Cisco

Exam 300-206

Implementing Cisco Edge Network Security Solutions

Version: 11.0

[Total Questions: 222]

Question No : 1

Which Cisco TrustSec role does a Cisco ASA firewall serve within an identity architecture?

A. Access Requester
B. Policy Decision Point
C. Policy Information Point
D. Policy Administration Point
E. Policy Enforcement Point

Answer: E

Question No : 2

Which two features block traffic that is sourced from non-topological IPv6 addresses? (Choose two.)

A. DHCPv6 Guard
B. IPv6 Prefix Guard
C. IPv6 RA Guard
D. IPv6 Source Guard

Answer: B,D

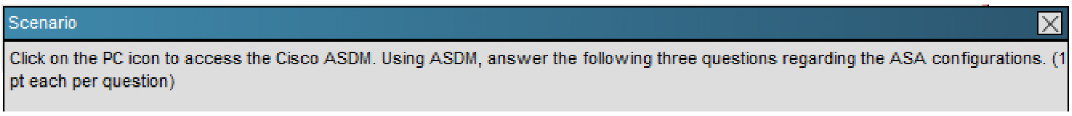
Question No : 3

Which Layer 2 security feature validates ARP packets?

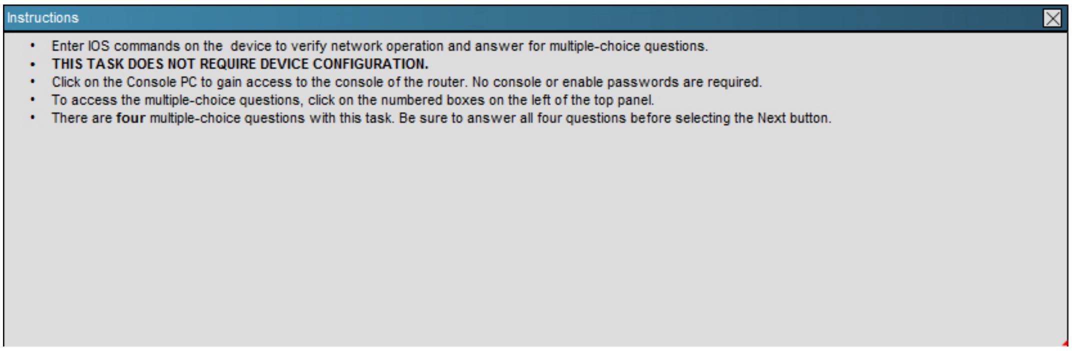
A. DAI
B. DHCP server
C. BPDU guard
D. BPDU filtering

