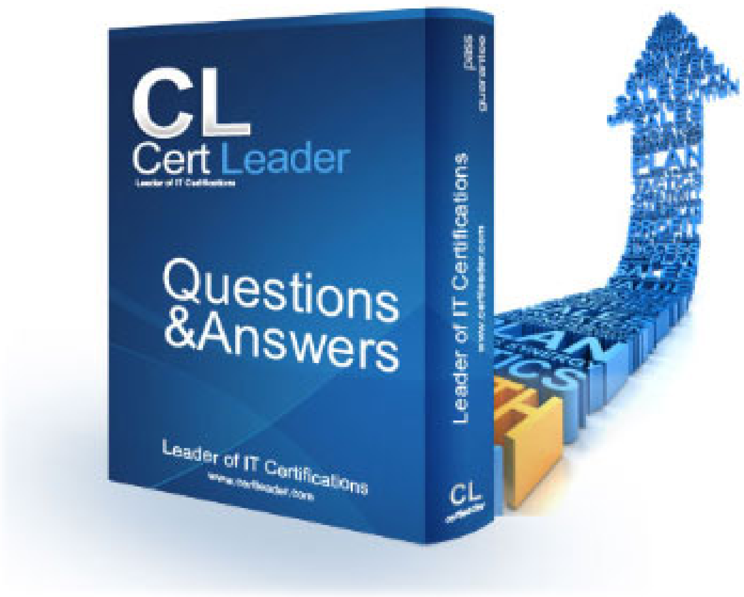
300-210 Dumps

Implementing Cisco Threat Control Solutions (SITCS)

https://www.certleader.com/300-210-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
Which Cisco technology secures the network through malware filtering, category-based control, and reputation-based control?

A. Cisco ASA 5500 Series appliances
B. Cisco IPS
C. Cisco remote-access VPNs
D. Cisco WSA

Answer: D

NEW QUESTION 2
- (Exam Topic 1)
What is the function of the Web Proxy Auto Discovery protocol?

A. It enables a web client's traffic flows to be redirected in real time.
B. It enables web clients to dynamically resolve hostname records.
C. It enables a web client to download a script or configuration file that is named by a URL.
D. It enables a web client to discover the URL of a configuration file.

Answer: D

NEW QUESTION 3
- (Exam Topic 1)
Which SSL traffic decryption feature is used when decrypting traffic from an external host to a server on your network?

A. Decrypt by stripping the server certificate.
B. Decrypt by resigning the server certificate
C. Decrypt with a known private key
D. Decypt with a known public key

Answer: B

NEW QUESTION 4
- (Exam Topic 1)
In cisco firePOWER 5.x and 6.0, which type of traffic causes a web page to be displayed by the appliance when Block or Interactive Block is selected as an access control action?

A. FTP
B. decrypted HTTP
C. encrypted HTTP
D. unencrypted HHTP

Answer: D

NEW QUESTION 5
- (Exam Topic 1)
When using Cisco AMP for Networks, which feature copies a file to the Cisco AMP cloud for analysis?

A. Spero analysis
B. dynamic analysis
C. sandbox analysis
D. malware analysis

Answer: B

NEW QUESTION 6
- (Exam Topic 1)
A university policy has to allow open access to resources on the Internet for research, but internal workstations have been exposed to malware. Which AMP feature allows the engineering team to determine whether a file is installed on a selected few workstations?

A. file manager
B. file conviction
C. file determination
D. file prevalence
E. file discovery

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
An engineer is configuring a Cisco Email Security Appliance (ESA) and chooses "Preferred" as the settings for TLS on a HAT Mail Flow Policy. Which result occurs?.

A. TLS is allowed for outgoing connections to MTA

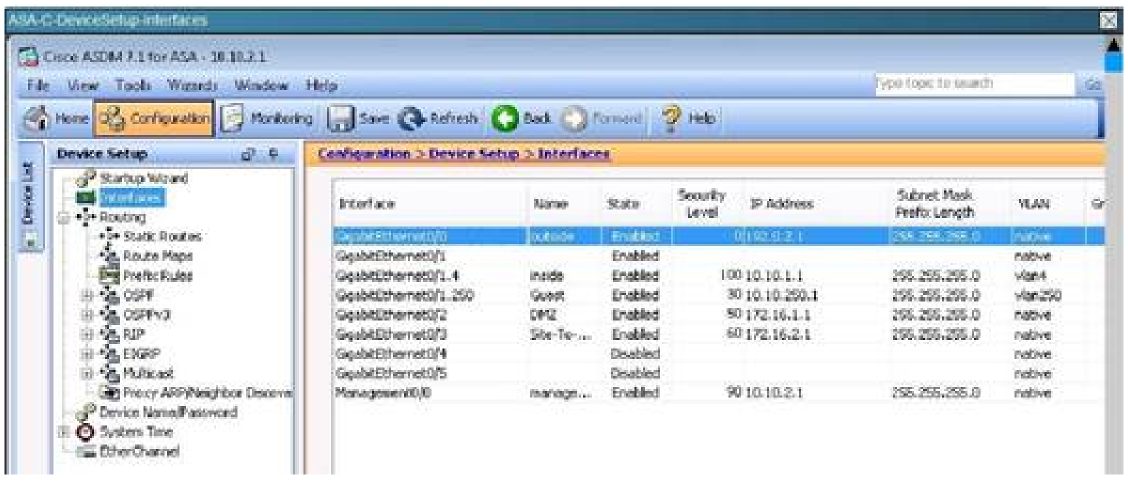
B. Connection to the listener require encrypted Simp Mail Transfer Protocol conversations
C. TLS is allowed for incoming connections to the listener from MTAs, even after a STARTTLS command received
D. TLS is allowed for incoming connections to the listener from MTA
E. Until a STARTTLS command received, the ESA responds with an error message to every command other than No Option, EHLO, or QUIT.
F. TLS is allowed for outgoing connections to the listener from MTA
G. Until a STARTTLS command received, the ESA responds with an error message to every command other than No Option (NOOP), EHLO, or QUIT.

Answer: D

NEW QUESTION 8
- (Exam Topic 1)
The Web Cache Communication Protocol (WCCP) is a content-routing protocol that can facilitate the redirection of traffic flows in real time. Your organization has deployed WCCP to redirect web traffic that traverses their Cisco Adaptive Security Appliances (ASAs) to their Cisco Web Security Appliances (WSAs).
The simulator will provide access to the graphical user interfaces of one Cisco ASA and one Cisco WSA that are participating in a WCCP service. Not all aspects of the GUIs are implemented in the simulator. The options that have been implemented are sufficient to determine the best answer to each of the questions that are presented.
Your task is to examine the details available in the simulated graphical user interfaces and select the best answer.

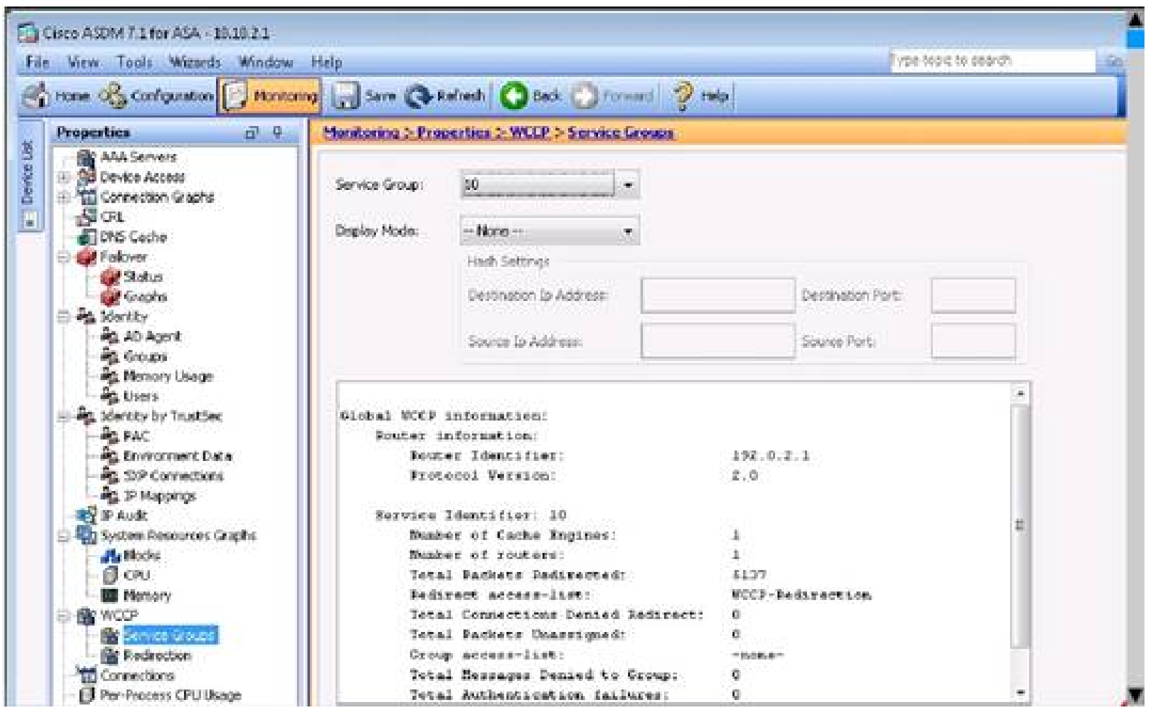
Adaptive
Security Appliance

Web
Security Appliance


ASA-C-DeviceSetup-interfaces
Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
Device Setup
Device List
Startup Wizard
Interfaces
Routing
Static Routes
Route Maps
Prefix Rules
OSPF
OSPFv3
RIP
EIGRP
Multicast
Proxy ARP/Neighbor Discove
Device Name/Password
System Time
EtherChannel

Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN
GigabitEthernet0/0	outside	Enabled	0	192.0.2.1	255.255.255.0	native
GigabitEthernet0/1		Enabled				native
GigabitEthernet0/1.4	inside	Enabled	100	10.10.1.1	255.255.255.0	vlan4
GigabitEthernet0/1.250	Guest	Enabled	30	10.10.250.1	255.255.255.0	vlan250
GigabitEthernet0/2	DMZ	Enabled	50	172.16.1.1	255.255.255.0	native
GigabitEthernet0/3	Site-To-...	Enabled	60	172.16.2.1	255.255.255.0	native
GigabitEthernet0/4		Disabled				native
GigabitEthernet0/5		Disabled				native
Management0/0	manage...	Enabled	90	10.10.2.1	255.255.255.0	native

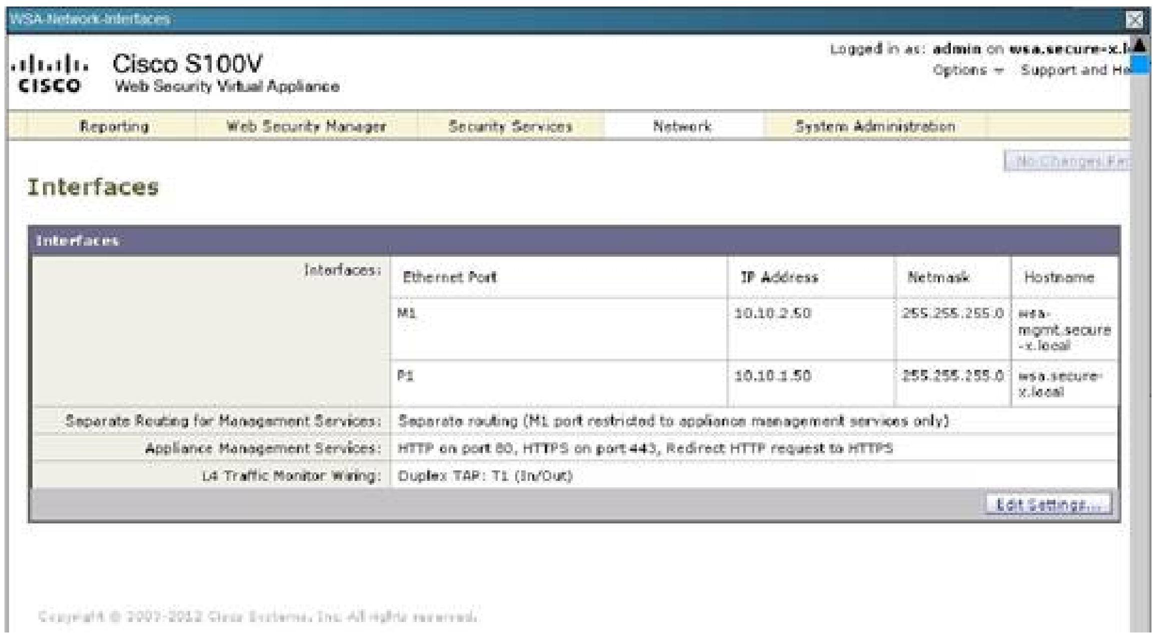


Monitoring > Properties > WCCP > Service Groups

Service Group: 10
Deploy Mode: -- None --
Destination Ip Address:
Destination Port:
Source Ip Address:
Source Port:

```
Global WCCP information:
    Router information:
        Router Identifier:                  192.0.2.1
        Protocol Version:                   2.0

    Service Identifier: 10
        Number of Cache Engines:            1
        Number of routers:                  1
        Total Packets Redirected:           6137
        Redirect access-list:               WCCP-Redirection
        Total Connections Denied Redirect:  0
        Total Packets Unassigned:           0
        Group access-list:                  -none-
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
```



Logged in as: admin on wsa.secure-x.l

Interfaces

Interfaces

Interfaces:	Ethernet Port	IP Address	Netmask	Hostname
	M1	10.10.2.50	255.255.255.0	wsa-mgmt.secure-x.local
	P1	10.10.1.50	255.255.255.0	wsa.secure-x.local
Separate Routing for Management Services:	Separate routing (M1 port restricted to appliance management services only)			
Appliance Management Services:	HTTP on port 80, HTTPS on port 443, Redirect HTTP request to HTTPS			
L4 Traffic Monitor Wiring:	Duplex TAP: T1 (In/Out)			

Copyright © 2003-2012 Cisco Systems, Inc. All rights reserved.

How many Cisco ASAs and how many Cisco WSAs are participating in the WCCP service?

A. One Cisco ASA or two Cisco ASAs configured as an Active/Standby failover pair, and one Cisco WSA.
B. One Cisco ASA or two Cisco ASAs configured as an Active/Active failover pair, and one Cisco WSA.
C. One Cisco ASA or two Cisco ASAs configured as an Active/Standby failover pair, and two Cisco WSAs.
D. One Cisco ASA or two Cisco ASAs configured as an Active/Active failover pair, and two Cisco WSAs.
E. Two Cisco ASAs and one Cisco WSA.
F. Two Cisco ASAs and two Cisco WSAs.

Answer: A

Explanation:
We can see from the output that the number of routers (ASA's) is 1, so there is a single ASA or an active/ standby pair being used, and 1 Cache Engine. If the ASA's were in a active/active role it would show up as 2 routers.

NEW QUESTION 9
- (Exam Topic 1)
Which two statement about Cisco Firepower file and intrusion inspection under control policies are true? (Choose two.)

A. File inspection occurs before intrusion prevention.
B. Intrusion Inspection occurs after traffic is blocked by file type.
C. File and intrusion drop the same packet.
D. Blocking by file type takes precedence over malware inspection and blocking
E. File inspection occurs after file discovery

Answer: AE

NEW QUESTION 10
- (Exam Topic 1)
Which two dynamic routing protocols are supported in FirePower Threat Defense v6.0? (Choose Two)

A. IS-IS
B. BGP
C. OSPF
D. static routing
E. EIGRP

Answer: BC

NEW QUESTION 10
- (Exam Topic 1)
An enginner manages a Cisco Intrusion Prevention System via IME. A new user must be able to tune signatures, but must not be able to create new users. Which role for the new user is correct?

A. viewer
B. service
C. operator
D. administrator

Answer: C

NEW QUESTION 13
- (Exam Topic 1)
In the predefined URL category filtering configuration page in a cisco WSA, which two actions are valid?

A. Restrict
B. Guarantee
C. Block
D. Notification
E. Time based

Answer: AD

NEW QUESTION 18
- (Exam Topic 1)
Which two TCP ports can allow the Cisco Firepower Management Center to communication with FireAMP cloud for file disposition information? (Choose two.)

A. 8080
B. 22
C. 8305
D. 32137
E. 443

Answer: DE

Explanation:
http://www.cisc
o.com/c/en/us/support/docs/security/sourcefire-fireamp-private-cloud-virtual-appliance/118336-configure-fiream

page=http://www.cisco.com/c/en/us/support/docs/security/sourcefire-amp-appliances/118121-technote-so urcefire-00.html

NEW QUESTION 20
- (Exam Topic 1)
Which license is required for Cisco Security Intelligence to work on the Cisco Next Generation Intrusion Prevention System?

A. control
B. matware
C. URL filtering
D. protect

Answer: D

NEW QUESTION 22
- (Exam Topic 1)
An engineering team has implemented Transparent User Identification on their Cisco Web Security Appliance. How is the User success authenticated?

A. trusted source
B. public key
C. certificate
D. host name

Answer: A

NEW QUESTION 26
- (Exam Topic 1)
With Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two.)

A. Speed
B. Duplex
C. Media Type
D. Redundant Interface
E. EtherChannel

Answer: AB

NEW QUESTION 29
- (Exam Topic 1)
A web security appliance is inspecting inbound traffic. In which sequence is inbound https traffic inspected?

A. Routing Policy > Decryption Policy > Access Policy
B. Access Policy > Decryption Policy > Routing Policy
C. Routing Policy > Access Policy > Decryption Policy
D. Decryption Policy > Access Policy > Routing Policy
E. Decryption Policy > Routing Policy > Access Policy
F. Access Policy > Routing Policy > Decryption Policy

Answer: B

NEW QUESTION 32
- (Exam Topic 1)
Which protocols can be specified in a Snort rule header for analysis?

A. TCP, UDP, ICMP, and IP
B. TCP, UDP, and IP
C. TCP, UDP, and ICMP
D. TCP, UDP, ICMP, IP, and ESP
E. TCP and UDP

Answer: A

NEW QUESTION 35
- (Exam Topic 1)
Which statement about Cisco ASA multicast routing support is true?

A. The Cisco ASA appliance supports PIM dense mode, sparse mode, and BIDIR-PIM.
B. The Cisco ASA appliance supports only stub multicast routing by forwarding IGMP messages from multicast receivers to the upstream multicast router.
C. The Cisco ASA appliance supports DVMRP and PIM.
D. The Cisco ASA appliance supports either stub multicast routing or PIM, but both cannot be enabled at the same time.
E. The Cisco ASA appliance supports only IGMP v1.

Answer: D

NEW QUESTION 37
- (Exam Topic 1)
When you configure the Cisco ESA to perform blacklisting, what are two items you can disable to enhance performance? (Choose two.)

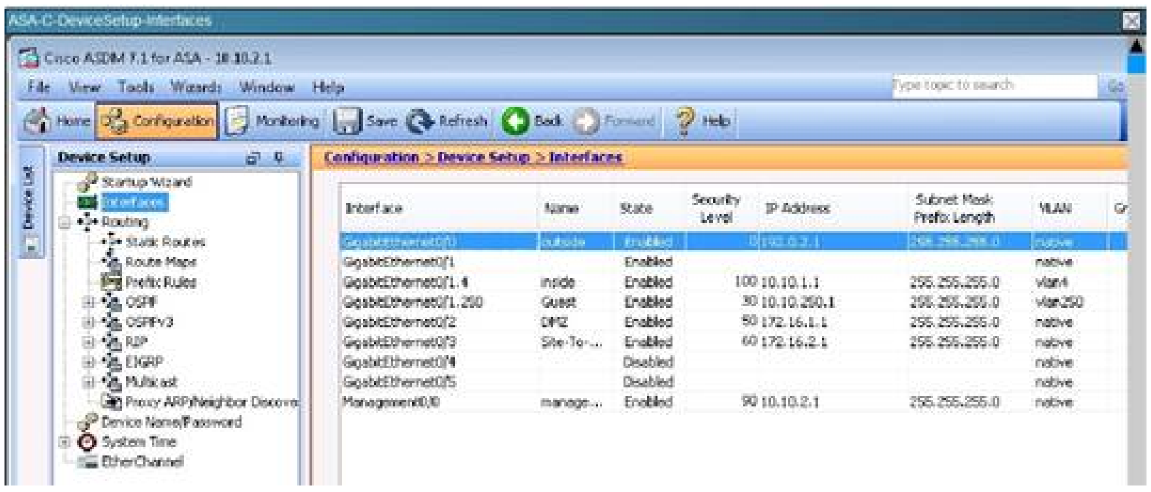
A. rootkit detection
B. spam scanning
C. APT detection
D. antivirus scanning
E. URL filtering

Answer: BD

NEW QUESTION 42
- (Exam Topic 1)
The Web Cache Communication Protocol (WCCP) is a content-routing protocol that can facilitate the redirection of traffic flows in real time. Your organization has deployed WCCP to redirect web traffic that traverses their Cisco Adaptive Security Appliances (ASAs) to their Cisco Web Security Appliances (WSAs).
The simulator will provide access to the graphical user interfaces of one Cisco ASA and one Cisco WSA that are participating in a WCCP service. Not all aspects of the GUIs are implemented in the simulator. The options that have been implemented are sufficient to determine the best answer to each of the questions that are presented.
Your task is to examine the details available in the simulated graphical user interfaces and select the best answer.

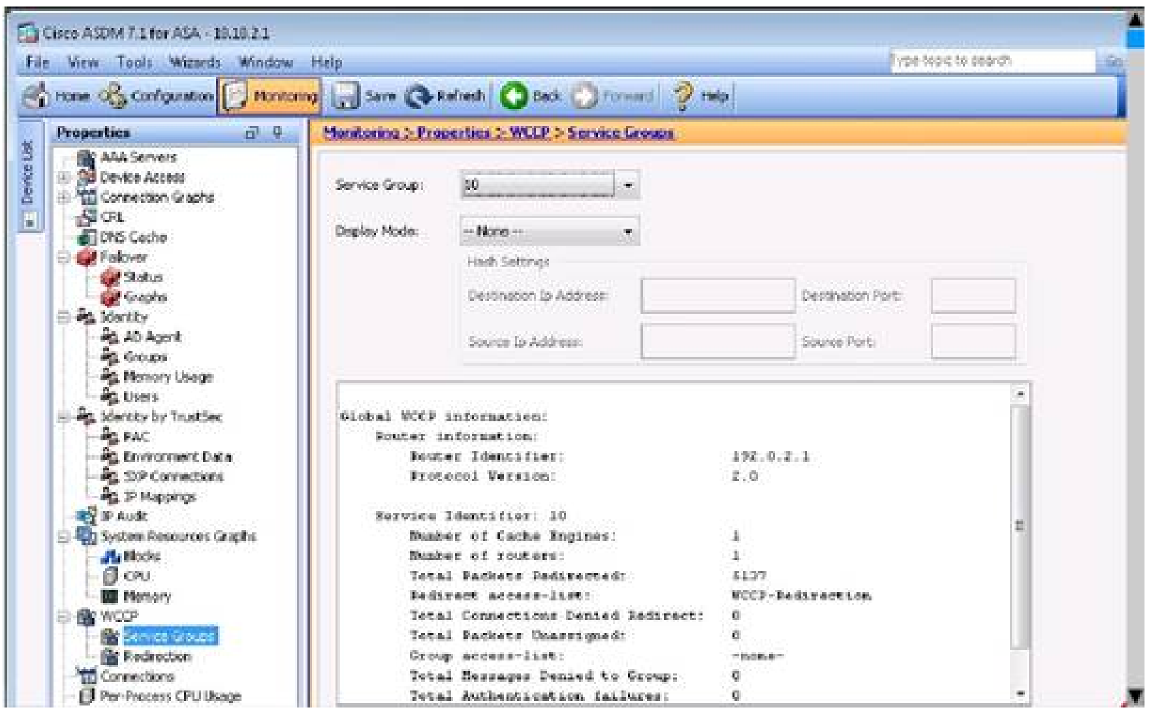
Adaptive
Security Appliance

Web
Security Appliance


ASA-C-DeviceSetup-Interfaces
Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Device Setup
Startup Wizard
Interfaces
Routing
Static Routes
Route Maps
Prefix Rules
OSPF
OSPFv3
RIP
EIGRP
Multicast
Proxy ARP/Neighbor Discove
Device Name/Password
System Time
EtherChannel
Device List

Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN
GigabitEthernet0/0	outside	Enabled	0	192.0.2.1	255.255.255.0	native
GigabitEthernet0/1		Enabled				native
GigabitEthernet0/1.4	inside	Enabled	100	10.10.1.1	255.255.255.0	vlan4
GigabitEthernet0/1.250	Guest	Enabled	30	10.10.250.1	255.255.255.0	vlan250
GigabitEthernet0/2	DMZ	Enabled	50	172.16.1.1	255.255.255.0	native
GigabitEthernet0/3	Site-To-...	Enabled	60	172.16.2.1	255.255.255.0	native
GigabitEthernet0/4		Disabled				native
GigabitEthernet0/5		Disabled				native
Management0/0	manage...	Enabled	90	10.10.2.1	255.255.255.0	native

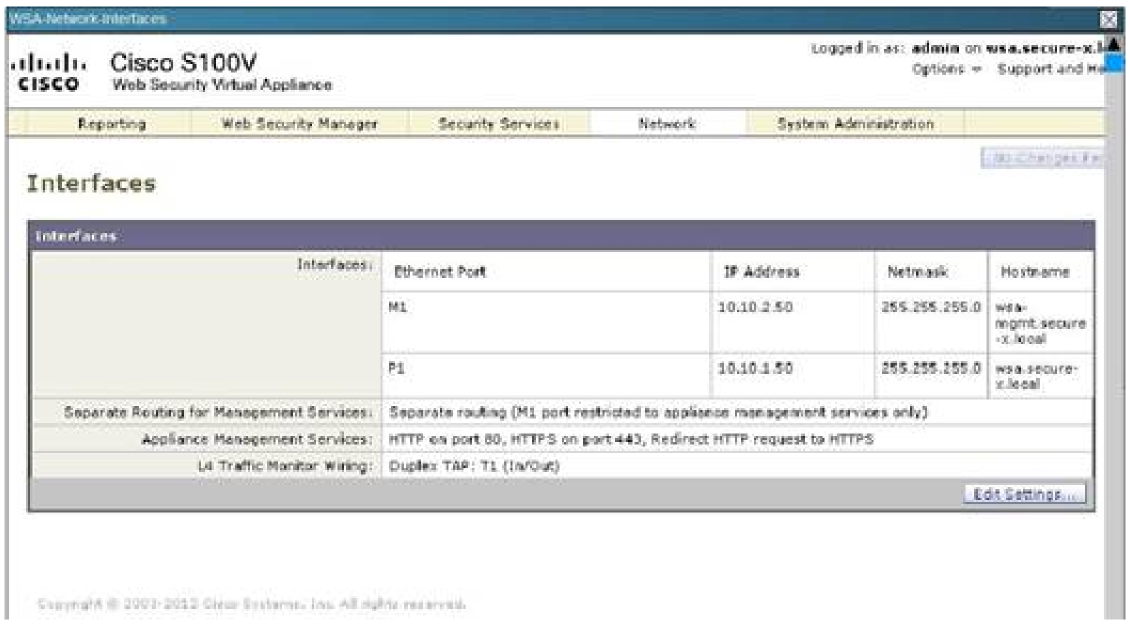


Monitoring > Properties > WCCP > Service Groups

Service Group: 10
Display Mode: -- None --
Hash Settings
Destination Ip Address:
Destination Port:
Source Ip Address:
Source Port:

```
Global WCCP information:
    Router information:
        Router Identifier:                    192.0.2.1
        Protocol Version:                     2.0

    Service Identifier: 10
        Number of Cache Engines:              1
        Number of routers:                    1
        Total Packets Redirected:             5137
        Redirect access-list:                 WCCP-Redirection
        Total Connections Denied Redirect:    0
        Total Packets Unassigned:             0
        Group access-list:                    -none-
        Total Messages Denied to Group:       0
        Total Authentication failures:        0
```



Interfaces

Interfaces

Interfaces:	Ethernet Port	IP Address	Netmask	Hostname
	M1	10.10.2.50	255.255.255.0	wsa-mgmt.secure-x.local
	P1	10.10.1.50	255.255.255.0	wsa.secure-x.local
Separate Routing for Management Services:	Separate routing (M1 port restricted to appliance management services only)			
Appliance Management Services:	HTTP on port 80, HTTPS on port 443, Redirect HTTP request to HTTPS			
L4 Traffic Monitor Wiring:	Duplex TAP: T1 (In/Out)			

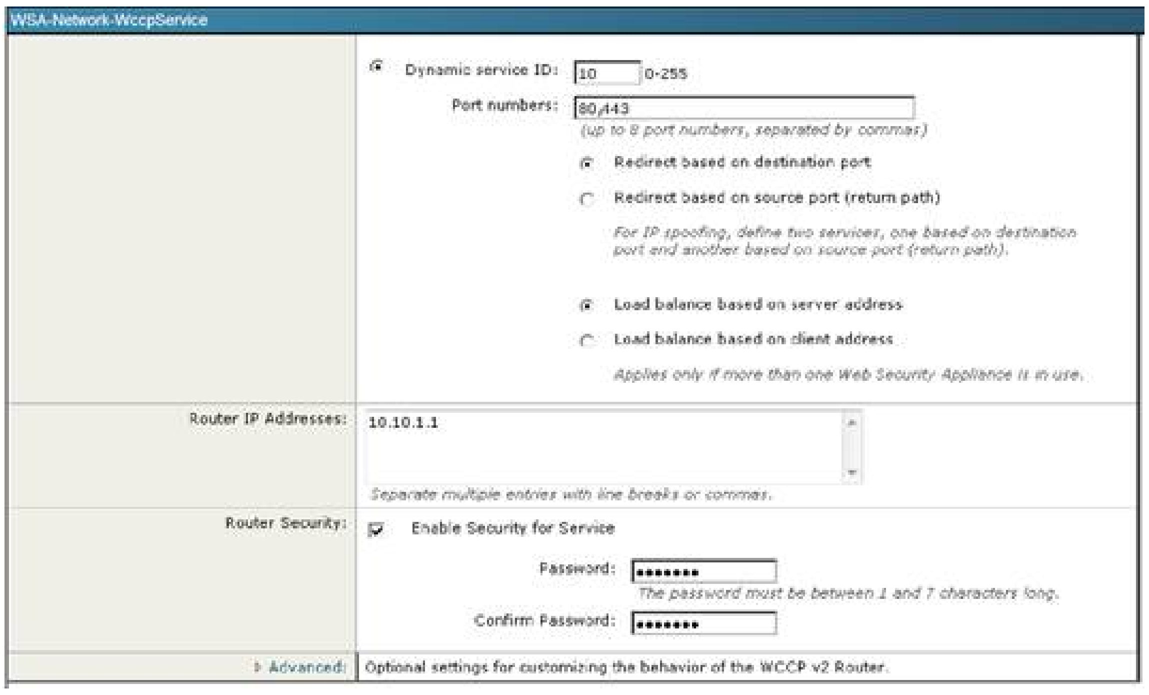
Copyright © 2003-2012 Cisco Systems, Inc. All rights reserved.

Between the Cisco ASA configuration and the Cisco WSA configuration, what is true with respect to redirected ports?

A. Both are configured for port 80 only.
B. Both are configured for port 443 only.
C. Both are configured for both port 80 and 443.
D. Both are configured for ports 80, 443 and 3128.
E. There is a configuration mismatch on redirected ports.

Answer: C

Explanation:
This can be seen from the WSA Network tab shown below:



WSA-Network-WccpService

● Dynamic service ID: 10 0-255
Port numbers: 80,443
(up to 8 port numbers, separated by commas)
● Redirect based on destination port
○ Redirect based on source port (return path)
For IP spoofing, define two services, one based on destination port and another based on source port (return path).
● Load balance based on server address
○ Load balance based on client address
Applies only if more than one Web Security Appliance is in use.

Router IP Addresses: 10.10.1.1
Separate multiple entries with line breaks or commas.

Router Security: ☑ Enable Security for Service
Password: •••••••
The password must be between 1 and 7 characters long.
Confirm Password: •••••••

Advanced: Optional settings for customizing the behavior of the WCCP v2 Router.

NEW QUESTION 43
- (Exam Topic 1)
which two tasks can the network discovery feature perform? (choose two)

A. host discovery
B. Block traffic
C. user discovery
D. reset connection
E. route traffic

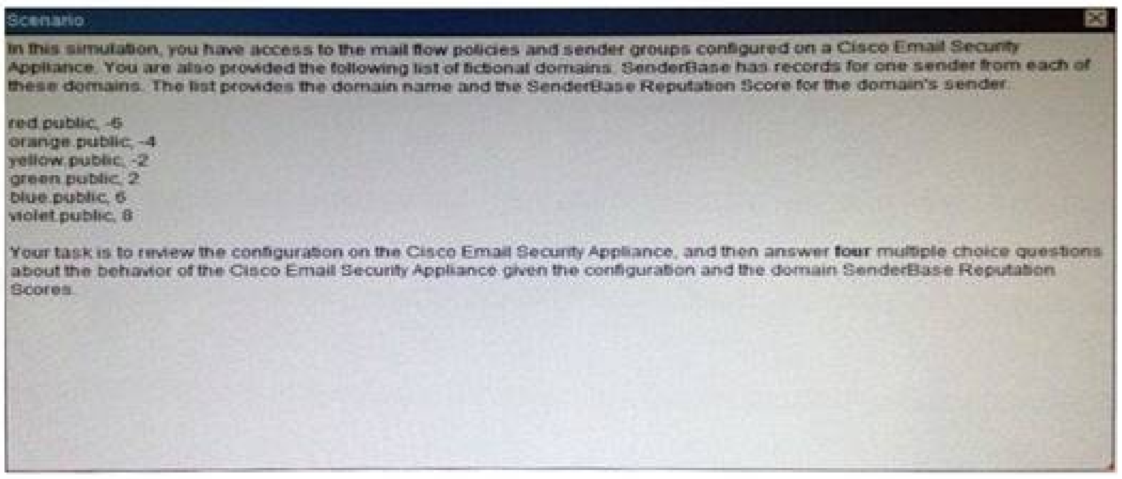
Answer: AC

NEW QUESTION 47
- (Exam Topic 1)
Which type of policy is used to define the scope for applications that are running on hosts?

A. access control policy.
B. application awareness policy.
C. application detector policy.
D. network discovery policy.

Answer: C

NEW QUESTION 51
- (Exam Topic 1)

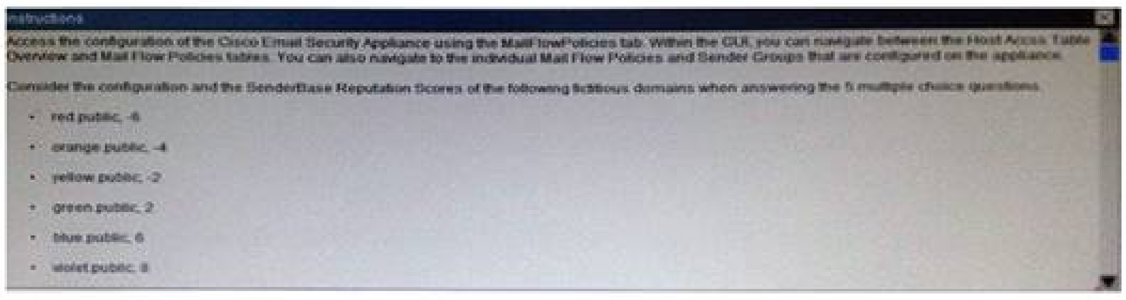


Scenario

In this simulation, you have access to the mail flow policies and sender groups configured on a Cisco Email Security Appliance. You are also provided the following list of fictional domains. SenderBase has records for one sender from each of these domains. The list provides the domain name and the SenderBase Reputation Score for the domain's sender.

red.public, -6
orange.public, -4
yellow.public, -2
green.public, 2
blue.public, 6
violet.public, 8

Your task is to review the configuration on the Cisco Email Security Appliance, and then answer **four** multiple choice questions about the behavior of the Cisco Email Security Appliance given the configuration and the domain SenderBase Reputation Scores.

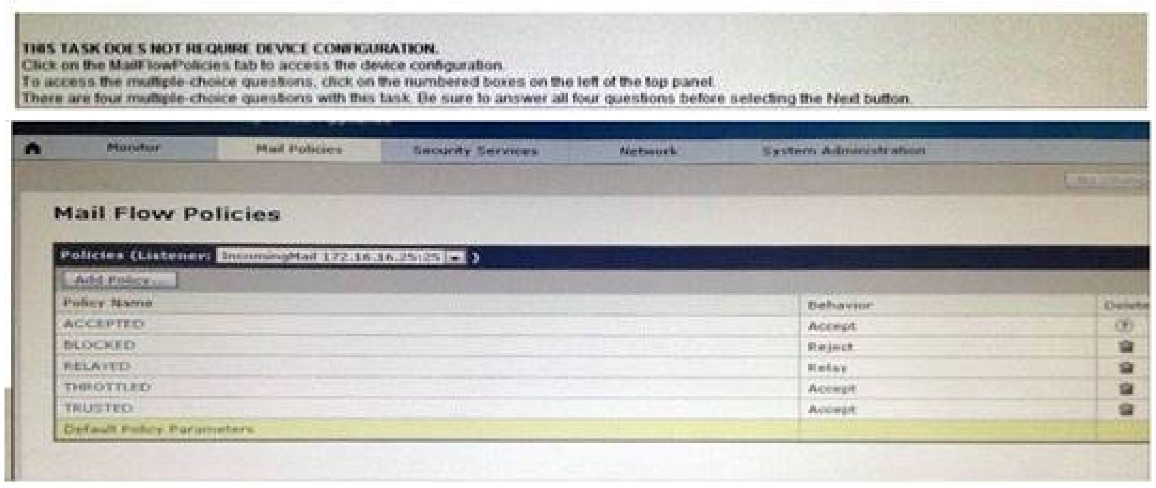


Instructions

Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the Host Access Table Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance.

Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the 5 multiple choice questions.

- red.public, -6
- orange.public, -4
- yellow.public, -2
- green.public, 2
- blue.public, 6
- violet.public, 8



THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
Click on the MailFlowPolicies tab to access the device configuration.
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.

Mail Flow Policies

Policies (Listener: IncomingMail 172.16.16.25:25)

Policy Name	Behavior	Delete
ACCEPTED	Accept	
BLOCKED	Reject	
RELAYED	Relay	
THROTTLED	Accept	
TRUSTED	Accept	
Default Policy Parameters		

What is the maximum message size that the Cisco Email Security Appliance will accept from the violet.public domain?

A. 1 KB
B. 100 KB
C. 1 MB
D. 10 MB
E. 100 MB
F. Unlimited

Answer: D

NEW QUESTION 55
- (Exam Topic 1)
Which website can be used to validate group information about connections that flow through Cisco CWS?

A. whoami.scansafe.com
B. policytrace.scansafe.com
C. policytrace.scansafe.net
D. whoami.scansafe.net

Answer: C

NEW QUESTION 58
- (Exam Topic 1)
An engineer wants to configure a method to verify the authenticity of emails on cisco ESA and noticed the sender policy framework. How can the SPF help in that task?

A. SPF allows the sender to sign the email using presharekey
B. SPF allows the sender to sign the email using public key
C. SPF allow the owner of internal domain to use DNS record which machines are

Answer: B

NEW QUESTION 63
- (Exam Topic 1)
Which three operating systems are supported with Cisco AMP for Endpoints? (Choose three.)

A. Windows
B. AWS
C. Android
D. Cisco IOS
E. OS X
F. ChromeOS

Answer: ACE

Explanation:
http://www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html

NEW QUESTION 66
- (Exam Topic 1)
A customer is concerned with their employee’s internet usage and has asked for more web traffic control. Which two features of the cisco web security appliance help with issue? (choose two)

A. Advanced Malware Protection
B. Dynamic ARP Inspection
C. DHCP spoofing Protection
D. Network Address Translation
E. Application Visibility and Control

Answer: AE

NEW QUESTION 69

- (Exam Topic 1)
Which Cisco FirePOWER setting is used to reduce the number of events received in a period of time and avoid being overwhelmed?

A. thresholding
B. rate-limiting
C. limiting
D. correlation

Answer: D

NEW QUESTION 71
- (Exam Topic 1)
An engineer is configuring a cisco ESA and wants to control whether to accept or reject email messages to a messages to a recipient address. Which list contains the allowed recipient addresses?

A. BAT
B. HAT
C. SAT
D. RAT

Answer: B

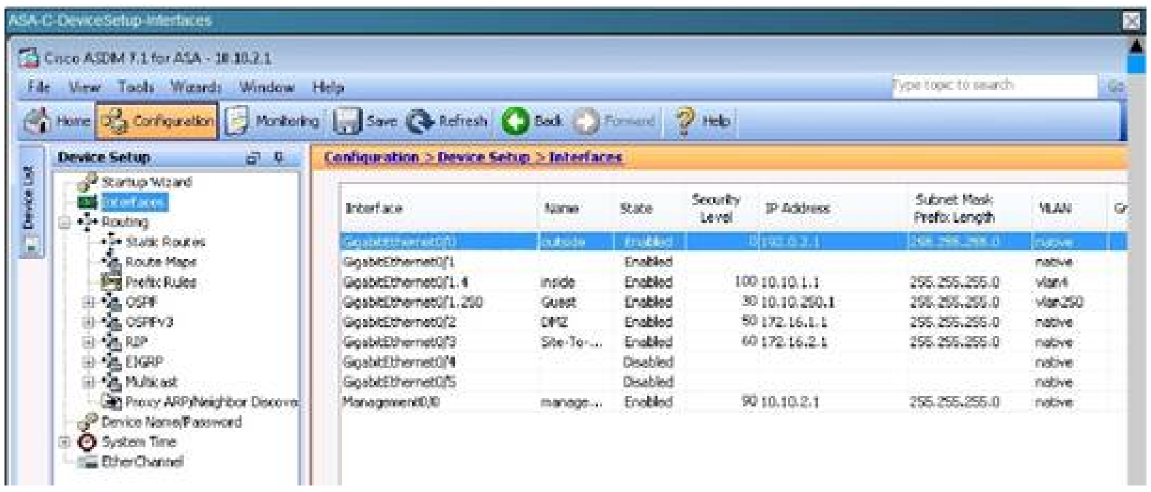
NEW QUESTION 74
- (Exam Topic 1)
Which CLI command is used to register a Cisco FirePOWER sensor to Firepower Management Center?

