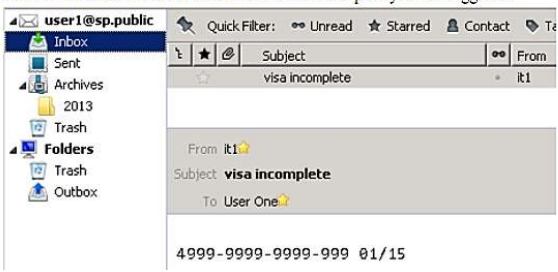
Step 8

Verify that the Cisco ESA passes information that is not classified as credit card data:

A) From the internal email client on Employee PC, send an email with incomplete credit card information to **user1@sp.public**. Remove one digit from the credit card number.

```
4999-9999-9999-999 01/15
```

B) Verify that the email reached the destination and that the DLP policy is not triggered.



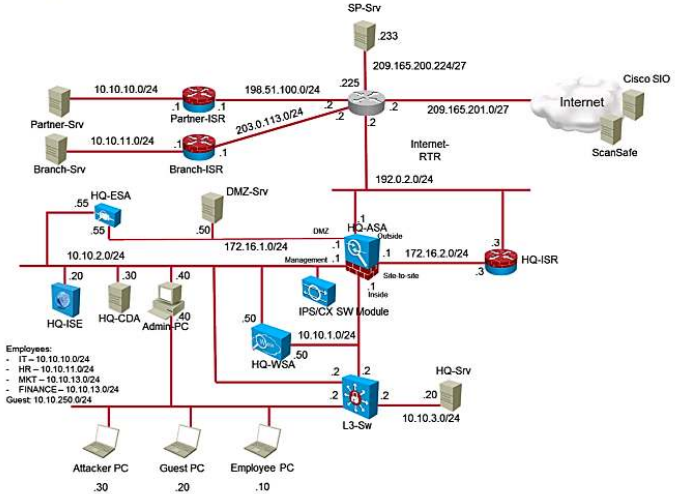
https://t.me/learningnets

Step 9

Verify that sensitive network information is blocked to untrusted destinations:

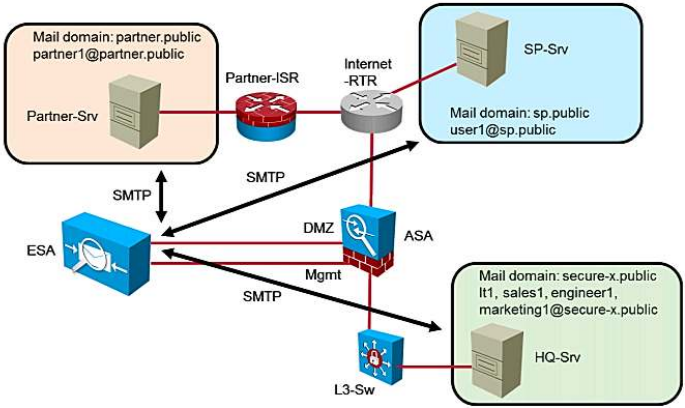
A) From the internal email client (**it1@secure-x.public**) on Employee PC, send two emails to **user1@sp.public** with attachments that each have a .pptx extension.

- The attachment in the first email is located at **D:\Network Diagrams \CCNPSec_Lab_Addressing.pptx**. The file contains addressing information for the CCNP Security lab:

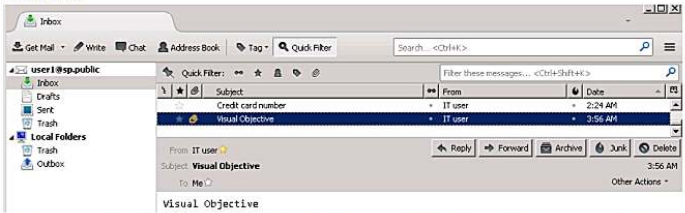


- The attachment in the second mail is located at **D:\Network Diagrams \CCNPSec_LAB_ESA_Visual.pptx**. The file is the Visual Objective as shown below.

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

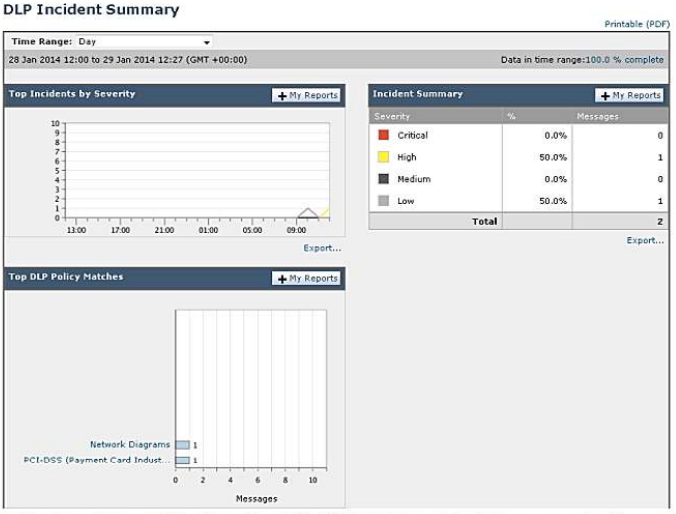


B) Verify that only the email with the Visual Objective reached the destination and that the email contains its attachment.



C) Go to **Monitor > DLP Incidents**. Verify that a breach against the Network Diagrams policy has been identified and the email with Lab Addressing attachment has been dropped.

https://t.me/learningnets

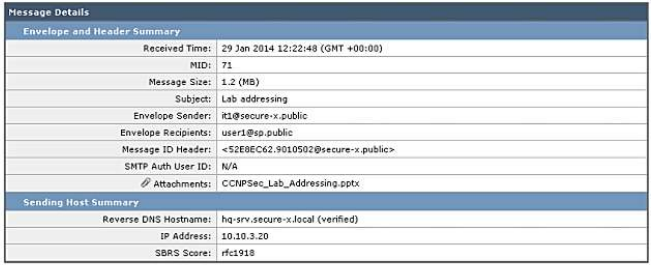


D) Go to **Monitor > Message Tracking**. Search for **DLP violations**. Matched messages should appear.



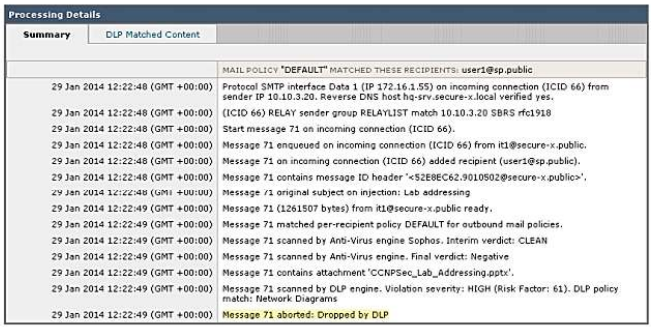
E) View the details by clicking the **Show Details** button. You should see the following: "Message scanned by DLP engine. Violation severity: HIGH (Risk Factor: 61). DLP match: Network Diagrams."