Answer: A

Question No : 4

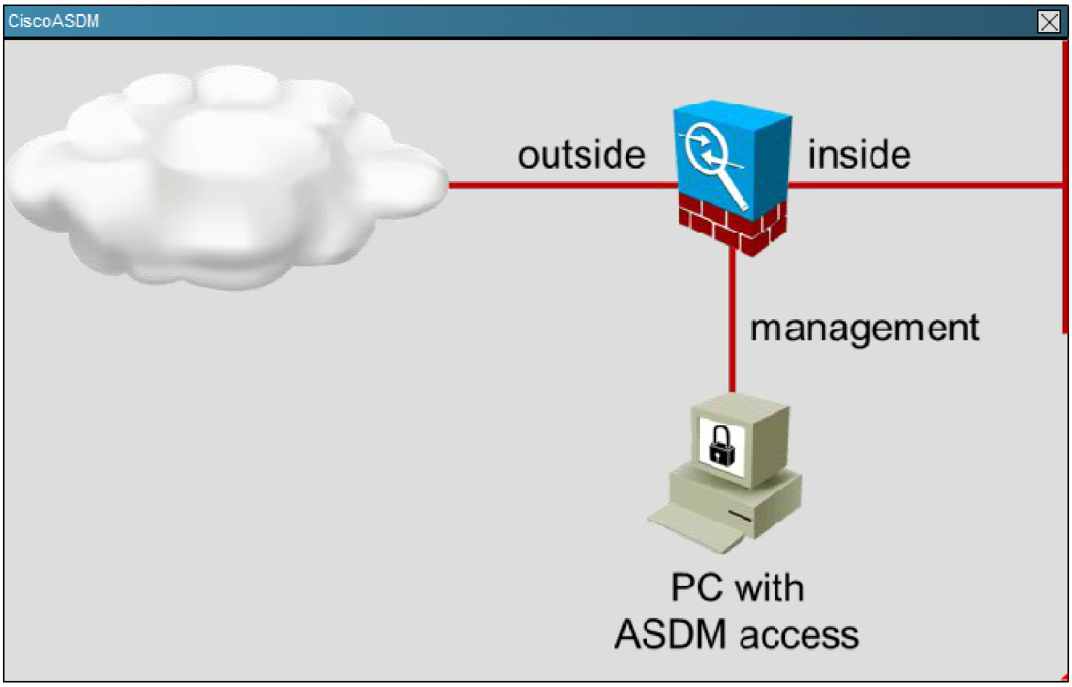


Click on the PC icon to access the Cisco ASDM. Using ASDM, answer the following three questions regarding the ASA configurations. (1 pt each per question)



Instructions

- Enter IOS commands on the device to verify network operation and answer for multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on the Console PC to gain access to the console of the router. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.



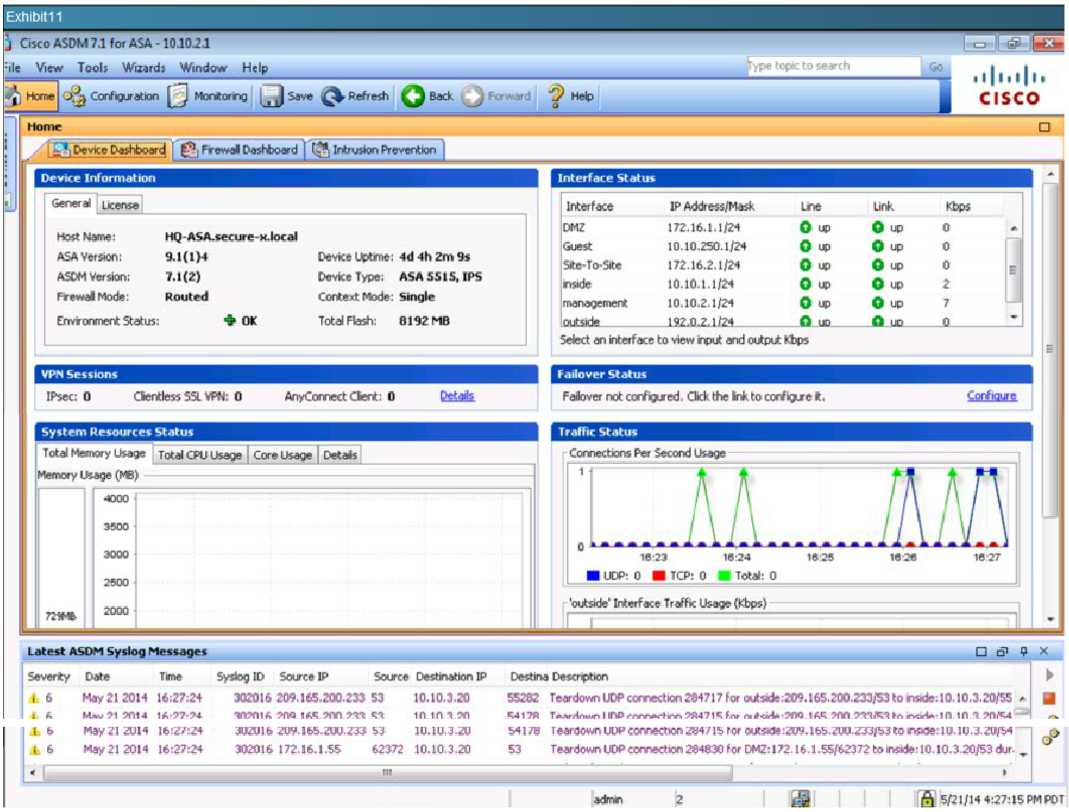


Exhibit11

Cisco ASDM 7.1 for ASA - 10.10.2.1

Device Information

General | License

Host Name: HQ-ASA.secure-x.local
ASA Version: 9.1(1)4
ASDM Version: 7.1(2)
Firewall Mode: Routed
Environment Status: OK
Device Uptime: 4d 4h 2m 9s
Device Type: ASA 5515, IPS
Context Mode: Single
Total Flash: 8192 MB