A. configure system add <host><key>
B. configure manager <key> add host
C. configure manager delete
D. configure manger add <host><key>

Answer: A

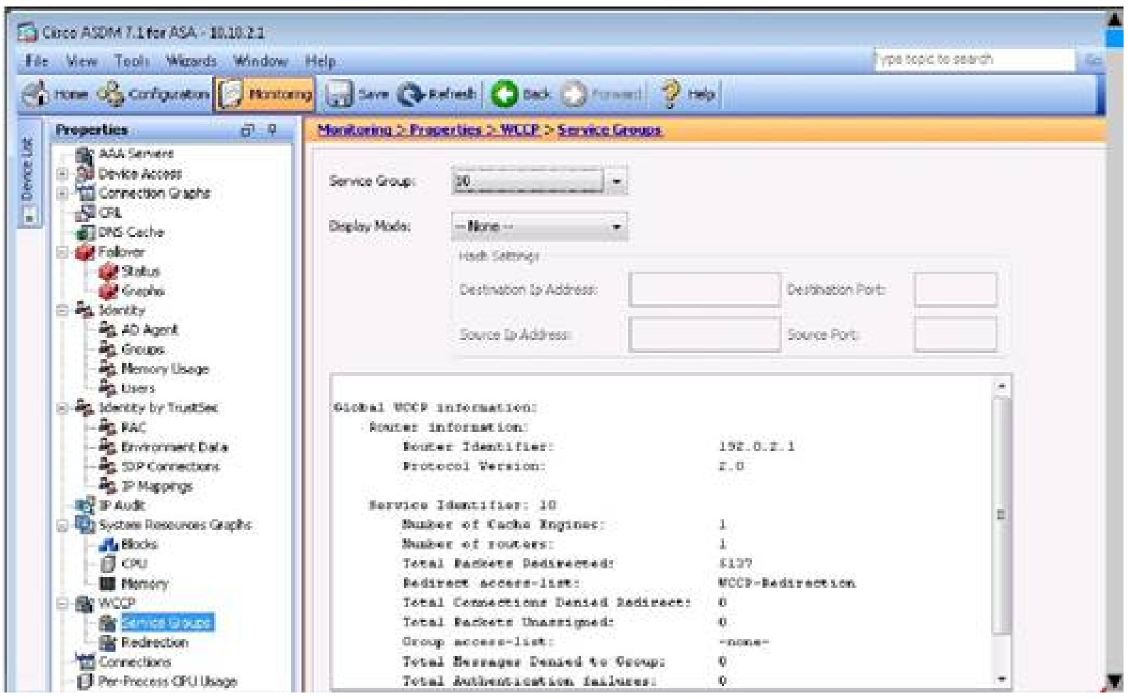
Explanation:
http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide
/fpmc-config-guide-v60/fpmc-config-guide-v60_appendix_01011110.html#ID-2201-00000005

NEW QUESTION 79
- (Exam Topic 1)
The Web Cache Communication Protocol (WCCP) is a content-routing protocol that can facilitate the redirection of traffic flows in real time. Your organization has deployed WCCP to redirect web traffic that traverses their Cisco Adaptive Security Appliances (ASAs) to their Cisco Web Security Appliances (WSAs).
The simulator will provide access to the graphical user interfaces of one Cisco ASA and one Cisco WSA that are participating in a WCCP service. Not all aspects of the GUIs are implemented in the simulator. The options that have been implemented are sufficient to determine the best answer to each of the questions that are presented.
Your task is to examine the details available in the simulated graphical user interfaces and select the best answer.


ASA-C-DeviceSetup-Interfaces
Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Device Setup
Startup Wizard
Interfaces
Routing
Static Routes
Route Maps
Prefix Rules
OSPF
OSPFv3
RIP
EIGRP
Multicast
Proxy ARP/Neighbor Discove
Device Name/Password
System Time
EtherChannel

Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN
GigabitEthernet0/0	outside	Enabled	0	192.0.2.1	255.255.255.0	native
GigabitEthernet0/1		Enabled				native
GigabitEthernet0/1.4	inside	Enabled	100	10.10.1.1	255.255.255.0	vlan4
GigabitEthernet0/1.250	Guest	Enabled	30	10.10.250.1	255.255.255.0	vlan250
GigabitEthernet0/2	DMZ	Enabled	50	172.16.1.1	255.255.255.0	native
GigabitEthernet0/3	Site-To-...	Enabled	60	172.16.2.1	255.255.255.0	native
GigabitEthernet0/4		Disabled				native
GigabitEthernet0/5		Disabled				native
Management0/0	manage...	Enabled	90	10.10.2.1	255.255.255.0	native



Service Group: 10

Display Mode: -- None --

Hash Settings

Destination Ip Address:

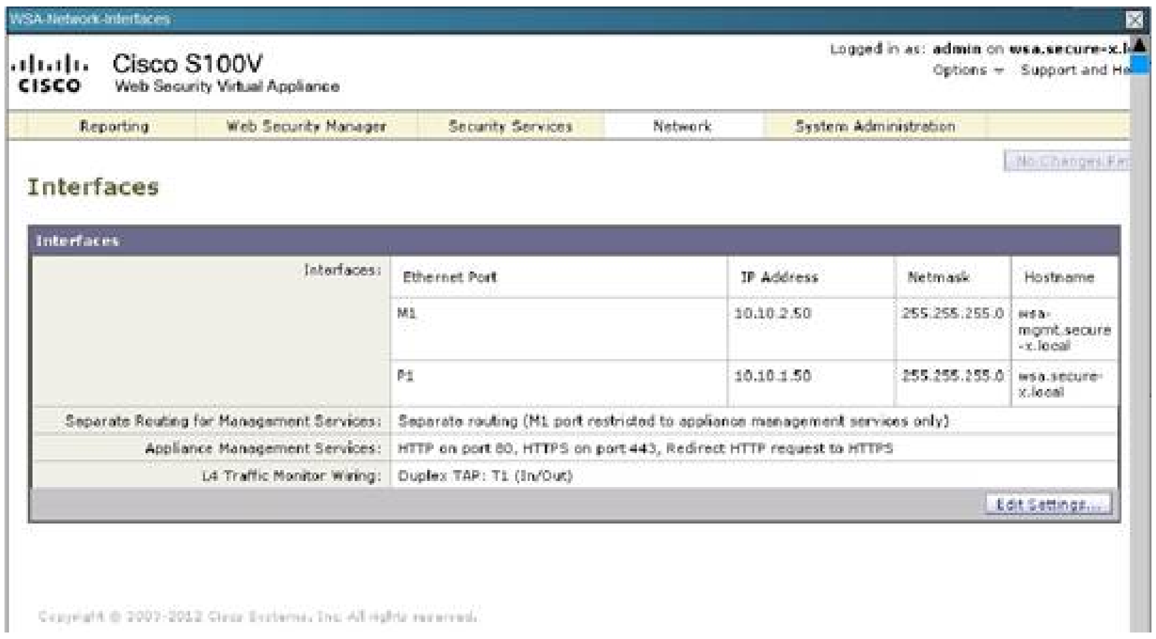
Destination Port:

Source Ip Address:

Source Port:

```
Global WCCP information:
    Router information:
        Router Identifier:                  192.0.2.1
        Protocol Version:                   2.0

    Service Identifier: 10
        Number of Cache Engines:            1
        Number of routers:                  1
        Total Packets Redirected:           5137
        Redirect access-list:               WCCP-Redirection
        Total Connections Denied Redirect:  0
        Total Packets Unassigned:           0
        Group access-list:                  -none-
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
```



Interfaces

Interfaces

Interfaces:

Ethernet Port	IP Address	Netmask	Hostname
M1	10.10.2.50	255.255.255.0	wsa-mgmt.secure-x.local
P1	10.10.1.50	255.255.255.0	wsa.secure-x.local

Separate Routing for Management Services: Separate routing (M1 port restricted to appliance management services only)

Appliance Management Services: HTTP on port 80, HTTPS on port 443, Redirect HTTP request to HTTPS

L4 Traffic Monitor Wiring: Duplex TAP: T1 (In/Out)

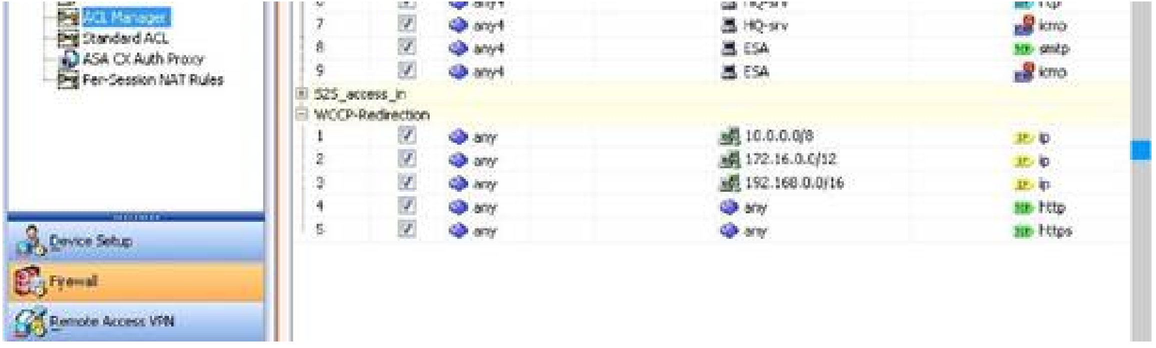
Copyright © 2007-2012 Cisco Systems, Inc. All rights reserved.

What traffic is not redirected by WCCP?

A. Traffic destined to public address space
B. Traffic sent from public address space
C. Traffic destined to private address space
D. Traffic sent from private address space

Answer: B

Explanation:
From the screen shot below we see the WCCP-Redirection ACL is applied, so all traffic from the Private IP space to any destination will be redirected.



```
7   ☑  any4   HQ-srv          icmp
8   ☑  any4   ESA             smtp
9   ☑  any4   ESA             icmp
S2S_access_in
WCCP-Redirection
1   ☑  any    10.0.0.0/8      ip
2   ☑  any    172.16.0.0/12   ip
3   ☑  any    192.168.0.0/16  ip
4   ☑  any    any             http
5   ☑  any    any             https
```

NEW QUESTION 81
- (Exam Topic 1)
With Cisco FirePOWER Threat Defense software, which interface mode do you configure to passively receive traffic that passes the appliance?

A. transparent
B. routed
C. passive
D. inline set
E. inline tap

Answer: C

NEW QUESTION 83
- (Exam Topic 1)
which two options are the basic parts of a Snort rule? (Choose two)

A. rule policy
B. rule header
C. Rule assignment and ports
D. rule options

E. Rule footer

Answer: BD

NEW QUESTION 85
- (Exam Topic 1)
After configuring an ISR with the Cisco Cloud Web security connector, which command does a network engineer run to verify connectivity to the CVV proxy?

A. show content-scan summary
B. show content-scan statistics
C. show scansafe server
D. show scansafe statistics

Answer: A

NEW QUESTION 86
- (Exam Topic 1)
Which two appliances support logical routed interfaces? (Choose two.)

A. FirePOWER services for ASA-5500-X
B. FP-4100-series
C. FP-8000-series
D. FP-7000-series
E. FP-9300-series

Answer: D

NEW QUESTION 87
- (Exam Topic 1)
Which two routing options are valid with cisco firePOWER threat Defense version 6.0?(choose two)

A. ECMP with up to three equal cost paths across multiple interfaces
B. BGPv6
C. BGPv4 with nonstop forwarding
D. BGPv4 unicast address family
E. ECMP with up to four equal cost paths

Answer: AD

NEW QUESTION 88
- (Exam Topic 1)
Which option lists the minimum requirements to deploy a managed device inline?

A. passive interface, security zone, MTU, and link mode.
B. passive interface, MTU, MDI/MDIX, and link mode.
C. inline interfaces, MTU, MDI/MDIX, and link mode.
D. inline interfaces, security zones, MTU, and link mode.

Answer: A

NEW QUESTION 90
- (Exam Topic 1)
Which policy must you edit to make changes to the Snort preprocessors?

A. access control policy
B. network discovery policy
C. intrusion policy
D. file policy
E. network analysis policy

Answer: A

NEW QUESTION 93
- (Exam Topic 1)
An engineer wants to cluster an existing ESA physical appliance with an ESA virtual appliance. Which statement is true?

A. This action is possible as long as the devices are running the identical AsyncOS
B. This action is not possible for virtual appliances
C. This action is possible between different models and OS
D. This action is not possible because the devices are not identical models

Answer: A

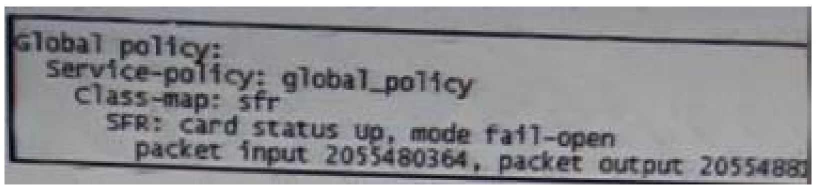
NEW QUESTION 94
- (Exam Topic 1)

User wants to deploy your managed device in Layer 3 routed mode and must configure a virtual router and a routed interface. Which managed shows this configuration?

A. Cisco FirePOWER services on a Cisco ASA 5500x.
B. virtual NGIPS
C. Cisco FirePOWER module on a Cisco ASA 5585x.
D. Cisco FirePOWER appliance.

Answer: C

NEW QUESTION 96
- (Exam Topic 1)
Exhibit:



```
Global policy:
  Service-policy: global_policy
    Class-map: sfr
      SFR: card status up, mode fail-open
        packet input 2055480364, packet output 20554880
```

Which configuration below would result in this output of the show server?

A. Option A
B. Option B
C. Option C

Answer: C

NEW QUESTION 98
- (Exam Topic 1)
Which three sender reputation ranges identify the default behavior of the Cisco Email Security Appliance? (Choose three.)

A. If it is between -1 and +10, the email is accepted
B. If it is between +1 and +10, the email is accepted
C. If it is between -3 and -1, the email is accepted and additional emails from the sender are throttled
D. If it is between -3 and +1, the email is accepted and additional emails from the sender are throttled
E. If it is between -4 and +1, the email is accepted and additional emails from the sender are throttled
F. If it is between -10 and -3, the email is blocked
G. If it is between -10 and -3, the email is sent to the virus and spam engines for additional scanning
H. If it is between -10 and -4, the email is blocked

Answer: ACF

NEW QUESTION 99
- (Exam Topic 1)
Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the Host Access Table Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance. Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the four multiple choice questions.

A. red.public, -6
B. orange.public, -4
C. yellow.public, -2
D. gree
E. .public, 2
F. blue.public, 6
G. violet.public, 8

Answer: D

NEW QUESTION 102
- (Exam Topic 1)
To enable the Cisco ASA Host Scan with remediation capabilities, an administrator must have which two Cisco ASA licenses enabled on its security appliance? (Choose two.)

A. Cisco AnyConnect Premium license
B. Cisco AnyConnect Essentials license
C. Cisco AnyConnect Mobile license
D. Host Scan license
E. Advanced Endpoint Assessment license
F. Cisco Security Agent license

Answer: AE

NEW QUESTION 106
- (Exam Topic 1)
Which detection method is also known as machine learning on Network-based Cisco Advanced Malware Protection?

A. custom file detection
B. hashing

C. Spero engine
D. dynamic analysis

Answer: D

NEW QUESTION 109
- (Exam Topic 1)
An engineer must deploy email security to a large enterprise with multiple offices. Each office cannot support its own ESA appliance. What technology best supports email security across the organization?

A. Cloud Email Security
B. Hybrid Email Security
C. Virtual Email Security Appliance
D. Physical Email Security Appliance

Answer: C

NEW QUESTION 111
- (Exam Topic 2)
Joe was asked to secure access to the Cisco Web Security Appliance to prevent unauthorized access. Which four steps should Joe implement to accomplish this goal? (Choose four.)

A. Implement IP access lists to limit access to the management IP address in the Cisco Web Security Appliance GUI.
B. Add the Cisco Web Security Appliance IP address to the local access list.
C. Enable HTTPS access via the GUI/CLI with redirection from HTTP.
D. Replace the Cisco self-signed certificate with a publicly signed certificate.
E. Put the Cisco WSA Management interface on a private management VLAN.
F. Change the netmask on the Cisco WSA Management interface to a 32-bit mask.
G. Create an MX record for the Cisco Web Security Appliance in DNS.

Answer: ACDE

NEW QUESTION 115
- (Exam Topic 2)
What are three benefits of the Cisco AnyConnect Secure Mobility Solution? (Choose three.)

A. It can protect against command-injection and directory-traversal attacks.
B. It provides Internet transport while maintaining corporate security policies.
C. It provides secure remote access to managed computers.
D. It provides clientless remote access to multiple network-based systems.
E. It enforces security policies, regardless of the user location.
F. It uses ACLs to determine best-route connections for clients in a secure environment.

Answer: BCE

NEW QUESTION 117
- (Exam Topic 2)
Which Cisco Web Security Appliance design requires minimal change to endpoint devices?

A. Transparent Mode
B. Explicit Forward Mode
C. Promiscuous Mode
D. Inline Mode

Answer: A

NEW QUESTION 118
- (Exam Topic 2)
Which four statements are correct regarding management access to a Cisco Intrusion Prevention System? (Choose four.)

A. The Telnet protocol is enabled by default
B. The Telnet protocol is disabled by default
C. HTTP is enabled by default
D. HTTP is disabled by default
E. SSH is enabled by default
F. SSH is disabled by default
G. HTTPS is enabled by default
H. HTTPS is disabled by default

Answer: BDEG

NEW QUESTION 121
- (Exam Topic 2)
Which Cisco technology is a customizable web-based alerting service designed to report threats and vulnerabilities?

A. Cisco Security Intelligence Operations
B. Cisco Security IntelliShield Alert Manager Service

C. Cisco Security Optimization Service
D. Cisco Software Application Support Service

Answer: B

NEW QUESTION 125
- (Exam Topic 2)
What is the default CX Management 0/0 IP address on a Cisco ASA 5512-X appliance?

A. 192.168.1.1
B. 192.168.1.2
C. 192.168.1.3
D. 192.168.1.4
E. 192.168.1.5
F. 192.168.8.8

Answer: F

NEW QUESTION 128
- (Exam Topic 2)
Which Cisco IPS CLI command shows the most fired signature?

A. show statistics virtual-sensor
B. show event alert
C. show alert
D. show version

Answer: A

NEW QUESTION 129
- (Exam Topic 2)
Which three functions can Cisco Application Visibility and Control perform? (Choose three.)

A. Validation of malicious traffic
B. Traffic control
C. Extending Web Security to all computing devices
D. Application-level classification
E. Monitoring
F. Signature tuning

Answer: BDE

NEW QUESTION 133
- (Exam Topic 2)
Which three zones are used for anomaly detection? (Choose three.)

A. Internal zone
B. External zone
C. Illegal zone
D. Inside zone
E. Outside zone
F. DMZ zone

Answer: ABC

NEW QUESTION 137
- (Exam Topic 2)
The Web Security Appliance has identities defined for faculty and staff, students, and default access. The faculty and staff identity identifies users based on the source network and authenticated credentials. The identity for students identifies users based on the source network along with successful authentication credentials. The global identity is for guest users not authenticated against the domain.
Recently, a change was made to the organization's security policy to allow faculty and staff access to a social network website, and the security group changed the access policy for faculty and staff to allow the social networking category.
Which are the two most likely reasons that the category is still being blocked for a faculty and staff user? (Choose two.)

A. The user is being matched against the student policy because the user did not enter credentials.
B. The user is using an unsupported browser so the credentials are not working.
C. The social networking URL was entered into a custom URL category that is blocked in the access policy.
D. The user is connected to the wrong network and is being blocked by the student policy.
E. The social networking category is being allowed but the AVC policy is still blocking the website.

Answer: CE

NEW QUESTION 141
- (Exam Topic 2)
Which five system management protocols are supported by the Cisco Intrusion Prevention System? (Choose five.)

A. SNMPv2c
B. SNMPv1
C. SNMPv2
D. SNMPv3
E. Syslog
F. SDEE
G. SMTP

Answer: ABCFG

NEW QUESTION 142
- (Exam Topic 2)
Which two options are features of the Cisco Email Security Appliance? (Choose two.)

A. Cisco Anti-Replay Services
B. Cisco Destination Routing
C. Cisco Registered Envelope Service
D. Cisco IronPort SenderBase Network

Answer: CD

NEW QUESTION 146
- (Exam Topic 2)
The helpdesk was asked to provide a record of delivery for an important email message that a customer claims it did not receive. Which feature of the Cisco Email Security Appliance provides this record?

A. Outgoing Mail Reports
B. SMTP Routes
C. Message Tracking
D. Scheduled Reports
E. System Administration

Answer: C

NEW QUESTION 150
- (Exam Topic 2)
Which configuration option causes an ASA with IPS module to drop traffic matching IPS signatures and to block all traffic if the module fails?

A. Inline Mode, Permit Traffic
B. Inline Mode, Close Traffic
C. Promiscuous Mode, Permit Traffic
D. Promiscuous Mode, Close Traffic

Answer: B

NEW QUESTION 154
- (Exam Topic 2)
Which two options are characteristics of router-based IPS? (Choose two.)

A. It supports custom signatures
B. It supports virtual sensors.
C. It supports multiple VRFs.
D. It uses configurable anomaly detection.
E. Signature definition files have been deprecated.

Answer: CE

NEW QUESTION 157
- (Exam Topic 2)
Which two benefits are provided by the dynamic dashboard in Cisco ASDM Version 5.2? (Choose two.)

A. It configures system polices for NAC devices.
B. It forwards traffic to destination devices.
C. It provides statistics for device health.
D. It replaces syslog, RADIUS, and TACACS+ servers.
E. It automatically detects Cisco security appliances to configure.

Answer: CE

NEW QUESTION 159
- (Exam Topic 2)
Which two statements about Cisco Cloud Web Security functionality are true? (Choose two.)

A. It integrates with Cisco Integrated Service Routers.
B. It supports threat avoidance and threat remediation.
C. It extends web security to the desktop, laptop, and PDA.
D. It integrates with Cisco ASA Firewalls.

Answer: AD

NEW QUESTION 162
- (Exam Topic 2)
Which version of AsyncOS for web is required to deploy the Web Security Appliance as a CWS connector?

A. AsyncOS version 7.7.x
B. AsyncOS version 7.5.x
C. AsyncOS version 7.5.7
D. AsyncOS version 7.5.0

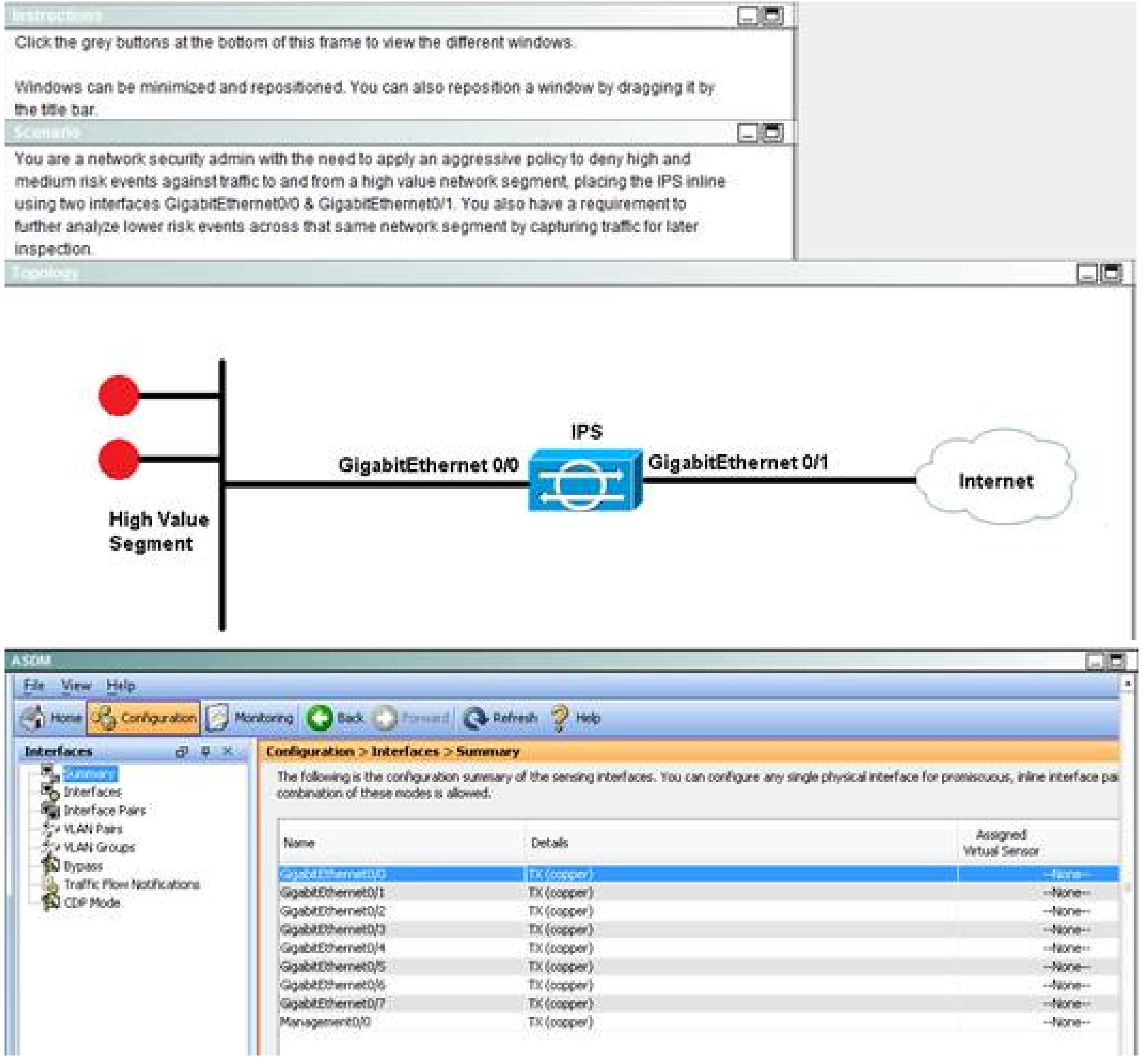
Answer: C

NEW QUESTION 165
- (Exam Topic 2)
Which antispam technology assumes that email from server A, which has a history of distributing spam, is more likely to be spam than email from server B, which does not have a history of distributing spam?

A. Reputation-based filtering
B. Context-based filtering
C. Cisco ESA multilayer approach
D. Policy-based filtering

Answer: A

NEW QUESTION 167
- (Exam Topic 2)



Instructions

Click the grey buttons at the bottom of this frame to view the different windows.

Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

Scenario

You are a network security admin with the need to apply an aggressive policy to deny high and medium risk events against traffic to and from a high value network segment, placing the IPS inline using two interfaces GigabitEthernet0/0 & GigabitEthernet0/1. You also have a requirement to further analyze lower risk events across that same network segment by capturing traffic for later inspection.

Topology

Configuration > Interfaces > Summary

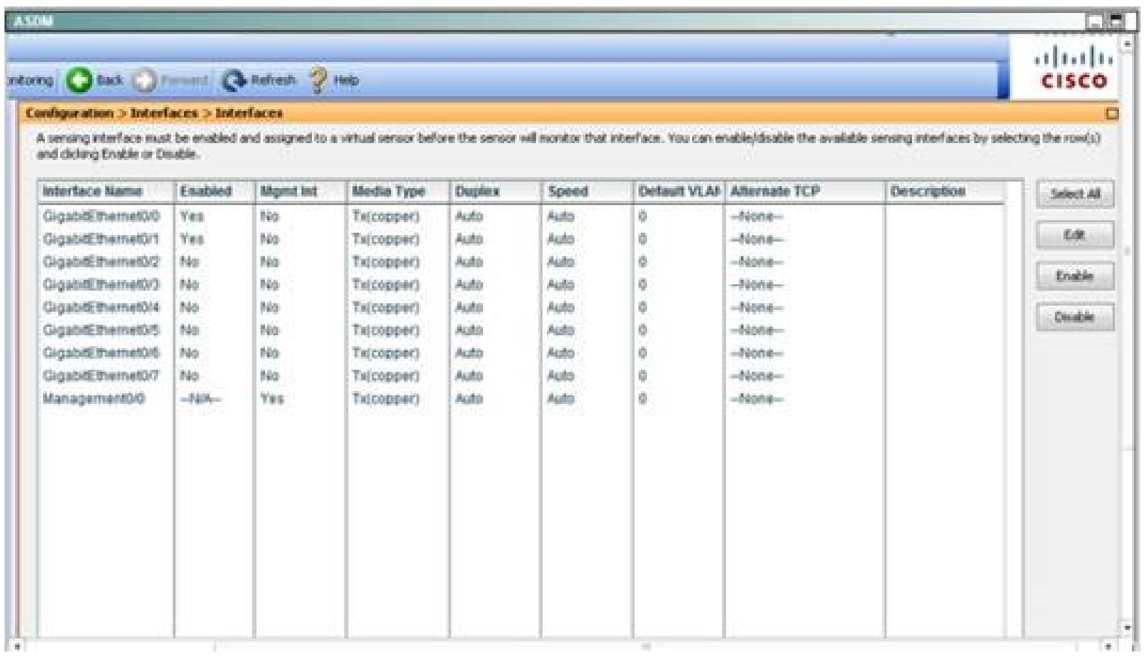
The following is the configuration summary of the sensing interfaces. You can configure any single physical interface for promiscuous, inline interface pai combination of these modes is allowed.

Name	Details	Assigned Virtual Sensor
GigabitEthernet0/0	TX (copper)	--None--
GigabitEthernet0/1	TX (copper)	--None--
GigabitEthernet0/2	TX (copper)	--None--
GigabitEthernet0/3	TX (copper)	--None--
GigabitEthernet0/4	TX (copper)	--None--
GigabitEthernet0/5	TX (copper)	--None--
GigabitEthernet0/6	TX (copper)	--None--
GigabitEthernet0/7	TX (copper)	--None--
Management0/0	TX (copper)	--None--

A. Mastered
B. Not Mastered

Answer: A

Explanation:
First, enable the Gig 0/0 and Gig 0/1 interfaces:

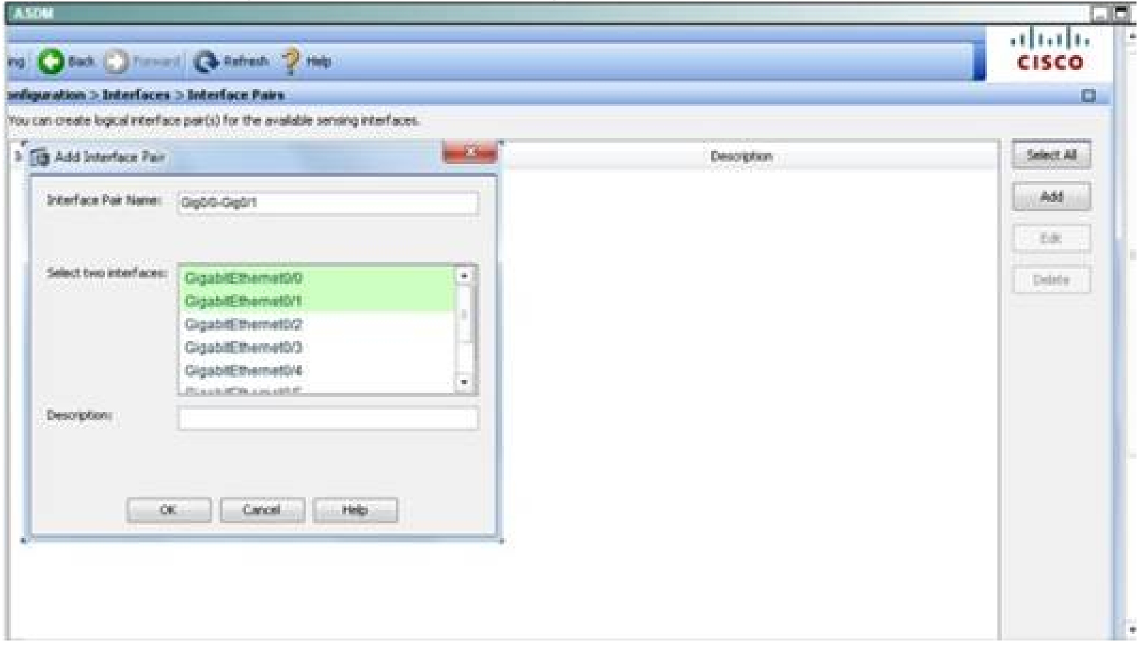


Configuration > Interfaces > Interfaces

A sensing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enable/disable the available sensing interfaces by selecting the row(s) and clicking Enable or Disable.

Interface Name	Enabled	Mgmt Int	Media Type	Duplex	Speed	Default VLAN	Alternate TCP	Description
GigabitEthernet0/0	Yes	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/1	Yes	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/2	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/3	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/4	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/5	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/6	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/7	No	No	Tx(copper)	Auto	Auto	0	--None--	
Management0/0	--N/A--	Yes	Tx(copper)	Auto	Auto	0	--None--	

Second, create the pair under the “interface pairs” taB.



Configuration > Interfaces > Interface Pairs

You can create logical interface pair(s) for the available sensing interfaces.

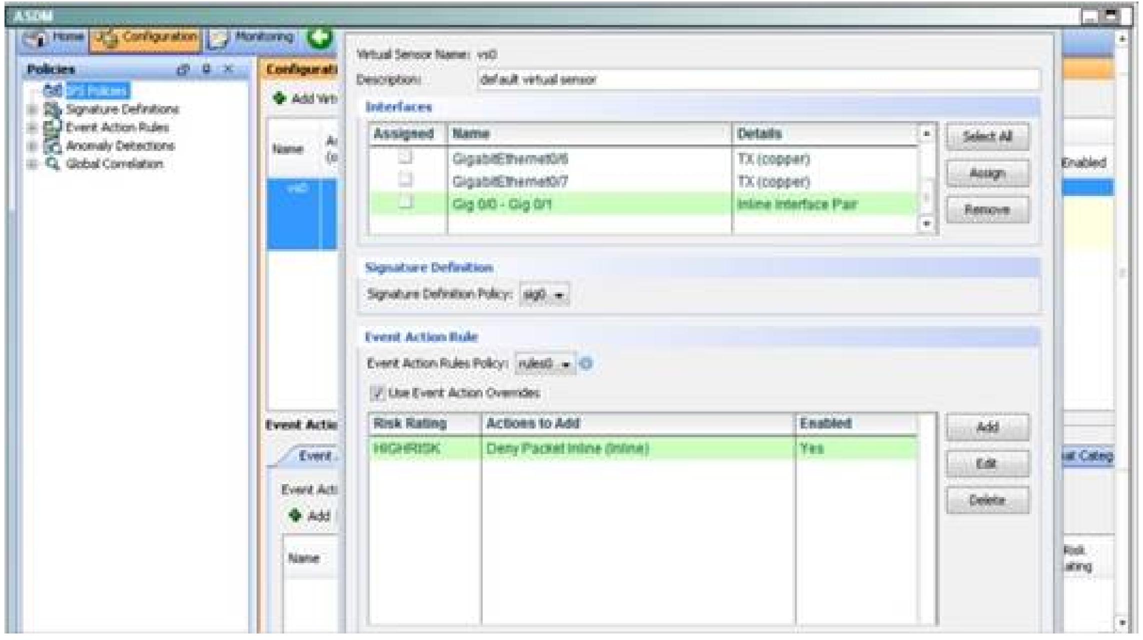
Add Interface Pair

Interface Pair Name: Gig0/0-Gig0/1

Select two interfaces: GigabitEthernet0/0, GigabitEthernet0/1 (selected); GigabitEthernet0/2; GigabitEthernet0/3; GigabitEthernet0/4

Description:

Then, apply the HIGHRISK action rule to the newly created interface pair:



Virtual Sensor Name: vs0

Description: default virtual sensor

Interfaces

Assigned	Name	Details
□	GigabitEthernet0/6	TX (copper)
□	GigabitEthernet0/7	TX (copper)
□	Gig 0/0 - Gig 0/1	Inline Interface Pair

Signature Definition

Signature Definition Policy: sig0

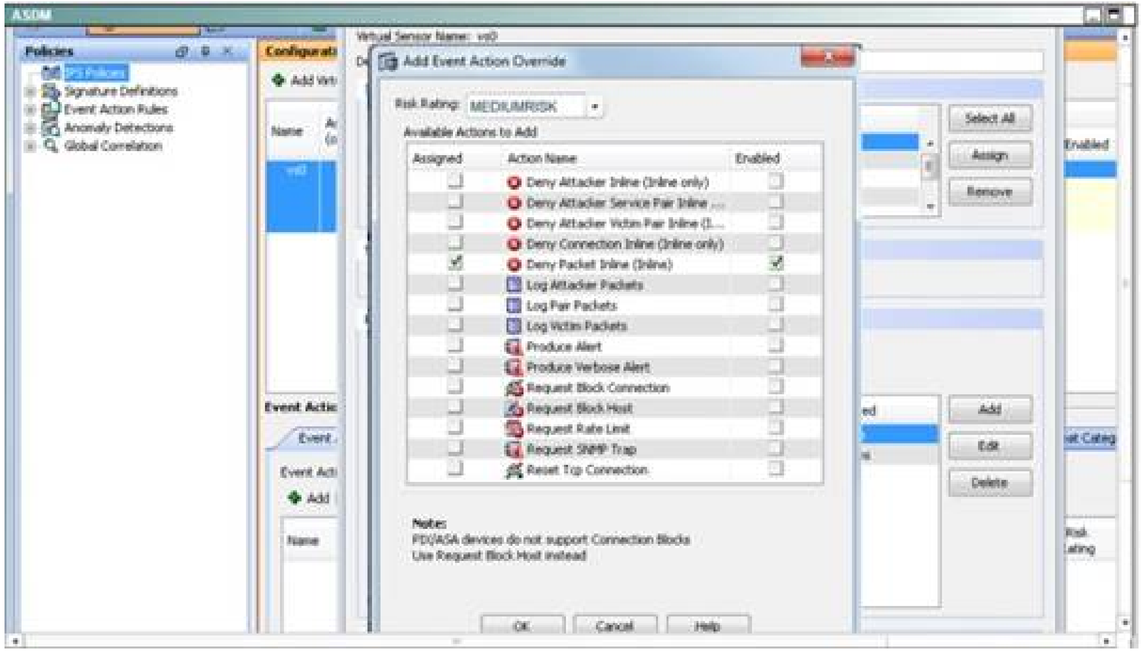
Event Action Rule

Event Action Rules Policy: rules0

☑ Use Event Action Overrides

Risk Rating	Actions to Add	Enabled
HIGHRISK	Deny Packet Inline (Inline)	Yes

Then apply the same for the MEDIUMRISK traffic (deny attacker inline)



Virtual Sensor Name: vs0

Add Event Action Override

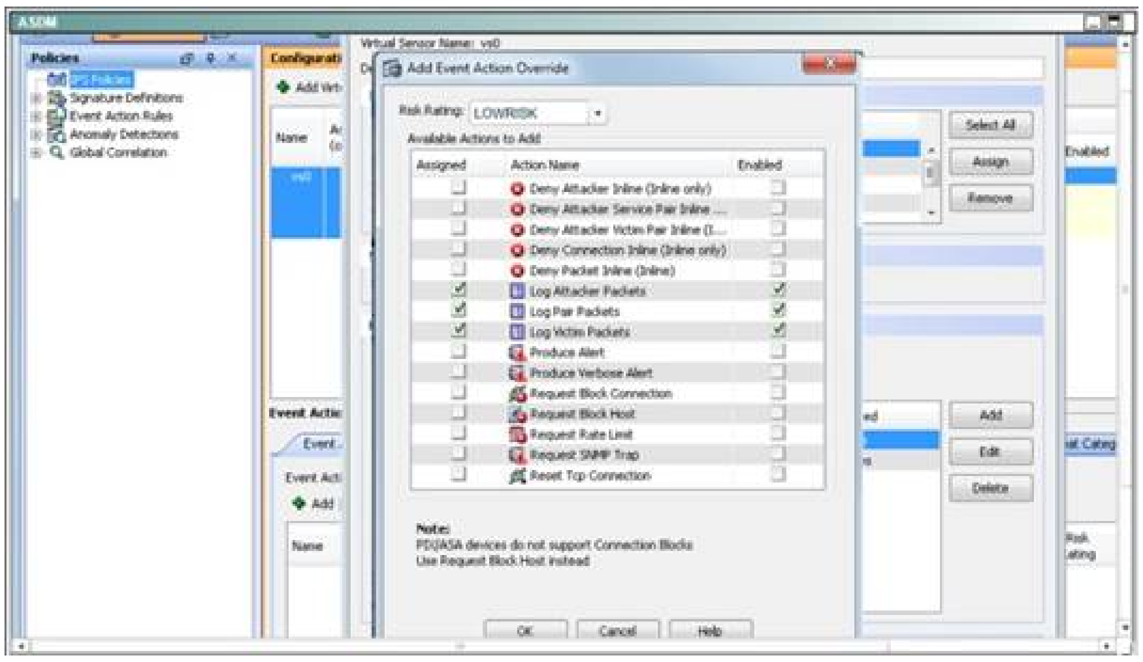
Risk Rating: MEDIUMRISK

Available Actions to Add

Assigned	Action Name	Enabled
□	Deny Attacker Inline (Inline only)	□
□	Deny Attacker Service Pair Inline ...	□
□	Deny Attacker Victim Pair Inline (I...	□
□	Deny Connection Inline (Inline only)	□
☑	Deny Packet Inline (Inline)	☑
□	Log Attacker Packets	□
□	Log Pair Packets	□
□	Log Victim Packets	□
□	Produce Alert	□
□	Produce Verbose Alert	□
□	Request Block Connection	□
□	Request Block Host	□
□	Request Rate Limit	□
□	Request SNMP Trap	□
□	Reset Tcp Connection	□

Note:
PIX/ASA devices do not support Connection Blocks
Use Request Block Host instead

Finally. Log the packets for the LOWRICK event:



Virtual Sensor Name: vs0

Add Event Action Override

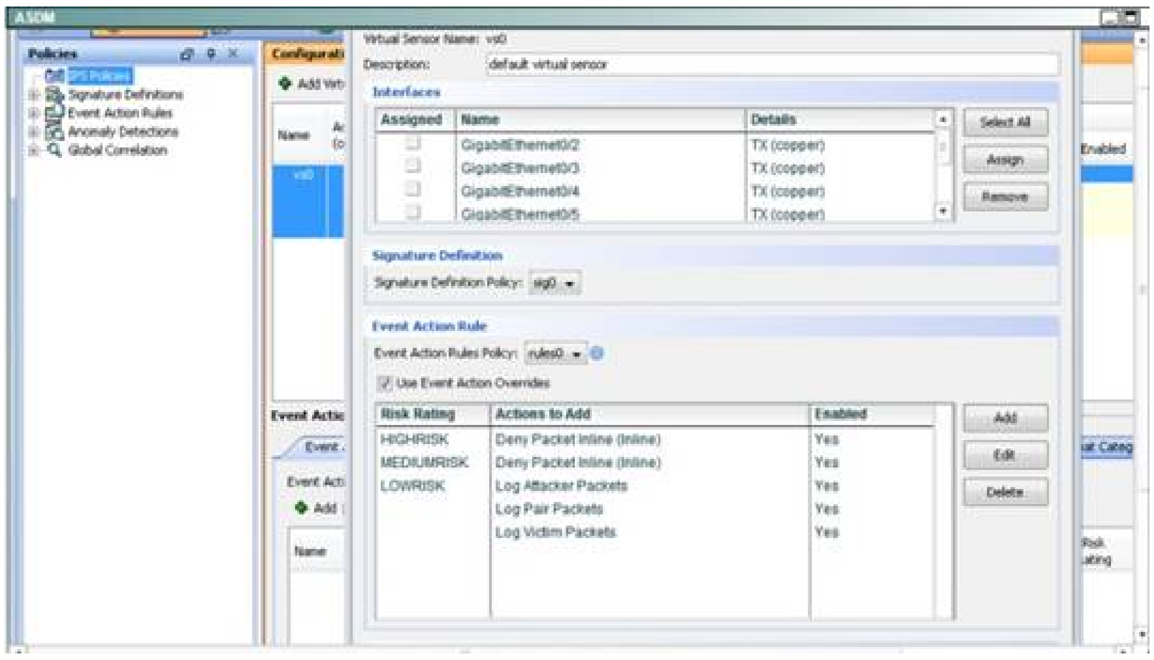
Risk Rating: LOWRISK

Available Actions to Add

Assigned	Action Name	Enabled
□	Deny Attacker Inline (Inline only)	□
□	Deny Attacker Service Pair Inline ...	□
□	Deny Attacker Victim Pair Inline (I...	□
□	Deny Connection Inline (Inline only)	□
□	Deny Packet Inline (Inline)	□
☑	Log Attacker Packets	☑
☑	Log Pair Packets	☑
☑	Log Victim Packets	☑
□	Produce Alert	□
□	Produce Verbose Alert	□
□	Request Block Connection	□
□	Request Block Host	□
□	Request Rate Limit	□
□	Request SNMP Trap	□
□	Reset Tcp Connection	□

Note:
PDI/ASA devices do not support Connection Blocks
Use Request Block Host instead

When done it should look like this:



Virtual Sensor Name: vs0

Description: default virtual sensor

Interfaces

Assigned	Name	Details
□	GigabitEthernet0/2	TX (copper)
□	GigabitEthernet0/3	TX (copper)
□	GigabitEthernet0/4	TX (copper)
□	GigabitEthernet0/5	TX (copper)

Signature Definition

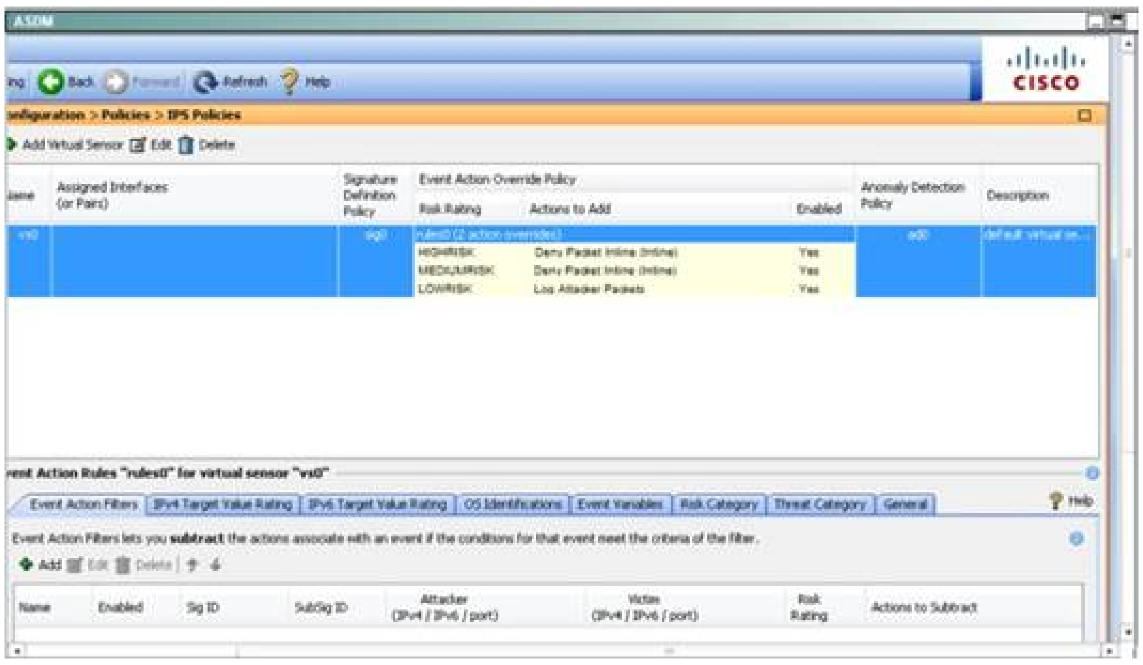
Signature Definition Policy: sig0

Event Action Rule

Event Action Rules Policy: rules0

☑ Use Event Action Overrides

Risk Rating	Actions to Add	Enabled
HIGHRISK	Deny Packet Inline (Inline)	Yes
MEDIUMRISK	Deny Packet Inline (Inline)	Yes
LOWRISK	Log Attacker Packets	Yes
	Log Pair Packets	Yes
	Log Victim Packets	Yes



Configuration > Policies > IPS Policies

Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy			Anomaly Detection Policy	Description
			Risk Rating	Actions to Add	Enabled		
vs0		sig0	rules0 (2 action overrides)			ad0	default virtual se...
			HIGHRISK	Deny Packet Inline (Inline)	Yes		
			MEDIUMRISK	Deny Packet Inline (Inline)	Yes		
			LOWRISK	Log Attacker Packets	Yes		

Event Action Rules "rules0" for virtual sensor "vs0"

Event Action Filters lets you **subtract** the actions associate with an event if the conditions for that event meet the criteria of the filter.