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



Message Details

Envelope and Header Summary	
Received Time:	29 Jan 2014 12:22:48 (GMT +00:00)
MID:	71
Message Size:	1.2 (MB)
Subject:	Lab addressing
Envelope Sender:	it1@secure-x.public
Envelope Recipients:	user1@sp.public
Message ID Header:	<52E8EC62.9010502@secure-x.public>
SMTP Auth User ID:	N/A
Attachments:	CCNPSec_Lab_Addressing.pptx
Sending Host Summary	
Reverse DNS Hostname:	hq-srv.secure-x.local (verified)
IP Address:	10.10.3.20
SBRS Score:	rfc1918



Processing Details

Summary | DLP Matched Content

	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: user1@sp.public
29 Jan 2014 12:22:48 (GMT +00:00)	Protocol SMTP interface Data 1 (IP 172.16.1.55) on incoming connection (ICID 66) from sender IP 10.10.3.20. Reverse DNS host hq-srv.secure-x.local verified yes.
29 Jan 2014 12:22:48 (GMT +00:00)	(ICID 66) RELAY sender group RELAYLIST match 10.10.3.20 SBRS rfc1918
29 Jan 2014 12:22:48 (GMT +00:00)	Start message 71 on incoming connection (ICID 66).
29 Jan 2014 12:22:48 (GMT +00:00)	Message 71 enqueued on incoming connection (ICID 66) from it1@secure-x.public.
29 Jan 2014 12:22:48 (GMT +00:00)	Message 71 on incoming connection (ICID 66) added recipient (user1@sp.public).
29 Jan 2014 12:22:48 (GMT +00:00)	Message 71 contains message ID header '<52E8EC62.9010502@secure-x.public>'.
29 Jan 2014 12:22:48 (GMT +00:00)	Message 71 original subject on injection: Lab addressing
29 Jan 2014 12:22:49 (GMT +00:00)	Message 71 (1261507 bytes) from it1@secure-x.public ready.
29 Jan 2014 12:22:49 (GMT +00:00)	Message 71 matched per-recipient policy DEFAULT for outbound mail policies.
29 Jan 2014 12:22:49 (GMT +00:00)	Message 71 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
29 Jan 2014 12:22:49 (GMT +00:00)	Message 71 scanned by Anti-Virus engine. Final verdict: Negative
29 Jan 2014 12:22:49 (GMT +00:00)	Message 71 contains attachment 'CCNPSec_Lab_Addressing.pptx'.
29 Jan 2014 12:22:49 (GMT +00:00)	Message 71 scanned by DLP engine. Violation severity: HIGH (Risk Factor: 61). DLP policy match: Network Diagrams
29 Jan 2014 12:22:49 (GMT +00:00)	Message 71 aborted: Dropped by DLP

https://t.me/learningnets

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

Lab 5-1: Configure Cisco ASA IPS Software Module

Activity Objective

Lab scenario: The CSO decides to implement an Intrusion Prevention System solution at the headquarter office using the IPS software module on the ASA 5500-X. You will enable and implement the IPS software module on the ASA 5500-X in the Secure-X test lab.

In this lab activity, you will deploy the Cisco Adaptive Security Appliance IPS software module to secure the enterprise resources. You will redirect all traffic from the ASA to the IPS module in inline mode and test its basic operations.

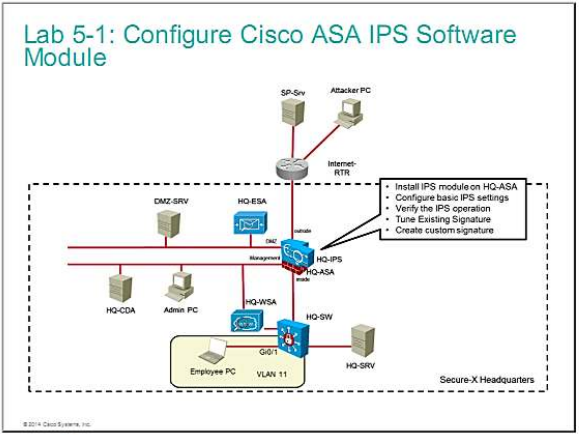
Upon completing this activity, you will be able to meet these objectives:

- Install the Cisco ASA IPS software module and configure basic IPS settings
- Verify the IPS operation
- Tune existing signature
- Create custom signature

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

ASA Commands

Command	Description
class-map *class_name*	Defines class map in global configuration mode.
class *class_name*	References the class map within the policy map
match *condition*	Defines which traffic to match within class map.
policy-map global_policy	Enters policy map configuration mode for global policy.
ips *{inline | promiscuous} {fail-close | fail-open}*	Diverts traffic from the adaptive security appliance to the IPS software module for inspection.

No additional commands are needed to complete this lab exercise. All tasks on IPS are performed with Cisco IDM GUI interface.

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 asacx-5500x-boot-9.1.2-42.img asacx-sys-9.1.2-42.pkg
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
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**
ASA CX	**admin**	**Admin123**
AD Server (installed on HQ-SRV)	**Administrator**	**Ci5coAdmin**
ScanSafe portal (https://scancenter.scansafe.com)	**ccnpsec.scansafe@yahoo.com**	**C!sco!23**

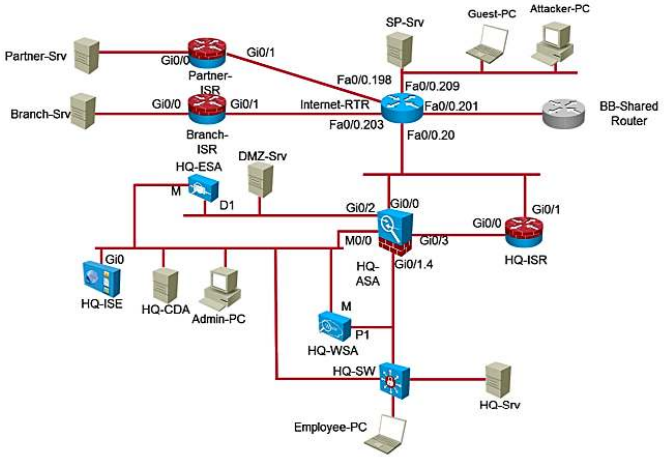
Employee PC is joined to the Active Directory domain.

AD User	AD password	AD Group	Email address in AD properties
it1	**cisco**	IT	**it1@secure-x.public**

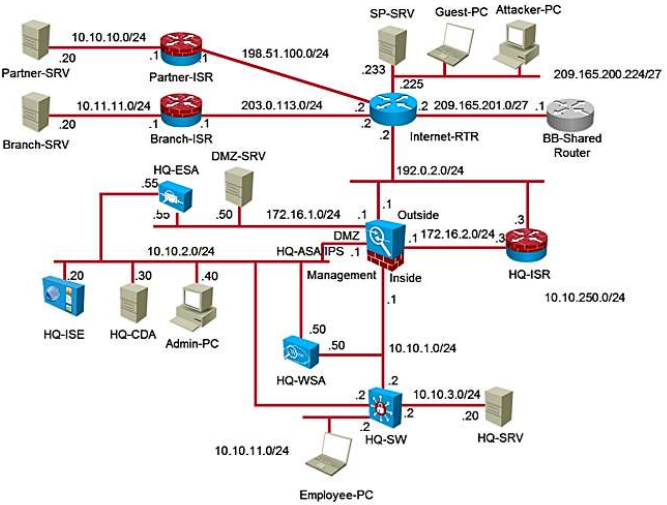
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

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

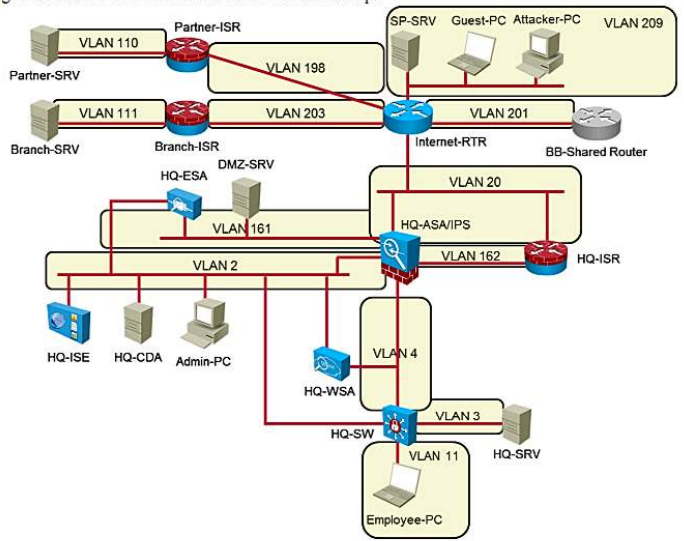


The figure shows the IP addresses that are used in this lab setup.