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
DMZ	172.16.1.1/24	up	up	0
Guest	10.10.250.1/24	up	up	0
Site-To-Site	172.16.2.1/24	up	up	0
inside	10.10.1.1/24	up	up	2
management	10.10.2.1/24	up	up	7
outside	192.0.2.1/24	up	up	0

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0 Details

Failover Status

Failover not configured. Click the link to configure it. Configure

System Resources Status

Traffic Status

Connections Per Second Usage
1
0
16:23
16:24
16:25
16:26
16:27
UDP: 0
TCP: 0
Total: 0
'outside' Interface Traffic Usage (Kbps)

Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	55282	Teardown UDP connection 284717 for outside:209.165.200.233/53 to inside:10.10.3.20/55
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	54178	Teardown UDP connection 284715 for outside:209.165.200.233/53 to inside:10.10.3.20/54
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	54178	Teardown UDP connection 284715 for outside:209.165.200.233/53 to inside:10.10.3.20/54
6	May 21 2014	16:27:24	302016	172.16.1.55	62372	10.10.3.20	53	Teardown UDP connection 284830 for DMZ:172.16.1.55/62372 to inside:10.10.3.20/53 dur.

admin 2 5/21/14 4:27:15 PM PDT

Which statement is true of the logging configuration on the Cisco ASA?

A. The contents of the internal buffer will be saved to an FTP server before the buffer is overwritten.
B. The contents of the internal buffer will be saved to flash memory before the buffer is overwritten.
C. System log messages with a severity level of six and higher will be logged to the internal buffer.
D. System log messages with a severity level of six and lower will be logged to the internal buffer.

Answer: C

Explanation:

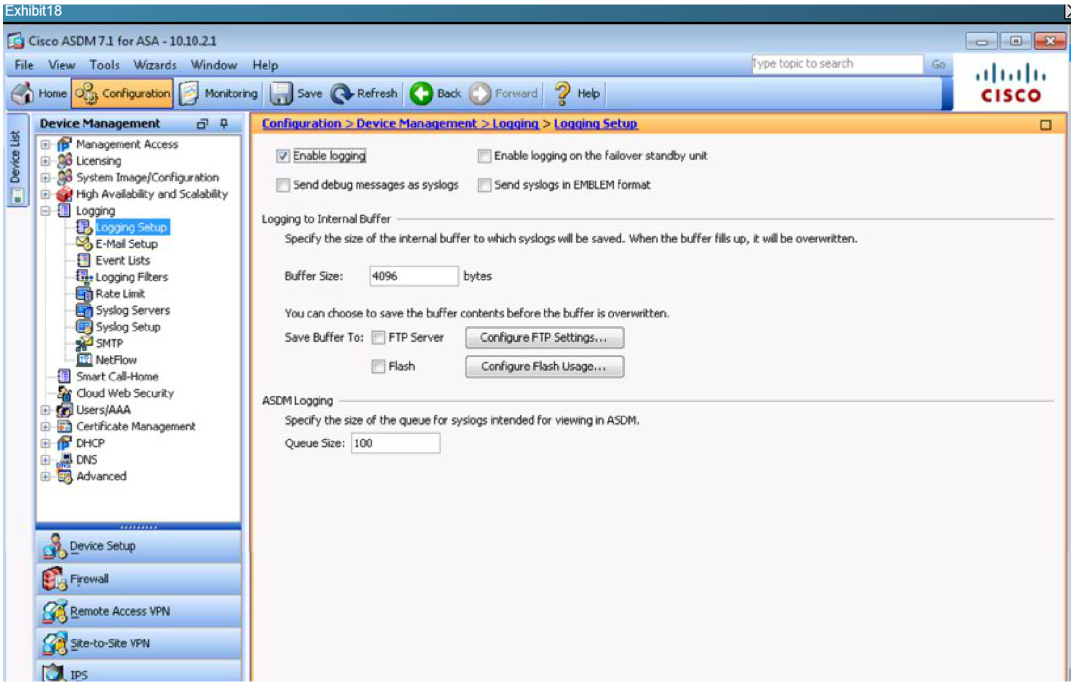


Exhibit18

Cisco ASDM 7.1 for ASA - 10.10.2.1

Configuration > Device Management > Logging > Logging Setup

☑ Enable logging

□ Enable logging on the failover standby unit

□ Send debug messages as syslogs

□ Send syslogs in EMBLEM format

Logging to Internal Buffer

Specify the size of the internal buffer to which syslogs will be saved. When the buffer fills up, it will be overwritten.