Name	Enabled	Sig ID	SubSig ID	Attacker (IPv4 / IPv6 / port)	Victim (IPv4 / IPv6 / port)	Risk Rating	Actions to Subtract

NEW QUESTION 170
- (Exam Topic 2)
Cisco AVC allows control of which three of the following? (Choose three.)

A. Facebook
B. LWAPP
C. IPv6
D. MySpace
E. Twitter
F. WCCP

Answer: ADE

NEW QUESTION 172
- (Exam Topic 2)
ACisco Web Security Appliance's policy can provide visibility and control of which two elements? (Choose two.)

A. Voice and Video Applications
B. Websites with a reputation between -100 and -60
C. Secure websites with certificates signed under an unknown CA
D. High bandwidth websites during business hours

Answer: CD

NEW QUESTION 175
- (Exam Topic 2)
ACisco Email Security Appliance uses which message filter to drop all executable attachments entering and leaving the Cisco Email Security Appliance?

A. drop-ex
B. if (attachment-filename == "\\.exe$") OR (attachment-filetype == "exe") { drop(); }
C. drop-ex
D. if (recv-listener == "InboundMail") AND ((attachment-filename == "\\.exe$") OR (attachment-filetype == "exe")) { drop(); }
E. drop-exe! if (attachment-filename == "\\.exe$") OR (attachment-filetype == "exe") { drop(); }
F. drop-exe! if (recv-listener == "InboundMail") AND ((attachment-filename == "\\.exe$") OR (attachment-filetype == "exe")) { drop(); }

Answer: A

NEW QUESTION 177
- (Exam Topic 2)
Which command is used to enable strong ciphers on the Cisco Web Security Appliance?

A. interfaceconfig
B. strictssl
C. etherconfig
D. adminaccessconfig

Answer: B

NEW QUESTION 182
- (Exam Topic 2)
An ASA with an IPS module must be configured to drop traffic matching IPS signatures and block all traffic if the module fails. Which describes the correct configuration?

A. Inline Mode, Permit Traffic
B. Inline Mode, Close Traffic
C. Promiscuous Mode, Permit Traffic
D. Promiscuous Mode, Close Traffic

Answer: B

NEW QUESTION 183
- (Exam Topic 2)
What is the default IP range of the external zone?

A. 0.0.0.0 0.0.0.0
B. 0.0.0.0 - 255.255.255.255
C. 0.0.0.0/8
D. The network of the management interface

Answer: B

NEW QUESTION 186
- (Exam Topic 2)
Connections are being denied because of SenderBase Reputation Scores. Which two features must be enabled in order to record those connections in the mail log on the Cisco ESA? (Choose two.)

A. Rejected Connection Handling
B. Domain Debug Logs
C. Injection Debug Logs
D. Message Tracking

Answer: AD

NEW QUESTION 191
- (Exam Topic 2)
Which IPS signature regular expression CLI command matches a host issuing a domain lookup for www.theblock.com?

A. regex-string (\x03[Tt][Hh][Ee]\x05[Bb][Ll][Oo][Cc][Kk])
B. regex-string (\x0b[theblock.com])
C. regex-string (\x03[the]\x05[block]0x3[com])
D. regex-string (\x03[T][H][E]\x05[B][L][O][C][K]\x03[.][C][O][M]

Answer: A

NEW QUESTION 195
- (Exam Topic 2)
The security team needs to limit the number of e-mails they receive from the Intellishield Alert Service. Which three parameters can they adjust to restrict alerts to

specific product sets? (Choose three.)

A. Vendor
B. Chassis/Module
C. Device ID
D. Service Contract
E. Version/Release
F. Service Pack/Platform

Answer: AEF

NEW QUESTION 197
- (Exam Topic 3)
An IPS is configured to fail-closed and you observe that all packets are dropped. What is a possible reason for this behavior?

A. Mainapp is unresponsive.
B. The global correlation update failed.
C. The IPS span session failed.
D. The attack drop file is misconfigured.

Answer: A

NEW QUESTION 199
- (Exam Topic 3)
Which option describes a customer benefit of the Cisco Security IntelliShield Alert Manager?

A. It provides access to threat and vulnerability information for Cisco related products only.
B. It consolidates vulnerability information from an internal Cisco source, which allows security personnel to focus on remediation and proactive protection versus research.
C. It provides effective and timely security intelligence via early warnings about new threats and technology vulnerabilities.
D. It enhances the efficiency of security staff with accurate, noncustomizable threat intelligence, critical remediation information, and easy-to-use workflow tools.

Answer: C

NEW QUESTION 201
- (Exam Topic 3)
Which two configuration steps are required for implementing SSH for management access to a Cisco router? (Choose two.)

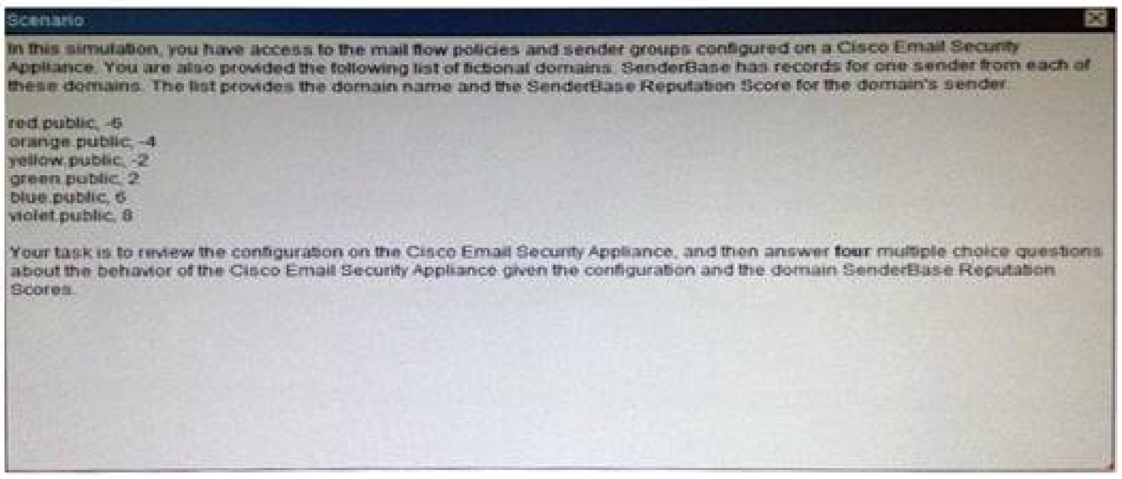
A. Configuring the SSH version with the ip ssh version 2 command.
B. Generating RSA key pairs with the crypto key generate rsa command.
C. Enabling AAA for authentication, authorization, and accounting with the aaa new-model command.
D. Enabling SSH transport with the transport input ssh command.
E. Configuring a domain name with the ip domain-name [name] command.

Answer: DE

Explanation:

Reference: http://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145ssh.html

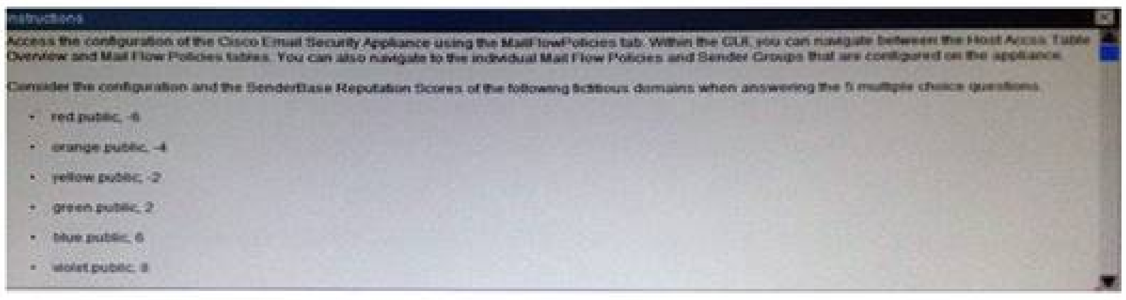
NEW QUESTION 203
- (Exam Topic 3)



In this simulation, you have access to the mail flow policies and sender groups configured on a Cisco Email Security Appliance. You are also provided the following list of fictional domains. SenderBase has records for one sender from each of these domains. The list provides the domain name and the SenderBase Reputation Score for the domain's sender.

red.public, -6
orange.public, -4
yellow.public, -2
green.public, 2
blue.public, 6
violet.public, 8

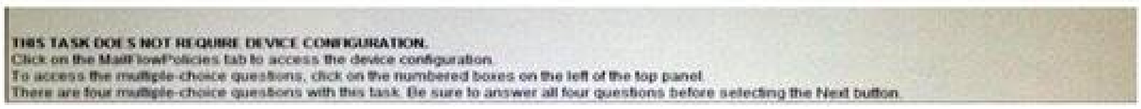
Your task is to review the configuration on the Cisco Email Security Appliance, and then answer **four** multiple choice questions about the behavior of the Cisco Email Security Appliance given the configuration and the domain SenderBase Reputation Scores.



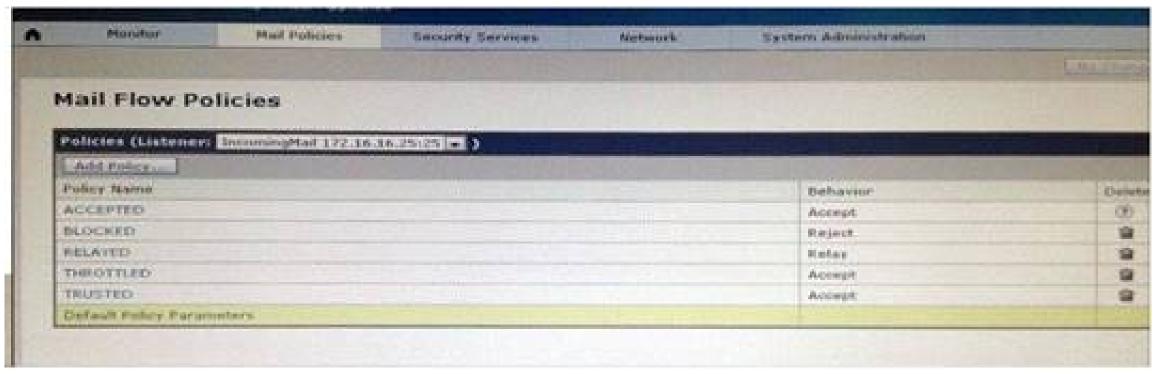
Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the Host Access Table Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance.

Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the 5 multiple choice questions.

- red.public, -6
- orange.public, -4
- yellow.public, -2
- green.public, 2
- blue.public, 6
- violet.public, 8



THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
Click on the MailFlowPolicies tab to access the device configuration.
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.



Mail Flow Policies

Policies (Listener: IncomingMail 172.16.16.25:25)

Policy Name	Behavior	Delete
ACCEPTED	Accept	?
BLOCKED	Reject	🗑
RELAYED	Relay	🗑
THROTTLED	Accept	🗑
TRUSTED	Accept	🗑
Default Policy Parameters		

What is the maximum number of recipients per hour that the Cisco Email Security Appliance will accept from the green. public domain?

A. 1
B. 20
C. 25
D. 50
E. 5000
F. Unlimited

Answer: C

NEW QUESTION 205
- (Exam Topic 3)
Refer to the Following. Which option describe the result of this configuration on a Cisco ASA firewall?
asafwl (config) #http server enable asafw1(config)#http 10.10.10.1 255.255.255.255 inside

A. The firewall allows command-line access from 10.10.10.1
B. The firewall allows ASDM access from a client on 10.10.10.1
C. The management IP address of the firewall is 10.10.10.1
D. The inside interface IP address of the firewall is 10.10.10.1

Answer: B

NEW QUESTION 208
- (Exam Topic 3)
A user is deploying a Cisco IPS appliance in a data center to mitigate most attacks, including atomic attacks. Which two modes does Cisco recommend using to configure for this? (Choose two.)

A. VLAN pair
B. interface pair
C. transparent mode
D. EtherChannel load balancing
E. promiscuous mode

Answer: AD

NEW QUESTION 213
- (Exam Topic 3)
Which three statements about Cisco CWS are true? (Choose three.)

A. It provides protection against zero-day threats.
B. Cisco SIO provides it with threat updates in near real time.
C. It supports granular application policies.
D. Its Roaming User Protection feature protects the VPN from malware and data breaches.
E. It supports local content caching.
F. Its Cognitive Threat Analytics feature uses cloud-based analysis and detection to block threats outside the network.

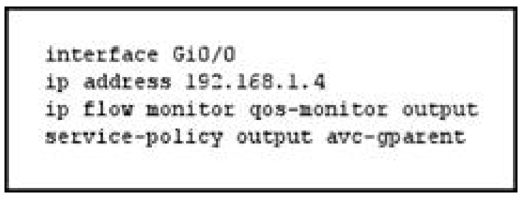
Answer: ABC

NEW QUESTION 218
- (Exam Topic 3)
What does the anomaly detection Cisco IOS IPS component detection?

A. ARP Spoofing
B. Worm-infected hosts
C. Signature changes
D. Network Congestion

Answer: B

NEW QUESTION 222
- (Exam Topic 3)
Refer to the exhibit.



```
interface Gi0/0
ip address 192.168.1.4
ip flow monitor qos-monitor output
service-policy output avc-gparent
```

What are two facts about the interface that you can determine from the given output? (Choose two.)

A. ACisco Flexible NetFlow monitor is attached to the interface.
B. A quality of service policy is attached to the interface.
C. Cisco Application Visibility and Control limits throughput on the interface.
D. Feature activation array is active on the interface.

Answer: AB

NEW QUESTION 224
- (Exam Topic 3)
Which technology is used to improve business-critical application performance?

A. Application Visibility and Control
B. Intrusion Prevention Services
C. Advanced Malware Protection
D. TrustSec

Answer: A

NEW QUESTION 228
- (Exam Topic 3)
Which description of an advantage of utilizing IPS virtual sensors is true?

A. Different configurations can be applied to different sets of traffic.
B. The persistent store is unlimited for the IPS virtual sensor.
C. The virtual sensor does not require 802.1q headers for inbound traffic.
D. Asymmetric traffic can be split between multiple virtual sensors

Answer: A

Explanation:
http://www.cisco.com/c/en/us/td/docs/security/ips/7-0/configuration/guide/cli/cliguide7/cli_virtual_sensors.pdf

NEW QUESTION 229
- (Exam Topic 3)
How are HTTP requests handled by the Cisco WSA?

A. transparent request has a destination IP address of the configured proxy.
B. The URI for an implicit request doest not contain the DNS host.
C. An explict request has a destination IP address of the intended web server.
D. The URI for an explicit request contains the host with the protocol information.

Answer: D

NEW QUESTION 234
- (Exam Topic 3)
Which Cisco Web Security Appliance feature enables the appliance to block suspicious traffic on all of its ports and IP addresses?

A. Layer 4 Traffic Monitor
B. Secure Web Proxy
C. explicit forward mode
D. transparent mode

Answer: A

NEW QUESTION 239
- (Exam Topic 3)
Which feature does Acceptable Use Controls use to implement Cisco AVC?

A. ISA
B. Cisco Web Usage Controls
C. Cisco WSA
D. Cisco ESA

Answer: B

NEW QUESTION 240
- (Exam Topic 3)
Which four methods are used to deploy transparent mode traffic redirection? (Choose four.)

A. PAC files
B. Web Cache Communication Protocol
C. policy-based routing
D. Microsoft GPO
E. Layer 4 switch
F. DHCP server
G. Layer 7 switch
H. manual browser configuration

Answer: BCEG

NEW QUESTION 245
- (Exam Topic 3)
When a Cisco IPS is deployed in fail-closed mode, what are two conditions that can result in traffic being dropped? (Choose two.)

A. The signature engine is undergoing the build process.
B. The SDF failed to load.
C. The built-in signatures are unavailable.
D. An ACL is configured.

Answer: AB

NEW QUESTION 247
- (Exam Topic 3)
Which Cisco IOS command uses the default class map to limit SNMP inspection to traffic from 10.1.1.0 to 192.168.1.0?

A. hostname(config)# access-list inspect extended permit ip 10.1.1.0.0.0.0.255 192.168.1.0.0.0.0.255hostname(config)# class-map inspection_default hostname(config-cmap)# match access-list inspect
B. hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0hostname(config-cmap)# match access-list inspect
C. hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0hostname(config)# class-map inspection_default hostname(config-cmap)# match access-list inspect
D. hostname(config)# access-list inspect extended permit ip 10.1.1.0.0.0.255 192.168.1.0.0.0.255hostname(config)# class-map inspection_default

Answer: C

Explanation:
Reference:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/inspect_overvi ew.html

NEW QUESTION 249
- (Exam Topic 3)
Refer to the following.
Router (config) #username admin secret cisco Router (config) #no service password-encryption
How is the “cisco” password stored?

A. As MD5 hash
B. As Type 0
C. As Type 7
D. As Clear Text

Answer: A

NEW QUESTION 250
- (Exam Topic 3)
Which option describes how the native VLAN is set up on an IPS sensor when VLAN groups are used in an inline deployment of the sensor?

A. The sensor looks at the native VLAN setup on the switch to determine the correct native VLAN to use.
B. The sensor does not care about VLANs.
C. A default VLAN variable must be associated with each physical interface on the sensor.
D. There is no way to set this, so you need to tag all traffic.
E. ISL links are only supported.

Answer: C

NEW QUESTION 252
- (Exam Topic 3)
Which option is a benefit of Cisco Email Security virtual appliance over the Cisco ESA appliance?

A. reduced space and power requirements
B. outbound message protection
C. automated administration
D. global threat intelligence updates from Talos

Answer: A

NEW QUESTION 256
- (Exam Topic 3)

You have configured a VLAN pair that is connected to a switch that is unable to pass traffic. If the IPS is configured correctly, which additional configuration must you perform to enable the switch to pass traffic?

A. Configure access ports on the switch.
B. Configure the trunk port on the switch.
C. Enable IP routing on the switch.
D. Enable ARP inspection on the switch.

Answer: A

NEW QUESTION 259
- (Exam Topic 3)
A security engineer is configuring user identity for the Cisco ASA connector for Cisco CWS. How many AAA server groups must the engineer configure?

A. 1
B. 3
C. 4
D. 2

Answer: D

NEW QUESTION 263
- (Exam Topic 3)
Which signature engine is responsible for ICMP inspection on Cisco IPS?

A. AICEngine
B. Fixed Engine
C. Service Engine
D. Atomic IP Engine

Answer: D

NEW QUESTION 268
- (Exam Topic 3)
What is the function of the Web Proxy Auto-Discovery protocol?

A. It enables a web client to discover the URL of a configuration file.
B. It enables a web client to download a script or configuration file that is named by a URL.
C. It enables a web client's traffic flows to be redirected in real time.
D. It enables web clients to dynamically resolve hostname records.

Answer: A

NEW QUESTION 272
- (Exam Topic 3)
Which technique is deployed to harden network devices?

A. port-by-port router ACLs
B. infrastructure ACLs
C. transmit ACLs
D. VLAN ACLs

Answer: B

NEW QUESTION 276
- (Exam Topic 3)
Which feature of the Cisco Hybrid Email Security services enables you to create multiple email senders on a single Cisco ESA?

A. Virtual Gateway
B. Sender Groups
C. Mail Flow Policy Connector
D. Virtual Routing and Forwarding
E. Email Marketing Connector

Answer: A

NEW QUESTION 281
- (Exam Topic 3)
Which two conditions must you configure in an event action rule to match all IPv4 addresses in the victim range and filter on the complete subsignature range? (Choose two.)

A. Disable event action override.
B. Leave the victim address range unspecified.
C. Set the subsignature ID-range to the default.
D. Set the deny action percentage to 100.
E. Set the deny action percentage to 0.

Answer: BC

NEW QUESTION 282
- (Exam Topic 3)
Which two commands are used to verify that CWS redirection is working on a Cisco ASA appliance? (Choose two.)

A. show scansafe statistics
B. show webvpn statistics
C. show service-policy inspect scansafe
D. show running-config scansafe
E. show running-config webvpn
F. show url-server statistics

Answer: AC

NEW QUESTION 283
- (Exam Topic 3)
Which action cloud reduce the security of the management interface of the Cisco ESA appliance?

A. Assign delegated administrator roles to engineers who manage the mail policies.
B. create a network access list to allow all connections to the management interface
C. Display a login banner indicating that all appliance use is logged and reviewed
D. configure a web UI session timeout of 30 minutes for connected users.

Answer: A

NEW QUESTION 286
- (Exam Topic 3)
In which way are packets handled when the IPS internal zone is set to "disabled"?

A. All packets are dropped to the external zone.
B. All packets are dropped to the internal zone.
C. All packets are ignored in the internal zone.
D. All packets are sent to the default external zone.

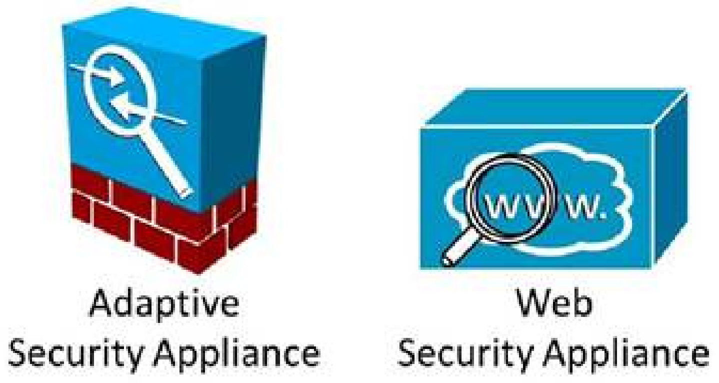
Answer: D

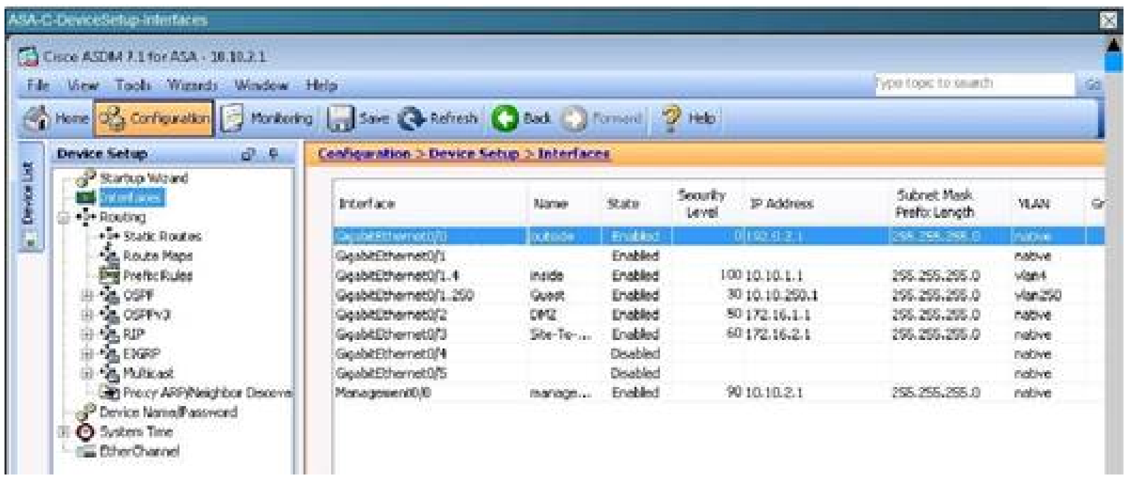
NEW QUESTION 290
- (Exam Topic 3)
What are the two policy types that can use a web reputation profile to perform reputation-based processing? (Choose two.)

A. profile policies
B. encryption policies
C. decryption policies
D. access policies

Answer: CD

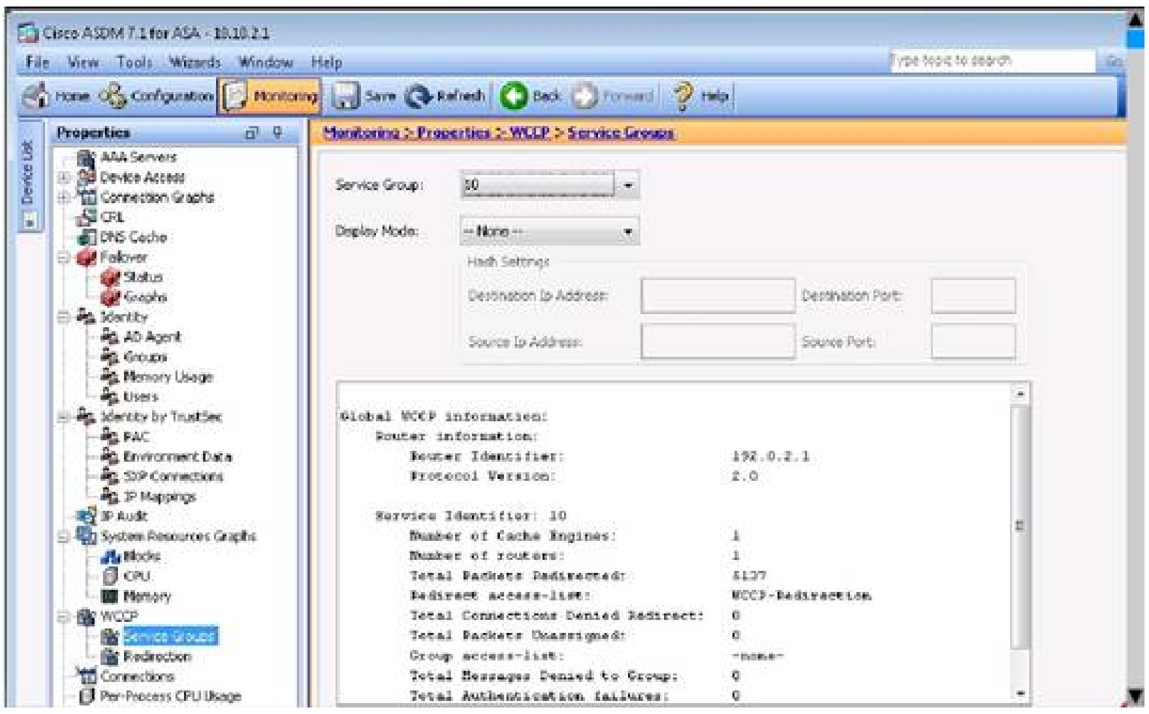
NEW QUESTION 294
- (Exam Topic 3)
The Web Cache Communication Protocol (WCCP) is a content-routing protocol that can facilitate the redirection of traffic flows in real time. Your organization has deployed WCCP to redirect web traffic that traverses their Cisco Adaptive Security Appliances (ASAs) to their Cisco Web Security Appliances (WSAs).
The simulator will provide access to the graphical user interfaces of one Cisco ASA and one Cisco WSA that are participating in a WCCP service. Not all aspects of the GUIs are implemented in the simulator. The options that have been implemented are sufficient to determine the best answer to each of the questions that are presented.
Your task is to examine the details available in the simulated graphical user interfaces and select the best answer.




ASA-C-DeviceSetup-Interfaces
Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Device Setup
Startup Wizard
Interfaces
Routing
Static Routes
Route Maps
Prefix Rules
OSPF
OSPFv3
RIP
EIGRP
Multicast
Proxy ARP/Neighbor Discove
Device Name/Password
System Time
EtherChannel

Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN
GigabitEthernet0/0	outside	Enabled	0	192.0.2.1	255.255.255.0	native
GigabitEthernet0/1		Enabled				native
GigabitEthernet0/1.4	inside	Enabled	100	10.10.1.1	255.255.255.0	vlan4
GigabitEthernet0/1.250	Guest	Enabled	30	10.10.250.1	255.255.255.0	vlan250
GigabitEthernet0/2	DMZ	Enabled	50	172.16.1.1	255.255.255.0	native
GigabitEthernet0/3	Site-To-...	Enabled	60	172.16.2.1	255.255.255.0	native
GigabitEthernet0/4		Disabled				native
GigabitEthernet0/5		Disabled				native
Management0/0	manage...	Enabled	90	10.10.2.1	255.255.255.0	native



Monitoring > Properties > WCCP > Service Groups

Service Group: 10

Display Mode: -- None --

Hash Settings

Destination Ip Address:

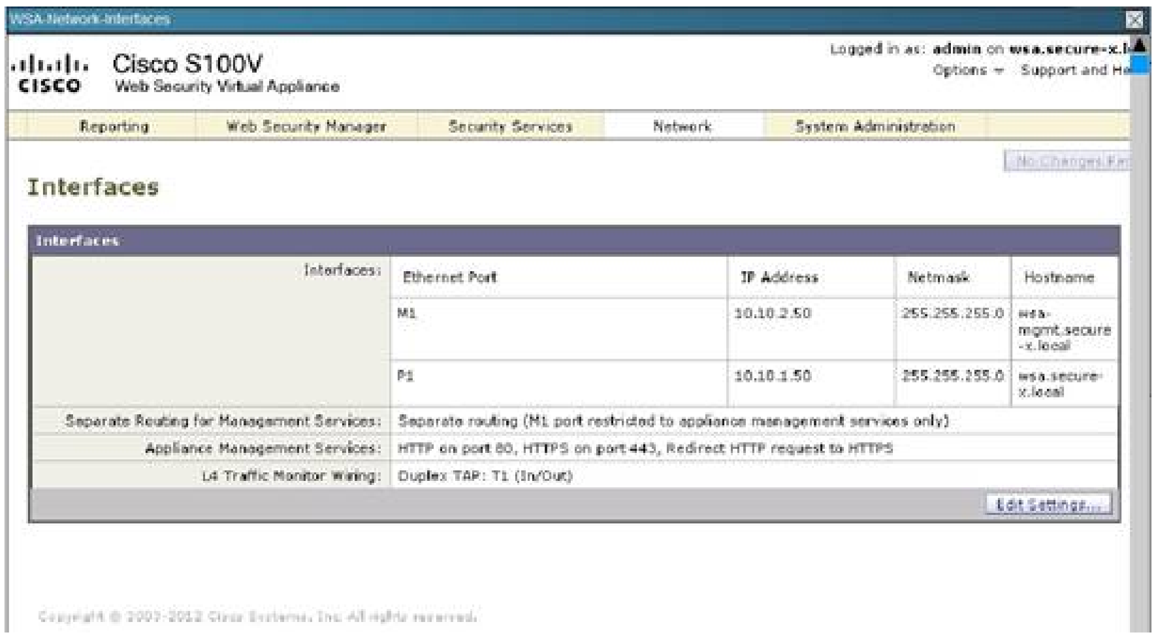
Destination Port:

Source Ip Address:

Source Port:

```
Global WCCP information:
    Router information:
        Router Identifier:                   192.0.2.1
        Protocol Version:                    2.0

    Service Identifier: 10
        Number of Cache Engines:             1
        Number of routers:                   1
        Total Packets Redirected:            5127
        Redirect access-list:                WCCP-Redirection
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   -none-
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
```



Interfaces

Interfaces

Interfaces:	Ethernet Port	IP Address	Netmask	Hostname
	M1	10.10.2.50	255.255.255.0	wsa-mgmt.secure-x.local
	P1	10.10.1.50	255.255.255.0	wsa.secure-x.local
Separate Routing for Management Services:	Separate routing (M1 port restricted to appliance management services only)			
Appliance Management Services:	HTTP on port 80, HTTPS on port 443, Redirect HTTP request to HTTPS			
L4 Traffic Monitor Wiring:	Duplex TAP: T1 (In/Out)			

Edit Settings...

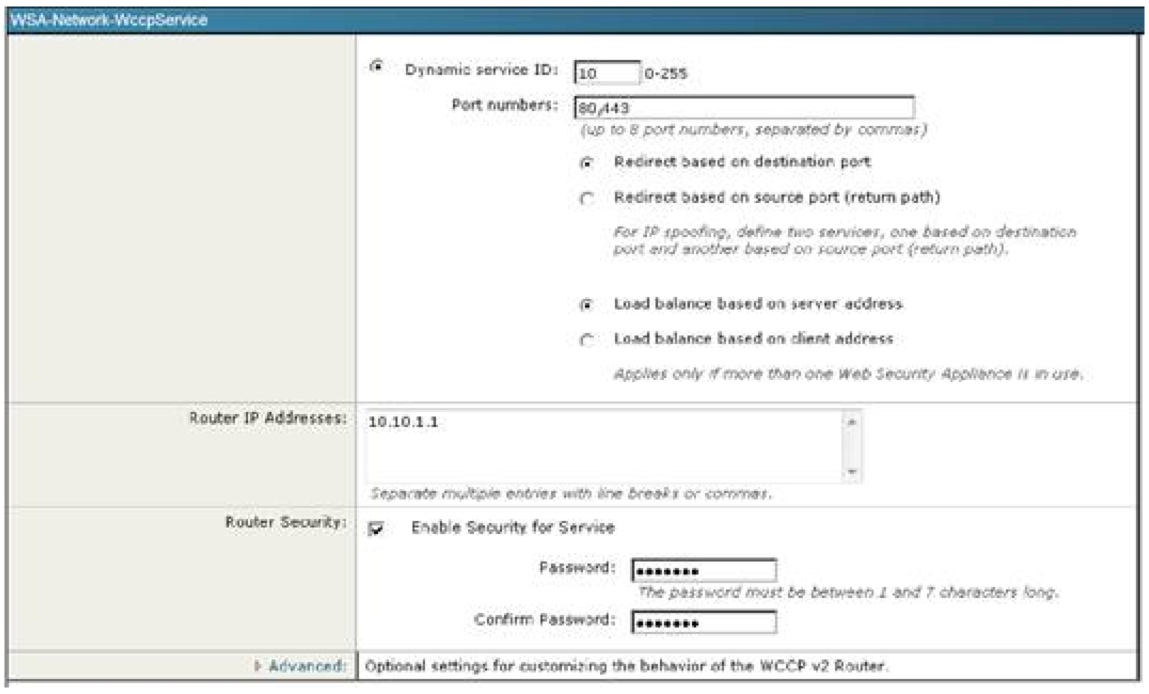
Copyright © 2003-2012 Cisco Systems, Inc. All rights reserved.

Between the Cisco ASA configuration and the Cisco WSA configuration, what is true with respect to redirected ports?

A. Both are configured for port 80 only.
B. Both are configured for port 443 only.
C. Both are configured for both port 80 and 443.
D. Both are configured for ports 80, 443 and 3128.
E. There is a configuration mismatch on redirected ports.

Answer: C

Explanation:
This can be seen from the WSA Network tab shown below:



WSA-Network-WccpService

● Dynamic service ID: 10 0-255

Port numbers: 80,443
(up to 8 port numbers, separated by commas)

● Redirect based on destination port

○ Redirect based on source port (return path)

For IP spoofing, define two services, one based on destination port and another based on source port (return path).

● Load balance based on server address

○ Load balance based on client address

Applies only if more than one Web Security Appliance is in use.

Router IP Addresses: 10.10.1.1
Separate multiple entries with line breaks or commas.

Router Security: ☑ Enable Security for Service

Password: •••••••
The password must be between 1 and 7 characters long.

Confirm Password: •••••••

▸ Advanced: Optional settings for customizing the behavior of the WCCP v2 Router.

NEW QUESTION 297
- (Exam Topic 3)
Which statement about the default configuration of an IPS sensor's management security settings is true?

A. There is no login banner
B. The web server port is TCP 80
C. Telnet and SSH are enable
D. User accounts lock after three attempts

Answer: A

NEW QUESTION 301
- (Exam Topic 3)
Which Option of SNMPv3 ensure authentication but no encryption?

A. priv
B. no auth
C. no priv
D. authNoPriv

Answer: D

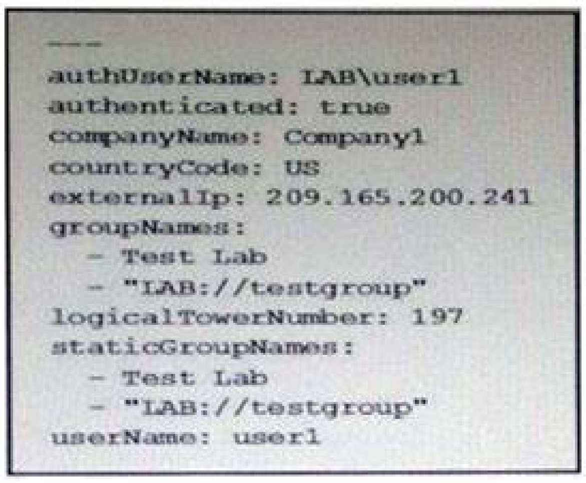
Explanation:
SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. The security model combines with the selected security level to determine the security mechanism applied when the
SNMP message is processed.
The security level determines the privileges required to view the message associated with an SNMP trap. The privilege level determines whether the message needs to be protected from disclosure or authenticated. The supported security level depends upon which security model is implemented. SNMP security levels support one or more of the following privileges:
SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.
Reference: http://www.cisco.com/en/US/

NEW QUESTION 306
- (Exam Topic 3)
Over the period of one day, several Atomic ARP engine alerts fired on the same IP address. You observe that each time an alert fired, requests on the IP address exceeded replies by the same number. Which configuration could cause this behavior?