VLAN Setup

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



Task 1: Install the Cisco ASA IPS Software Module and Configure the Basic IPS Settings

In this task, you will uninstall ASA CX module on HQ-ASA and install IPS module. You will configure the software IPS module on your HQ-ASA adaptive security appliance to operate in inline mode and set up basic management setting on IPS module.

Activity Procedure

Complete the following steps:

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

Step 1

Connect to the HQ-ASA console. Log in as **admin**/**Ci5coAdmin** and **cisco** enable password. Verify that the ASA CX module status is up using **show module** command. Also verify that the IPS module license status is enabled.

```
HQ-ASA# show module

Mod  Card Type                                    Model              Serial No.
---- -------------------------------------------- ------------------ -----------
   0 ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC ASA5515            FCH1709J7WQ
 ips Unknown                                      N/A                FCH1709J7WQ
cxsc ASA CX5515 Security Appliance                ASA CX5515         FCH1709J7WQ

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 4c4e.35ea.8d5c to 4c4e.35ea.8d63  1.0          2.1(9)8      9.1(1)4
 ips 4c4e.35ea.8d5a to 4c4e.35ea.8d5a  N/A          N/A
cxsc 4c4e.35ea.8d5a to 4c4e.35ea.8d5a  N/A          N/A          9.1.2

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- ------------------------
 ips Unknown                        No Image Present Not Applicable
cxsc ASA CX                         Up               9.1.2

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
 ips Unresponsive       Not Applicable
cxsc Up                 Up

Mod  License Name   License Status  Time Remaining
---- -------------- --------------- ---------------
 ips IPS Module     Enabled         177 days
```


https://t.me/learningnets

Step 2

From the ASA CLI, shut down the ASA CX module and verify that the ASA CX module has been shut down.

A) From the ASA CLI, use the **sw-module module cxsc shutdown** command to shut down the ASA CX module.

```
HQ-ASA# sw-module module cxsc shutdown
Shutdown module cxsc? [confirm] <Enter>
Shutdown issued for module cxsc.
```

B) The ASA CX module takes about one minute to go from the **Shutting Down** state to the **Down** state. Use the **show module cxsc** command to verify that the ASA CX module has been shut down.

```
HQ-ASA# show module cxsc
Mod  Card Type                                   Model              Serial No.
---- --------------------------------------------- ------------------ -----------
cxsc ASA CX5515 Security Appliance               ASA CX5515         FCH1710J2Q7
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
cxsc 4c4e.35ea.eabe to 4c4e.35ea.eabe  N/A          N/A          9.1.2
Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
cxsc ASA CX                         Not Applicable   9.1.2
Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
cxsc Down               Not Applicable
```

Step 3

From the ASA CLI, uninstall the ASA CX module after the ASA CX module has been shut down.

```
HQ-ASA# sw-module module cxsc uninstall
Module cxsc will be uninstalled. This will completely remove the disk image associated
with the sw-module including any configuration that existed within it.
Uninstall module cxsc? [confirm] <Enter>
Uninstall issued for module cxsc.
```

Step 4

Save the configuration and reload the HQ-ASA after the ASA CX module has been uninstalled.

A) Save the configuration using **write memory** or **copy running-config startup-config** command.

```
HQ-ASA# copy running-config startup-config
Source filename [running-config]?
Cryptochecksum: 7cf05d26 d1fd6701 1e8ae2cf a4a1a2a9
18046 bytes copied in 0.700 secs
```

B) Reload the HQ-ASA device using **reload** command.

```
HQ-ASA# reload
Proceed with reload? [confirm] <Enter>
```


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

Step 5

View the contents of disk0:. Identify the image for the IPS software module.

```
HHQ-ASA# show disk0
--#--  --length--  -----date/time------  path
   10  4096        Mar 15 2013 01:53:02  log
   22  4096        Mar 15 2013 01:53:18  crypto_archive
   23  4096        Mar 15 2013 01:53:24  coredumpinfo
   24  59          Mar 15 2013 01:53:24  coredumpinfo/coredump.cfg
  139  17989292    Apr 24 2013 16:59:34  asdm-712.bin
  140  42637312    Mar 15 2013 02:00:48  IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip
  141  37435392    Apr 24 2013 16:59:54  asa911-4-smp-k8.bin
  142  200         Oct 14 2013 12:39:44  upgrade_startup_errors_201310141239.log
  143  33699       Sep 17 2013 14:02:26  fr_csd.po
```

Step 6

Recover the IPS module using the image and boot the module using the recovery procedure.

A) Set the recovery image image using **sw-module module ips recover configure image** command.

```
HQ-ASA# sw-module module ips recover configure image disk0:/IPS-SSP_5515-K9-sys-1.1-
a-7.1-4-E4.aip
```

B) Recover the IPS module using **sw-module module ips recover boot** command.

```
HQ-ASA# sw-module module ips recover boot
Module ips will be recovered. This may erase all configuration and all data
on that device and attempt to download/install a new image for it. This may take
several minutes.
Recover module ips? [confirm] <Enter>
Recover issued for module ips.
```

C) The IPS module may take up to five minutes to recover. Check the information using **show module ips details** command to make sure that the status, application status, and data plane status are up

```
HQ-ASA# show module ips details
Getting details from the Service Module, please wait...
Card Type:          ASA 5515-X IPS Security Services Processor
Model:              ASA5515-IPS
Hardware version:   N/A
Serial Number:      FCH1710J2Q7
Firmware version:   N/A
Software version:   7.1(4)E4
MAC Address Range:  4c4e.35ea.eabe to 4c4e.35ea.eabe
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(4)E4
Data Plane Status:  Up
Status:             Up
License:            IPS Module  Enabled  179 days
Mgmt IP addr:       192.168.1.2
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.168.1.1
Mgmt web ports:     443
Mgmt TLS enabled:   true
```


https://t.me/learningnets

Step 7

Establish session from HQ-ASA console to the IPS module using **session ips** command. Log in using default username **cisco** and password **cisco**. You will be prompted to change the password. Use **Ci5coAdmin** as new password.

```
HQ-ASA# session ips
Opening command session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-^X'.
login: cisco
Password: cisco
You are required to change your password immediately (password aged)
Changing password for cisco.
(current) password: cisco
New password: Ci5coAdmin
Retype new password: Ci5coAdmin
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
***LICENSE NOTICE***
There is no license key installed on this IPS platform.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
```


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

Step 8

The CLI setup script will be started automatically. Use these paramaters to setup the IPS module:

Hostname: **HQ-IPS**

IP addresss: **10.10.2.5**

Default gateway: **10.10.2.2**

Allow management access from network: **10.10.2.0/24**

Other settings: Use the default

```
    --- Basic Setup ---
    --- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Current time: Sun Feb  2 16:40:14 2014
Setup Configuration last modified: Sun Feb 02 16:35:11 2014
Enter host name[sensor]: HQ-IPS
Enter IP interface[192.168.1.2/24,192.168.1.1]: 10.10.2.5/24,10.10.2.2
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.10.2.0/24
Permit:
Use DNS server for Global Correlation?[no]:
Use HTTP proxy server for Global Correlation?[no]:
Modify system clock settings?[no]:
Participation in the SensorBase Network allows Cisco to
collect aggregated statistics about traffic sent to your IPS.
SensorBase Network Participation level?[off]:
The following configuration was entered.
service host
network-settings
host-ip 10.10.2.5/24,10.10.2.2
host-name HQ-IPS
telnet-option disabled
access-list 10.10.2.0/24
ftp-timeout 300
no login-banner-text
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy no-proxy
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service global-correlation
network-participation off
exit
[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.
```


https://t.me/learningnets

```
Enter your selection[3]:2
sensor#
```

Step 9

Return to the console of HQ-ASA by pressing **<Ctrl, Shift, 6> <Ctrl, Shift, 6> x**.

```
sensor# <Ctrl, Shift, 6> <Ctrl, Shift, 6> x
HQ-ASA#
```

Step 10

Establish session from HQ-ASA console to the IPS module using **session ips** command again. Log in using default username **cisco** and password **Ci5coAdmin**. You will see the new hostname for IPS module, which is **HQ-IPS**.

```
HQ-ASA# session ips
Opening command session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-^X'.
login: cisco
Password: Ci5coAdmin
Last login: Mon Feb  3 09:53:38 from 127.0.1.1
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
***LICENSE NOTICE***
There is no license key installed on this IPS platform.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
HQ-IPS#
```


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

Step 11

Configure the ASA to direct all IP traffic to IPS module in inline mode.

A) Configure class map **IPS_TRAFFIC**, which matches all IP traffic.

```
HQ-ASA(config)# class-map IPS_TRAFFIC
HQ-ASA(config-cmap)#  match any
```

B) Append the newly crated class map to the global_policy service policy. Redirect traffic in inline mode and permit traffic if the IPS module fails.

```
HQ-ASA(config)# policy-map global_policy
HQ-ASA(config-pmap)# class IPS_TRAFFIC
HQ-ASA(config-pmap-c)# ips inline fail-open
```

Task 2: Verify the IPS Operations

Since IPS module is set to operate in inline mode, you will now test that suspicious traffic activates one of the default IPS signature. You will access the IPS GUI called IDM from the Admin PC.

https://t.me/learningnets

Activity Procedure

Step 1

Launch the IPS Device Manager (IDM) from the Admin PC.

A) Connect to Admin PC. Log in as **student** with the password **Ci5coAdmin**.

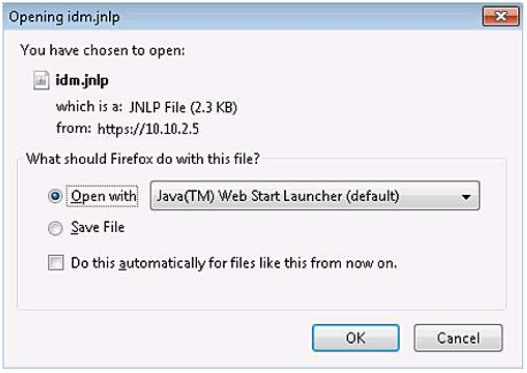
B) Open a browser and connect via HTTPS to the IPS IP address (https://10.10.2.5).

C) Accept certificate warning issue and proceed.

D) Click **Run IDM**.



E) Select **Open with** and click **OK**.



F) Click **Continue**.

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



G) Check the **I accpet the risk and want to run this application** and click **Run**.



H) Log in using username **cisco** and password **Ci5coAdmin**. Click **OK**.

https://t.me/learningnets

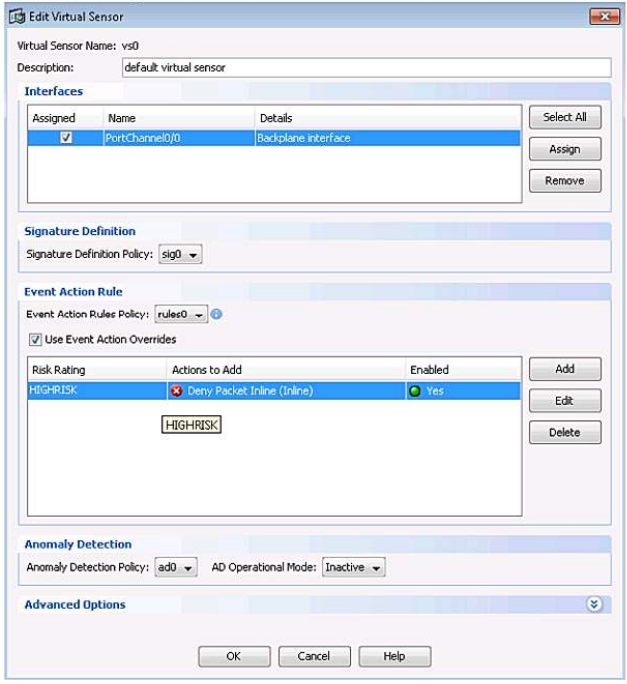


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 2

Make sure that IPS backplane interface is assigned to the default virtual sensor **vs0**.

In Cisco IDM, navigate to **Configuration > Policies > IPS Policies**, select **vs0** virtual sensor and click **Edit**. Make sure that **Assigned** checkbox is selected in the **Interfaces** section.





https://t.me/learningnets

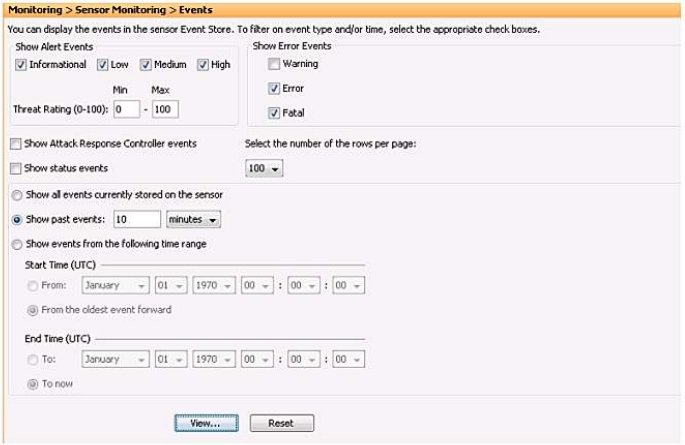
Step 3

Launch the **Apache Server .ht file access** attack from Attacker PC to the DMZ-Srv. Verify that traffic arriving at HQ-ASA is redirected to the IPS module and the 5194 signature ID is triggered.

A) Connect to Attacker PC. Log in as **root** with the password **Ci5coAdmin**. Navigate to **Applications > Internet > Iceweasel Internet Browser** and open web browser. Try to browse to DMZ-Srv at www.secure-x.public/sales-app.htaccesscode. This will fire alarm on IPS upon detecting an HTTP request for the **.htaccess** file. The **.htaccess** file can provide a way for attackers to make configuration changes to override the security features configured on an Apache server.

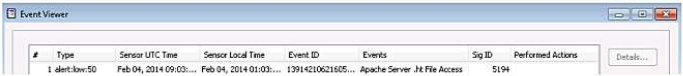


B) Return to Admin PC and in Cisco IDM, choose **Monitoring > Sensor Monitoring > Events**. Examine the events for last **10 minutes** and click **View**.