Buffer Size: 4096 bytes

You can choose to save the buffer contents before the buffer is overwritten.

Save Buffer To: □ FTP Server [Configure FTP Settings...]

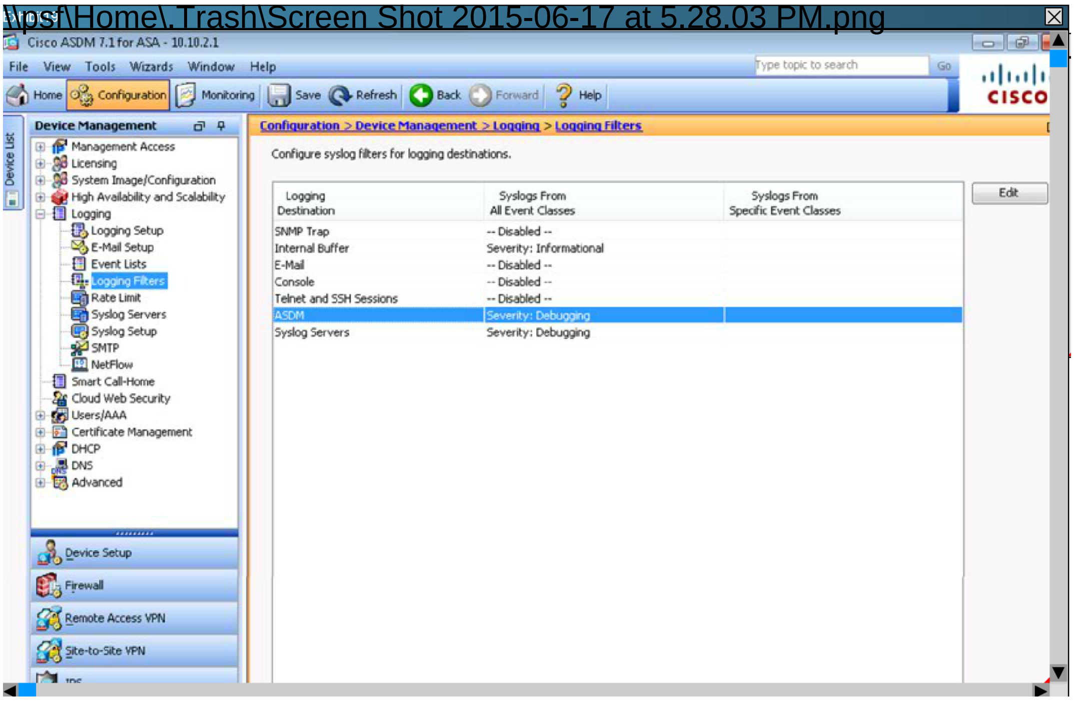
□ Flash [Configure Flash Usage...]

ASDM Logging

Specify the size of the queue for syslogs intended for viewing in ASDM.

Queue Size: 100

\\psf\Home\.Trash\Screen Shot 2015-06-17 at 5.28.03 PM.png



Cisco ASDM 7.1 for ASA - 10.10.2.1

Configuration > Device Management > Logging > Logging Filters

Configure syslog filters for logging destinations.

Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	-- Disabled --	
Internal Buffer	Severity: Informational	
E-Mail	-- Disabled --	
Console	-- Disabled --	
Telnet and SSH Sessions	-- Disabled --	
ASDM	Severity: Debugging	
Syslog Servers	Severity: Debugging	

\\psf\Home\.Trash\Screen Shot 2015-06-17 at 5.26.32 PM.png

Question No : 5

Which two options are purposes of the packet-tracer command? (Choose two.)