A. The reply-ratio parameter is enabled.
B. MAC flip is enabled.
C. The inspection condition is disabled.
D. The IPS is misconfigured.

Answer: A

NEW QUESTION 311
- (Exam Topic 3)
Refer to the exhibit.



```
---
authUserName: LAB\user1
authenticated: true
companyName: Company1
countryCode: US
externalIp: 209.165.200.241
groupNames:
  - Test Lab
  - "LAB://testgroup"
logicalTowerNumber: 197
staticGroupNames:
  - Test Lab
  - "LAB://testgroup"
userName: user1
```

The security engineer has configured Cisco cloud web security redirection on a Cisco ASA firewall. Which statement describes what can be determined from exhibit?

A. In case of issues, the next step should be to perform debugging on the Cisco ASA.
B. The URL visited by the user was LAB://testgroup.
C. This out has been obtained by browsing to whoami.scansafe.net
D. The IP address of the Scansafe tower is 209.165.200.241

Answer: C

NEW QUESTION 313
- (Exam Topic 3)
When https traffic is scanned, which component of the full URL does CWS log?

A. not log
B. only hosthost and query path and query

Answer: B

NEW QUESTION 316
- (Exam Topic 3)
Which commands are required to configure SSH on router? (Choose two.)

A. Configure domain name using ip domain-name command
B. Generate a key using crypto key generate rsa
C. Configure a DHCP host for the router using dhcpname#configure terminal
D. Generate enterprise CA self-sign certificate

Answer: AB

Explanation:
Here are the steps:
Configure a hostname for the router using these commands. yourname#configure terminal
Enter configuration commands, one per line. End with CNTL/Z. yourname (config)#hostname LabRouter
LabRouter(config)#
Configure a domain name with the ip domain-name command followed by whatever you would like your domain name to be. I used CiscoLab.com.
LabRouter(config)#ip domain-name CiscoLab.com
We generate a certificate that will be used to encrypt the SSH packets using the crypto key generate rsa command.
Take note of the message that is displayed right after we enter this command: "The name for the keys will be: LabRouter.CiscoLab.com" -- it combines the hostname of the router along with the domain name we configured to get the name of the encryption key generated; this is why it was important for us to, first of all, configure a hostname then a domain name before we generated the keys.
Reference: https://www.pluralsight.com/blog/tutorials/configure-secure-shell-ssh-on-cisco-router

NEW QUESTION 319
- (Exam Topic 3)
Which website can be used to validate group information about connections that flow through Cisco CWS?

A. whoami.scansafe.net
B. policytrace.scansafe.net
C. whoami.scansafe.com
D. policytrace.scansafe.com

Answer: B

NEW QUESTION 321
- (Exam Topic 3)
Which command can change the HTTPS SSL method on the Cisco ESA?

A. sslconfig
B. strictssl
C. sshconfig
D. adminaccessconfig

Answer: A

NEW QUESTION 325
- (Exam Topic 3)
A network security design engineer is considering using a Cisco Intrusion Detection System in the DMZ of the network. Which option is the drawback to using IDS in the DMZ as opposed to using
Intrusion Prevention System?

A. Sensors, when placed in-line, can impact network functionality during sensor failure.
B. IDS has impact on the network (that is, latency and jitter).
C. Response actions cannot stop triggered packet or guarantee to stop a connection techniques.
D. Response actions cannot stop malicious packets or cannot guarantee to stop any DOS attack.

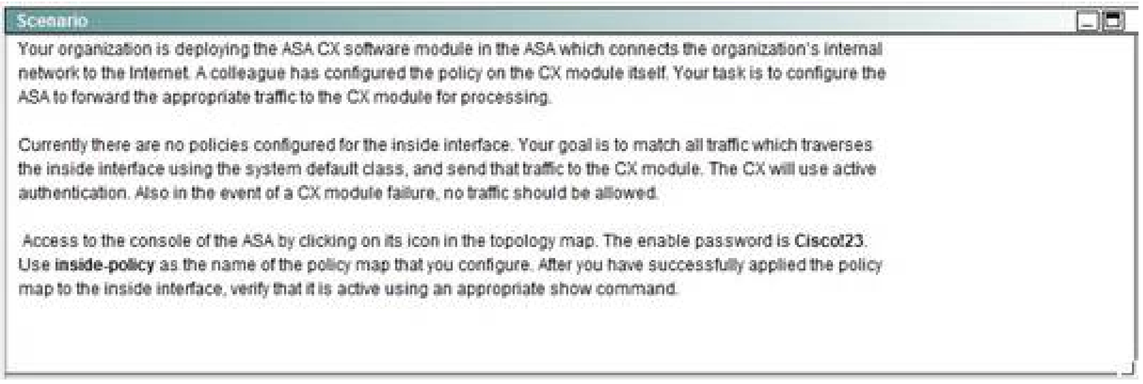
Answer: B

NEW QUESTION 330
- (Exam Topic 3)
Which Cisco ESA predefined sender group uses parameter-matching to reject senders?

A. BLACKLIST
B. WHITELIST
C. SUSPECTLIST
D. UNKNOWNLIST

Answer: A

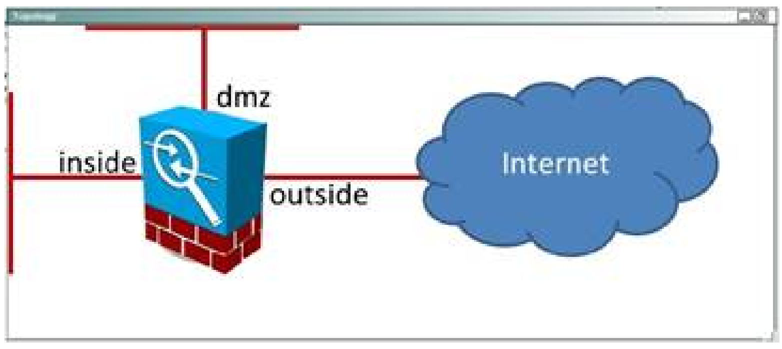
NEW QUESTION 334
- (Exam Topic 3)

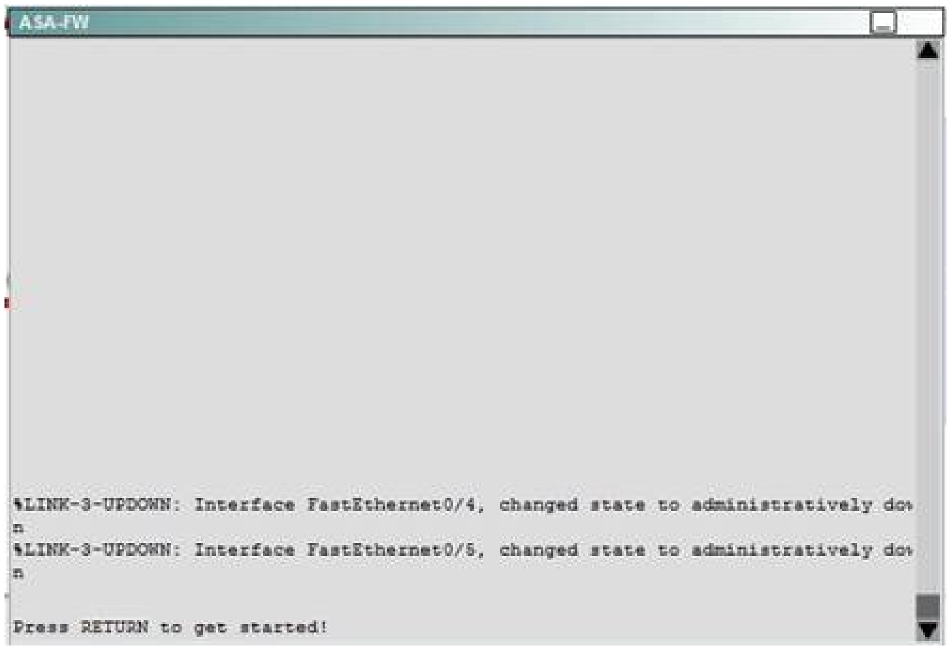


Your organization is deploying the ASA CX software module in the ASA which connects the organization's internal network to the Internet. A colleague has configured the policy on the CX module itself. Your task is to configure the ASA to forward the appropriate traffic to the CX module for processing.

Currently there are no policies configured for the inside interface. Your goal is to match all traffic which traverses the inside interface using the system default class, and send that traffic to the CX module. The CX will use active authentication. Also in the event of a CX module failure, no traffic should be allowed.

Access to the console of the ASA by clicking on its icon in the topology map. The enable password is **Cisco!23**. Use **inside-policy** as the name of the policy map that you configure. After you have successfully applied the policy map to the inside interface, verify that it is active using an appropriate show command.





```
%LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to administratively dow
n
%LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to administratively dow
n

Press RETURN to get started!
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
We need to create a policy map named inside-policy and send the traffic to the CXSC blade:
ASA-FW# config t
ASA-FW(config)# policy-map inside-policy
ASA-FW(config-pmap)# policy-map inside-policy ASA-FW(config-pmap)# class class-default
ASA-FW(config-pmap-c)# cxsc fail-close auth-proxy ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit

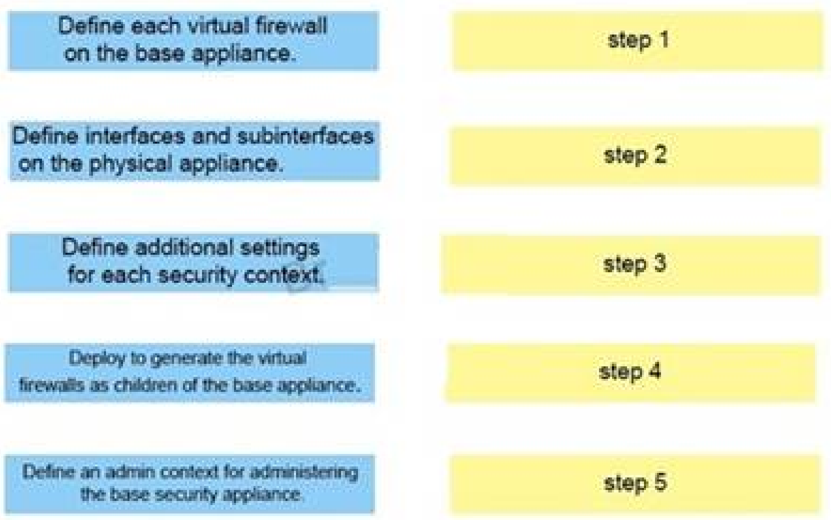
The fail-close is needed as per instructions that if the CX module fails, no traffic should be allowed. The auth-proxy keyword is needed for active authentication. Next, we need to apply this policy map to the inside interface: ASA-FW(config)#service-policy inside-policy interface inside. Finally, verify that the policy is active:
ASA-FW# show service-policy interface inside Interface inside:
Service-policy: inside-policy Class-map: class-default
Default QueueingCXSC: card status Up, mode fail-close, auth-proxy enabled Packet input 181, packet output 183, drop 0, reset-drop 0, proxied 0 Configuration guidelines can be found at this reference link:
Reference:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/modules_cx.pdf

NEW QUESTION 337
- (Exam Topic 3)
Which IPS signature engine inspects the IP protocol packets and the Layer TCP?

A. String TCP
B. Atomic TCP
C. Service HTTP
D. Atomic IP

Answer: D

NEW QUESTION 340
- (Exam Topic 3)
Drag and drop the steps on the left into the correct order on the right to configure a Cisco ASA NGFW with multiple security contexts.



Define each virtual firewall on the base appliance.
Define interfaces and subinterfaces on the physical appliance.
Define additional settings for each security context.
Deploy to generate the virtual firewalls as children of the base appliance.
Define an admin context for administering the base security appliance.

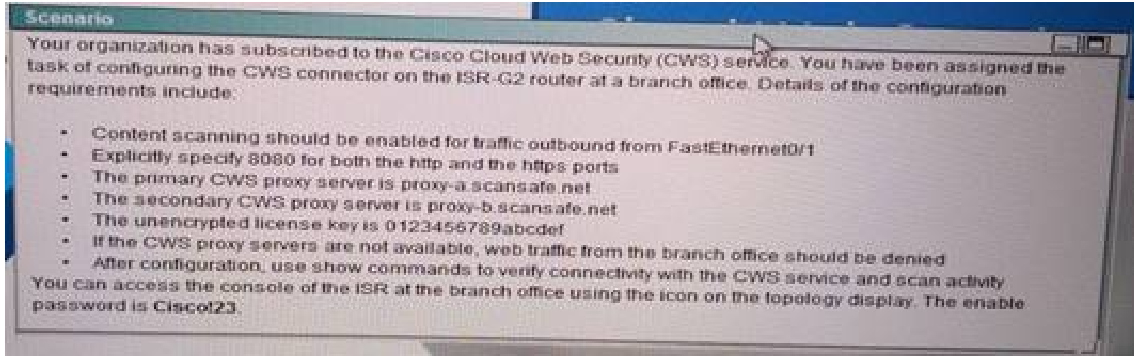
step 1
step 2
step 3
step 4
step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-4/user/guide/CSMUserGuide_wrapper/pxcontexts.pdf (page 2 to 4)

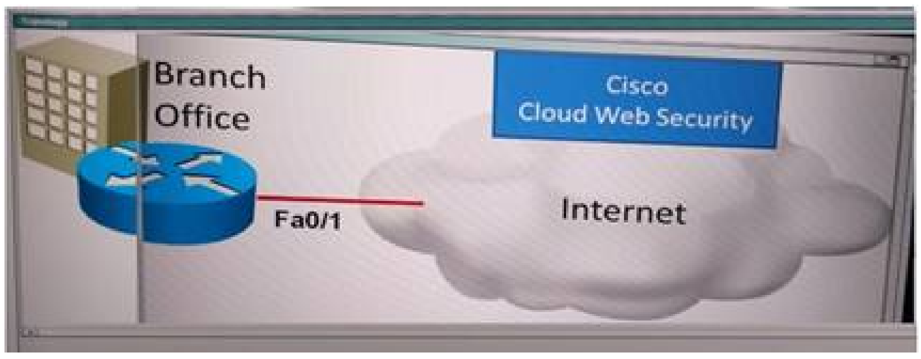
NEW QUESTION 342
- (Exam Topic 3)



Your organization has subscribed to the Cisco Cloud Web Security (CWS) service. You have been assigned the task of configuring the CWS connector on the ISR-G2 router at a branch office. Details of the configuration requirements include:

- Content scanning should be enabled for traffic outbound from FastEthernet0/1
- Explicitly specify 8080 for both the http and the https ports
- The primary CWS proxy server is proxy-a.scansafe.net
- The secondary CWS proxy server is proxy-b.scansafe.net
- The unencrypted license key is 0123456789abcdef
- If the CWS proxy servers are not available, web traffic from the branch office should be denied
- After configuration, use show commands to verify connectivity with the CWS service and scan activity

You can access the console of the ISR at the branch office using the icon on the topology display. The enable password is Cisco!23.



```
Press RETURN to get started!
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
We need to define the parameter map, specifying port 8080 for http and https and define the servers and the license:
Branch-ISR#config t
Branch-ISR(config)#parameter-map type content-scan global
Branch-ISR(config-profile)#server scansafe primary name proxy-a.scansafe.net port http 8080 https 8080 Branch-ISR(config-profile)#server scansafe secondary name proxy-b.scansafe.net port http 8080 https 8080 Branch-ISR(config-profile)#license 0 0123456789abcdef
If the CWS proxy servers are not available, we traffic should be denied. This is done by the following configuration:
Branch-ISR(config-profile)#server scansafe on-failure block-all Now we need to apply this to the fastethernet 0/1 interface outbound: Branch-ISR(config)#interface Fastethernet 0/1
Branch-ISR(config-if)#content-scan outbound
Branch-ISR(config-if)#exit Branch-ISR(config)#exit
Finally, we can verify out configuration by using the “show content-scan summary command: Branch-ISR#show content-scan summary
Primary: 72.37.244.203(Up)* Secondary: 70.39.231.99 (Up) Interfaces: Fastethernet0/1

NEW QUESTION 343
- (Exam Topic 3)
Which Cisco technology provides spam filtering and email protection?

A. IPS
B. ESA
C. WSA
D. CX

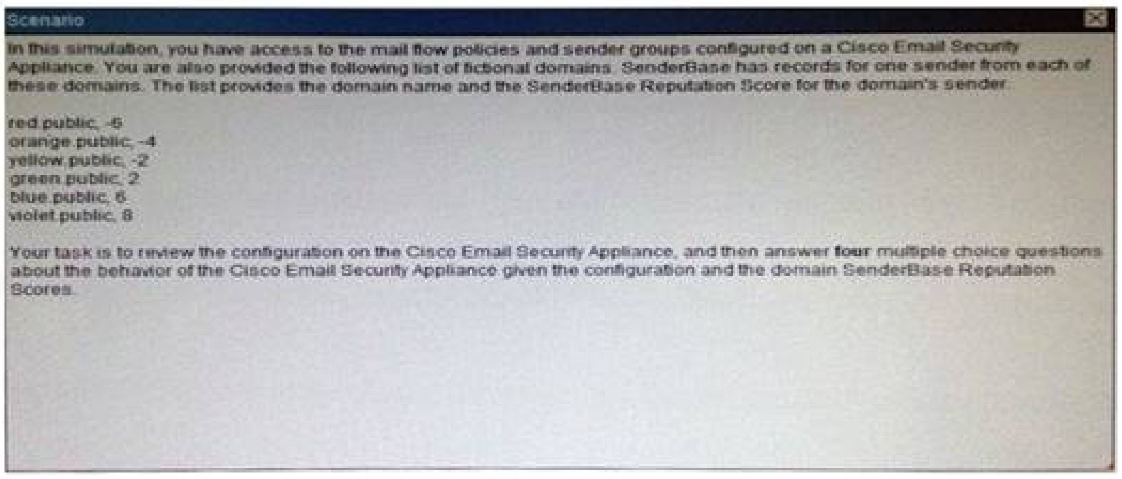
Answer: B

NEW QUESTION 348
- (Exam Topic 3)
Which step is required when you configure URL filtering to Cisco Cloud Web Security?

A. configure URL filtering policies in Cisco ScanCenter
B. install the ASA FirePOWER module on the Cisco ASA.
C. Implement Next Generation IPS instrusion rules.
D. Configure URL filtering criteria in the Cisco ASA FirePOWER access rules.

Answer: A

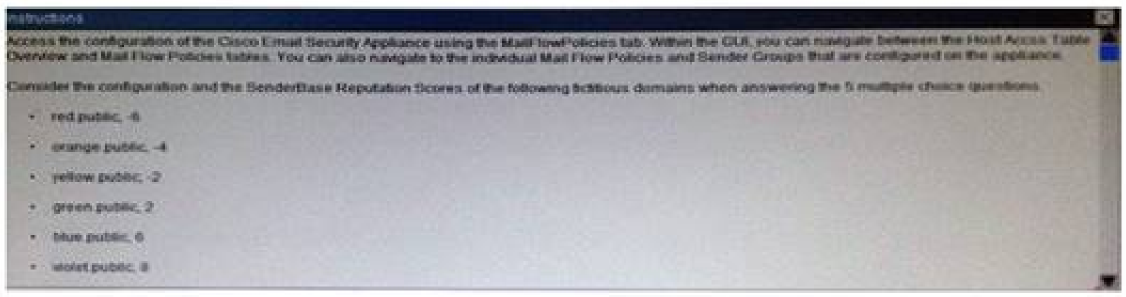
NEW QUESTION 352
- (Exam Topic 3)



In this simulation, you have access to the mail flow policies and sender groups configured on a Cisco Email Security Appliance. You are also provided the following list of fictional domains. SenderBase has records for one sender from each of these domains. The list provides the domain name and the SenderBase Reputation Score for the domain's sender.

red.public, -6
orange.public, -4
yellow.public, -2
green.public, 2
blue.public, 6
violet.public, 8

Your task is to review the configuration on the Cisco Email Security Appliance, and then answer **four** multiple choice questions about the behavior of the Cisco Email Security Appliance given the configuration and the domain SenderBase Reputation Scores.

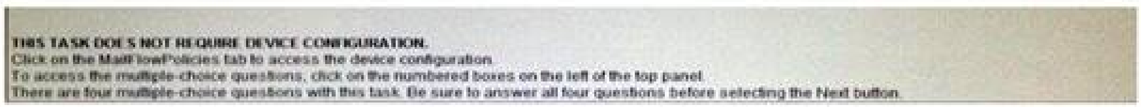


Instructions

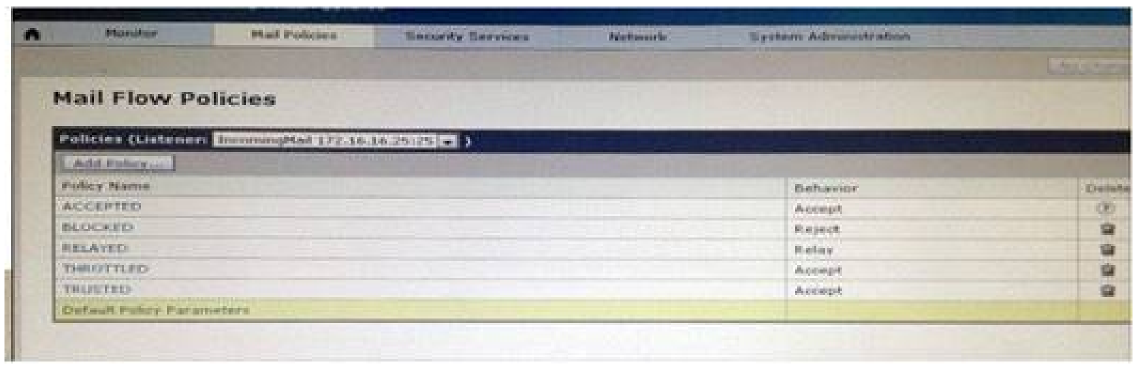
Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the Host Access Table Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance.

Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the 5 multiple choice questions.

- red.public, -6
- orange.public, -4
- yellow.public, -2
- green.public, 2
- blue.public, 6
- violet.public, 8



THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
Click on the MailFlowPolicies tab to access the device configuration.
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.



Mail Flow Policies

Policies (Listener: IncomingMail 172.16.16.25:25)

Add Policy...

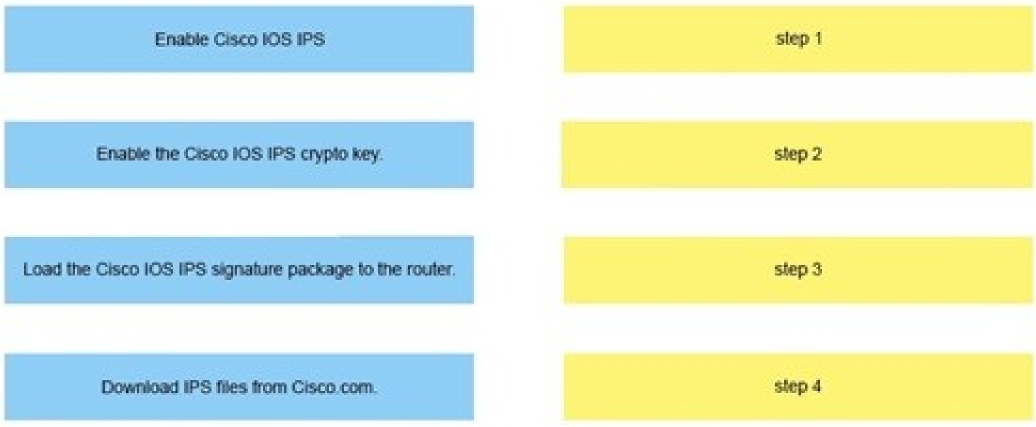
Policy Name	Behavior	Delete
ACCEPTED	Accept	
BLOCKED	Reject	
RELAYED	Relay	
THROTTLED	Accept	
TRUSTED	Accept	
Default Policy Parameters		

The Cisco Email Security Appliance will reject messages from which domains?

A. re
B. public
C. re
D. public and orang
E. public
F. re
G. public, orang
H. Public and yello
I. public
J. orang
K. public
L. viole
M. public
N. viole
O. public and blue.public
P. None of the listed domains

Answer: C

NEW QUESTION 357
- (Exam Topic 3)
Drag and drop the steps on the left into the correct order of initial Cisco IOS IPS configuration on the right.

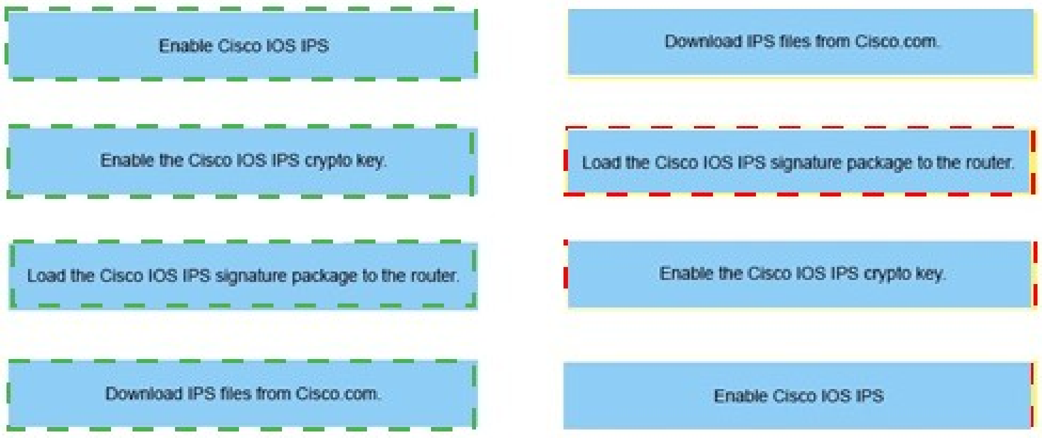


Enable Cisco IOS IPS
step 1
Enable the Cisco IOS IPS crypto key.
step 2
Load the Cisco IOS IPS signature package to the router.
step 3
Download IPS files from Cisco.com.
step 4

A. Mastered
B. Not Mastered

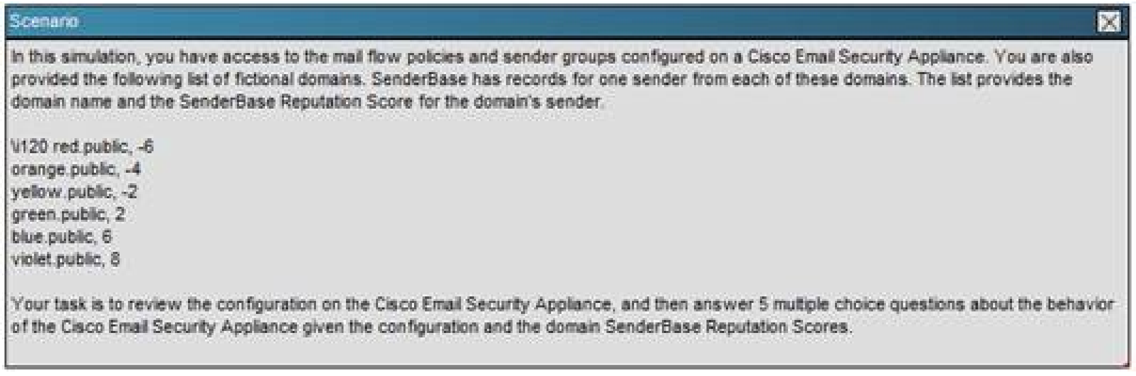
Answer: A

Explanation:



Enable Cisco IOS IPS
Download IPS files from Cisco.com.
Enable the Cisco IOS IPS crypto key.
Load the Cisco IOS IPS signature package to the router.
Load the Cisco IOS IPS signature package to the router.
Enable the Cisco IOS IPS crypto key.
Download IPS files from Cisco.com.
Enable Cisco IOS IPS

NEW QUESTION 359
- (Exam Topic 3)

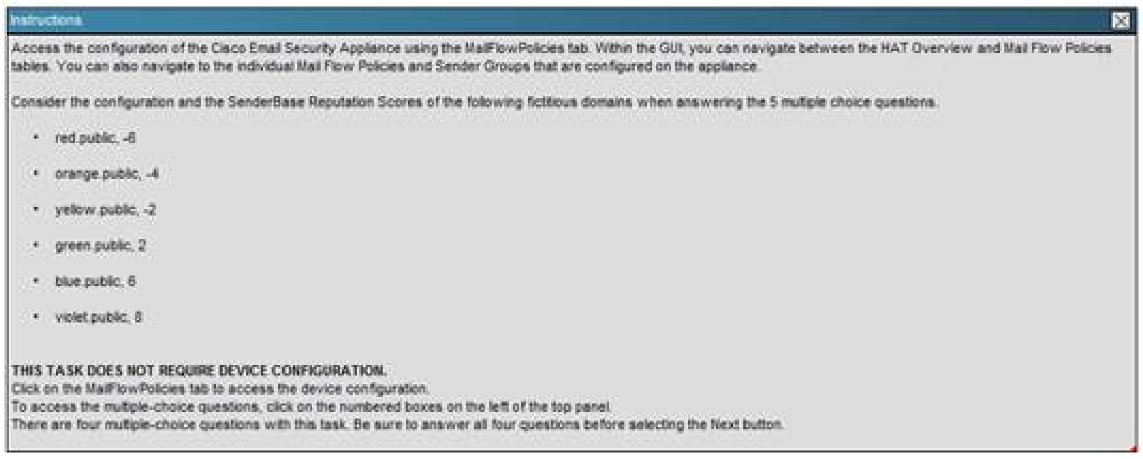


Scenario

In this simulation, you have access to the mail flow policies and sender groups configured on a Cisco Email Security Appliance. You are also provided the following list of fictional domains. SenderBase has records for one sender from each of these domains. The list provides the domain name and the SenderBase Reputation Score for the domain's sender.

\120 red.public, -6
orange.public, -4
yellow.public, -2
green.public, 2
blue.public, 6
violet.public, 8

Your task is to review the configuration on the Cisco Email Security Appliance, and then answer 5 multiple choice questions about the behavior of the Cisco Email Security Appliance given the configuration and the domain SenderBase Reputation Scores.



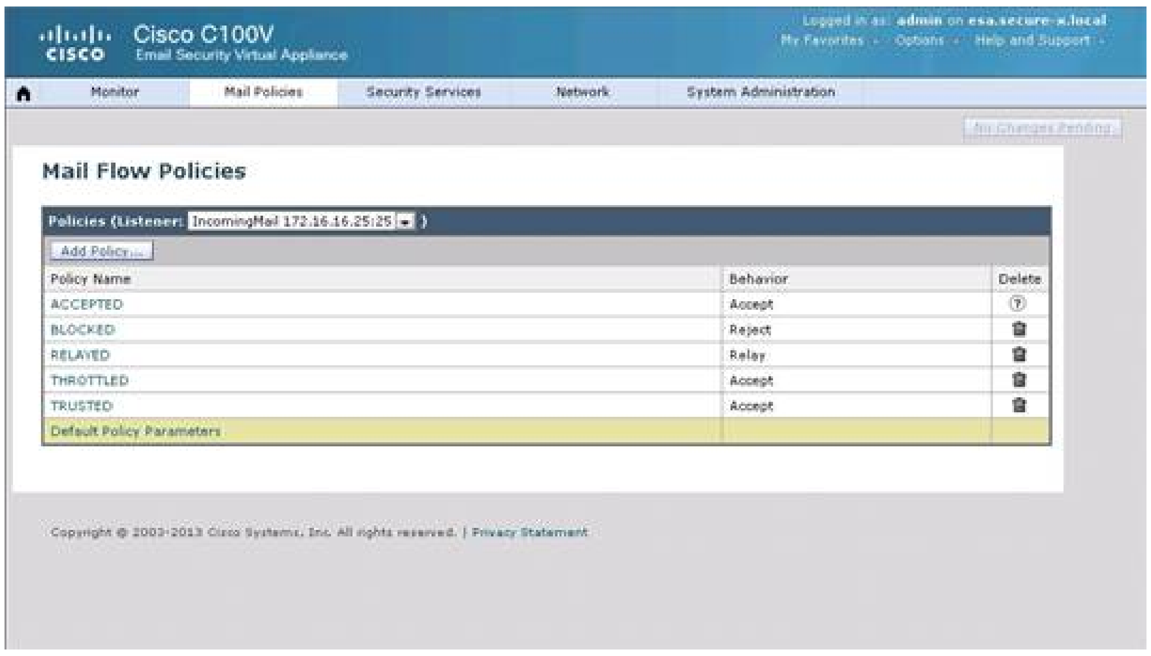
Instructions

Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the HAT Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance.

Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the 5 multiple choice questions.

- red.public, -6
- orange.public, -4
- yellow.public, -2
- green.public, 2
- blue.public, 6
- violet.public, 8

THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
Click on the MailFlowPolicies tab to access the device configuration.
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.



Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

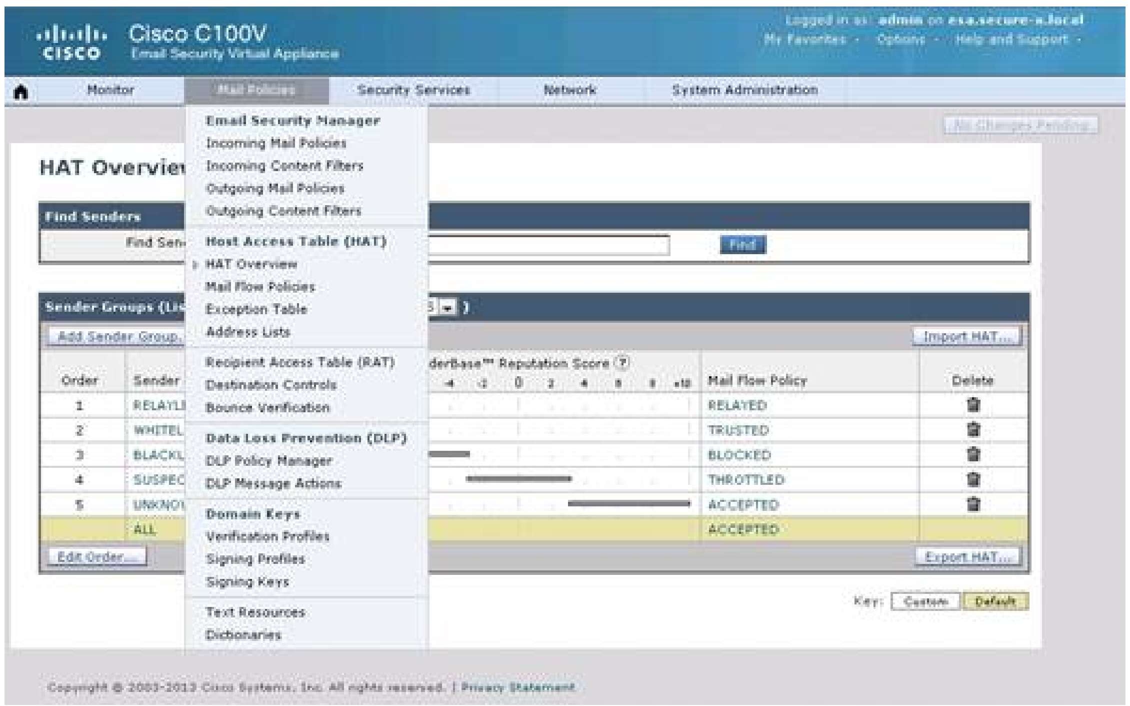
Mail Flow Policies

Policies (Listener: IncomingMail 172.16.16.25:25)

Add Policy...

Policy Name	Behavior	Delete
ACCEPTED	Accept	?
BLOCKED	Reject	🗑
RELAYED	Relay	🗑
THROTTLED	Accept	🗑
TRUSTED	Accept	🗑
Default Policy Parameters		

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



HAT Overvie

Find Senders

Find Sen Find

Sender Groups (Lis 5)

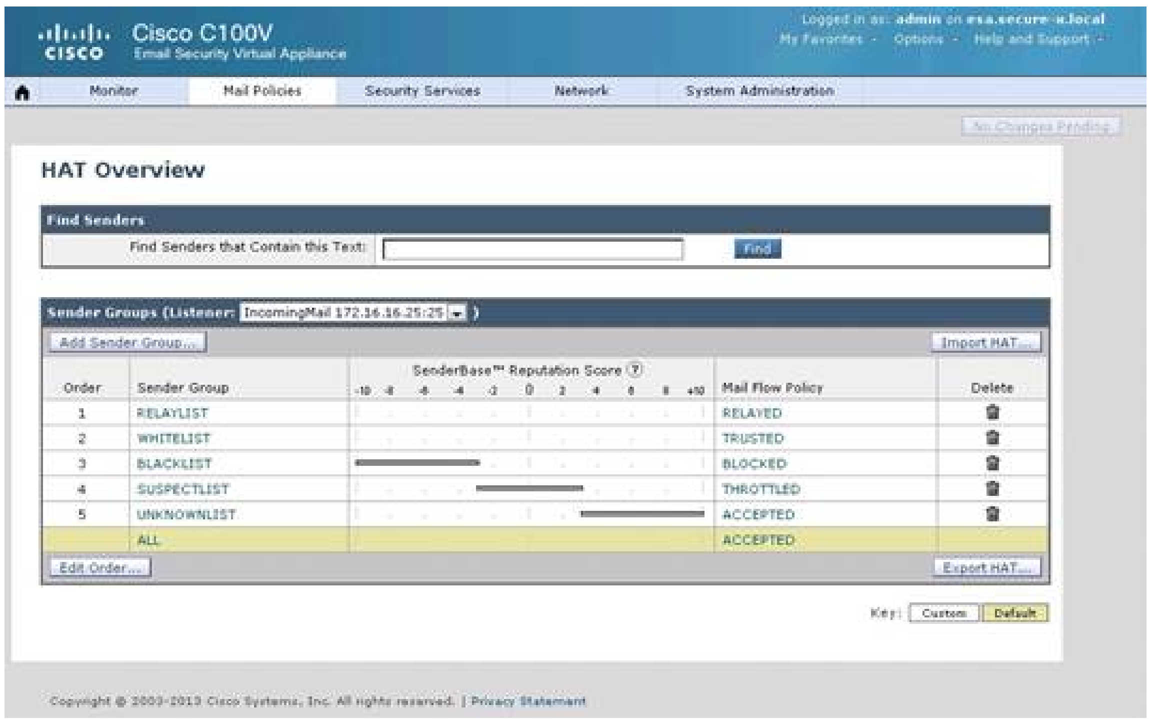
Add Sender Group... Import HAT...

Order	Sender	derBase™ Reputation Score -4 -2 0 2 4 6 8 +10	Mail Flow Policy	Delete
1	RELAYLI		RELAYED	🗑
2	WHITEL		TRUSTED	🗑
3	BLACKL		BLOCKED	🗑
4	SUSPEC		THROTTLED	🗑
5	UNKNOV		ACCEPTED	🗑
	ALL		ACCEPTED	

Edit Order... Export HAT...