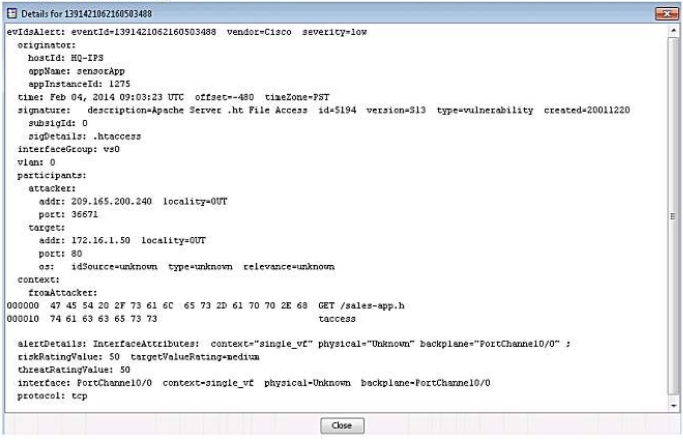


C) You will see that signature with ID **5194** (**Apache Server .ht File Access**) is triggered. This alarm fires upon detecting an HTTP request for the **.htaccess** file.

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



D) Select the triggered event and click **Details...** button. You should see attacker IP address for the event is **209.165.200.240** (Attacker PC) and target IP address is **172.16.1.50** (DMZ-Srv). You can also see the risk rating and threat rating values for the event.



Note The IP address for Attacker PC might differ in your case as it is DHCP assigned.

Task 3: Tune Existing Signature

In this task, you will tune the **Apache Server .ht File Access** IPS signature to improve the prevention capabilities in this specific lab environment. You will tune the **Apache Server .ht File Access** signature (ID 5194) by using the event action filters to ensure that attacks only from specific sources will trigger the signature . You will make sure that the signature is triggered when performed from all sources, except from the Admin PC.

Activity Procedure

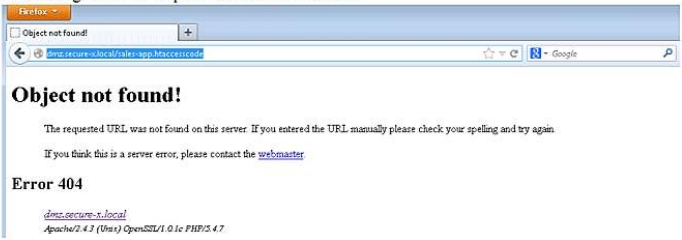
Complete the following steps:

https://t.me/learningnets

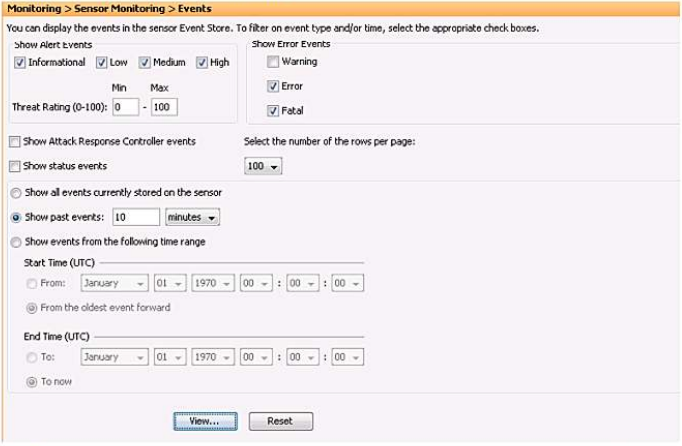
Step 1

Launch the **Apache Server .ht file access** attack from AdminPC to the DMZ-Srv.

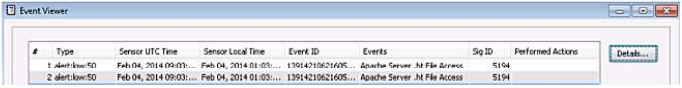
A) Connect to Admin PC logged in as **student** with the password **Ci5coAdmin**. Open web browser. Try to browse to DMZ-Srv at http://dmz.secure-x.local/sales-app.htaccesscode. This will fire alarm on IPS upon detecting an HTTP request for the **.htaccess** file.



B) Return to Admin PC and in Cisco IDM, choose **Monitoring > Sensor Monitoring > Events**. Examine the events for last **10 minutes** and click **View**.

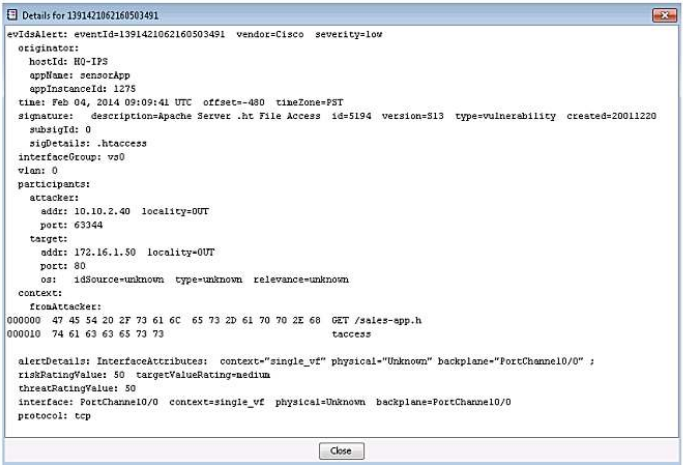


C) You will see that signature with ID **5194** is triggered. This alarm fires upon detecting an HTTP request for the **.htaccess** file.



D) Select the latest triggered event and click **Details...** button. You should see attacker IP address for the event is **10.10.2.40** (Admin PC) and target IP address is **172.16.1.50** (DMZ-Srv). You can also see the risk rating and threat rating values for the event.

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



https://t.me/learningnets

Step 2

Tune the **Apache Server .htaccess File Access** signature (signature ID **5194**) by using the event action filters to ensure that only attacks from specific sources trigger the alarm. In this scenario, Admin PC is assumed to have a legitimate access to **.htaccess** file on DMZ-Srv. Admin PC should not trigger **Apache Server .htaccess File Access** signature.

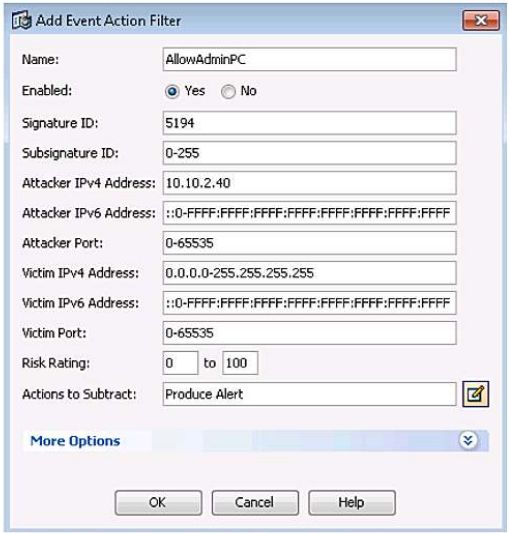
A) In IDM, choose **Configuration > Policies > Signature Definitions > sig0 > All Signatures** and search for ID **5194**. Examine the signature configuration. You should see that the action is set to **Produce Alert** for all three of the 5194 sub-signature IDs. The 5194 signature fires upon detecting an HTTP request for a specific .ht file. Each sub-signature fires upon a different file request: SubSig 0 fires on request of the .htaccess file, SubSig 1 fires on request of the .htpasswd file, SubSig 2 fires on request of the .htgroup file.



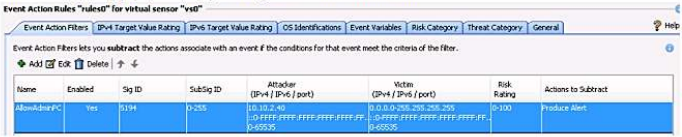
B) Create an action filter that subtracts the alerts when the .ht file access is initiated from the legitimate system (Admin PC).