A. to filter and monitor ingress traffic to a switch

B. to configure an interface-specific packet trace
C. to simulate network traffic through a data path
D. to debug packet drops in a production network
E. to automatically correct an ACL entry in an ASA

Answer: C,D

Question No : 6

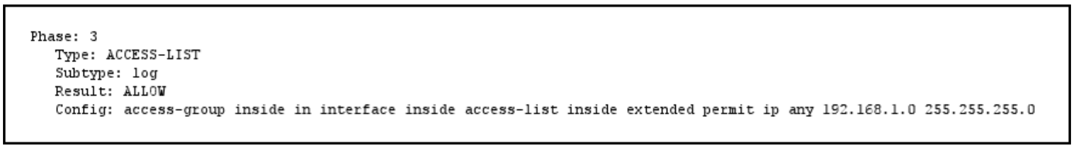
Which three options are default settings for NTP parameters on a Cisco device? (Choose three.)

A. NTP authentication is enabled.
B. NTP authentication is disabled.
C. NTP logging is enabled.
D. NTP logging is disabled.
E. NTP access is enabled.
F. NTP access is disabled.

Answer: B,D,E

Question No : 7

Refer to the exhibit.



```
Phase: 3
   Type: ACCESS-LIST
   Subtype: log
   Result: ALLOW
   Config: access-group inside in interface inside access-list inside extended permit ip any 192.168.1.0 255.255.255.0
```

Which two statements about this firewall output are true? (Choose two.)

A. The output is from a packet tracer debug.
B. All packets are allowed to 192.168.1.0 255.255.0.0.
C. All packets are allowed to 192.168.1.0 255.255.255.0.
D. All packets are denied.
E. The output is from a debug all command.

Answer: A,C

Question No : 8

Which three statements about transparent firewall are true? (Choose three)

A. Transparent firewall works at Layer 2
B. Both interfaces must be configured with private IP Addresses
C. It can have only a management IP address
D. It does not support dynamic routing protocols
E. It only support PAT

Answer: A,C,D

Question No : 9

When configuring security contexts on the Cisco ASA, which three resource class limits can be set using a rate limit? (Choose three.)

A. address translation rate
B. Cisco ASDM session rate
C. connections rate
D. MAC-address learning rate (when in transparent mode)
E. syslog messages rate
F. stateful packet inspections rate

Answer: C,E,F

Question No : 10

Which two web browsers are supported for the Cisco ISE GUI? (Choose two.)

A. HTTPS-enabled Mozilla Firefox version 3.x
B. Netscape Navigator version 9
C. Microsoft Internet Explorer version 8 in Internet Explorer 8-only mode
D. Microsoft Internet Explorer version 8 in all Internet Explorer modes
E. Google Chrome (all versions)

Answer: A,C

Question No : 11

Which function in the Cisco ADSM ACL Manager pane allows an administrator to search for a specfic element?

A. Find
B. Device Management
C. Search
D. Device Setup

Answer: A

Question No : 12

Which action is needed to set up SSH on the Cisco ASA firewall?

A. Create an ACL to aloew the SSH traffic to the Cisco ASA.
B. Configure DHCP for the client that will connect via SSH.
C. Generate a crypto key
D. Specify the SSH version level as either 1 or 2.
E. Enable the HTTP server to allow authentication.

Answer: C

Question No : 13

Which three options are hardening techniques for Cisco IOS routers? (Choose three.)

A. limiting access to infrastructure with access control lists
B. enabling service password recovery
C. using SSH whenever possible
D. encrypting the service password
E. using Telnet whenever possible
F. enabling DHCP snooping

Answer: A,C,D

Question No : 14 CORRECT TEXT

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

The CSO has tasked you with enable Botnet traffic filter on the Cisco ASA to detect and deny further connection attempts from infected PCs to malware destinations. You are also required to test your configurations by initiating connections through the Cisco ASA and then display and observe the Real-Time Log Viewer in ASDM.

To successfully complete this activity, you must perform the following tasks:

* Download the dynamic database and enable use of it.

• Enable the ASA to download of the dynamic database

• Enable the ASA to download of the dynamic database.