Key: Custom Default

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Find
Add Sender Group...
Import HAT...
Edit Order...
Export HAT...
Key: Custom Default
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

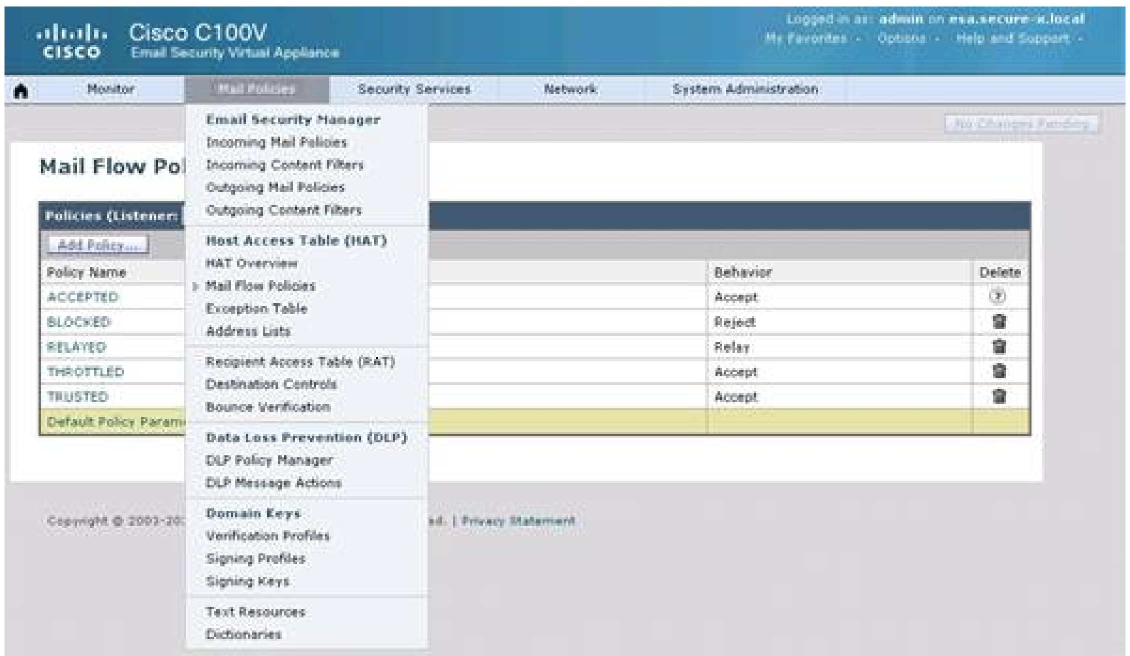
HAT Overview

Find Senders

Find Senders that Contain this Text:

Sender Groups (Listener: IncomingMail 172.16.16.25:25)

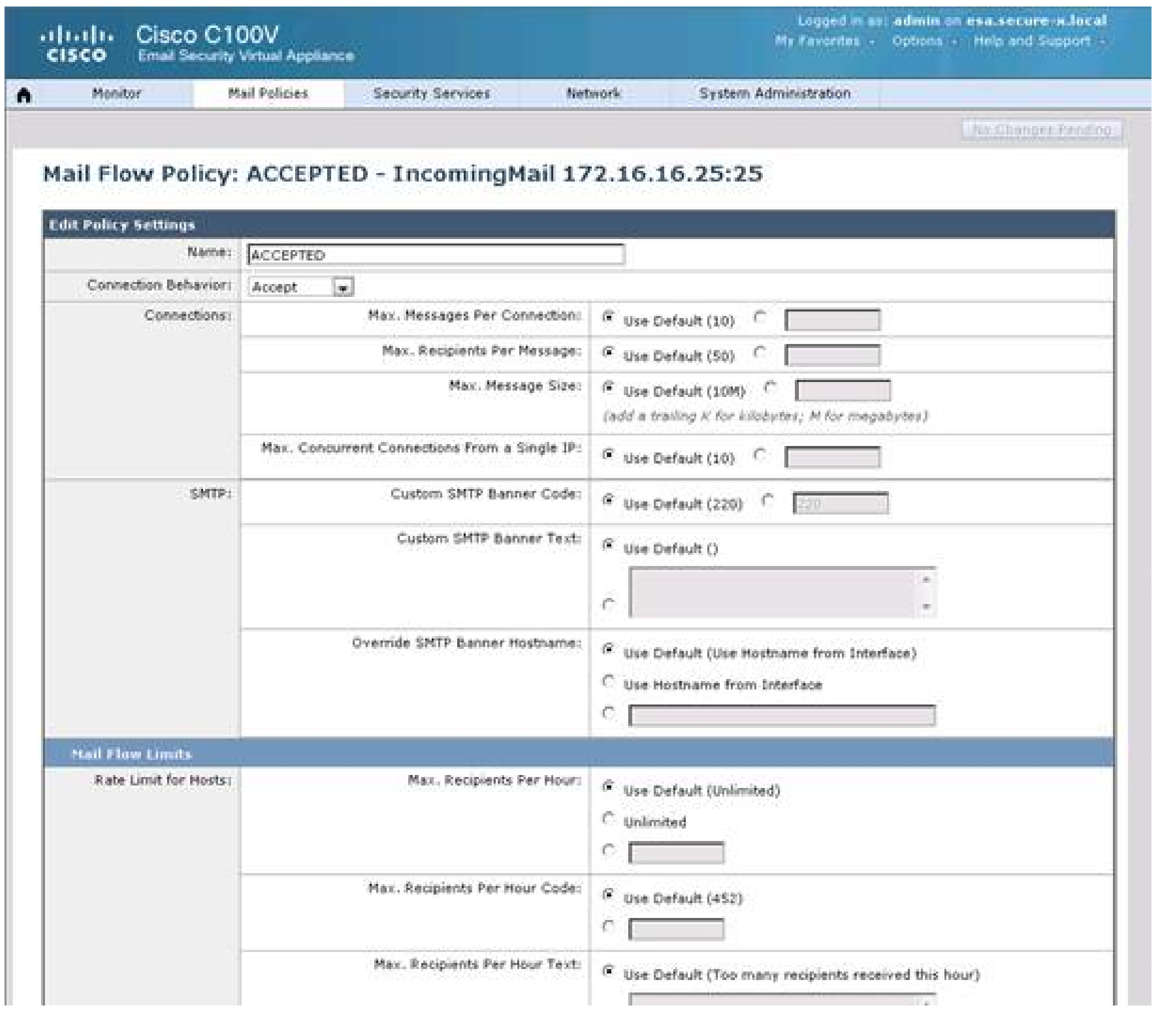
Order	Sender Group	SenderBase™ Reputation Score -10 -8 -6 -4 -2 0 2 4 6 8 +10	Mail Flow Policy	Delete
1	RELAYLIST		RELAYED	🗑
2	WHITELIST		TRUSTED	🗑
3	BLACKLIST	-10 to -3	BLOCKED	🗑
4	SUSPECTLIST	-3 to 1	THROTTLED	🗑
5	UNKNOWNLIST	1 to +10	ACCEPTED	🗑
	ALL		ACCEPTED	



Mail Flow Pol

Policies (Listener:

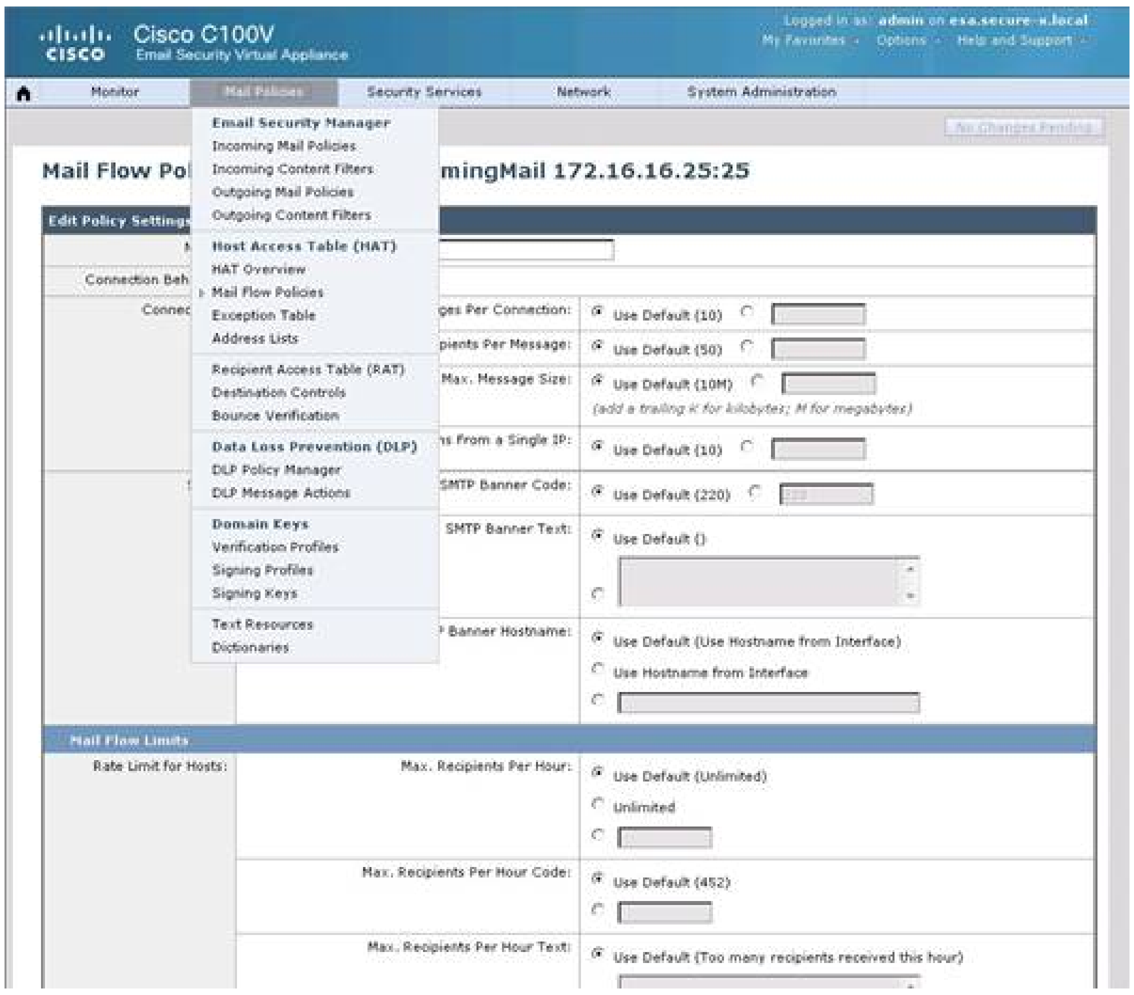
Policy Name	Behavior	Delete
ACCEPTED	Accept	?
BLOCKED	Reject	🗑
RELAYED	Relay	🗑
THROTTLED	Accept	🗑
TRUSTED	Accept	🗑
Default Policy Param		


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Mail Flow Policy: ACCEPTED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name:	ACCEPTED	
Connection Behavior:	Accept	
Connections:	Max. Messages Per Connection:	● Use Default (10) ○
	Max. Recipients Per Message:	● Use Default (50) ○
	Max. Message Size:	● Use Default (10M) ○ (add a trailing K for kilobytes; M for megabytes)
	Max. Concurrent Connections From a Single IP:	● Use Default (10) ○
SMTP:	Custom SMTP Banner Code:	● Use Default (220) ○ 220
	Custom SMTP Banner Text:	● Use Default () ○
	Override SMTP Banner Hostname:	● Use Default (Use Hostname from Interface) ○ Use Hostname from Interface ○
Mail Flow Limits		
Rate Limit for Hosts:	Max. Recipients Per Hour:	● Use Default (Unlimited) ○ Unlimited ○
	Max. Recipients Per Hour Code:	● Use Default (452) ○
	Max. Recipients Per Hour Text:	● Use Default (Too many recipients received this hour)



Mail Flow Pol mingMail 172.16.16.25:25

Edit Policy Settings

Connection Beh

Connec

ges Per Connection: ● Use Default (10) ○

pients Per Message: ● Use Default (50) ○

Max. Message Size: ● Use Default (10M) ○
(add a trailing k for kilobytes; M for megabytes)

ns From a Single IP: ● Use Default (10) ○

SMTP Banner Code: ● Use Default (220) ○

SMTP Banner Text: ● Use Default ()
○

P Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○

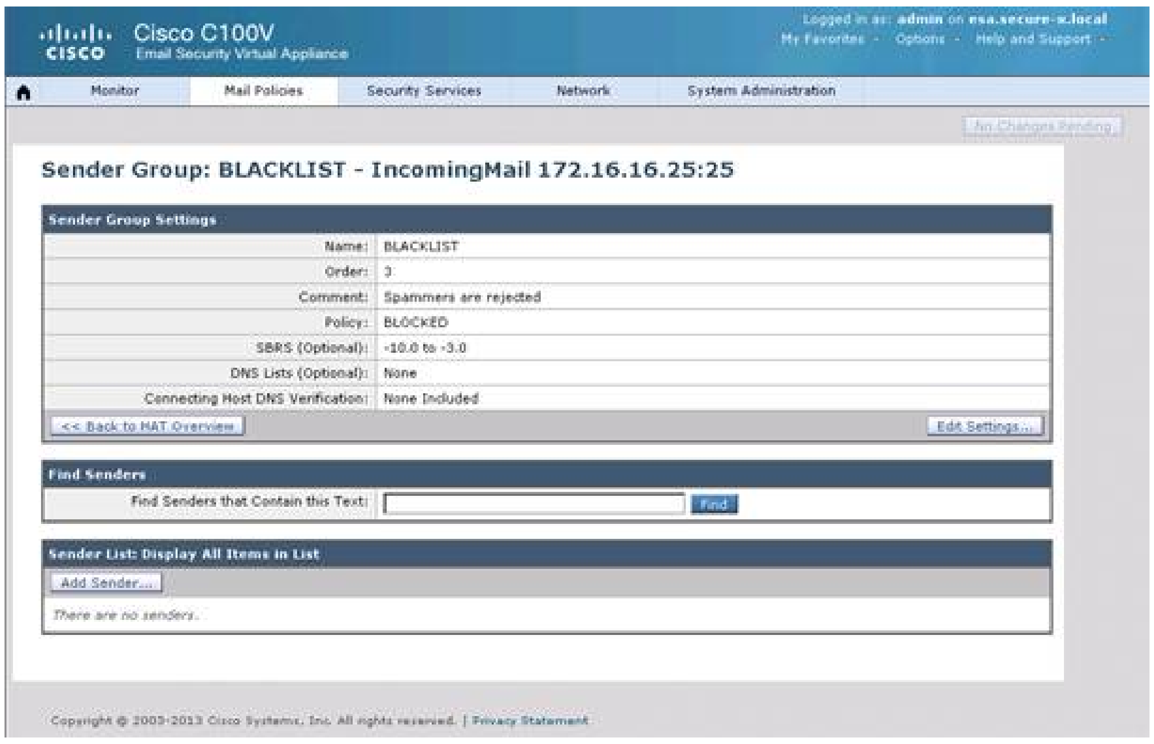
Mail Flow Limits

Rate Limit for Hosts:

Max. Recipients Per Hour: ● Use Default (Unlimited)
○ Unlimited
○

Max. Recipients Per Hour Code: ● Use Default (452)
○

Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Sender Group: BLACKLIST - IncomingMail 172.16.16.25:25

Sender Group Settings	
Name:	BLACKLIST
Order:	3
Comment:	Spammers are rejected
Policy:	BLOCKED
SBRS (Optional):	-10.0 to -3.0
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

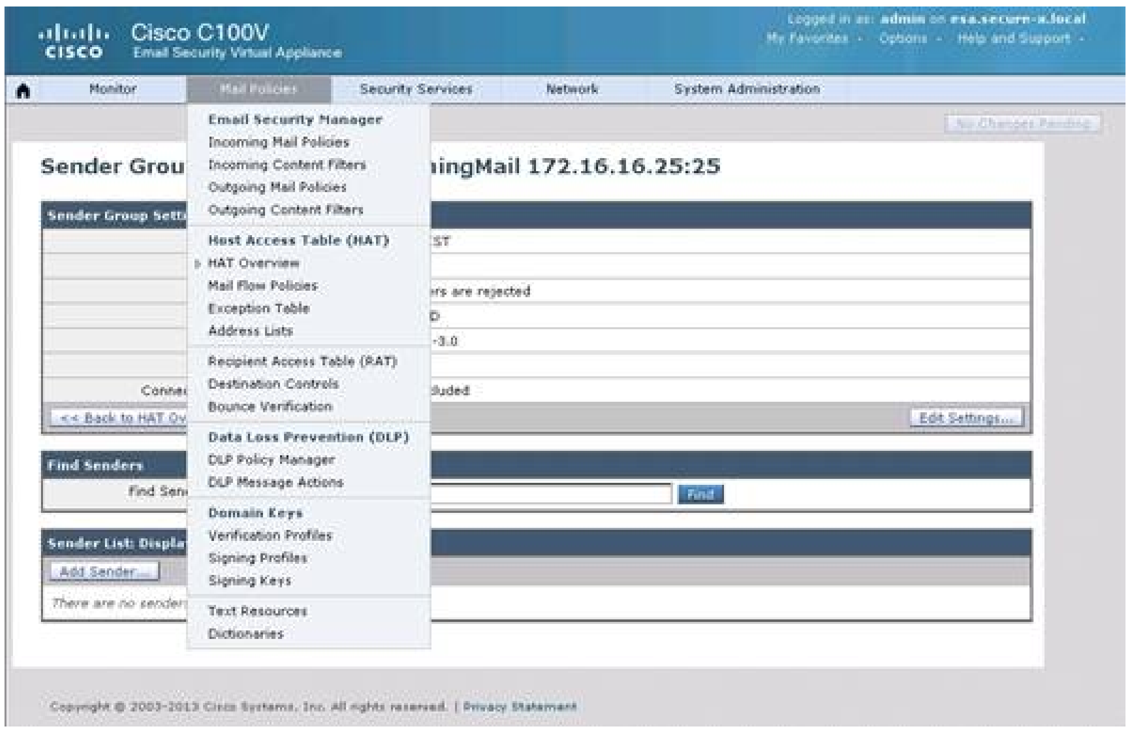
Find Senders

Find Senders that Contain this Text: Find

Sender List: Display All Items in List

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



Sender Grou ingMail 172.16.16.25:25

Sender Group Setti

ST

rs are rejected

D

-3.0

Connec luded

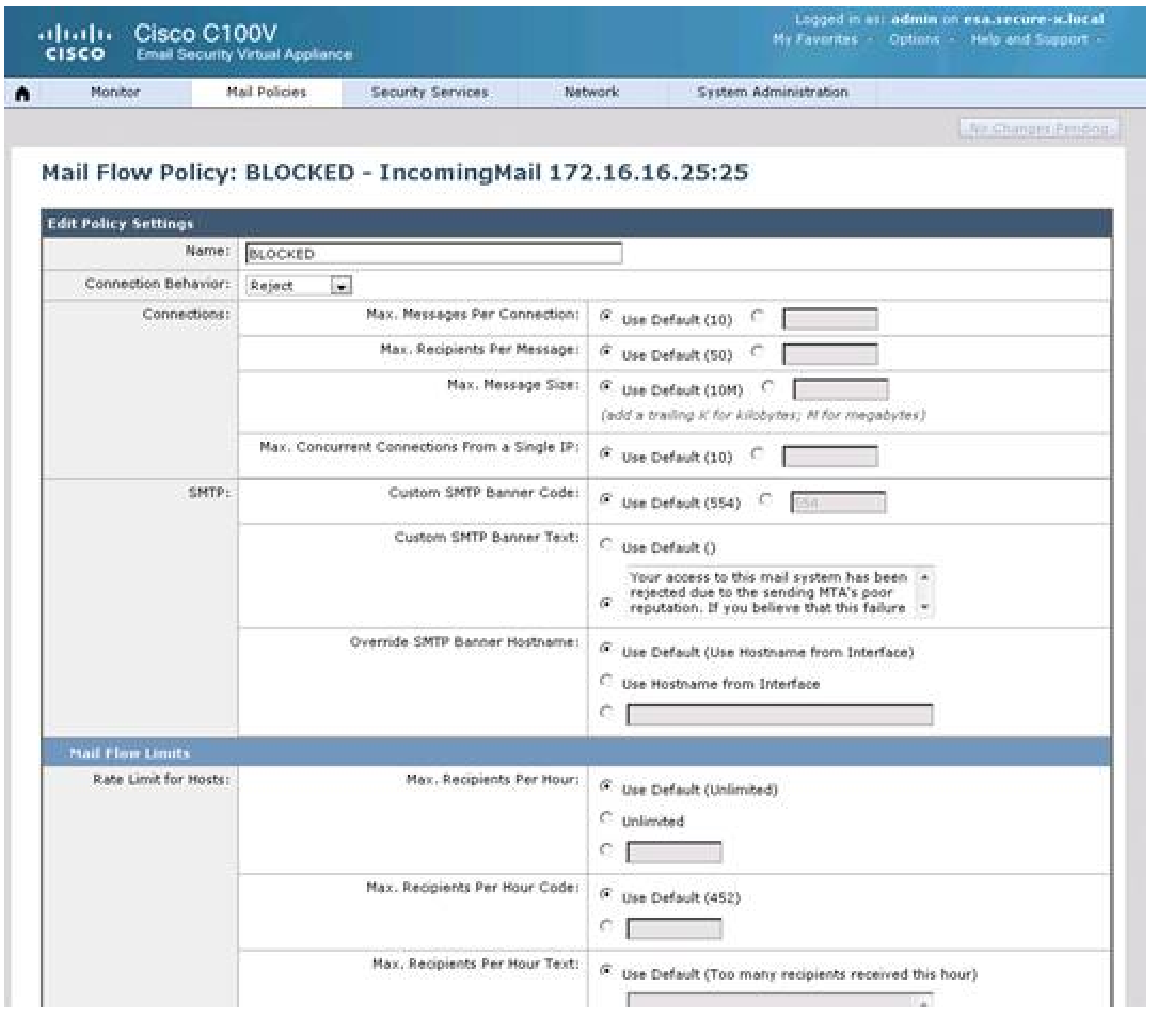
Find Senders

Find Sen

Sender List: Displa

There are no sender

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·

Monitor | Mail Policies | Security Services | Network | System Administration

No Changes Pending

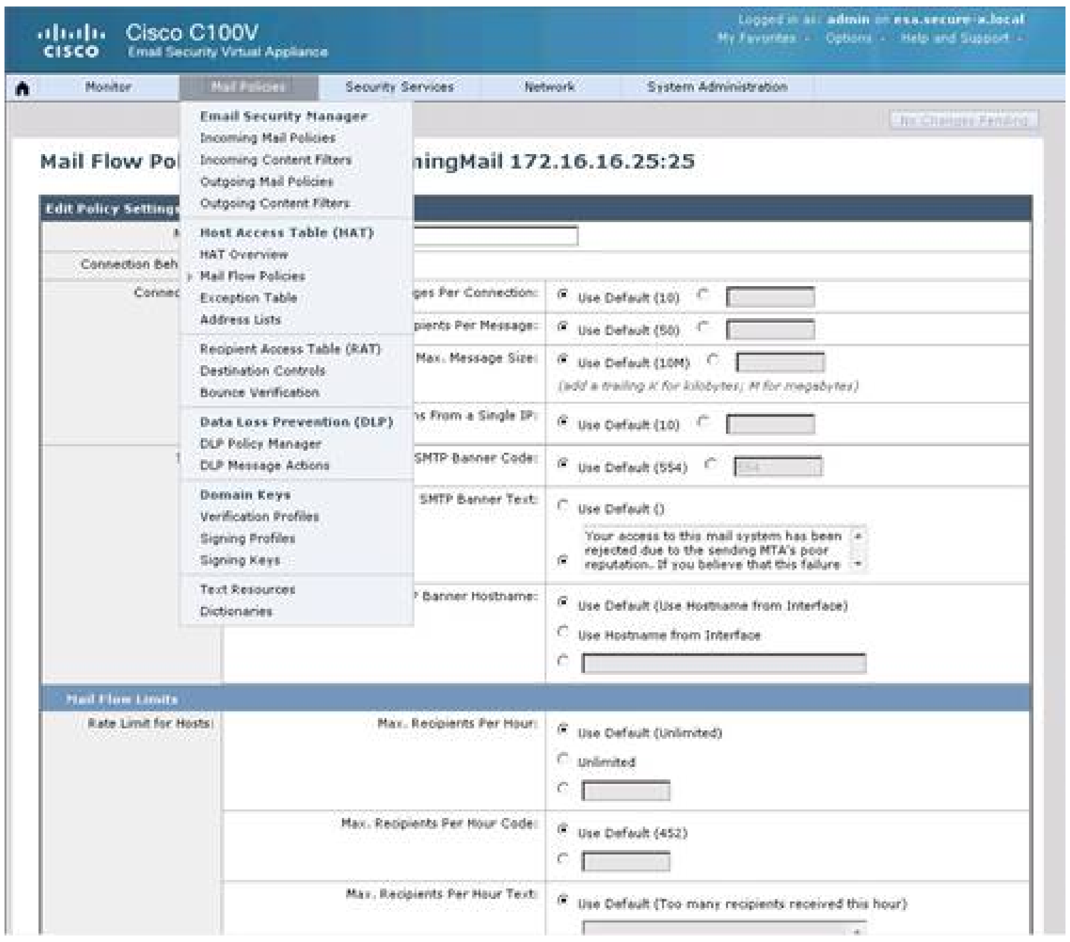
Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name:	BLOCKED	
Connection Behavior:	Reject	
Connections:	Max. Messages Per Connection:	● Use Default (10) ○
	Max. Recipients Per Message:	● Use Default (50) ○
	Max. Message Size:	● Use Default (10M) ○ (add a trailing K for kilobytes; M for megabytes)
	Max. Concurrent Connections From a Single IP:	● Use Default (10) ○
SMTP:	Custom SMTP Banner Code:	● Use Default (554) ○ 554
	Custom SMTP Banner Text:	○ Use Default () ● Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure
	Override SMTP Banner Hostname:	● Use Default (Use Hostname from Interface) ○ Use Hostname from Interface ○

Mail Flow Limits

Rate Limit for Hosts:	Max. Recipients Per Hour:	● Use Default (Unlimited) ○ Unlimited ○
	Max. Recipients Per Hour Code:	● Use Default (452) ○
	Max. Recipients Per Hour Text:	● Use Default (Too many recipients received this hour)



Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·

Monitor | Mail Policies | Security Services | Network | System Administration

No Changes Pending

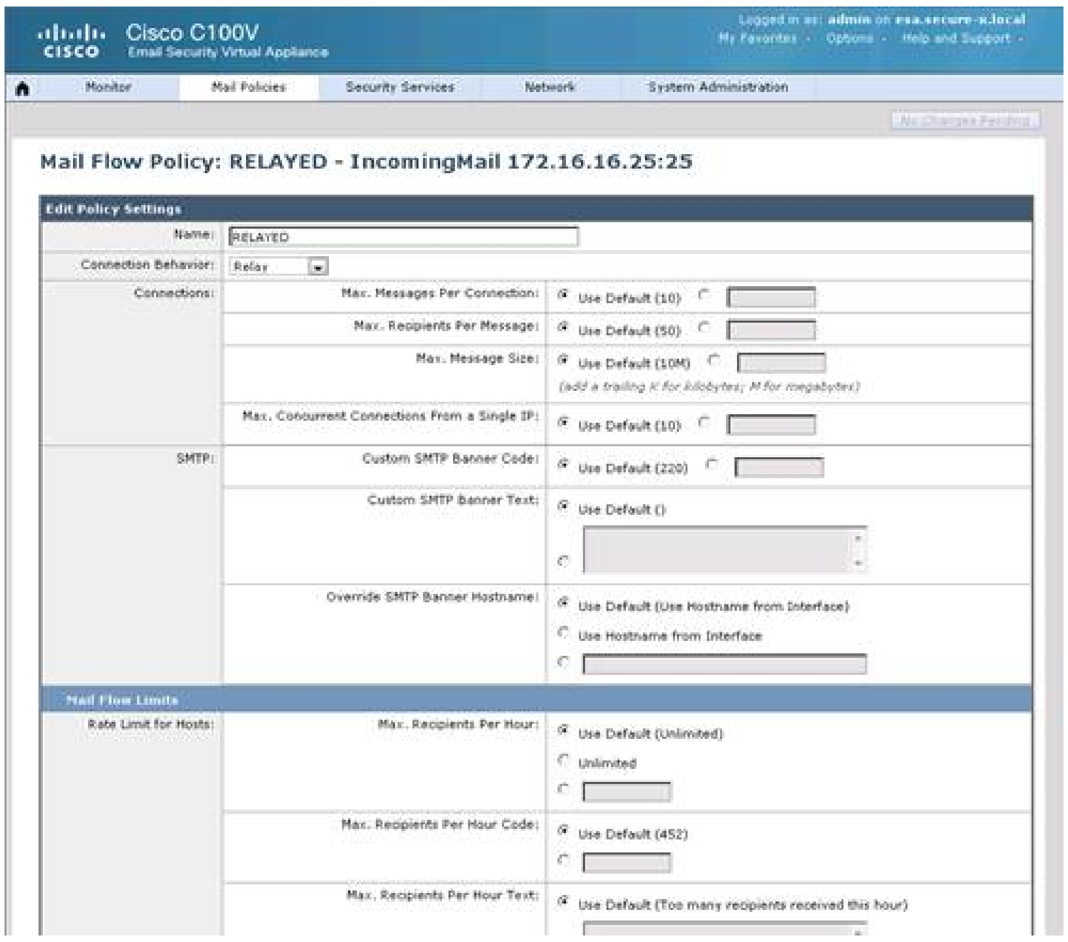
Mail Flow Po… …ningMail 172.16.16.25:25

Edit Policy Setting…

Connection Beh…		
Connec…	…ges Per Connection:	● Use Default (10) ○
	…pients Per Message:	● Use Default (50) ○
	Max. Message Size:	● Use Default (10M) ○ (add a trailing K for kilobytes; M for megabytes)
	…s From a Single IP:	● Use Default (10) ○
	SMTP Banner Code:	● Use Default (554) ○ 554
	SMTP Banner Text:	○ Use Default () ● Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure
	…P Banner Hostname:	● Use Default (Use Hostname from Interface) ○ Use Hostname from Interface ○

Mail Flow Limits

Rate Limit for Hosts:	Max. Recipients Per Hour:	● Use Default (Unlimited) ○ Unlimited ○
	Max. Recipients Per Hour Code:	● Use Default (452) ○
	Max. Recipients Per Hour Text:	● Use Default (Too many recipients received this hour)



Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·

Monitor | Mail Policies | Security Services | Network | System Administration

No Changes Pending

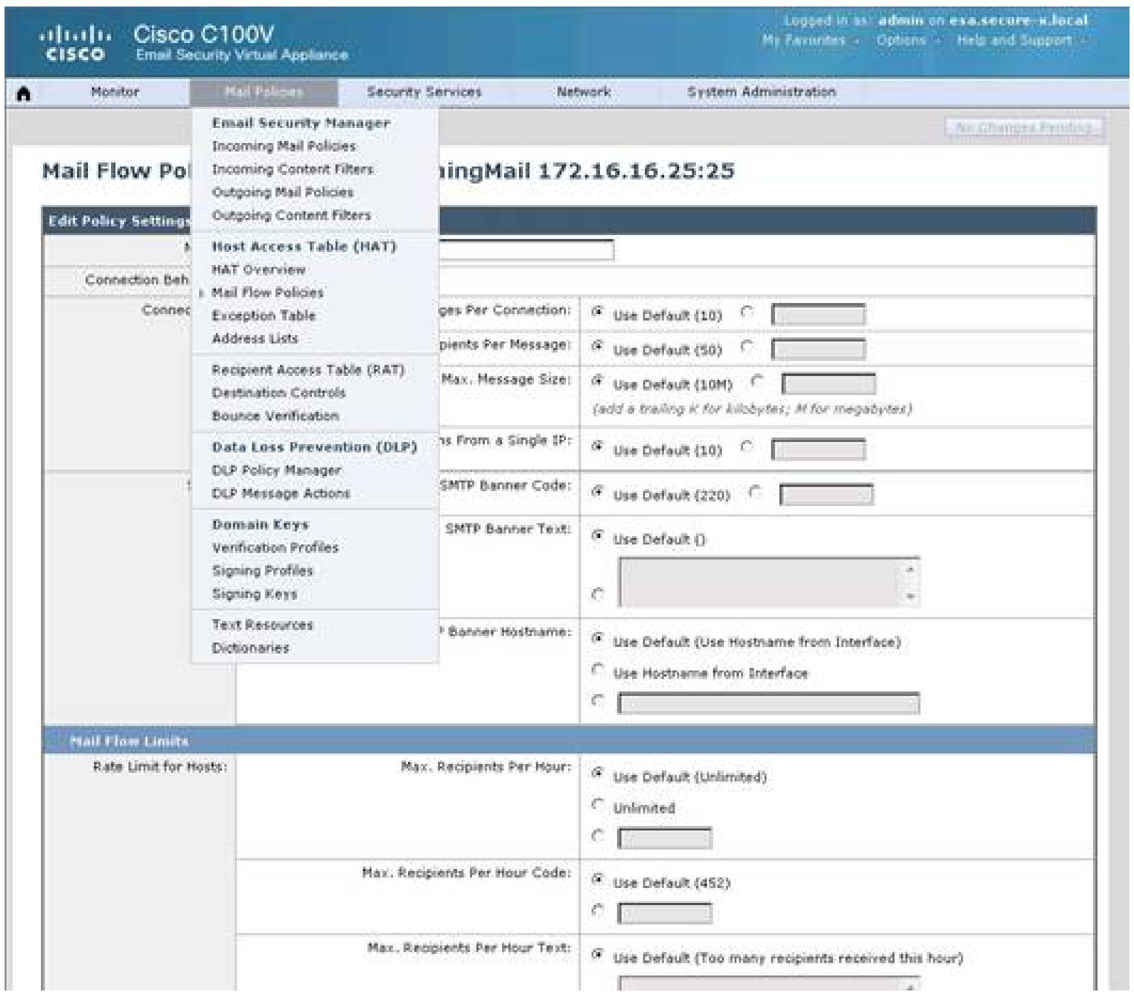
Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name:	RELAYED	
Connection Behavior:	Relay	
Connections:	Max. Messages Per Connection:	● Use Default (10) ○
	Max. Recipients Per Message:	● Use Default (50) ○
	Max. Message Size:	● Use Default (10M) ○ (add a trailing K for kilobytes; M for megabytes)
	Max. Concurrent Connections From a Single IP:	● Use Default (10) ○
SMTP:	Custom SMTP Banner Code:	● Use Default (220) ○
	Custom SMTP Banner Text:	● Use Default () ○
	Override SMTP Banner Hostname:	● Use Default (Use Hostname from Interface) ○ Use Hostname from Interface ○

Mail Flow Limits

Rate Limit for Hosts:	Max. Recipients Per Hour:	● Use Default (Unlimited) ○ Unlimited ○
	Max. Recipients Per Hour Code:	● Use Default (452) ○
	Max. Recipients Per Hour Text:	● Use Default (Too many recipients received this hour)



Mail Flow Pol… ingMail 172.16.16.25:25

Edit Policy Settings

Connection Beh…

Connec…

…ges Per Connection: ● Use Default (10) ○

…pients Per Message: ● Use Default (50) ○

Max. Message Size: ● Use Default (10M) ○
(add a trailing k for kilobytes; M for megabytes)

…s From a Single IP: ● Use Default (10) ○

SMTP Banner Code: ● Use Default (220) ○

SMTP Banner Text: ● Use Default ()
○

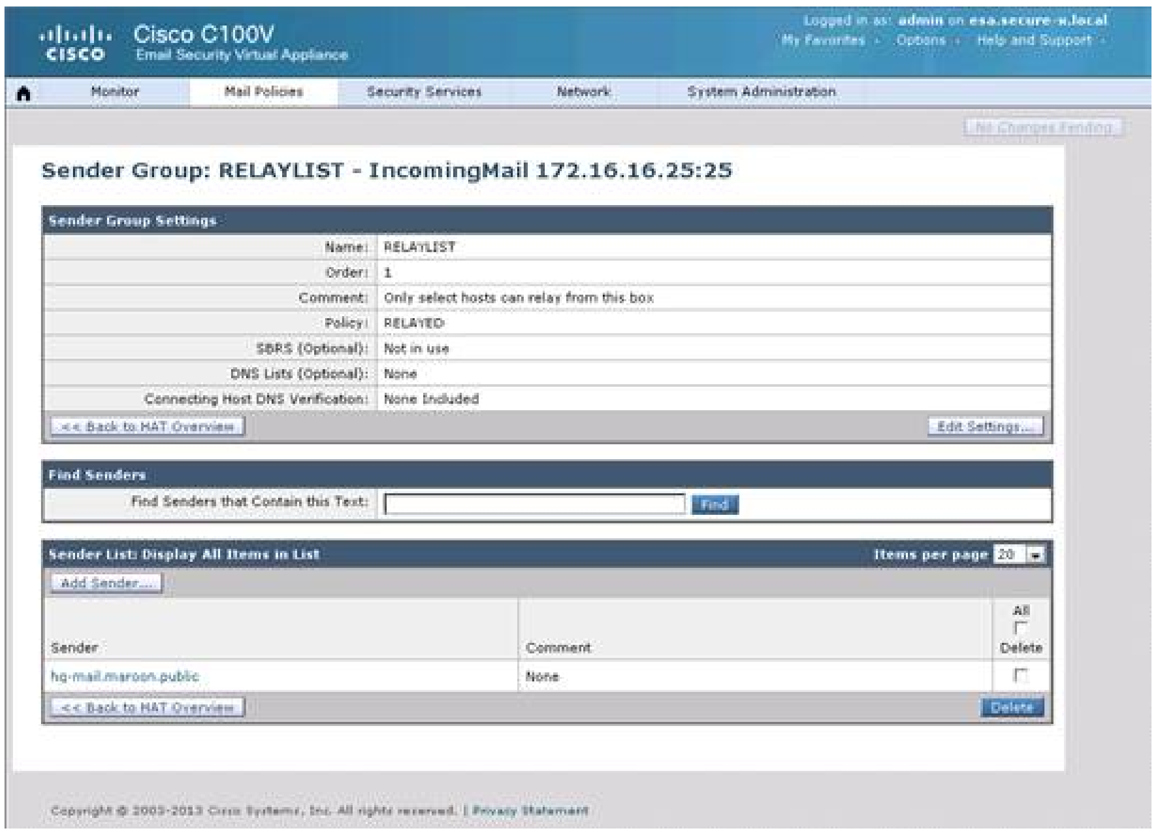
…P Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○

Mail Flow Limits

Rate Limit for Hosts: Max. Recipients Per Hour: ● Use Default (Unlimited)
○ Unlimited
○

Max. Recipients Per Hour Code: ● Use Default (452)
○

Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)



Sender Group: RELAYLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	RELAYLIST
Order:	1
Comment:	Only select hosts can relay from this box
Policy:	RELAYED
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

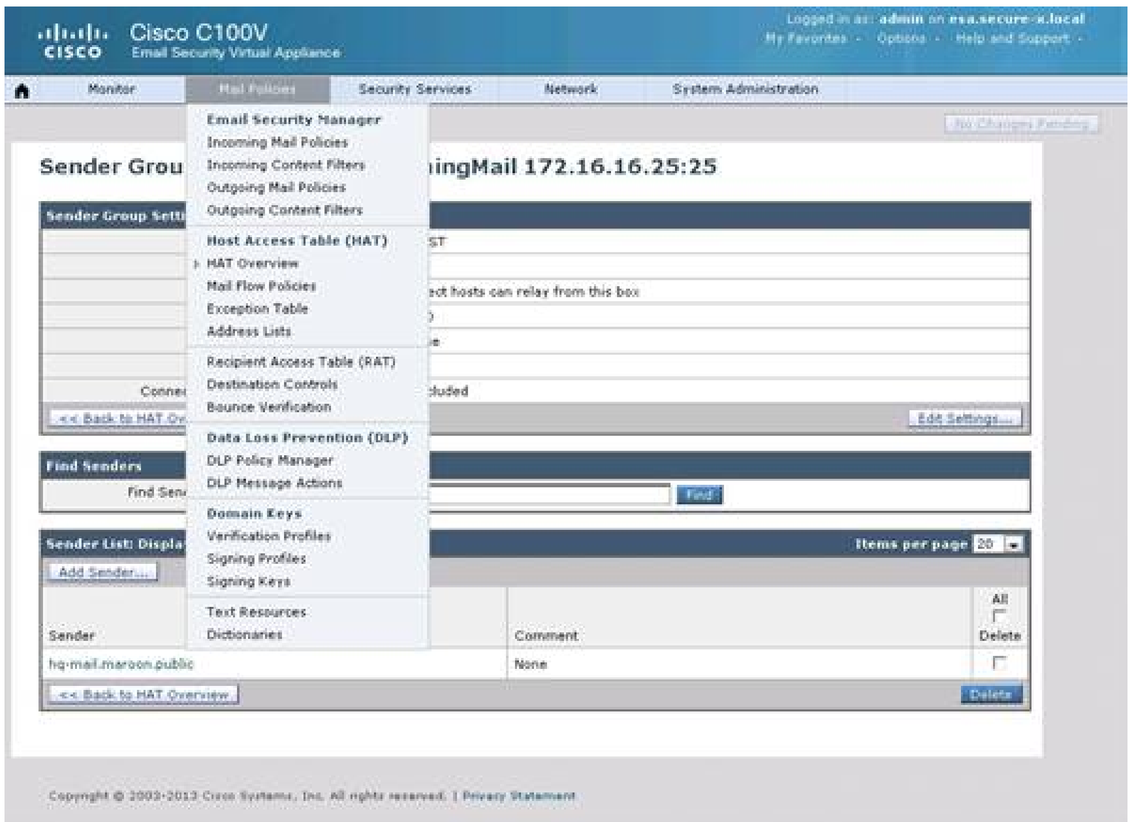
Find Senders

Find Senders that Contain this Text:

Sender List: Display All Items in List — Items per page 20

Sender	Comment	All □ Delete
hq-mail.maroon.public	None	□

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



Sender Grou… ingMail 172.16.16.25:25

Sender Group Setti…

…ST

…ct hosts can relay from this box

…)

…e

Connec… …luded

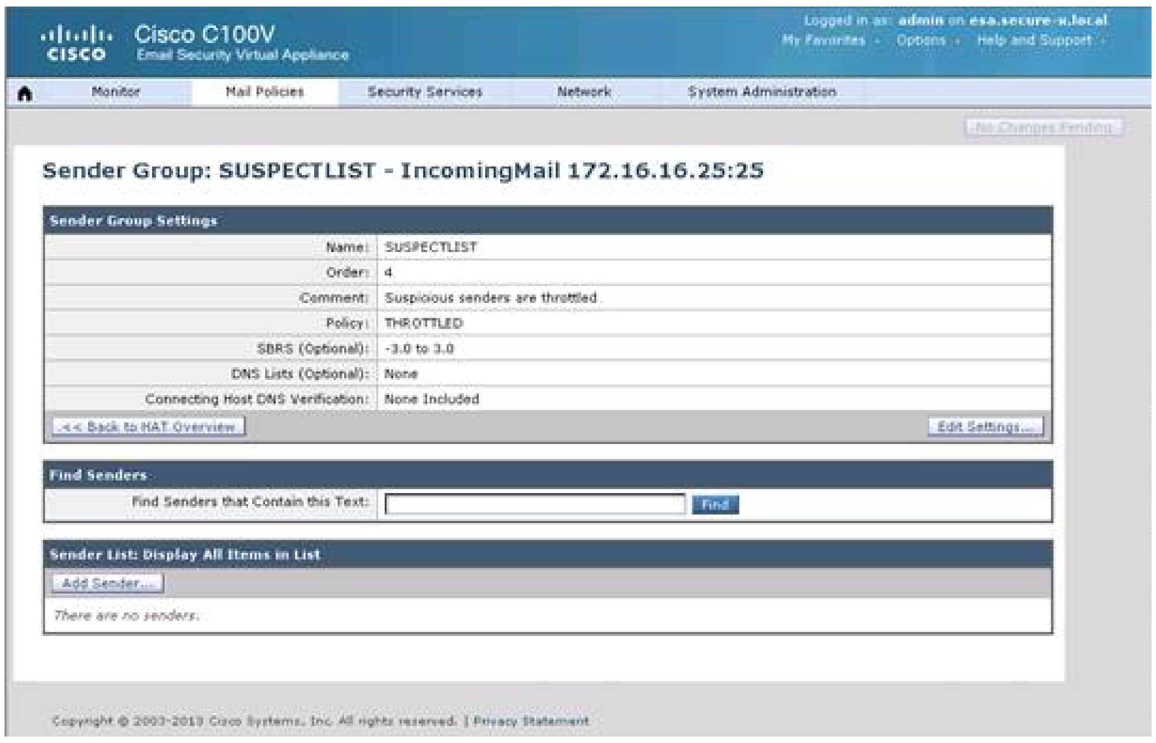
Find Senders

Find Sen…

Sender List: Displa… Items per page 20

Sender	Comment	All □ Delete
hq-mail.maroon.public	None	□

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Sender Group: SUSPECTLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	SUSPECTLIST
Order:	4
Comment:	Suspicious senders are throttled
Policy:	THROTTLED
SBRS (Optional):	-3.0 to 3.0
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