- Choose **Configuration > Policies > IPS Policies**. In the **Event Action Rules** section, click the **Event Action Filters** tab.
- Create a new filter (**AllowAdminPC**) that subtracts the action **Produce Alert** for the signature ID **5194** for the Admin PC's attacker IP address (**10.10.2.40**).

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



– Click **OK** and **Apply** and verify setting for event action filter.

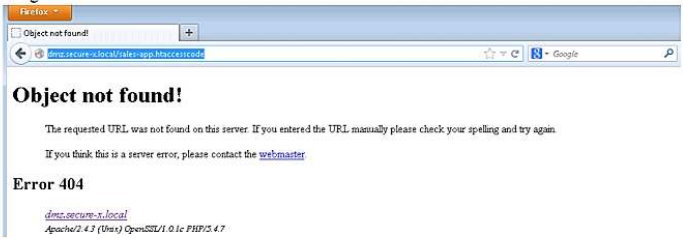


https://t.me/learningnets

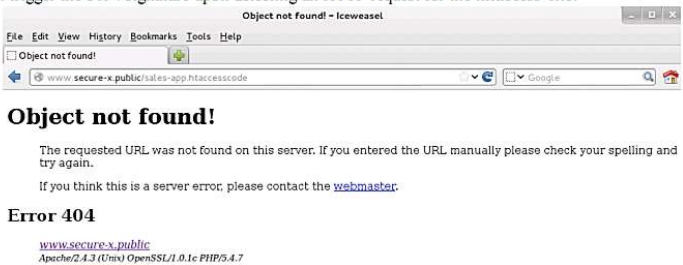
Step 3

Launch the **Apache Server .ht file access** attacks again from AdminPC to the DMZ-Srv and from Attacker PC to DMZ-Srv.

A) Connect to Admin PC. Try to browse to http://dmz.secure-x.local/sales-app.htaccesscode. This should not fire alarm on IPS upon detecting an HTTP request for the **.htaccess** file, because of configured event action filter. From the Cisco IDM, choose **Monitoring > Sensor Monitoring > Events**. Examine the events for last 10 minutes again and click View, you should not see a new event triggered by the 5194 signature.

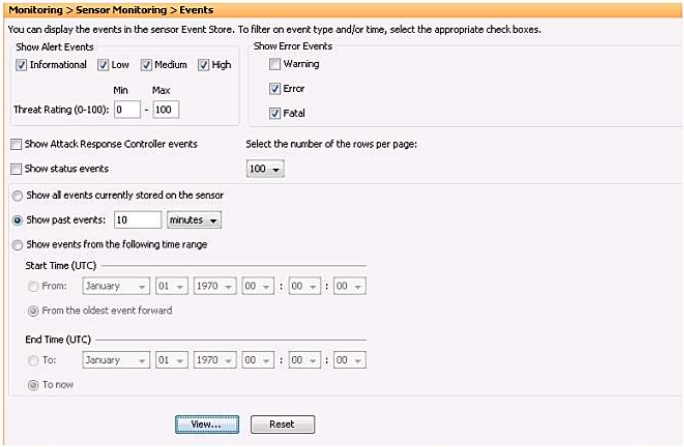


B) Connect to Attacker PC. Navigate to **Applications > Internet > Iceweasel Internet Browser** and open web browser. Try to browse to DMZ-Srv at www.secure-x.public/sales-app.htaccesscode. This should still trigger the 5194 signature upon detecting an HTTP request for the **.htaccess** file.

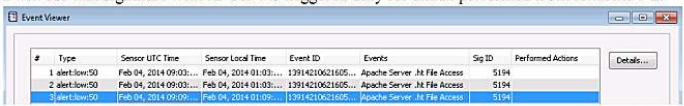


C) Return to the Admin PC and in Cisco IDM, choose **Monitoring > Sensor Monitoring > Events**. Examine the events for last **10 minutes** and click **View**.

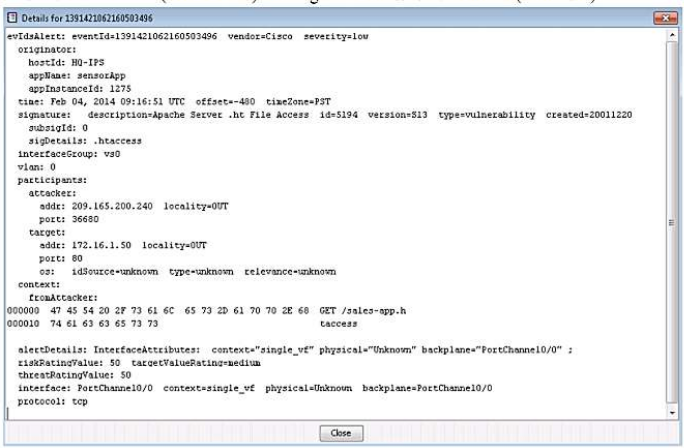
https://t.me/learningnets
© 2014 Cisco Systems, Inc.



D) You will see that signature with ID **5194** is triggered only for attack performed from Attacker PC.



E) Select the latest triggered event and click **Details...** button. You should see attacker IP address for the event is **209.165.200.240** (Attacker PC) and target IP address is **172.16.1.50** (DMZ-Srv).



Note	The IP address for Attacker PC might differ in your case as it is DHCP assigned.

Task 4: Create Custom Signature

In this task, you will implement custom signature. The signature should block web-based access to the **calc.exe** application, which has been found to contain a bug.

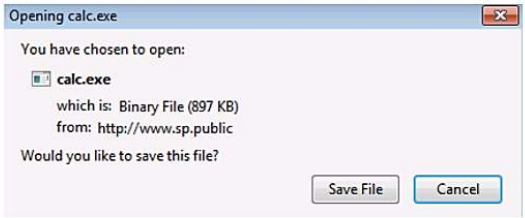
Activity Procedure

Complete the following steps:

Step 1

Connect and log in to Employee PC as the **it1** secure-x domain user with the **cisco** password. Open a browser, and browse the content in the **Files** folder on the SP Server (www.sp.public). Click the **Windows Calculator Program (.exe)** link. You should be able to save the **calc.exe** application, which has been found to have a bug.





Note	If you get prompted for username and password by HQ-WSA, restart the Employee PC to be transparently authenticated. Web traffic destined from Employee PC is diverted through HQ-WSA, which was configured to authenticate users transparently.

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

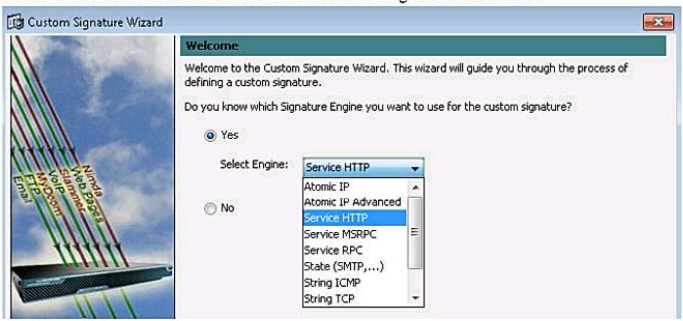
Step 2

Use the signature wizard to create a custom signature that fires after detecting the string **calc.exe** in **HTTP URI**.