• Enable DNS snooping for existing DNS inspection service policy rules..

• Enable Botnet Traffic Filter classification on the outside interface for All Traffic.

• Configure the Botnet Traffic Filter to drop blacklisted traffic on the outside interface. Use the default Threat Level settings

NOTE: The database files are stored in running memory; they are not stored in flash memory.

NOTE:DNS is enabled on the inside interface and set to the HQ-SRV (10.10.3.20).

NOTE: Not all ASDM screens are active for this exercise.

• Verify that the ASA indeed drops traffic to blacklisted destinations by doing the following:

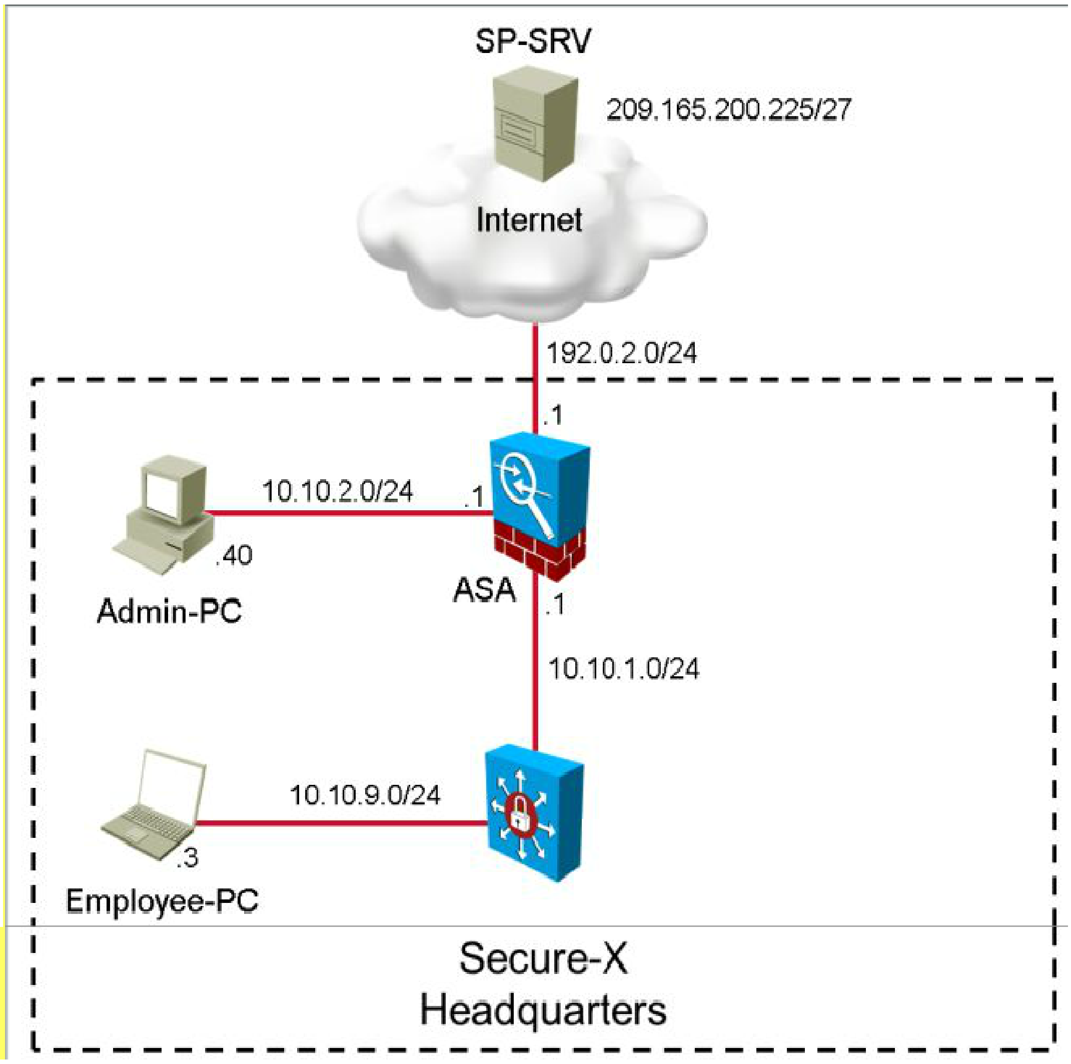
• From the Employee PC, navigate to http://www.google.com to make sure that access to the Internet is working.