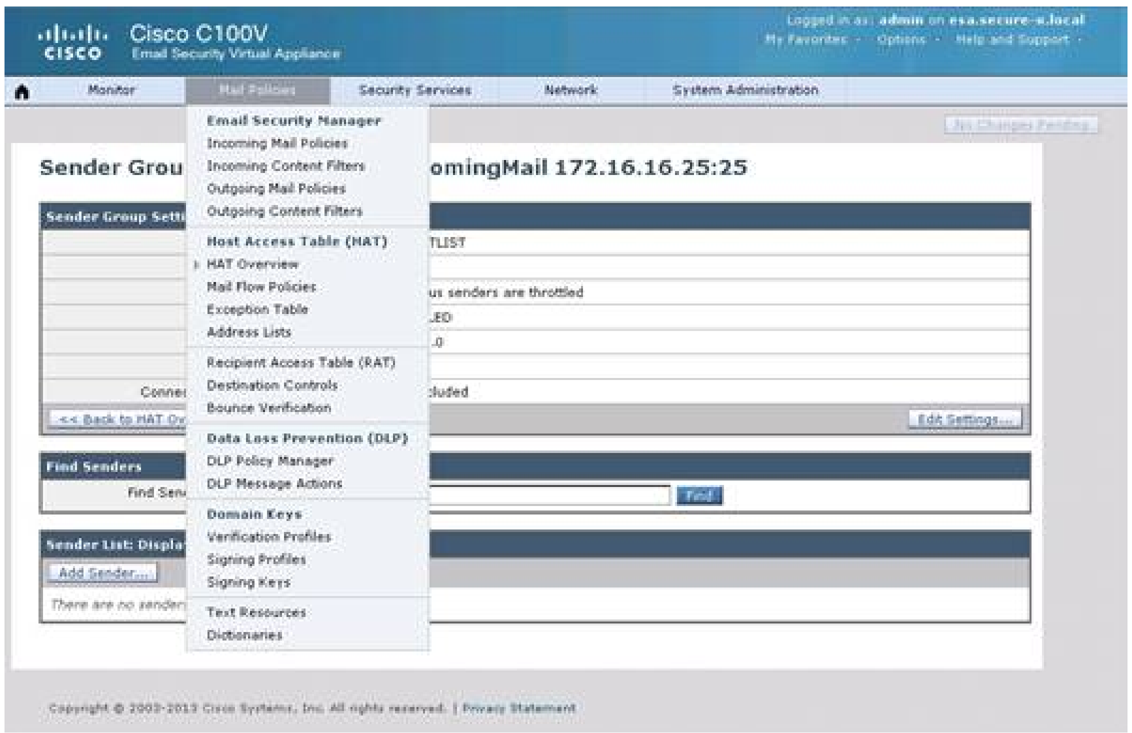
Find Senders

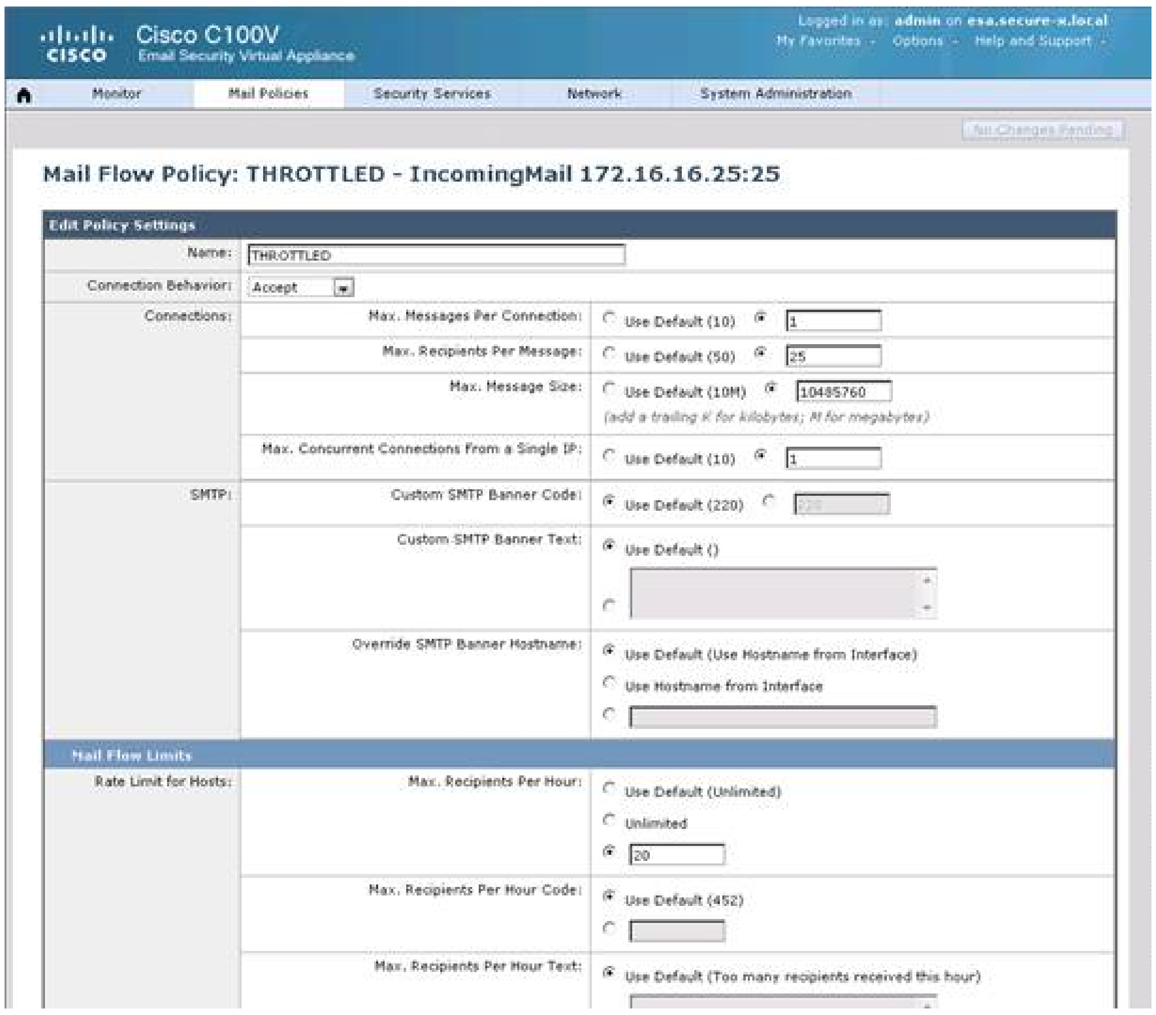
Find Senders that Contain this Text:

Sender List: Display All Items in List

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

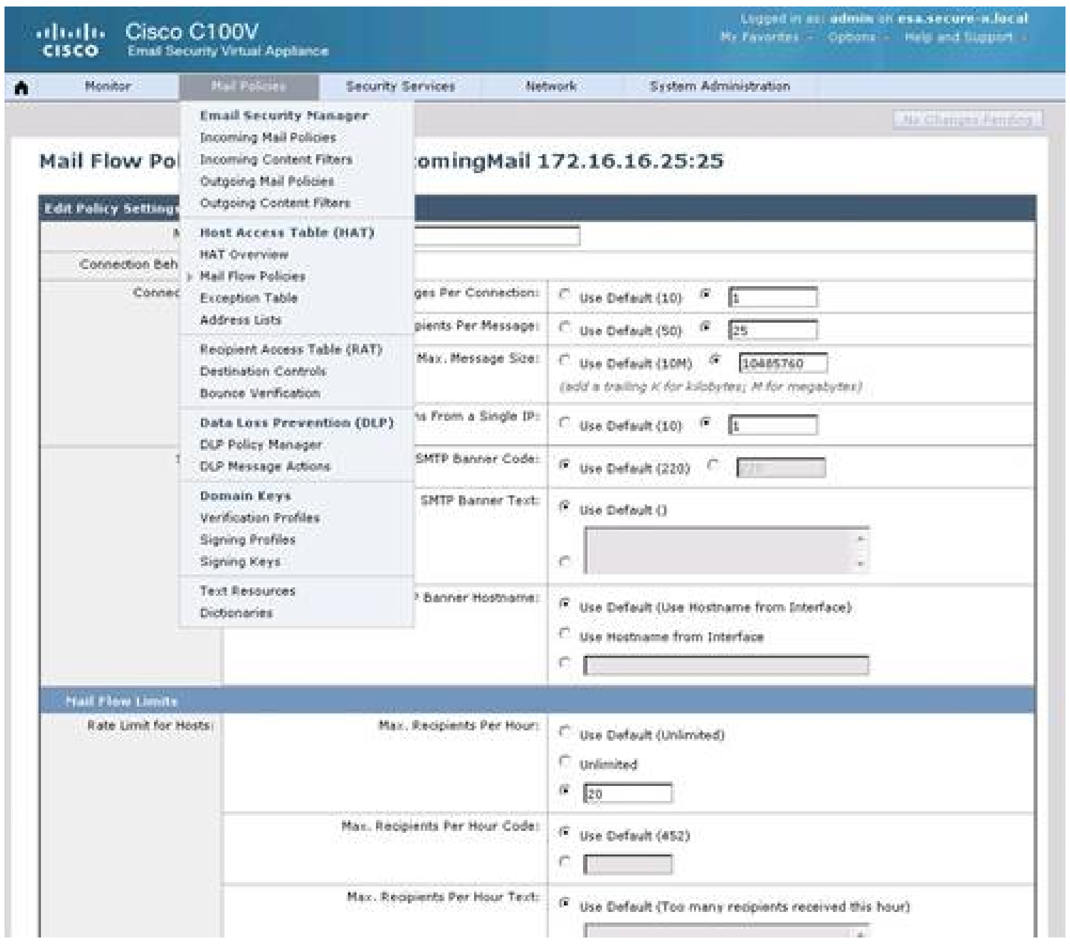



Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Mail Flow Policy: THROTTLED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name:	THROTTLED	
Connection Behavior:	Accept	
Connections:	Max. Messages Per Connection:	○ Use Default (10) ● 1
	Max. Recipients Per Message:	○ Use Default (50) ● 25
	Max. Message Size:	○ Use Default (10M) ● 10485760 *(add a trailing K for kilobytes; M for megabytes)*
	Max. Concurrent Connections From a Single IP:	○ Use Default (10) ● 1
SMTP:	Custom SMTP Banner Code:	● Use Default (220) ○ 220
	Custom SMTP Banner Text:	● Use Default () ○
	Override SMTP Banner Hostname:	● Use Default (Use Hostname from Interface) ○ Use Hostname from Interface ○
Mail Flow Limits		
Rate Limit for Hosts:	Max. Recipients Per Hour:	○ Use Default (Unlimited) ○ Unlimited ● 20
	Max. Recipients Per Hour Code:	● Use Default (452) ○
	Max. Recipients Per Hour Text:	● Use Default (Too many recipients received this hour)



Mail Flow Pol… …omingMail 172.16.16.25:25

Edit Policy Setting…

Connection Beh…

Connec…

…ges Per Connection: ○ Use Default (10) ● 1

…pients Per Message: ○ Use Default (50) ● 25

Max. Message Size: ○ Use Default (10M) ● 10485760
(add a trailing K for kilobytes; M for megabytes)

…s From a Single IP: ○ Use Default (10) ● 1

SMTP Banner Code: ● Use Default (220) ○ 220

SMTP Banner Text: ● Use Default ()
○

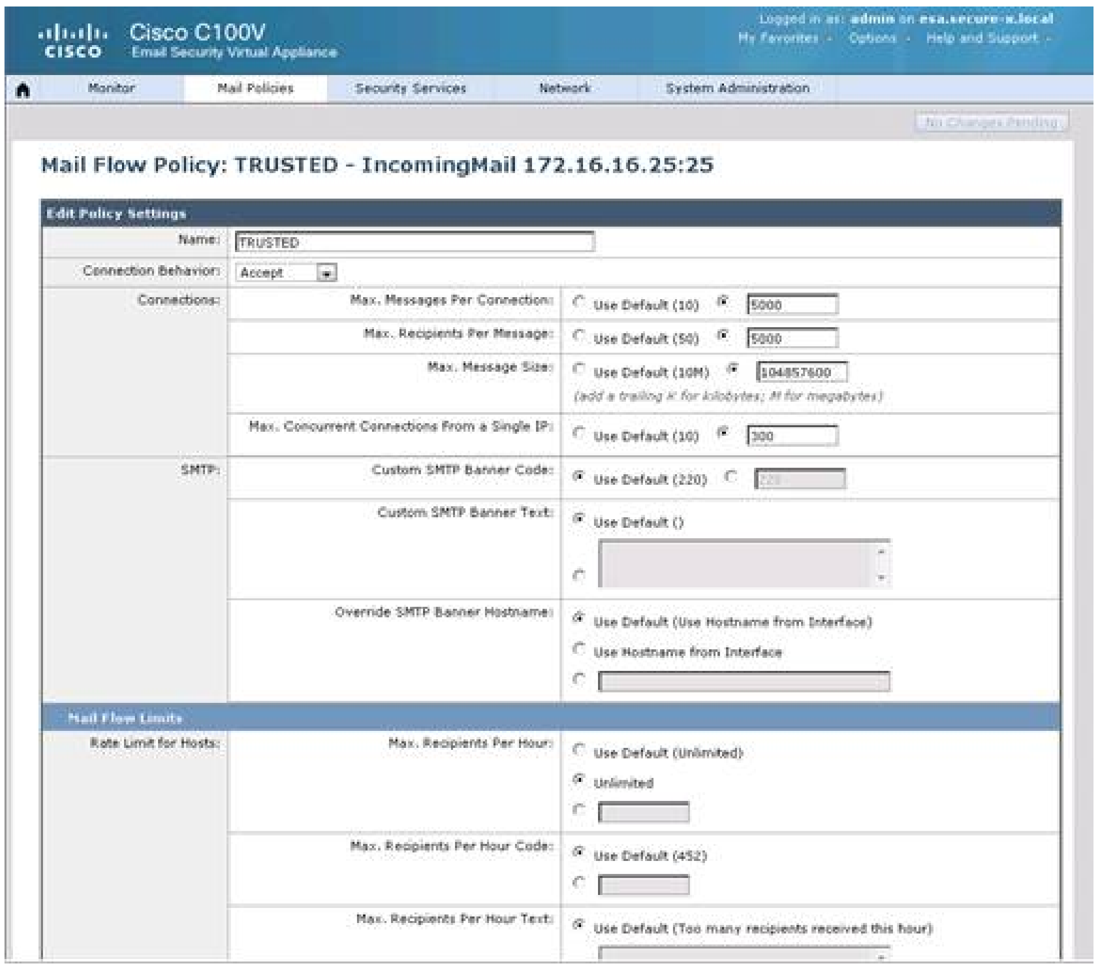
…Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○

Mail Flow Limits

Rate Limit for Hosts: Max. Recipients Per Hour: ○ Use Default (Unlimited)
○ Unlimited
● 20

Max. Recipients Per Hour Code: ● Use Default (452)
○

Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name: TRUSTED

Connection Behavior: Accept

Connections: Max. Messages Per Connection: ○ Use Default (10) ● 5000

Max. Recipients Per Message: ○ Use Default (50) ● 5000

Max. Message Size: ○ Use Default (10M) ● 104857600
(add a trailing K for kilobytes; M for megabytes)

Max. Concurrent Connections From a Single IP: ○ Use Default (10) ● 300

SMTP: Custom SMTP Banner Code: ● Use Default (220) ○ 220

Custom SMTP Banner Text: ● Use Default ()
○

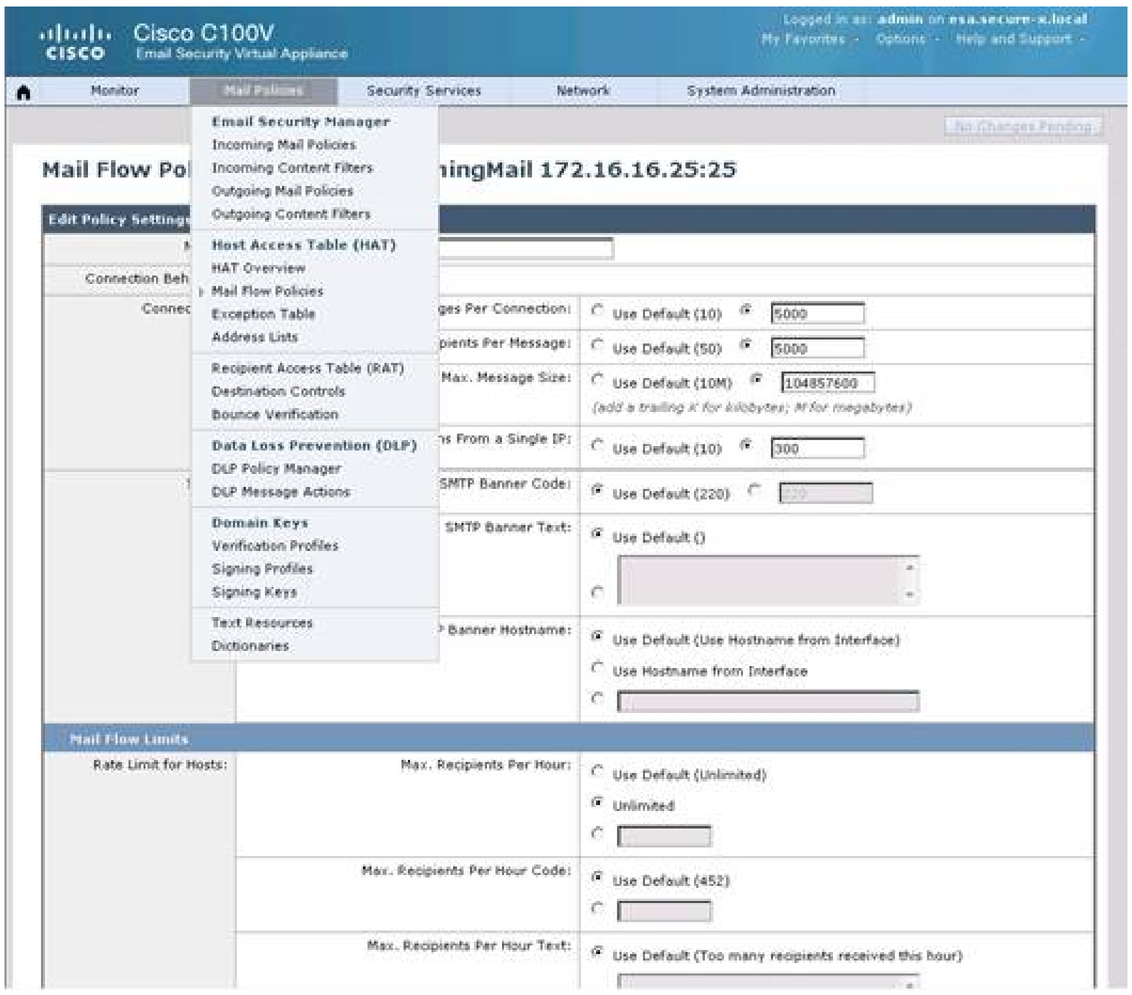
Override SMTP Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○

Mail Flow Limits

Rate Limit for Hosts: Max. Recipients Per Hour: ○ Use Default (Unlimited)
● Unlimited
○

Max. Recipients Per Hour Code: ● Use Default (452)
○

Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)



Mail Flow Pol… …ingMail 172.16.16.25:25

Edit Policy Setting…

Connection Beh…

Connec…

…ges Per Connection: ○ Use Default (10) ● 5000

…pients Per Message: ○ Use Default (50) ● 5000

Max. Message Size: ○ Use Default (10M) ● 104857600
(add a trailing K for kilobytes; M for megabytes)

…s From a Single IP: ○ Use Default (10) ● 300

SMTP Banner Code: ● Use Default (220) ○ 220

SMTP Banner Text: ● Use Default ()
○

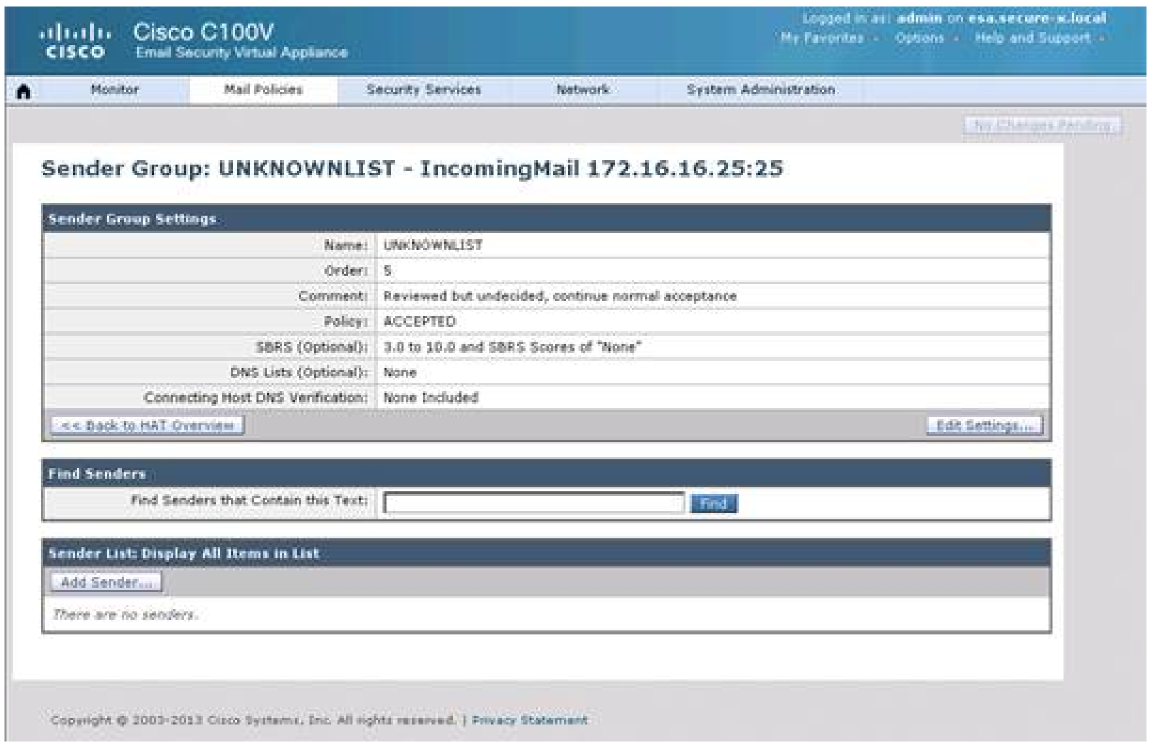
…Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○

Mail Flow Limits

Rate Limit for Hosts: Max. Recipients Per Hour: ○ Use Default (Unlimited)
● Unlimited
○

Max. Recipients Per Hour Code: ● Use Default (452)
○

Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
<< Back to HAT Overview
Edit Settings...
Find
Add Sender...
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Sender Group: UNKNOWNLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

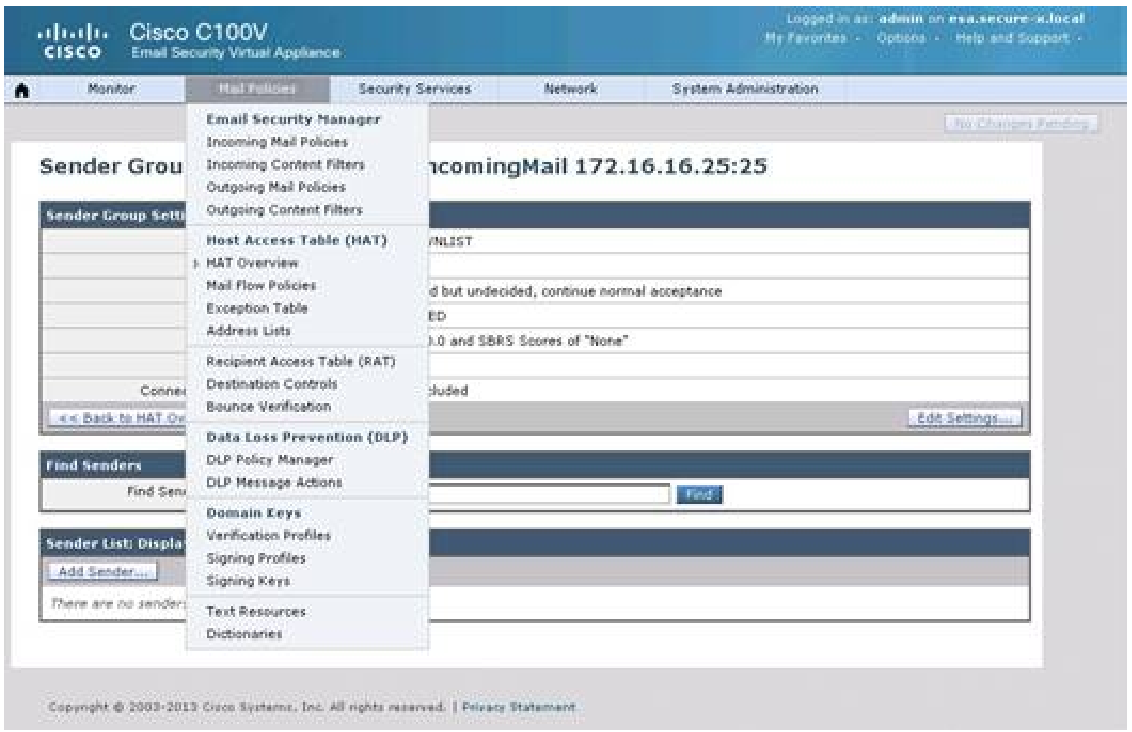
Name:	UNKNOWNLIST
Order:	5
Comment:	Reviewed but undecided, continue normal acceptance
Policy:	ACCEPTED
SBRS (Optional):	3.0 to 10.0 and SBRS Scores of "None"
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

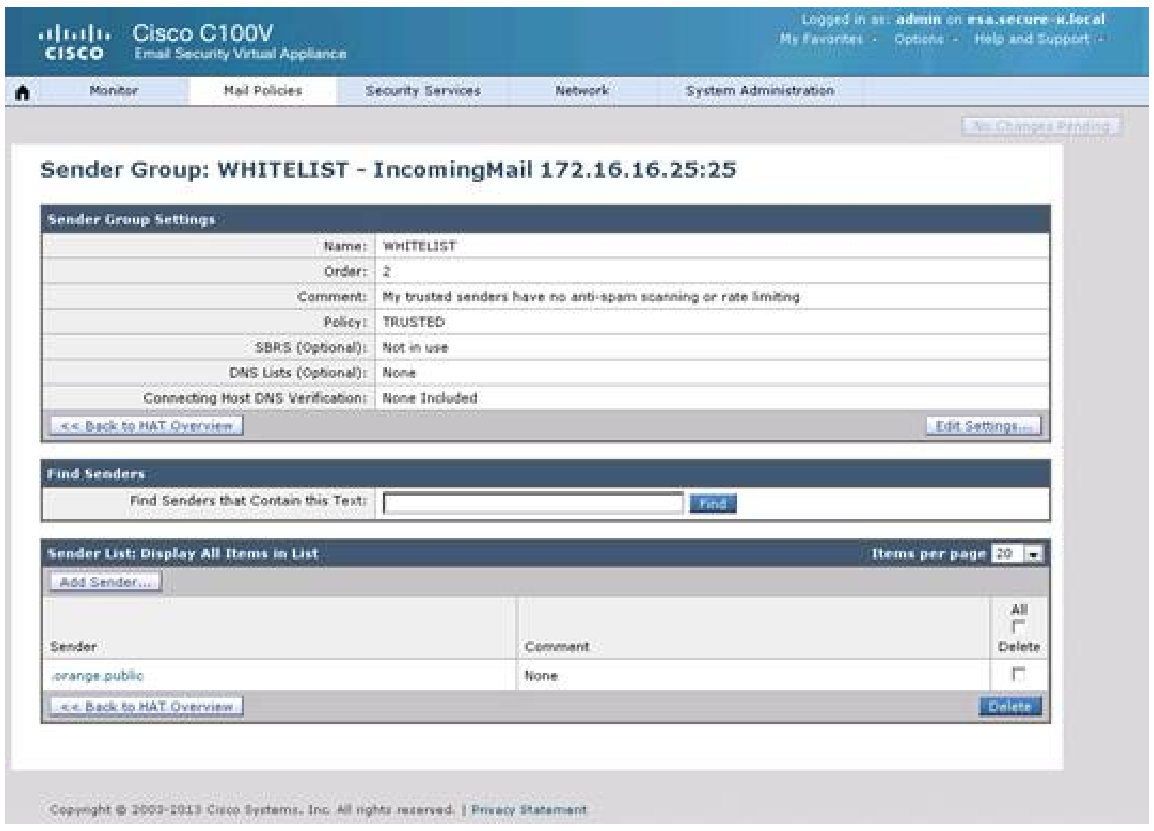
Find Senders

Find Senders that Contain this Text:

Sender List: Display All Items in List

There are no senders.




Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
<< Back to HAT Overview
Edit Settings...
Find
Add Sender...
Delete
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Sender Group: WHITELIST - IncomingMail 172.16.16.25:25

Sender Group Settings

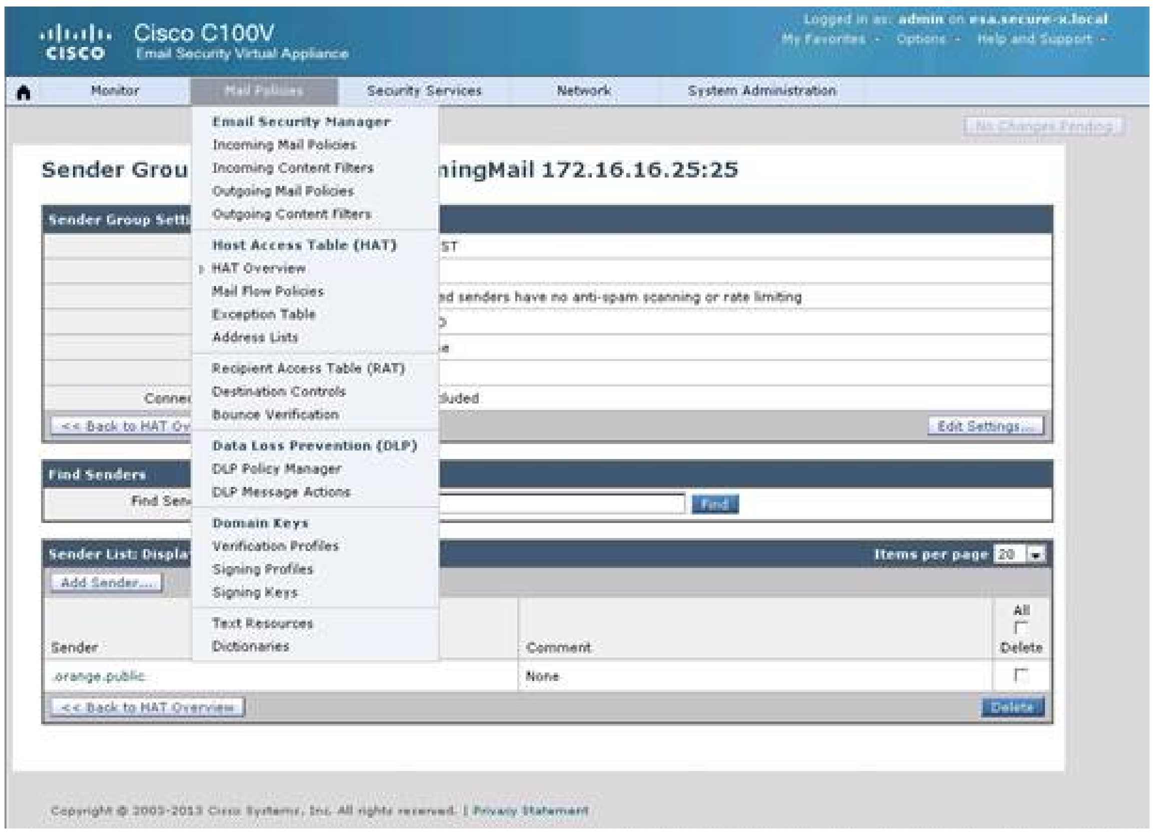
Name:	WHITELIST
Order:	2
Comment:	My trusted senders have no anti-spam scanning or rate limiting
Policy:	TRUSTED
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

Find Senders

Find Senders that Contain this Text:

Sender List: Display All Items in List — Items per page 20

Sender	Comment	All ☐ Delete
.orange.public	None	☐



Sender Grou ningMail 172.16.16.25:25

Sender Group Setti

ST

ed senders have no anti-spam scanning or rate limiting

Conne duded

Find Senders

Find Sen

Sender List: Displa

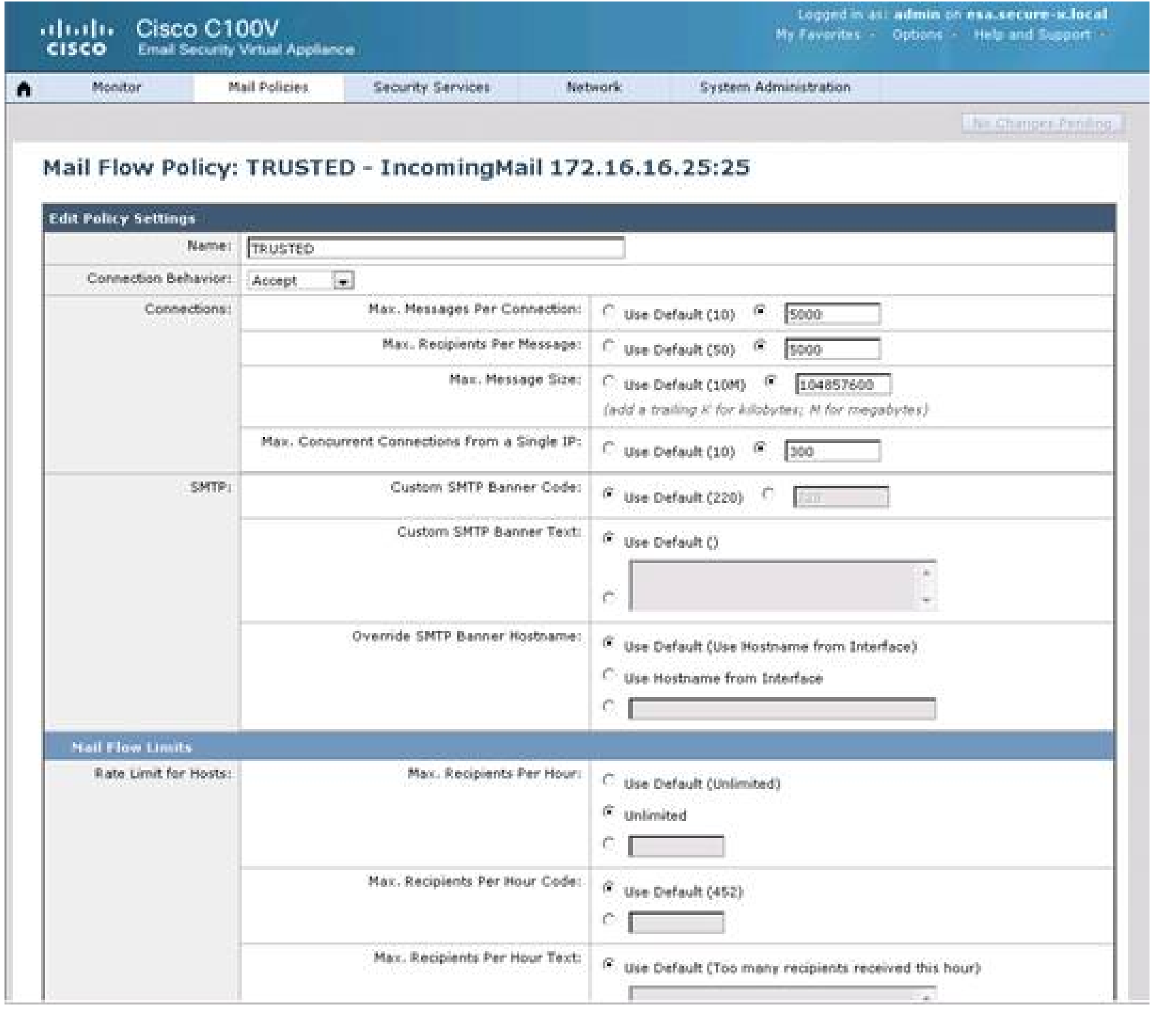
Sender	Comment	All □ Delete
.orange.public	None	□

For which domains will the Cisco Email Security Appliance allow up to 5000 recipients per message?

A. violet.public
B. violet.public and blue.public
C. violet.public, blue.public and green.public
D. red.public
E. orange.public
F. red.public and orange.public

Answer: E

Explanation:
Here we see that the TRUSTED policy is being throttled to 5000 recipients per message. Image%2075


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name: TRUSTED

Connection Behavior: Accept

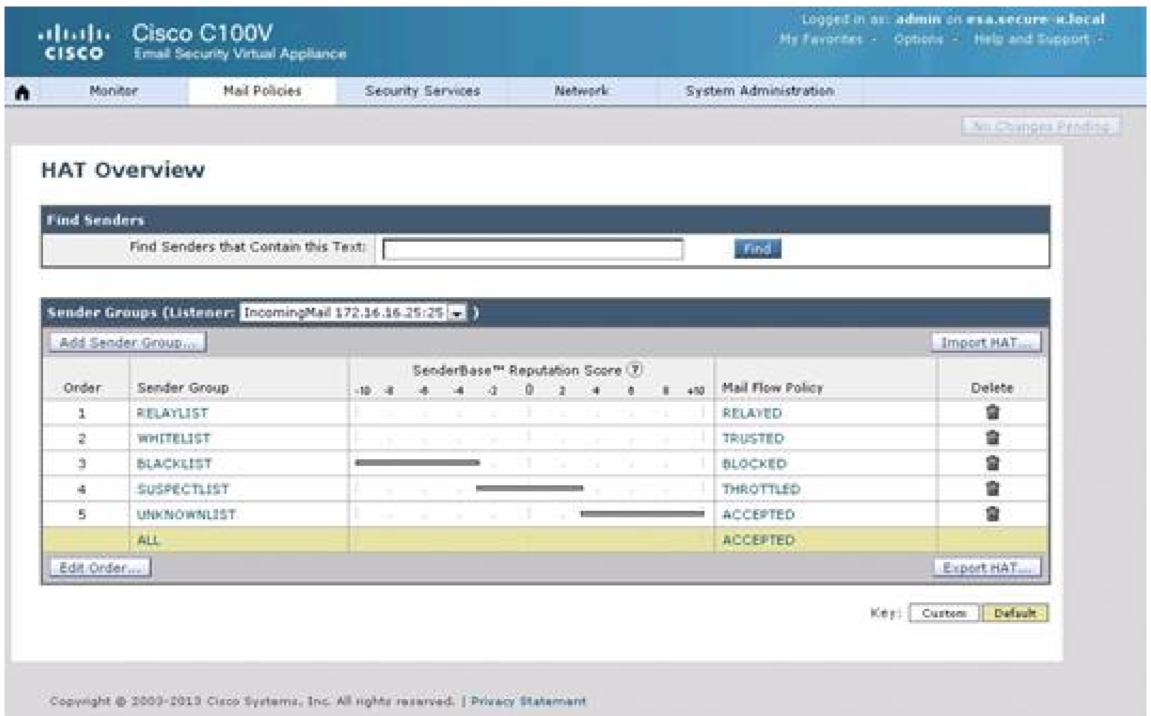
Connections:
Max. Messages Per Connection: ○ Use Default (10) ● 5000
Max. Recipients Per Message: ○ Use Default (50) ● 5000
Max. Message Size: ○ Use Default (10M) ● 104857600
(add a trailing K for kilobytes; M for megabytes)
Max. Concurrent Connections From a Single IP: ○ Use Default (10) ● 300

SMTP:
Custom SMTP Banner Code: ● Use Default (220) ○ 220
Custom SMTP Banner Text: ● Use Default () ○
Override SMTP Banner Hostname: ● Use Default (Use Hostname from Interface) ○ Use Hostname from Interface ○

Mail Flow Limits

Rate Limit for Hosts:
Max. Recipients Per Hour: ○ Use Default (Unlimited) ● Unlimited ○
Max. Recipients Per Hour Code: ● Use Default (452) ○
Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)

By looking at the HAT policy we see that the TRUSTED policy applies to the WHITELIST sender group.
Image 27


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

HAT Overview

Find Senders

Find Senders that Contain this Text: Find

Sender Groups (Listener: IncomingMail 172.16.16.25:25)

Add Sender Group... Import HAT...

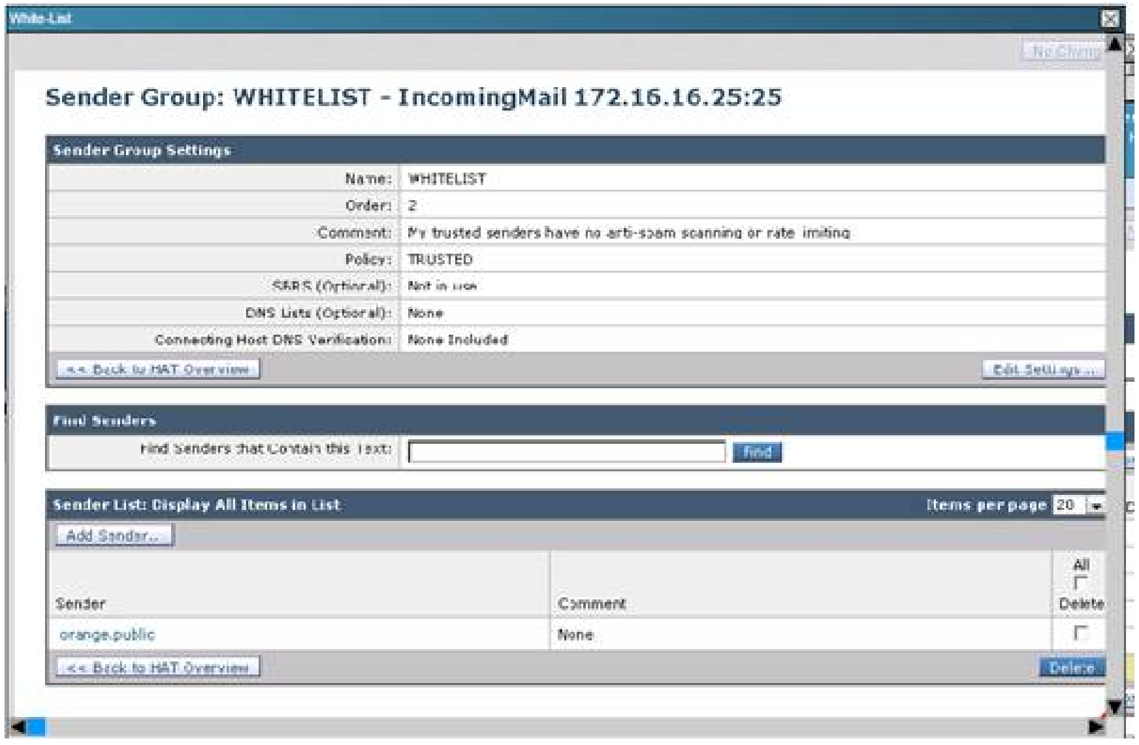
Order	Sender Group	SenderBase™ Reputation Score -10 -8 -6 -4 -2 0 2 4 6 8 +10	Mail Flow Policy	Delete
1	RELAYLIST		RELAYED	🗑
2	WHITELIST		TRUSTED	🗑
3	BLACKLIST		BLOCKED	🗑
4	SUSPECTLIST		THROTTLED	🗑
5	UNKNOWNLIST		ACCEPTED	🗑
	ALL		ACCEPTED	

Edit Order... Export HAT...

Key: Custom Default

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

By clicking on the WHITELIST sender group we can see that orange.public is listed as the sender. Capture



Sender Group: WHITELIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	WHITELIST
Order:	2
Comment:	My trusted senders have no anti-spam scanning or rate limiting
Policy:	TRUSTED
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text: Find

Sender List: Display All Items in List Items per page 20

Add Sender...

Sender	Comment	All □ Delete
orange.public	None	□

<< Back to HAT Overview Delete

NEW QUESTION 362

- (Exam Topic 3)

Which command applies WCCP redirection on the inside interface of a Cisco ASA 5500-x firewall?