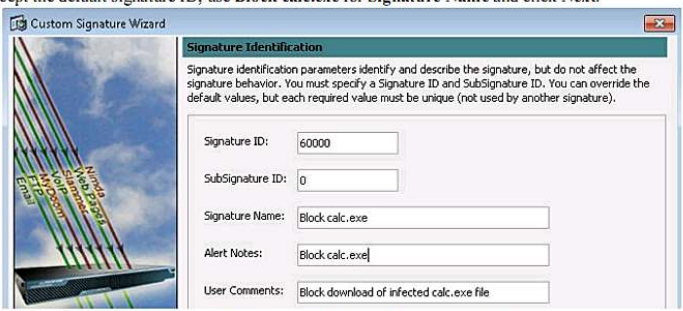
A) Return to the Admin PC and in Cisco IDM, choose **Configuration > Policies > Signature Definitions > sig 0** and click any signature category. Click the **Signature Wizard** button in the upper right corner.



B) Select the **Yes** radio button and select the **Service.HTTP** engine and click **Next**.

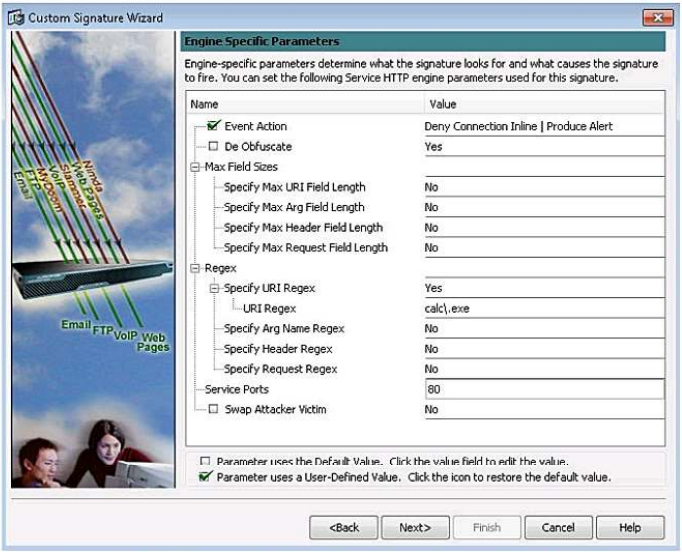


C) Accept the default signature ID, use **Block calc.exe** for **Signature Name** and click **Next**.

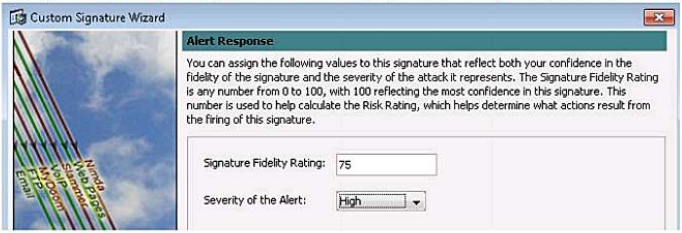


D) Set the actions to **Deny Connection Inline**, and **Produce Alert**. Use the URI Regex to match the string **calc.exe**. Set the service port to **80**. Click **Next**.

https://t.me/learningnets



E) Set the **Signature Fidelity Rating** to the default value (**75**) and the severity to **High**. Click **Next**.



F) Click the **Finish** button and **Apply** the configuration.

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

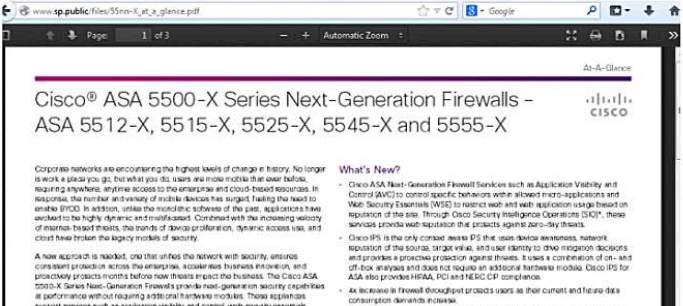

Custom Signature Wizard
Alert Behavior
The sensor sends the first alert for each address set, and then a summary of all the alerts that occur on this address set over the next 15 seconds.
The summary alert contains the same information as the original alert and provides an interval summary that shows the number of total alerts per time interval. A summary counts signature firings on attacker address.
The sensor will not automatically upgrade (or downgrade) to global summarization mode.
To accept this alert behavior and create the custom signature, click Finish. To change the alert behavior, click Advanced.
Advanced...
Email
FTP
VoIP
Web Pages
<Back
Next>
Finish
Cancel
Help

Step 3

On the Employee PC, close the browser, reopen it, and browse the **Files** folder on the SP Server (www.sp.public). Try to open the **Windows Calculator Program (.exe)** file. This should trigger the custom signature and the IPS should deny this connection inline. You should get the "This Page Cannot Be Displayed" message from the HQ-WSA, because the web traffic from the Employee PC is redirected to HQ-WSA proxy by the HQ-ASA using transparent proxy mode. WCCP redirection on ASA occurs before traffic being redirected to IPS module (which blocks attempt of downloading calc.exe file via HTTP page), this is why HQ-WSA cannot display web page containing **calc.exe** string in HTTP URI.



From the Employee PC, browse the **Files** folder again on the SP Server (www.sp.public). This time, try to open the **ASA 5500-X Series Datasheet** (.pdf) file instead of the **Windows Calculator Program (.exe)** file, the IPS should permit this connection since it will not match the custom signature.



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

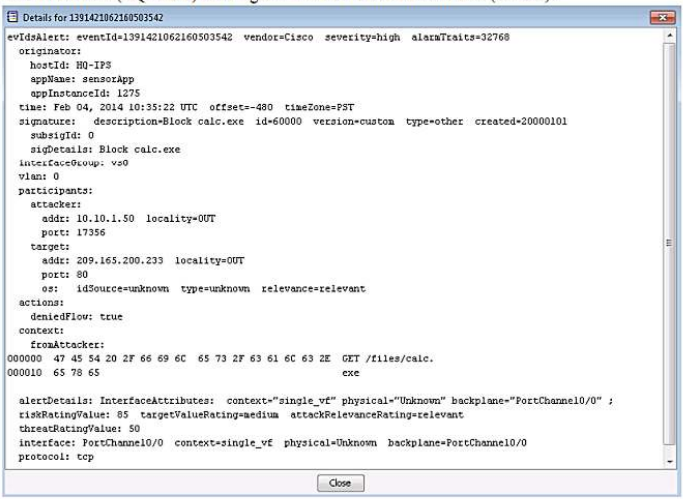
Step 4

Verify that custom signature was triggered.

Return to the Admin PC and in Cisco IDM, choose **Monitoring > Sensor Monitoring > Events**. Examine the events for last **10 minutes** and click **View**. You will see that custom signature with ID 60000 is triggered for attack performed from Employee PC.



Select the latest triggered event and click **Details...** button. You should see attacker IP address for the event is **10.10.1.50** (HQ-WSA) and target IP address is **209.165.200.233** (SP-Srv).



Note Web traffic destined from Employee PC was configured to be redirected to HQ-WSA, while web traffic destined from Admin PC is not being redirected.

https://t.me/learningnets

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

Lab Answer Keys

Lab 1-1: Explore the Cisco ASA (CX) NGFW and PRSM

Task 4: Explore the ASA (CX) NGFW CLI

Step 5

start and **stop**

Task 5: Explore the On-Box PRSM GUI

Step 3

Dashboard > Network overview. 9.1.2 (42) should be the current running software version in the lab.