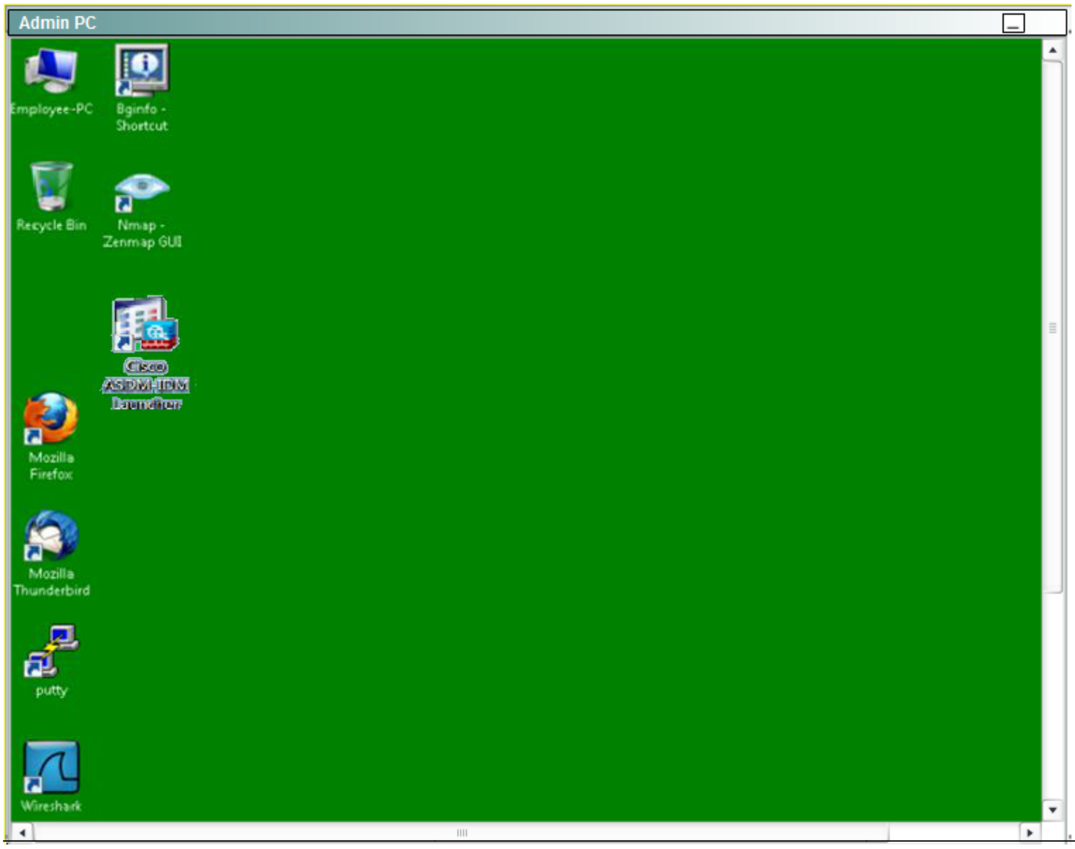
• From the Employee PC, navigate to http://bot-sparta.no-ip.org. This destination is classified as malware destination by the Cisco SIO database.

• From the Employee PC, navigate to http://superzarabotok-gid.ru/. This destination is classified as malware destination by the Cisco SIO database.

• From Admin PC, launch ASDM to display and observe the Real-Time Log Viewer.

You have completed this exercise when you have configured and successfully tested Botnet traffic filter on the Cisco ASA.


SP-SRV
209.165.200.225/27
Internet
192.0.2.0/24
.1
10.10.2.0/24
.1
.40
Admin-PC
ASA
.1
10.10.1.0/24
10.10.9.0/24
.3
Employee-PC
Secure-X
Headquarters


Admin PC
Employee-PC
Bginfo - Shortcut
Recycle Bin
Nmap - Zenmap GUI
Cisco ASDM-IDM Launcher
Mozilla Firefox
Mozilla Thunderbird
putty
Wireshark