A. wccp interface inside 90 redirect in
B. web-cache interface inside 90 redirect in
C. wccp interface inside redirect out
D. wccp web-cache

Answer: A

NEW QUESTION 365

- (Exam Topic 3)

Which Cisco ESA component receives connections from external mail servers?

A. MTA
B. public listener
C. private listener
D. recipient access table
E. SMTP incoming relay agent

Answer: B

NEW QUESTION 368

- (Exam Topic 3)

If learning accept mode is set to "auto" and the knowledge base is loaded only when explicitly requested on the IPS, which statement about the knowledge base is true?

A. The knowledge base is set to load dynamically.
B. The knowledge base is set to "save only."
C. The knowledge base is set to "discarded."
D. The knowledge base is set to load statically.

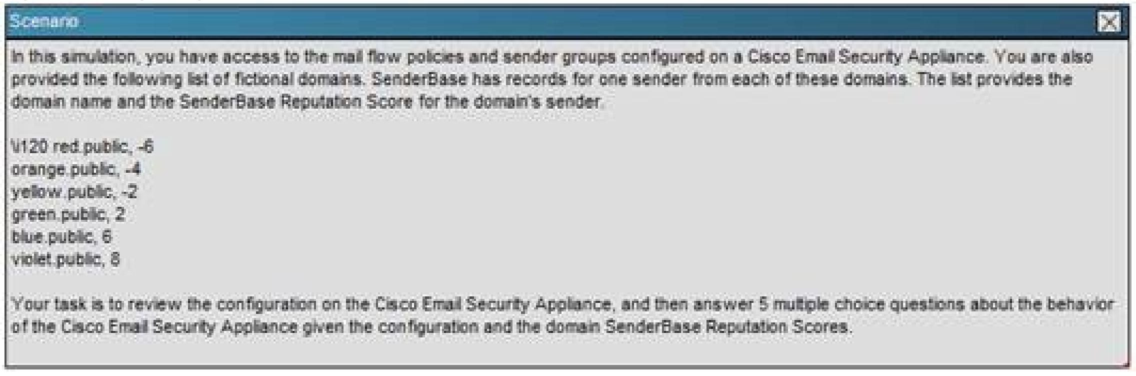
Answer: B

NEW QUESTION 369
- (Exam Topic 3)
Which statement about the Cisco CWS web filtering policy behavior is true?

A. Rules are comprised of three criteria and an action.
B. By default, the schedule is set to office hours.
C. At least one rule applies to a web request.
D. In the evaluation of a rule set, the best match wins.

Answer: A

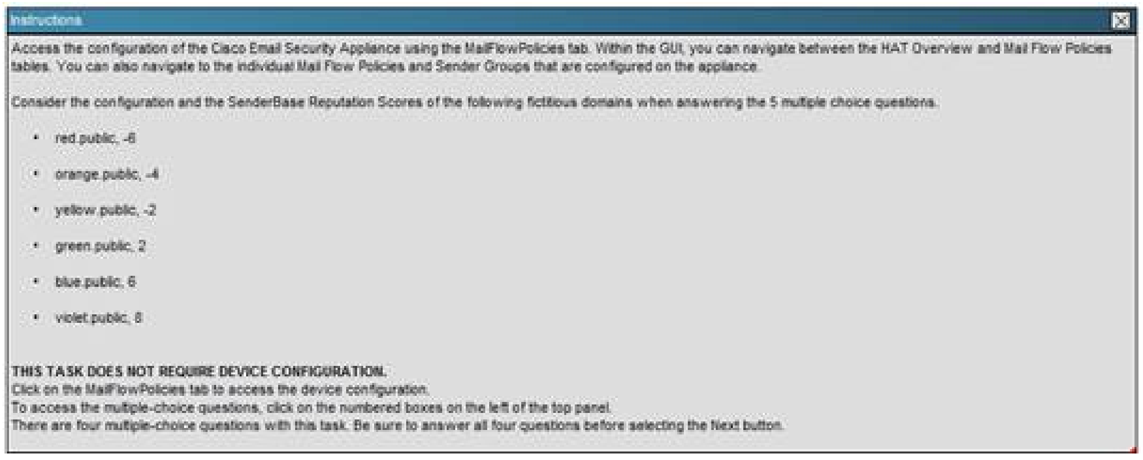
NEW QUESTION 374
- (Exam Topic 3)


Scenario

In this simulation, you have access to the mail flow policies and sender groups configured on a Cisco Email Security Appliance. You are also provided the following list of fictional domains. SenderBase has records for one sender from each of these domains. The list provides the domain name and the SenderBase Reputation Score for the domain's sender.

\120 red.public, -6
orange.public, -4
yellow.public, -2
green.public, 2
blue.public, 6
violet.public, 8

Your task is to review the configuration on the Cisco Email Security Appliance, and then answer 5 multiple choice questions about the behavior of the Cisco Email Security Appliance given the configuration and the domain SenderBase Reputation Scores.

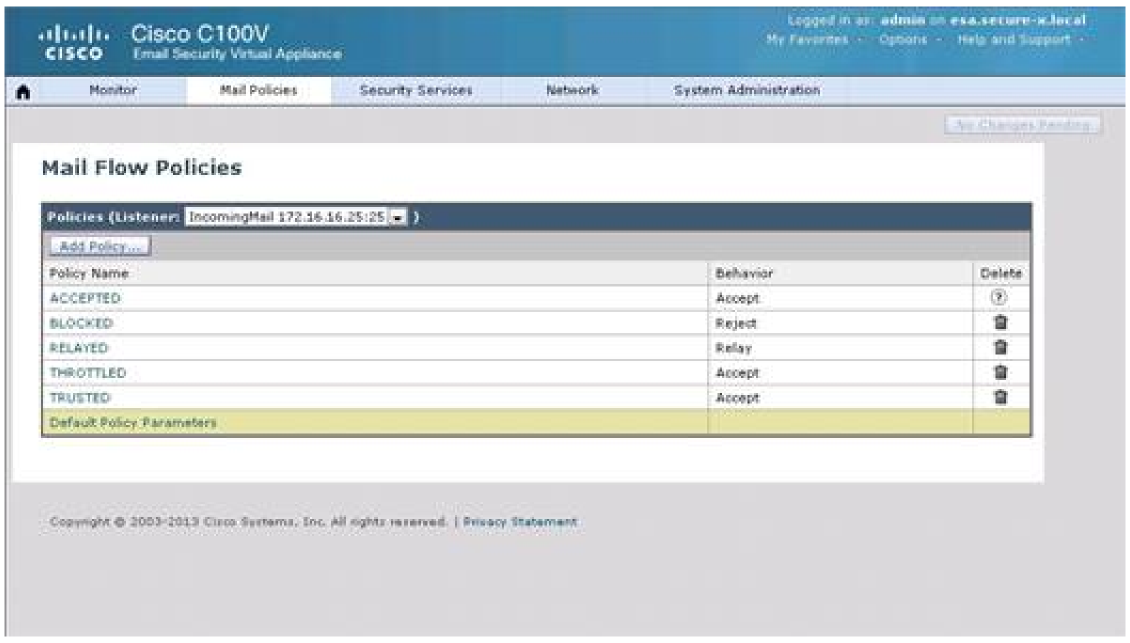

Instructions

Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the HAT Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance.

Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the 5 multiple choice questions.

- red.public, -6
- orange.public, -4
- yellow.public, -2
- green.public, 2
- blue.public, 6
- violet.public, 8

THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
Click on the MailFlowPolicies tab to access the device configuration.
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.


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

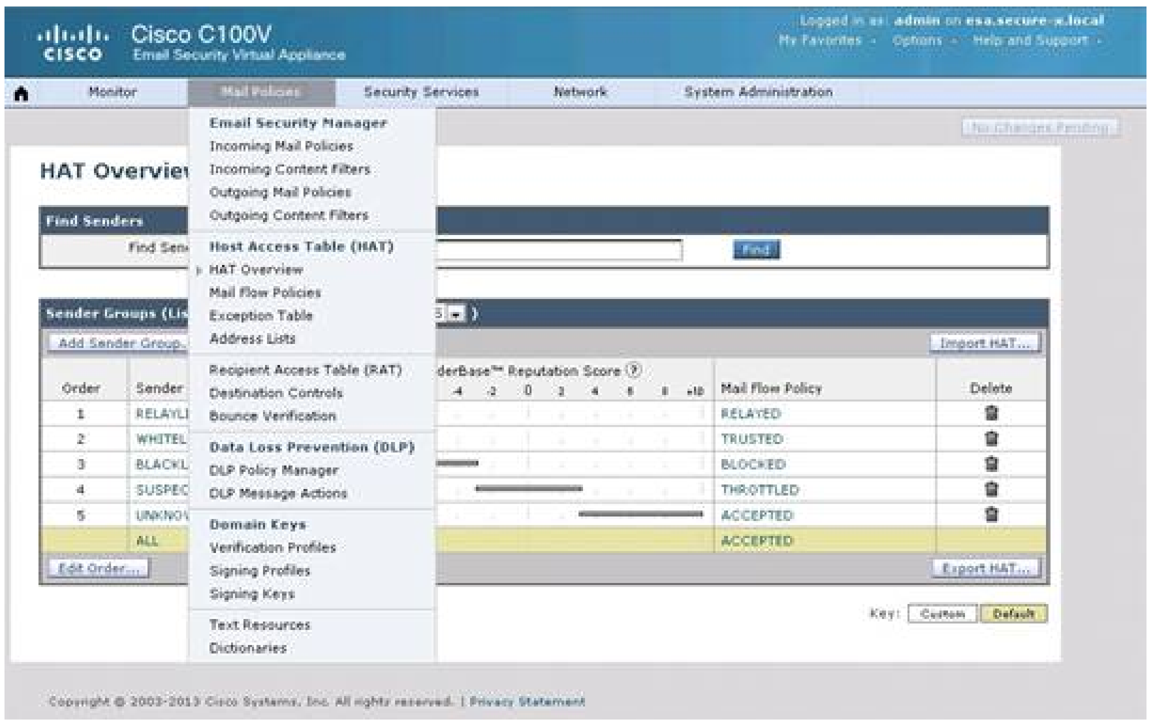
Mail Flow Policies

Policies (Listener: IncomingMail 172.16.16.25:25)

Add Policy...

Policy Name	Behavior	Delete
ACCEPTED	Accept	?
BLOCKED	Reject	🗑
RELAYED	Relay	🗑
THROTTLED	Accept	🗑
TRUSTED	Accept	🗑
Default Policy Parameters		

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



HAT Overvie

Find Senders

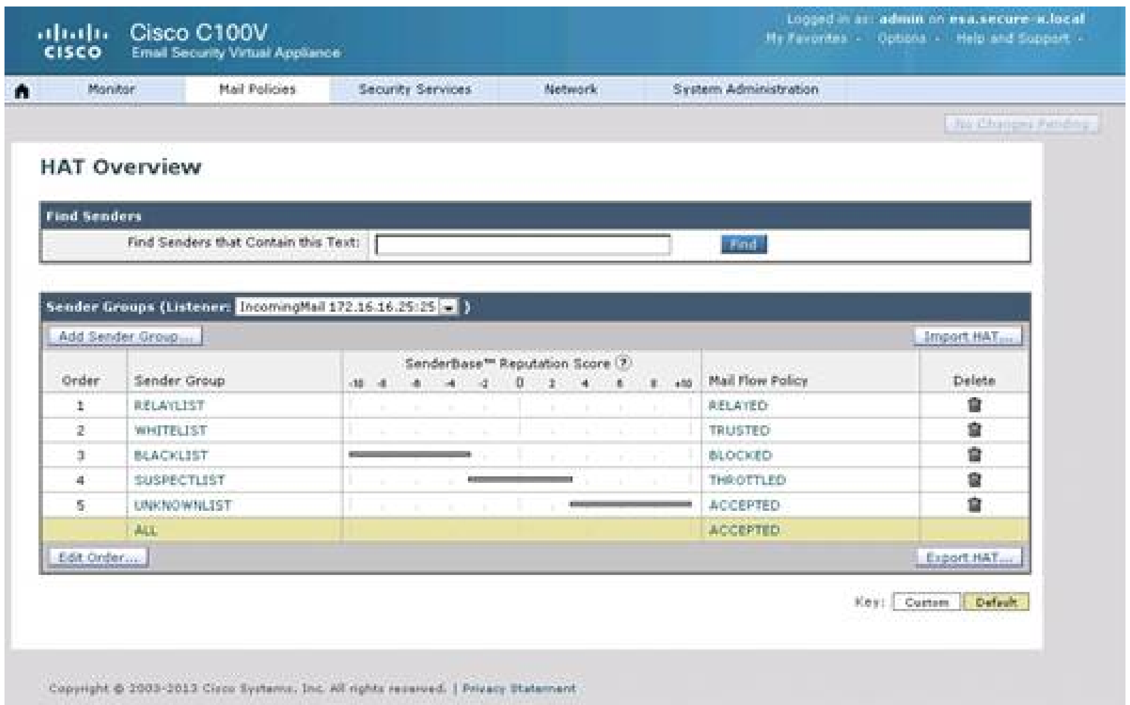
Find Sen

Sender Groups (Lis

Add Sender Group...

Order	Sender	derBase™ Reputation Score	Mail Flow Policy	Delete
1	RELAYLI		RELAYED	🗑
2	WHITEL		TRUSTED	🗑
3	BLACKL		BLOCKED	🗑
4	SUSPEC		THROTTLED	🗑
5	UNKNOV		ACCEPTED	🗑
	ALL		ACCEPTED	

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



HAT Overview

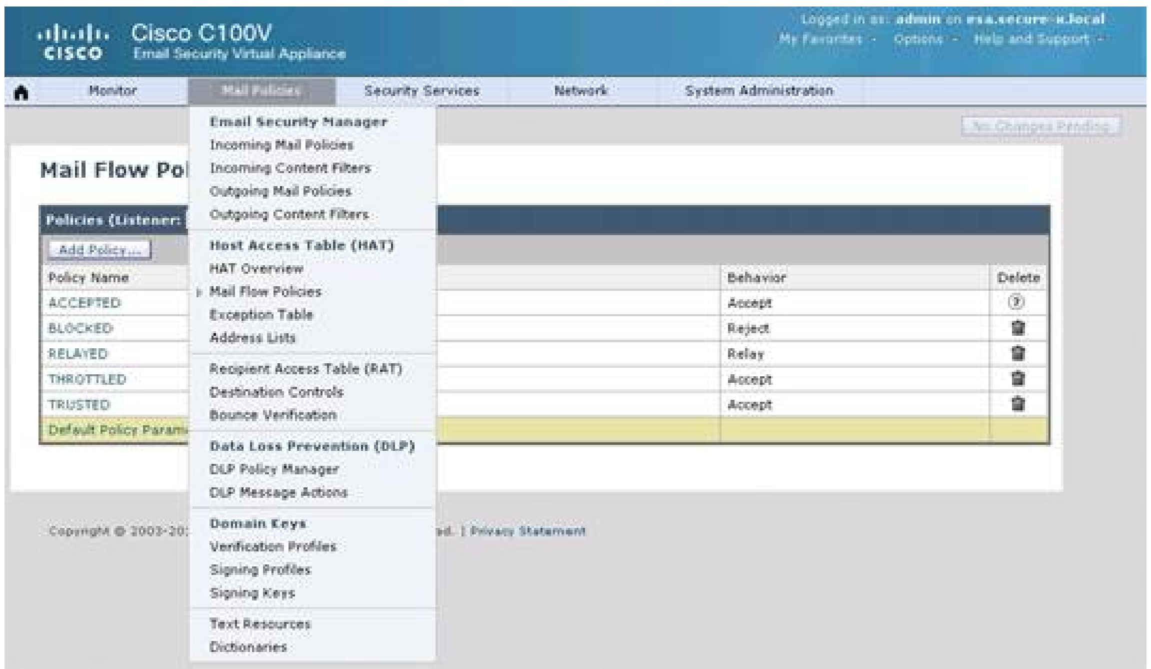
Find Senders

Find Senders that Contain this Text:

Sender Groups (Listener: IncomingMail 172.16.16.25:25)

Order	Sender Group	SenderBase™ Reputation Score (-10 -8 -6 -4 -2 0 2 4 6 8 +10)	Mail Flow Policy	Delete
1	RELAYLIST		RELAYED	🗑
2	WHITELIST		TRUSTED	🗑
3	BLACKLIST	-10 to -3	BLOCKED	🗑
4	SUSPECTLIST	-3 to 1	THROTTLED	🗑
5	UNKNOWNLIST	1 to 10	ACCEPTED	🗑
	ALL		ACCEPTED	

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

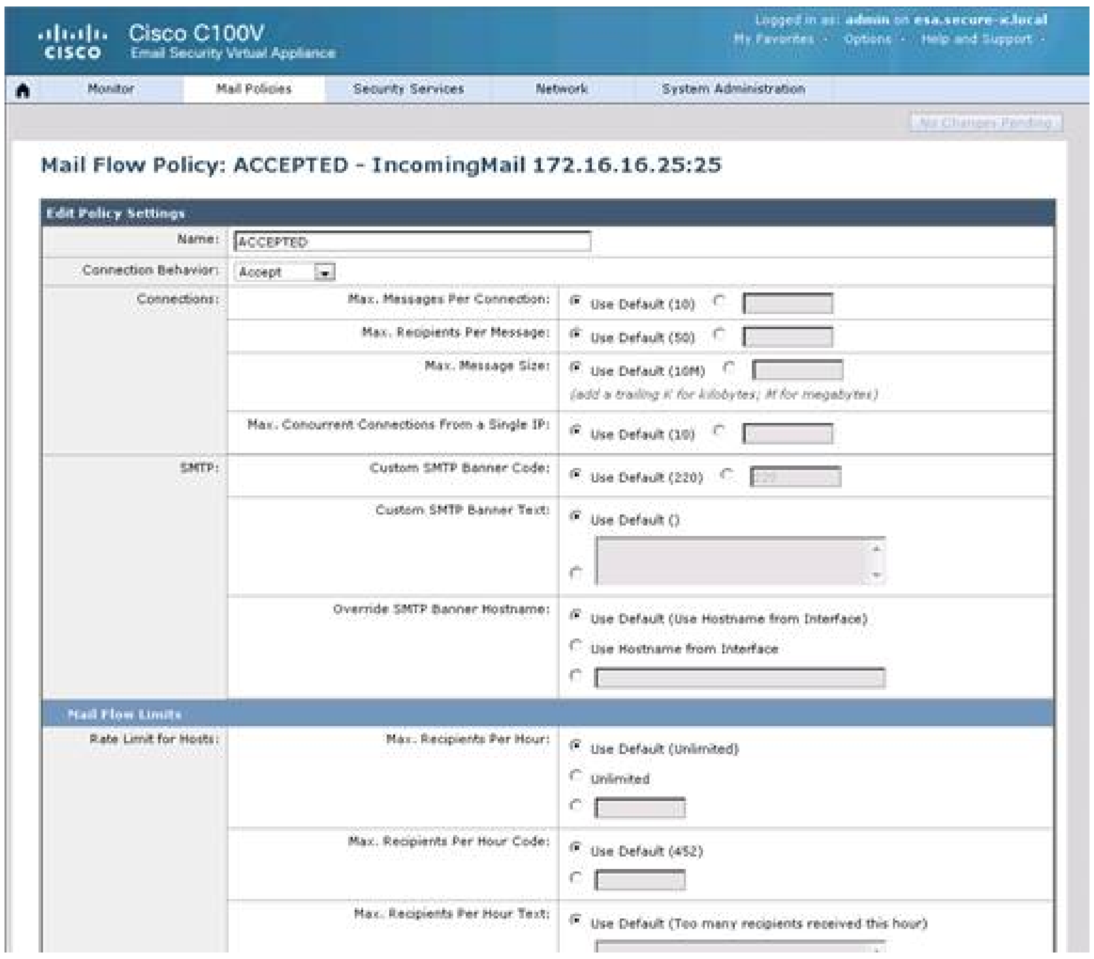


Mail Flow Po

Policies (Listener:

Policy Name	Behavior	Delete
ACCEPTED	Accept	?
BLOCKED	Reject	🗑
RELAYED	Relay	🗑
THROTTLED	Accept	🗑
TRUSTED	Accept	🗑
Default Policy Param		

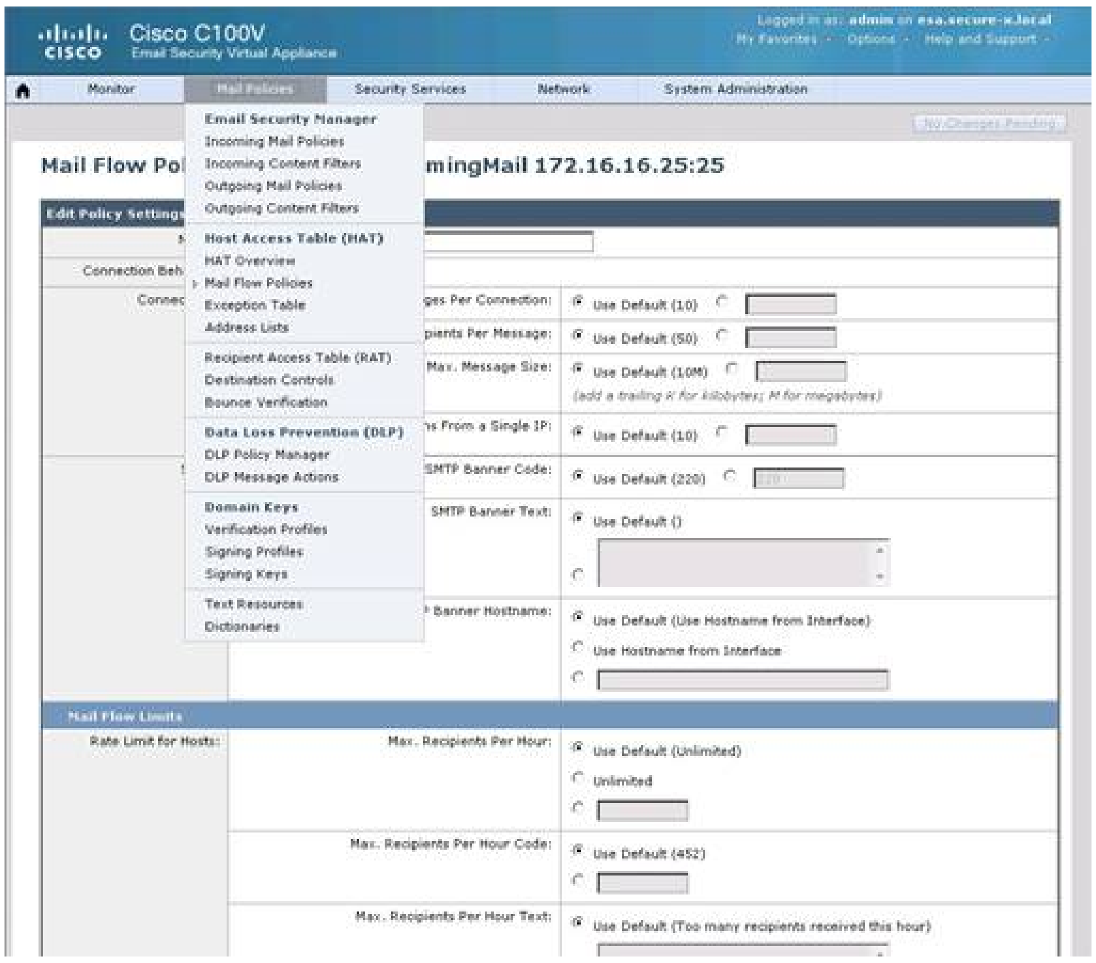
Copyright © 2003-20 d. | Privacy Statement


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Mail Flow Policy: ACCEPTED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name:	ACCEPTED	
Connection Behavior:	Accept	
Connections:	Max. Messages Per Connection:	● Use Default (10) ○
	Max. Recipients Per Message:	● Use Default (50) ○
	Max. Message Size:	● Use Default (10M) ○ (add a trailing K for kilobytes; M for megabytes)
	Max. Concurrent Connections From a Single IP:	● Use Default (10) ○
SMTP:	Custom SMTP Banner Code:	● Use Default (220) ○ 220
	Custom SMTP Banner Text:	● Use Default () ○
	Override SMTP Banner Hostname:	● Use Default (Use Hostname from Interface) ○ Use Hostname from Interface ○
Mail Flow Limits		
Rate Limit for Hosts:	Max. Recipients Per Hour:	● Use Default (Unlimited) ○ Unlimited ○
	Max. Recipients Per Hour Code:	● Use Default (452) ○
	Max. Recipients Per Hour Text:	● Use Default (Too many recipients received this hour)



Mail Flow Pol… mingMail 172.16.16.25:25

Edit Policy Settings

Connection Beh…

Connec…

…ges Per Connection: ● Use Default (10) ○

…pients Per Message: ● Use Default (50) ○

Max. Message Size: ● Use Default (10M) ○
(add a trailing K for kilobytes; M for megabytes)

…s From a Single IP: ● Use Default (10) ○

SMTP Banner Code: ● Use Default (220) ○ 220

SMTP Banner Text: ● Use Default ()
○

…P Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○

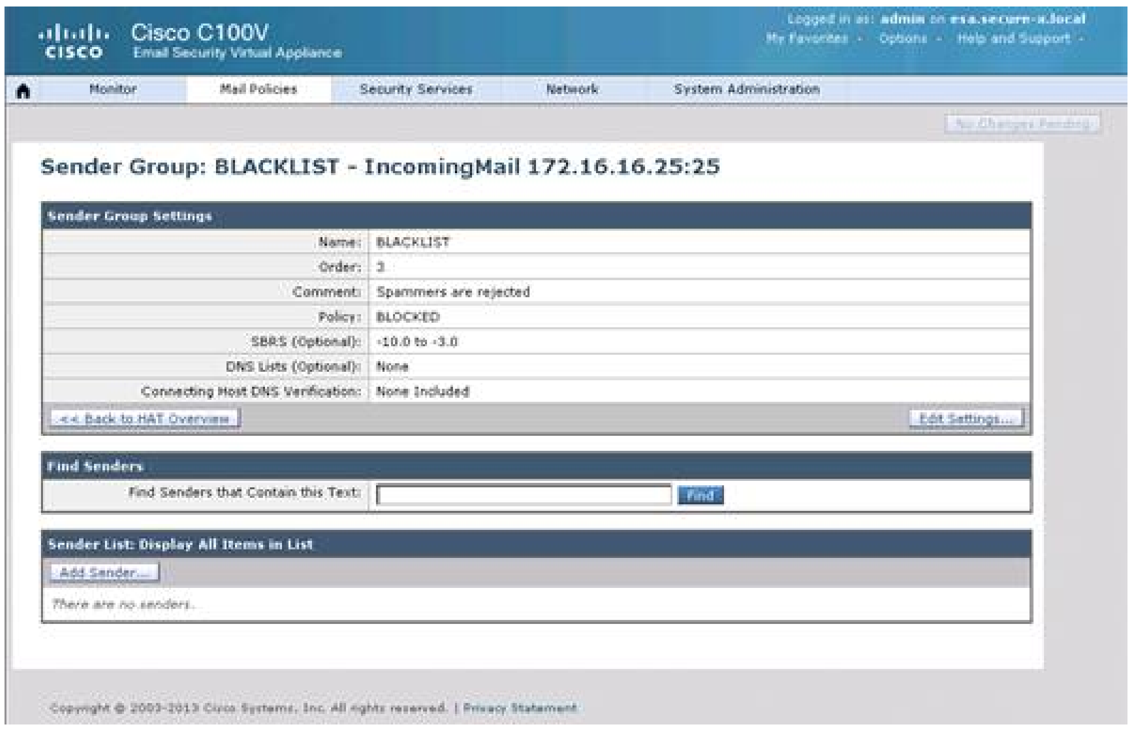
Mail Flow Limits

Rate Limit for Hosts:

Max. Recipients Per Hour: ● Use Default (Unlimited)
○ Unlimited
○

Max. Recipients Per Hour Code: ● Use Default (452)
○

Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)



Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites • Options • Help and Support •
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Sender Group: BLACKLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	BLACKLIST
Order:	3
Comment:	Spammers are rejected
Policy:	BLOCKED
SBRS (Optional):	-10.0 to -3.0
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

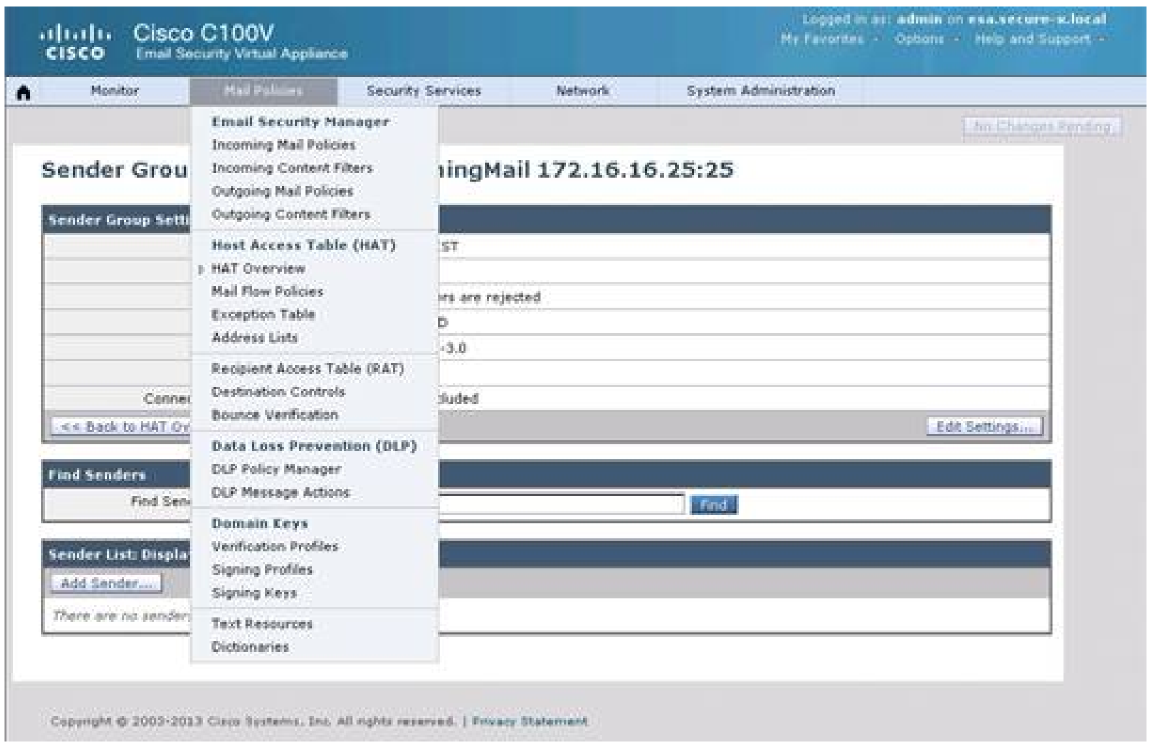
Find Senders

Find Senders that Contain this Text:

Sender List: Display All Items in List

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



Sender Grou… …ingMail 172.16.16.25:25

Sender Group Setti…

…ST

…rs are rejected

…D

…-3.0

Connec… …luded

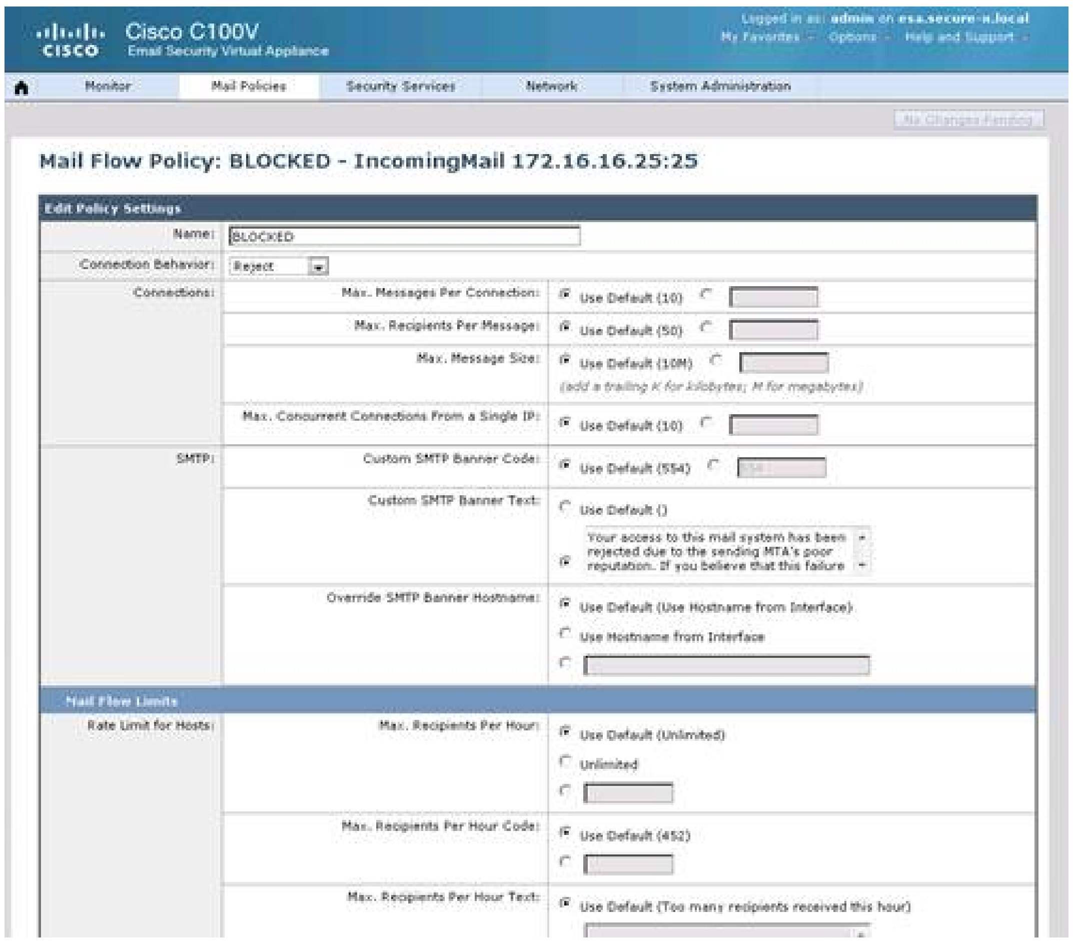
Find Senders

Find Sen…

Sender List: Displa…

There are no sender…

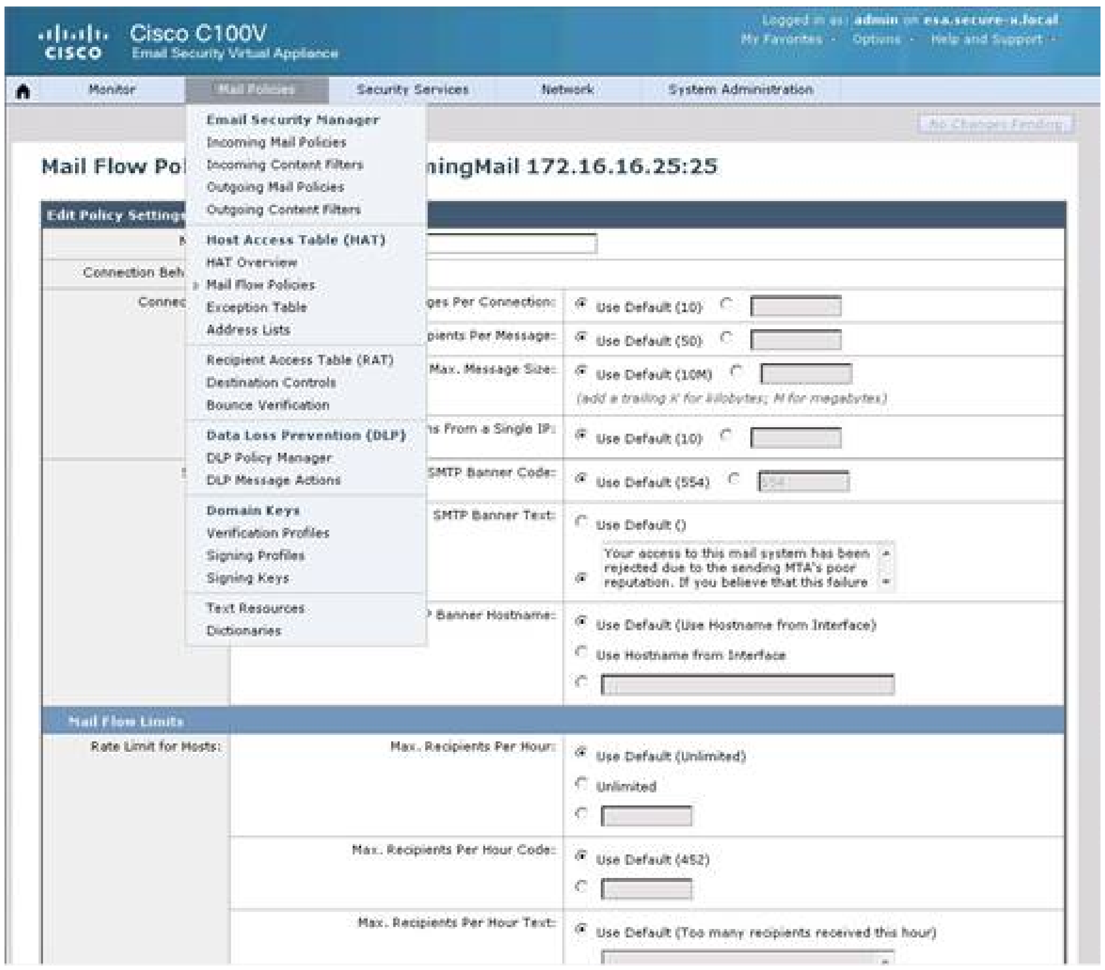
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor | Mail Policies | Security Services | Network | System Administration
No Changes Pending

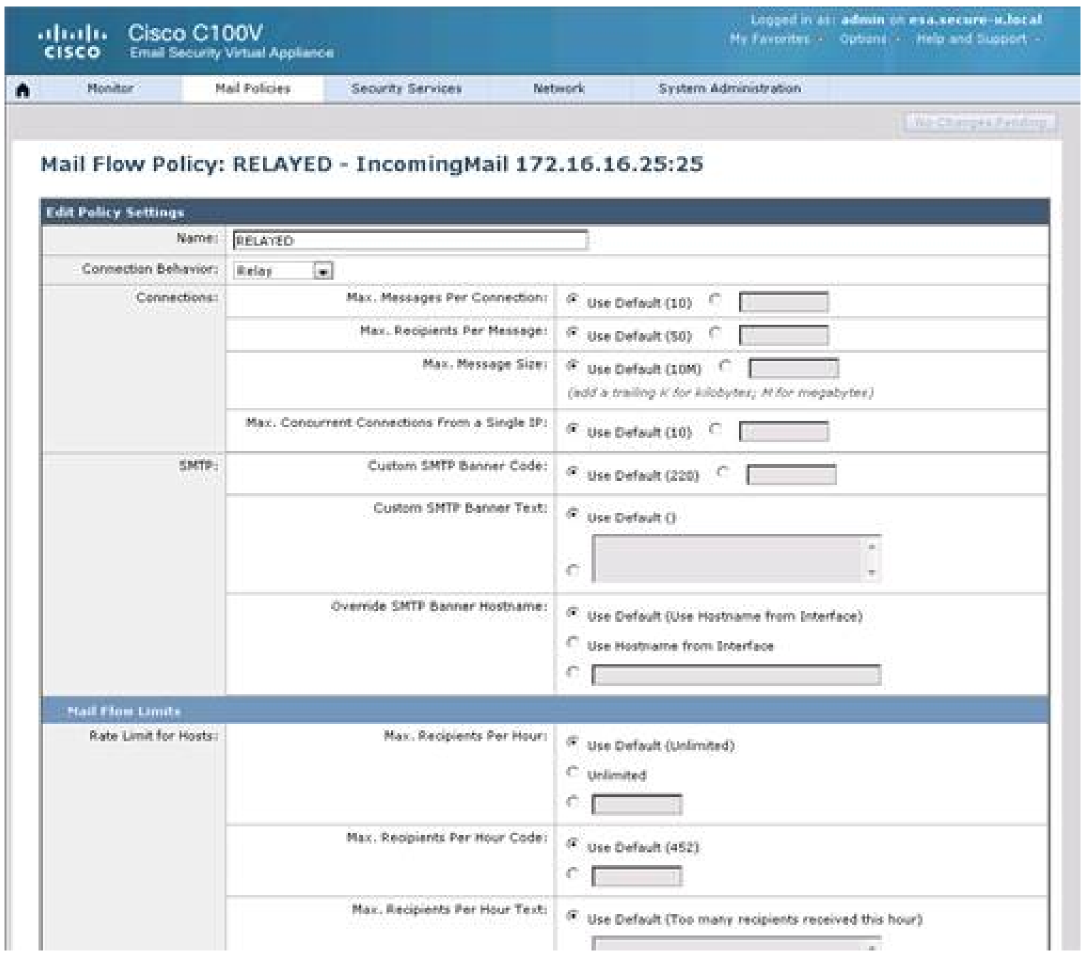
Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25

Edit Policy Settings
Name: BLOCKED
Connection Behavior: Reject
Connections: Max. Messages Per Connection: ● Use Default (10) ○
Max. Recipients Per Message: ● Use Default (50) ○
Max. Message Size: ● Use Default (10M) ○
(add a trailing K for kilobytes; M for megabytes)
Max. Concurrent Connections From a Single IP: ● Use Default (10) ○
SMTP: Custom SMTP Banner Code: ● Use Default (554) ○ 554
Custom SMTP Banner Text: ○ Use Default ()
● Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure
Override SMTP Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○
Mail Flow Limits
Rate Limit for Hosts: Max. Recipients Per Hour: ● Use Default (Unlimited)
○ Unlimited
○
Max. Recipients Per Hour Code: ● Use Default (452)
○
Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)



Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor | Mail Policies | Security Services | Network | System Administration
No Changes Pending