Step 4

Events, Policies, Device, and Administration

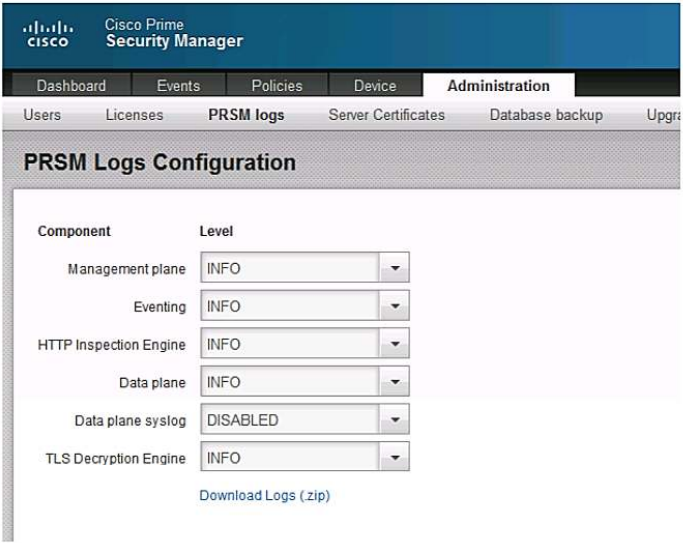
Step 5

Policies, Objects, and Applications

Step 8

Please see screen capture below for the default logging levels.

https://t.me/learningnets



Step 9

The Cisco ASA (CX) NGFW checks the Cisco SIO for application signature updates every 5 minutes by default.

Task 6: Redirect Traffic from the ASA to ASA (CX) NGFW

Step 2

By default, all traffic flow is allowed, no identity (user authentication) is required, and no traffic is decrypted.

Task 7: Explore the System Predefined Default ASA (CX) NGFW Policy Objects

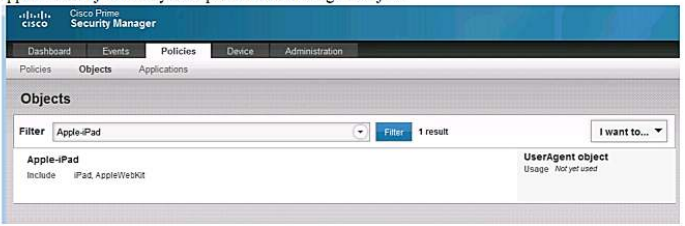
Step 1

The All Remote Devices object is a system predefined objects that can be viewed but cannot be edited or deleted.

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

Step 2

The Apple-iPad object is a system predefined user agent object.



Step 3

Web reputation profile object. From -10 to -6.



Step 4

icmp-echo.



Step 5

Known users and unknown users

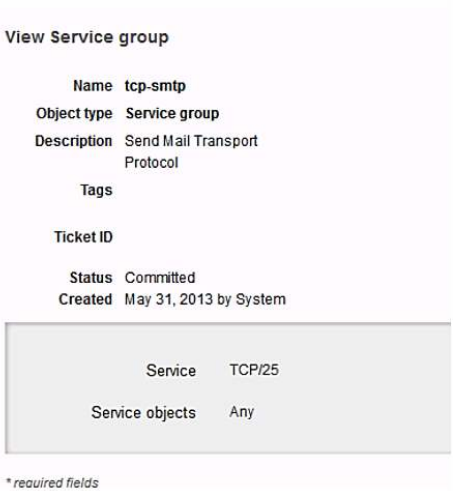


https://t.me/learningnets

Step 6

TCP/25





Step 7

TCP/53 or UDP/53



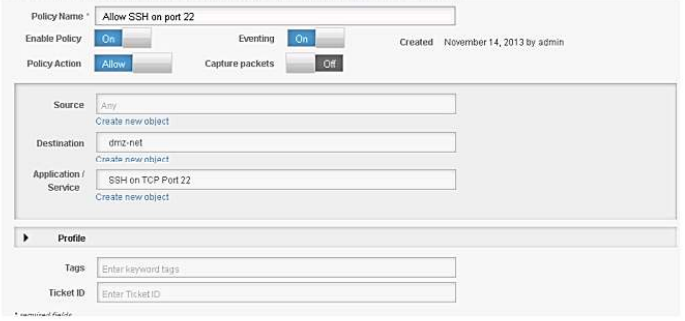
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

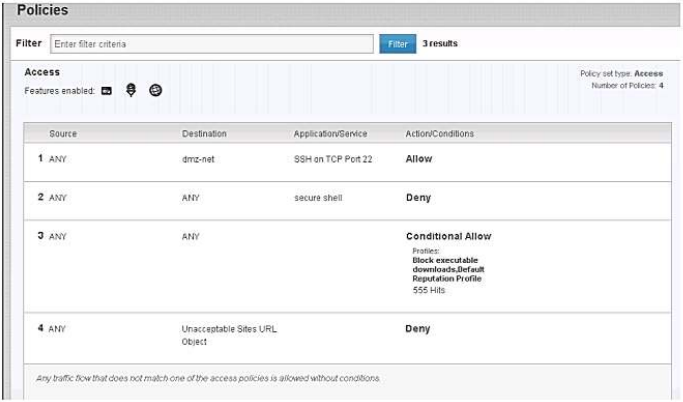
Lab 1-2: Configure Cisco ASA (CX) NGFW Access Policy

Task 4: Optional Challenge Lab Task: Configure ASA CX Access Policies

Step 2

The solution to the optional challenge lab task follows:
Be sure that the more specific access policy only allowing SSH traffic on TCP port 22 to any destinations on the DMZ network is above the access policy denying all SSH traffic.





Lab 1-3: Configure Cisco ASA (CX) NGFW Identity Policy

Task 1: Configure an ASA CX Identity Policy Using Active Authentication

Step 1

There are no solutions for this lab.

Lab 1-4: Configure Cisco ASA (CX) NGFW Decryption Policy

Task 1: Enable Cisco ASA (CX) NGFW Decryption

Step 1

There are no solutions for this lab.

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

Lab 2-1: Configure Cisco Web Security Appliance Explicit Proxy and User Authentication

Task 1: Verify Basic Cisco WSA Settings

Step 1

There are no solutions for this lab.

Lab 2-2: Configure Cisco Web Security Appliance Acceptable Use Controls

Task 1: Implement the Cisco WSA in Transparent Proxy Mode

Step 1

There are no solutions for this lab.

Lab 3-1: Configure Cisco Cloud Web Security Connector on ISR G2 and on AnyConnect

Task 1: Enable the CWS Connector on the Partner ISR G2 Router

Step 1

There are no solutions for this lab.

Step 5

Partner-ISR(config)#**parameter-map type content-scan global**
Partner-ISR(config-profile)#**server scansafe primary name proxy1753.scansafe.net port http 8080 https 8080**
Partner-ISR(config-profile)#**server scansafe secondary name proxy1363.scansafe.net port http 8080 https 8080**
Partner-ISR(config-profile)#**license 0 <to be provided by your instructor>**
Partner-ISR(config-profile)#**source interface GigabitEthernet0/1**
Partner-ISR(config-profile)#**server scansafe on-failure block-all**
Partner-ISR(config-profile)#**logging**

https://t.me/learningnets

Step 6

Partner-ISR(config)# **interface GigabitEthernet 0/1**
Partner-ISR(config-if)# **content-scan out**

Lab 4-1: Configure Cisco Email Security Appliance Basic Policies

Task 1: Verify the Initial Email Exchange Without the Cisco ESA

Step 1

There are no solutions for this lab.

Lab 5-1: Configure Cisco ASA IPS Software Module

Task 1: Install the Cisco ASA IPS Software Module and Configure the Basic IPS Settings

Step 1

There are no solutions for this lab.

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