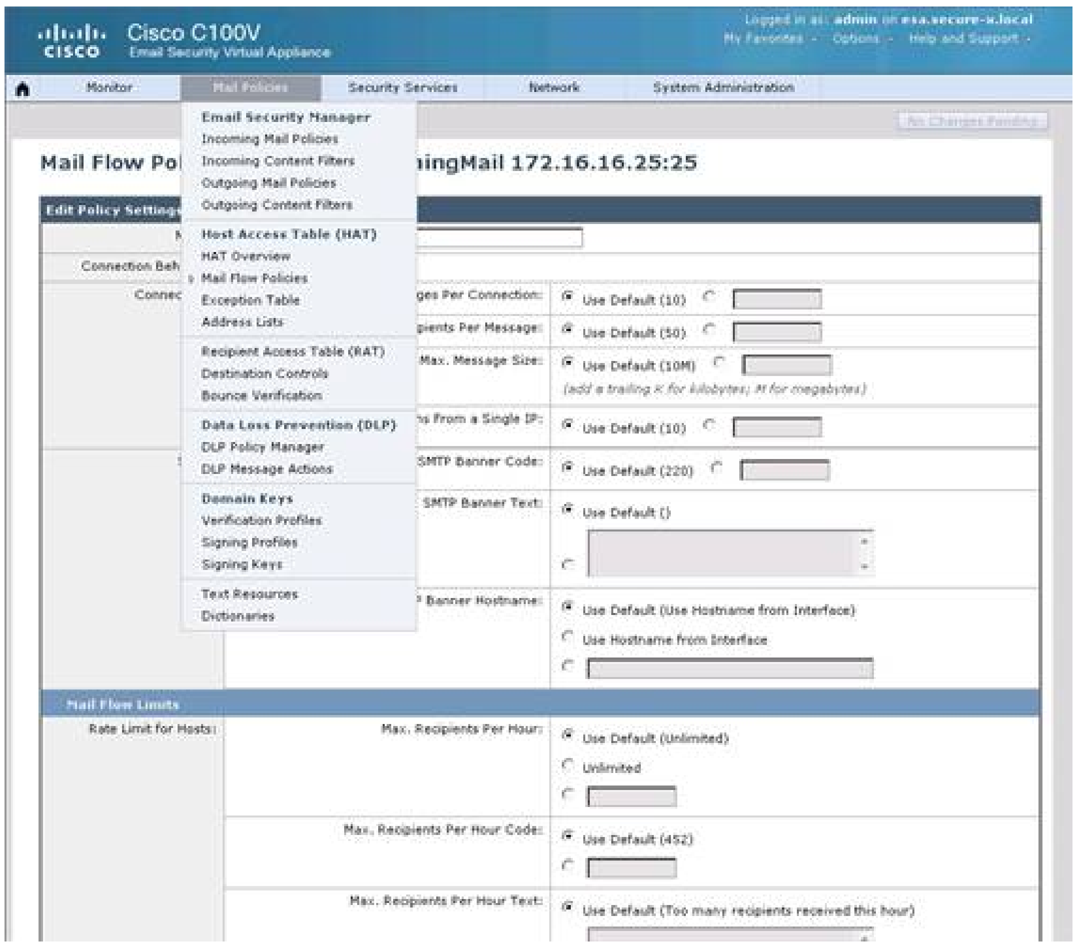
Mail Flow Po[…]ingMail 172.16.16.25:25
Edit Policy Settings
Connection Beh
Connec ges Per Connection: ● Use Default (10) ○
pients Per Message: ● Use Default (50) ○
Max. Message Size: ● Use Default (10M) ○
(add a trailing K for kilobytes; M for megabytes)
s From a Single IP: ● Use Default (10) ○
SMTP Banner Code: ● Use Default (554) ○ 554
SMTP Banner Text: ○ Use Default ()
● Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure
Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○
Mail Flow Limits
Rate Limit for Hosts: Max. Recipients Per Hour: ● Use Default (Unlimited)
○ Unlimited
○
Max. Recipients Per Hour Code: ● Use Default (452)
○
Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)



Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor | Mail Policies | Security Services | Network | System Administration
No Changes Pending

Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25

Edit Policy Settings
Name: RELAYED
Connection Behavior: Relay
Connections: Max. Messages Per Connection: ● Use Default (10) ○
Max. Recipients Per Message: ● Use Default (50) ○
Max. Message Size: ● Use Default (10M) ○
(add a trailing K for kilobytes; M for megabytes)
Max. Concurrent Connections From a Single IP: ● Use Default (10) ○
SMTP: Custom SMTP Banner Code: ● Use Default (220) ○
Custom SMTP Banner Text: ● Use Default ()
○
Override SMTP Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○
Mail Flow Limits
Rate Limit for Hosts: Max. Recipients Per Hour: ● Use Default (Unlimited)
○ Unlimited
○
Max. Recipients Per Hour Code: ● Use Default (452)
○
Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)



Mail Flow Po… …ingMail 172.16.16.25:25

Edit Policy Setting…

Connection Beh…

Connec…

…ges Per Connection: ● Use Default (10) ○

…pients Per Message: ● Use Default (50) ○

Max. Message Size: ● Use Default (10M) ○
(add a trailing K for kilobytes; M for megabytes)

…s From a Single IP: ● Use Default (10) ○

SMTP Banner Code: ● Use Default (220) ○

SMTP Banner Text: ● Use Default ()
○

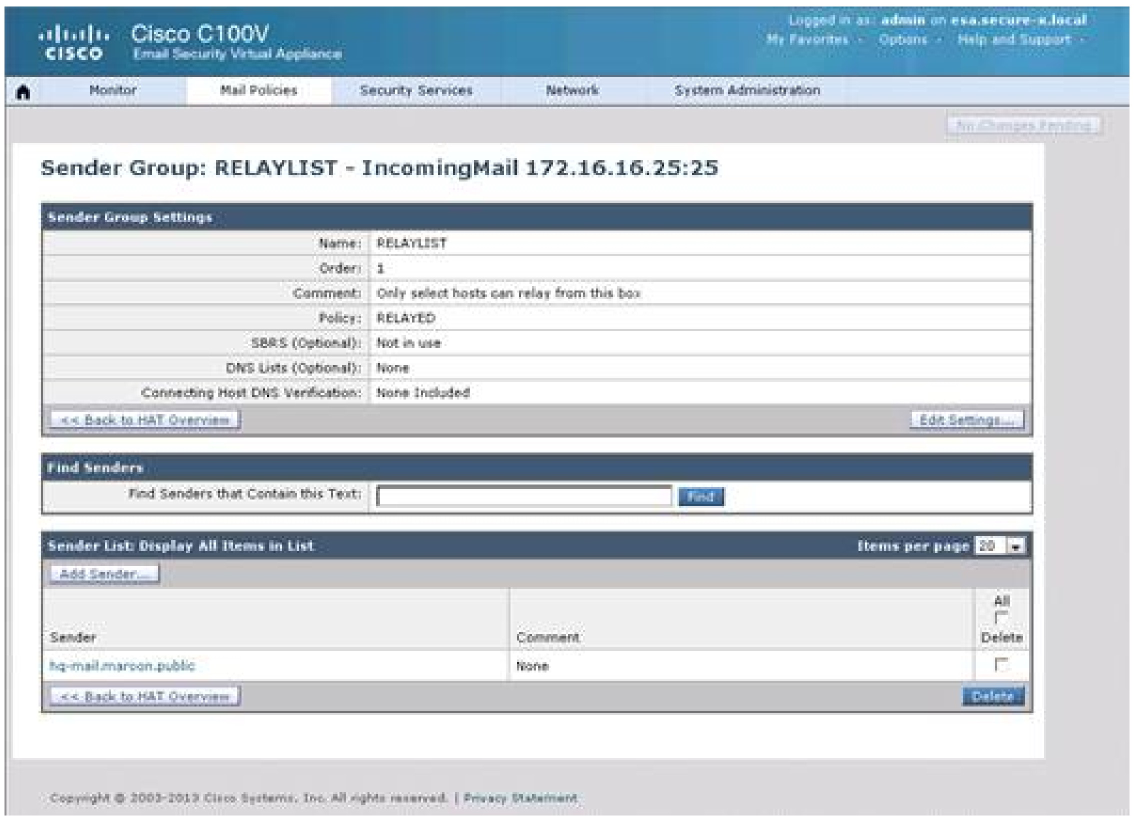
…P Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○

Mail Flow Limits

Rate Limit for Hosts: Max. Recipients Per Hour: ● Use Default (Unlimited)
○ Unlimited
○

Max. Recipients Per Hour Code: ● Use Default (452)
○

Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Sender Group: RELAYLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	RELAYLIST
Order:	1
Comment:	Only select hosts can relay from this box
Policy:	RELAYED
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

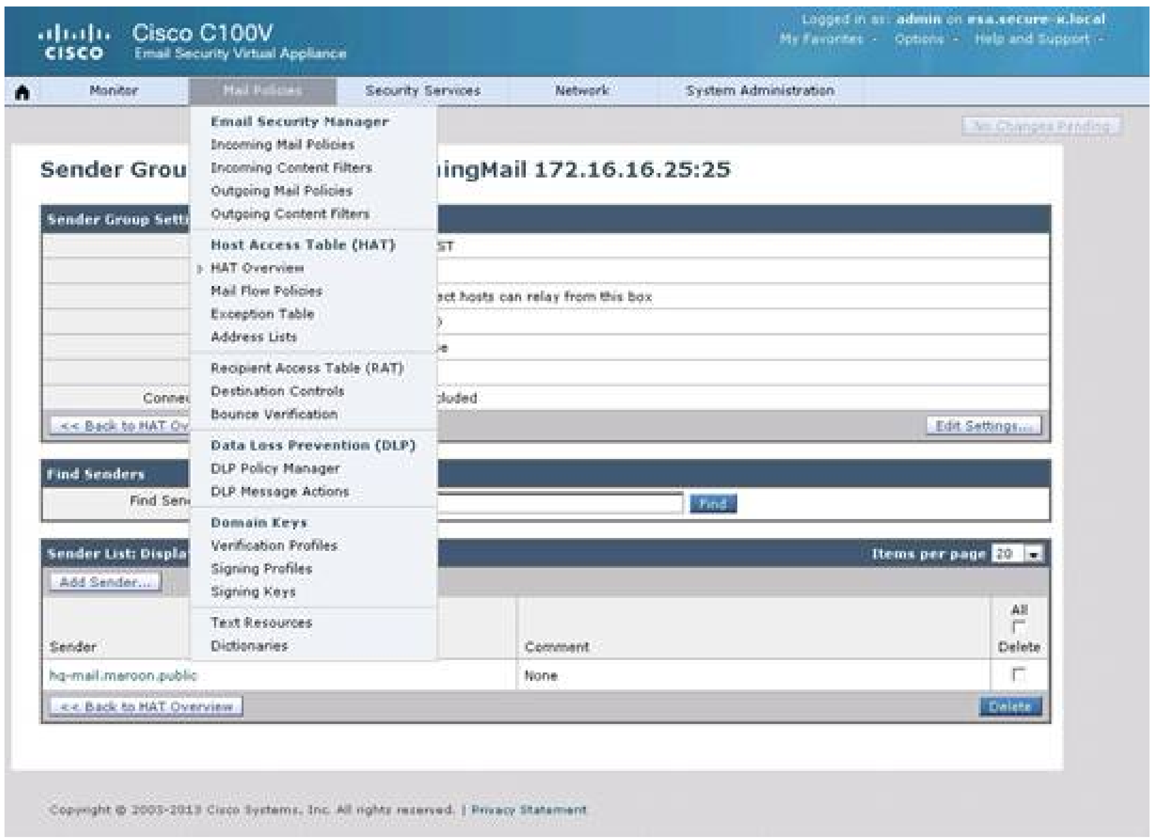
Find Senders

Find Senders that Contain this Text:

Sender List: Display All Items in List — Items per page 20

Sender	Comment	All □ Delete
hq-mail.maroon.public	None	□

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



Sender Grou… …ingMail 172.16.16.25:25

Sender Group Setti…

…ST

…ct hosts can relay from this box

…)

…e

Connec… …luded

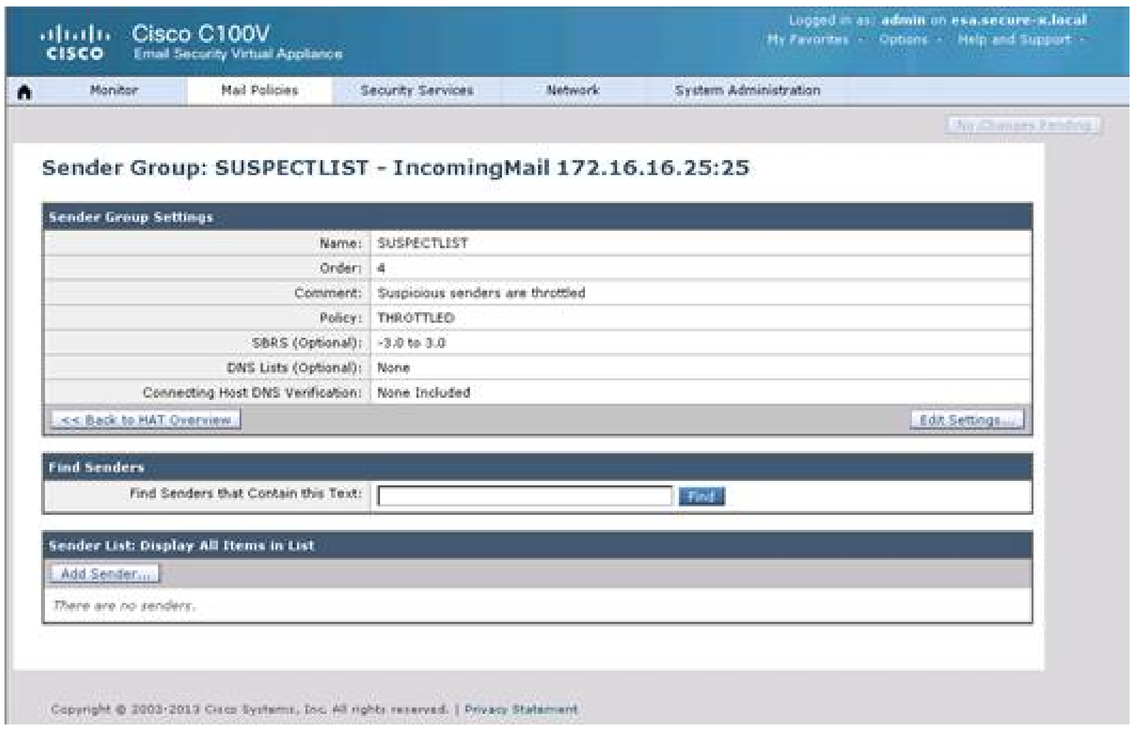
Find Senders

Find Sen…

Sender List: Displa… — Items per page 20

Sender	Comment	All □ Delete
hq-mail.maroon.public	None	□

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Sender Group: SUSPECTLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	SUSPECTLIST
Order:	4
Comment:	Suspicious senders are throttled
Policy:	THROTTLED
SBRS (Optional):	-3.0 to 3.0
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

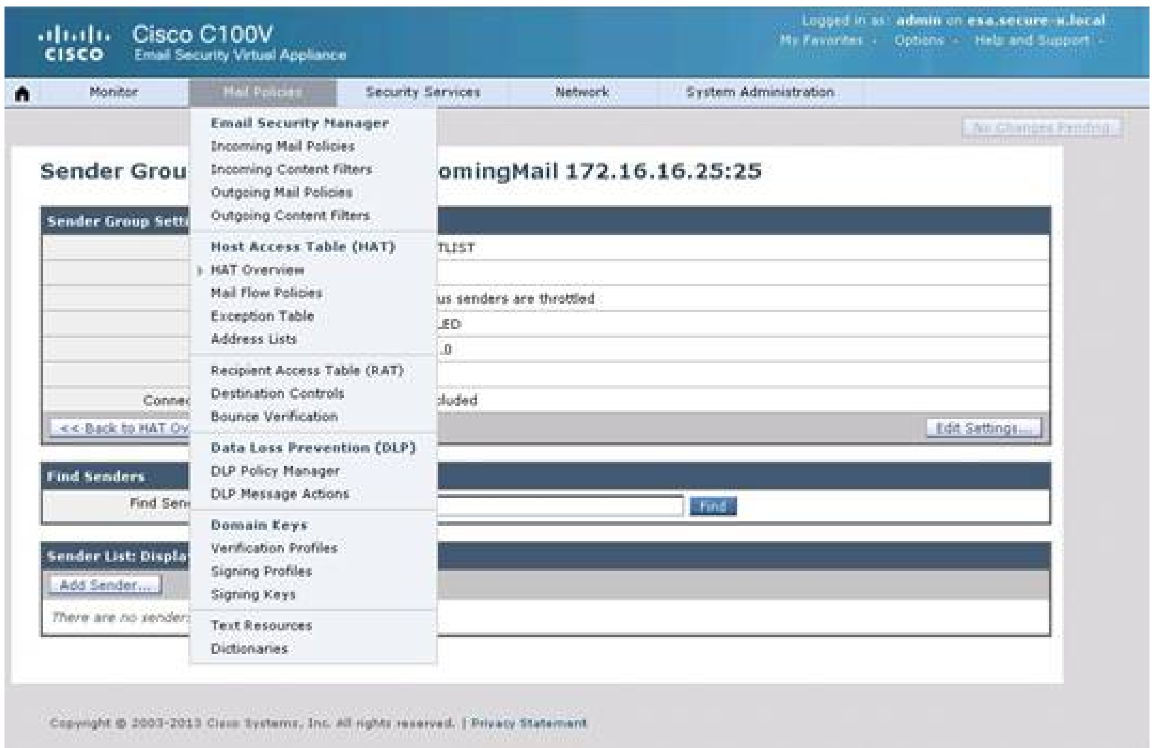
Find Senders

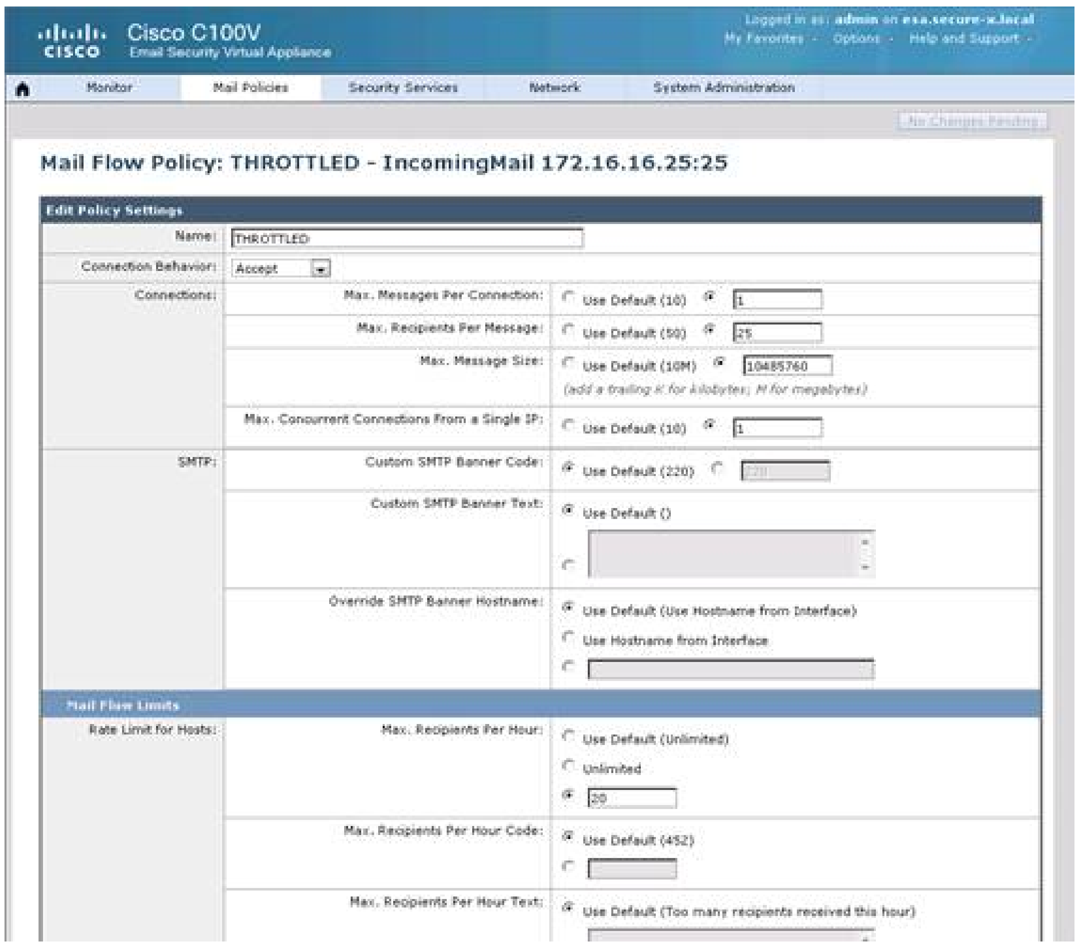
Find Senders that Contain this Text:

Sender List: Display All Items in List

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement




Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

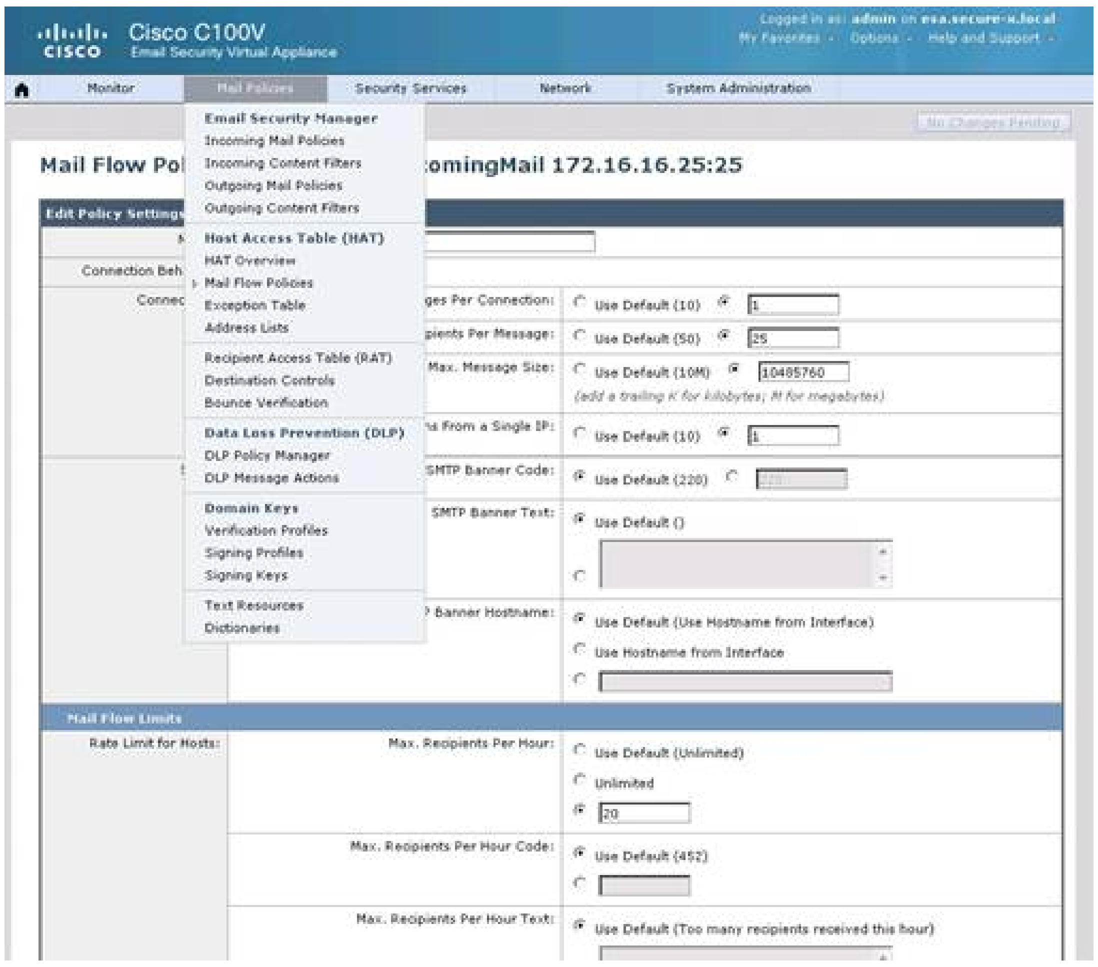
Mail Flow Policy: THROTTLED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name:	THROTTLED	
Connection Behavior:	Accept	
Connections:	Max. Messages Per Connection:	○ Use Default (10) ● 1
	Max. Recipients Per Message:	○ Use Default (50) ● 25
	Max. Message Size:	○ Use Default (10M) ● 10485760 (add a trailing K for kilobytes; M for megabytes)
	Max. Concurrent Connections From a Single IP:	○ Use Default (10) ● 1
SMTP:	Custom SMTP Banner Code:	● Use Default (220) ○ 220
	Custom SMTP Banner Text:	● Use Default () ○
	Override SMTP Banner Hostname:	● Use Default (Use Hostname from Interface) ○ Use Hostname from Interface ○

Mail Flow Limits

Rate Limit for Hosts:	Max. Recipients Per Hour:	○ Use Default (Unlimited) ○ Unlimited ● 20
	Max. Recipients Per Hour Code:	● Use Default (452) ○
	Max. Recipients Per Hour Text:	● Use Default (Too many recipients received this hour)



Mail Flow Pol ... omingMail 172.16.16.25:25

Edit Policy Settings

Connection Beh

Connec ... ges Per Connection: ○ Use Default (10) ● 1

pients Per Message: ○ Use Default (50) ● 25

Max. Message Size: ○ Use Default (10M) ● 10485760
(add a trailing K for kilobytes; M for megabytes)

s From a Single IP: ○ Use Default (10) ● 1

SMTP Banner Code: ● Use Default (220) ○

SMTP Banner Text: ● Use Default ()
○

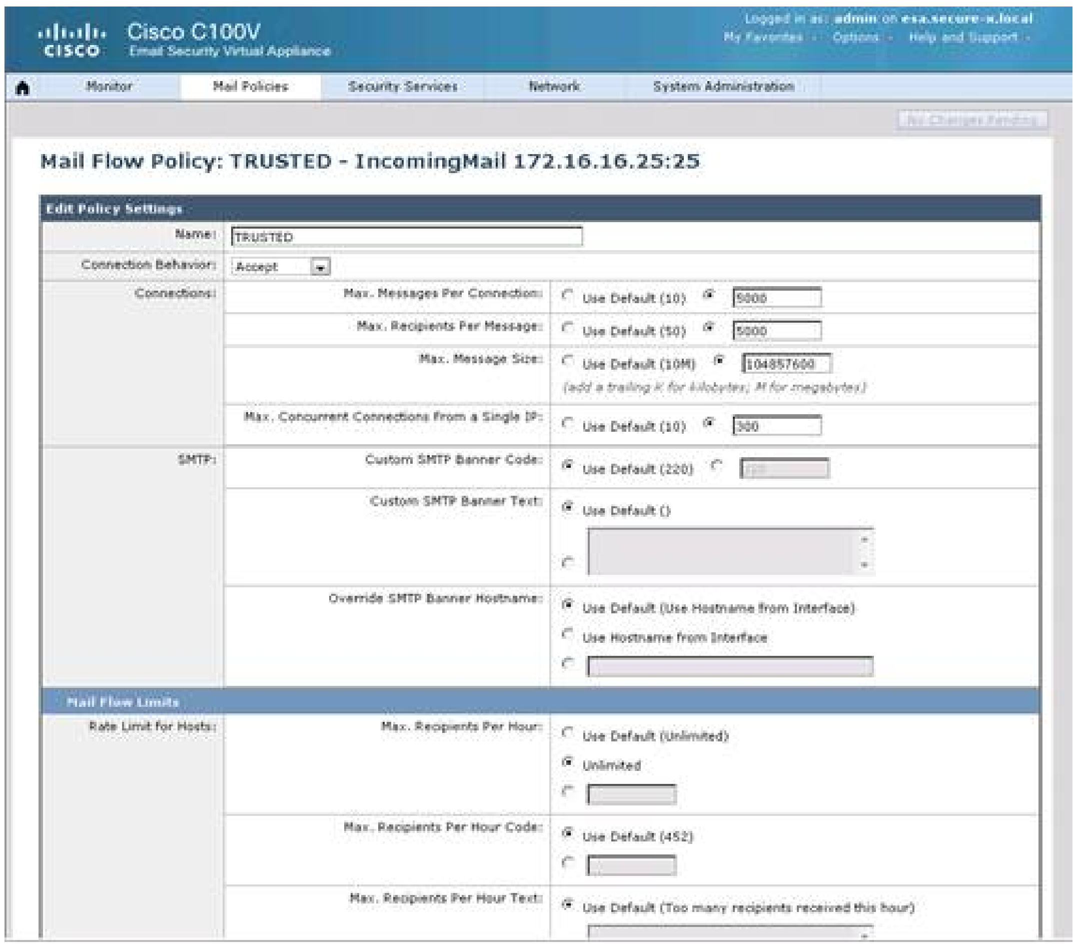
Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○

Mail Flow Limits

Rate Limit for Hosts: Max. Recipients Per Hour: ○ Use Default (Unlimited)
○ Unlimited
● 20

Max. Recipients Per Hour Code: ● Use Default (452)
○

Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name: TRUSTED

Connection Behavior: Accept

Connections: Max. Messages Per Connection: ○ Use Default (10) ● 5000

Max. Recipients Per Message: ○ Use Default (50) ● 5000

Max. Message Size: ○ Use Default (10M) ● 104857600
(add a trailing K for kilobytes; M for megabytes)

Max. Concurrent Connections From a Single IP: ○ Use Default (10) ● 300

SMTP: Custom SMTP Banner Code: ● Use Default (220) ○

Custom SMTP Banner Text: ● Use Default ()
○

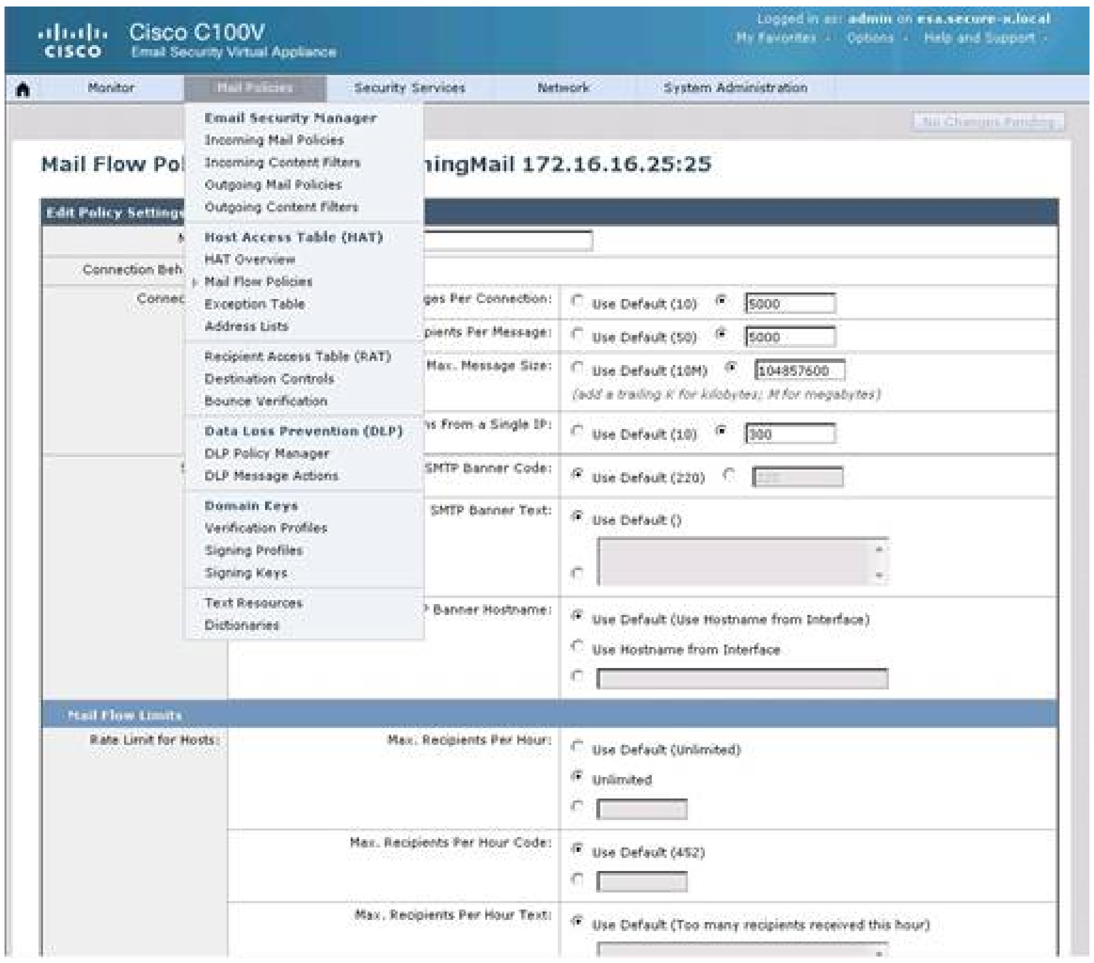
Override SMTP Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○

Mail Flow Limits

Rate Limit for Hosts: Max. Recipients Per Hour: ○ Use Default (Unlimited)
● Unlimited
○

Max. Recipients Per Hour Code: ● Use Default (452)
○

Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)



Mail Flow Pol ... ingMail 172.16.16.25:25

Edit Policy Settings

Connection Beh

Connec ... ges Per Connection: ○ Use Default (10) ● 5000

pients Per Message: ○ Use Default (50) ● 5000

Max. Message Size: ○ Use Default (10M) ● 104857600
(add a trailing K for kilobytes; M for megabytes)

s From a Single IP: ○ Use Default (10) ● 300

SMTP Banner Code: ● Use Default (220) ○

SMTP Banner Text: ● Use Default ()
○

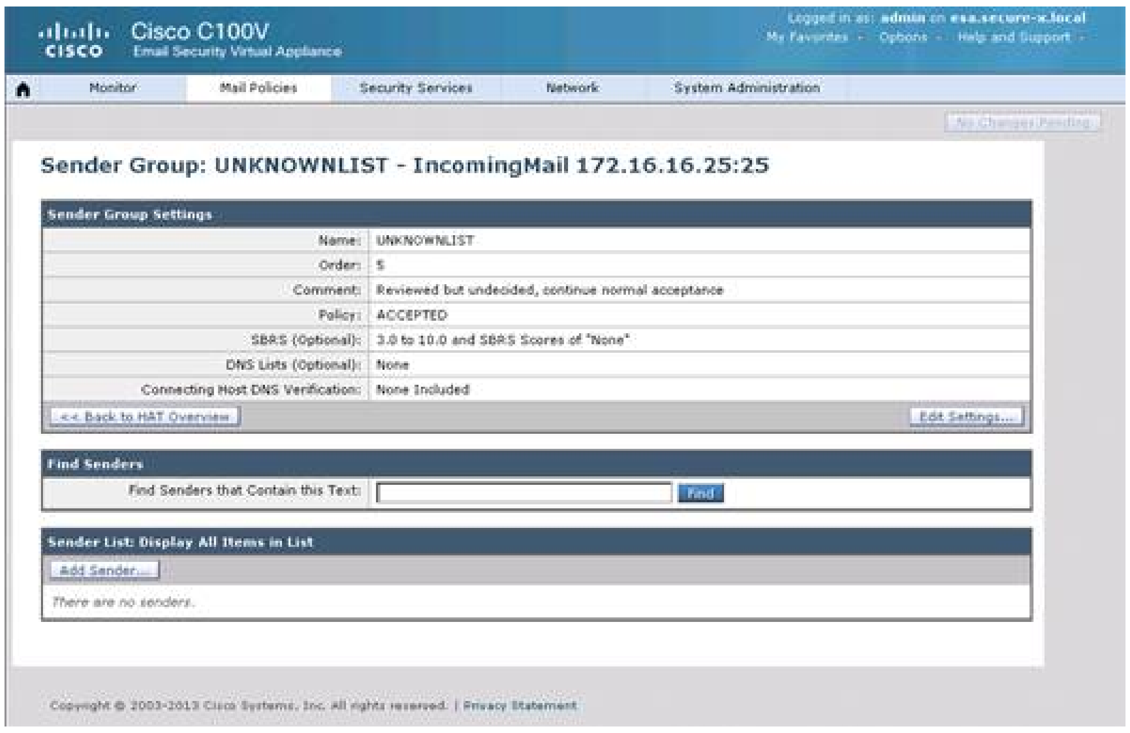
Banner Hostname: ● Use Default (Use Hostname from Interface)
○ Use Hostname from Interface
○

Mail Flow Limits

Rate Limit for Hosts: Max. Recipients Per Hour: ○ Use Default (Unlimited)
● Unlimited
○

Max. Recipients Per Hour Code: ● Use Default (452)
○

Max. Recipients Per Hour Text: ● Use Default (Too many recipients received this hour)


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Sender Group: UNKNOWNLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	UNKNOWNLIST
Order:	5
Comment:	Reviewed but undecided, continue normal acceptance
Policy:	ACCEPTED
SBRS (Optional):	3.0 to 10.0 and SBRS Scores of "None"
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

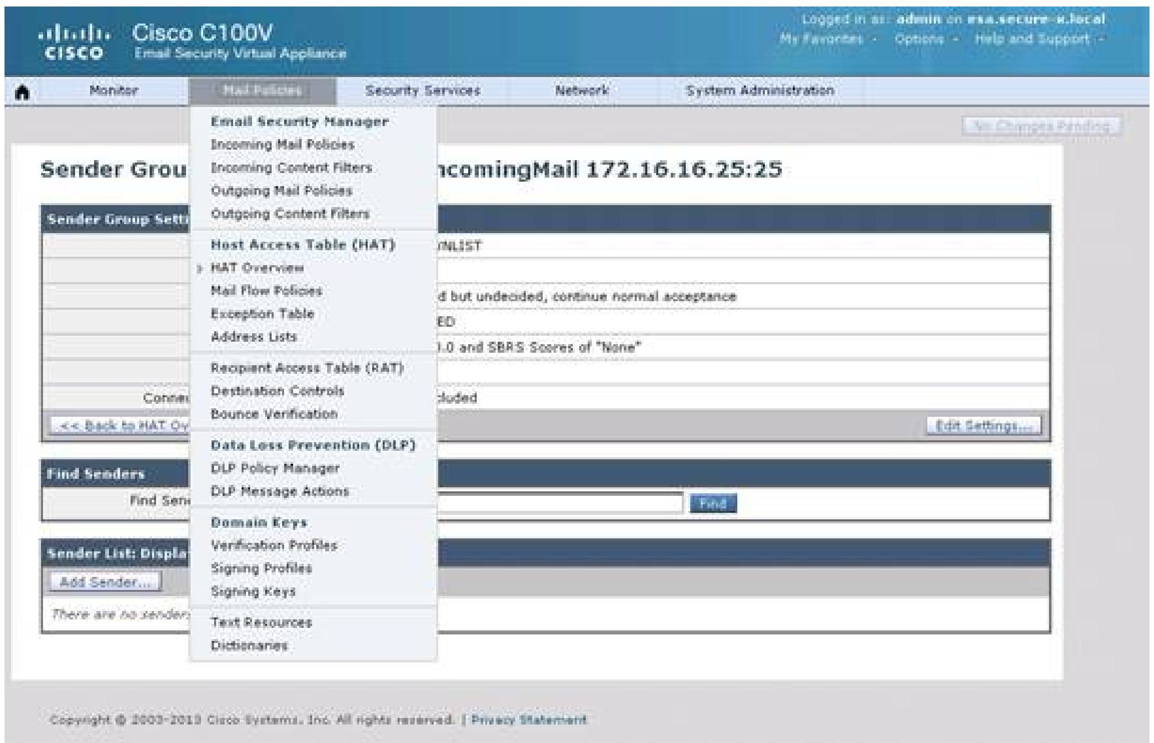
Find Senders

Find Senders that Contain this Text:

Sender List: Display All Items in List

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



Sender Grou ncomingMail 172.16.16.25:25

Sender Group Setti

NLIST

d but undecided, continue normal acceptance

ED

.0 and SBRS Scores of "None"

Conne luded

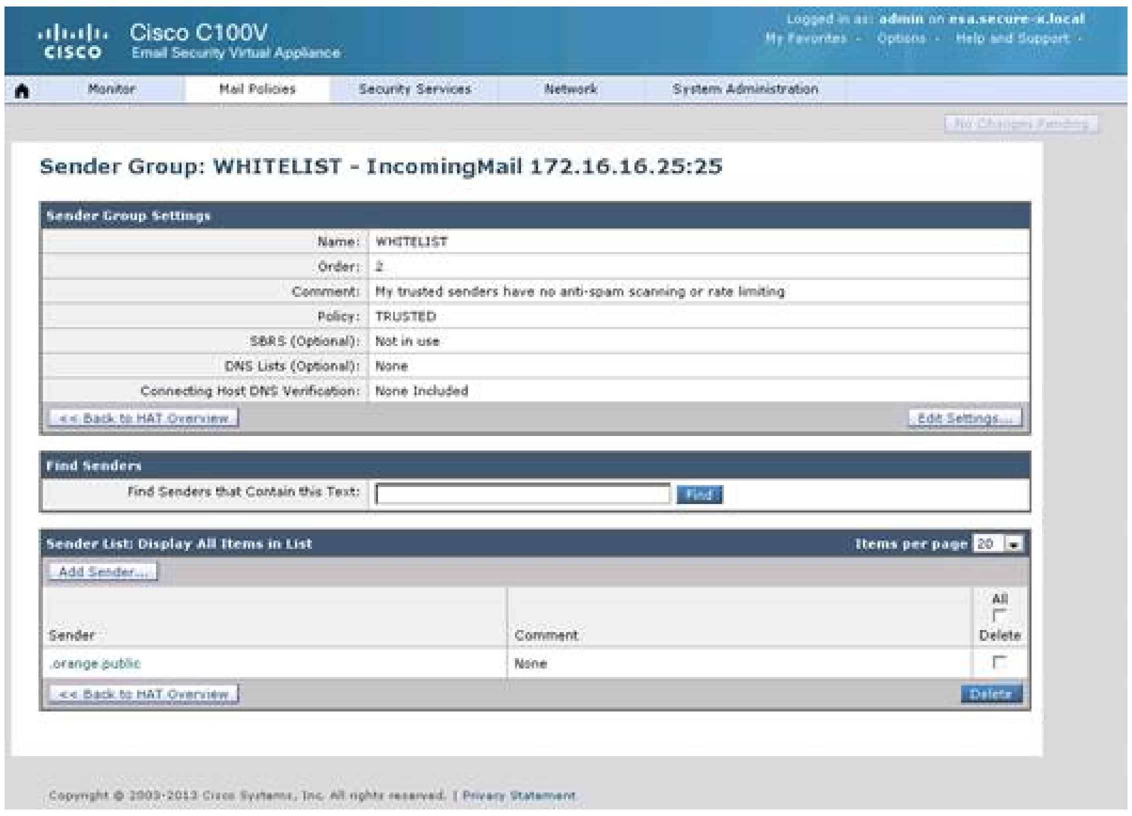
Find Senders

Find Sen

Sender List: Displa

There are no sender

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement


Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Sender Group: WHITELIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	WHITELIST
Order:	2
Comment:	My trusted senders have no anti-spam scanning or rate limiting
Policy:	TRUSTED
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

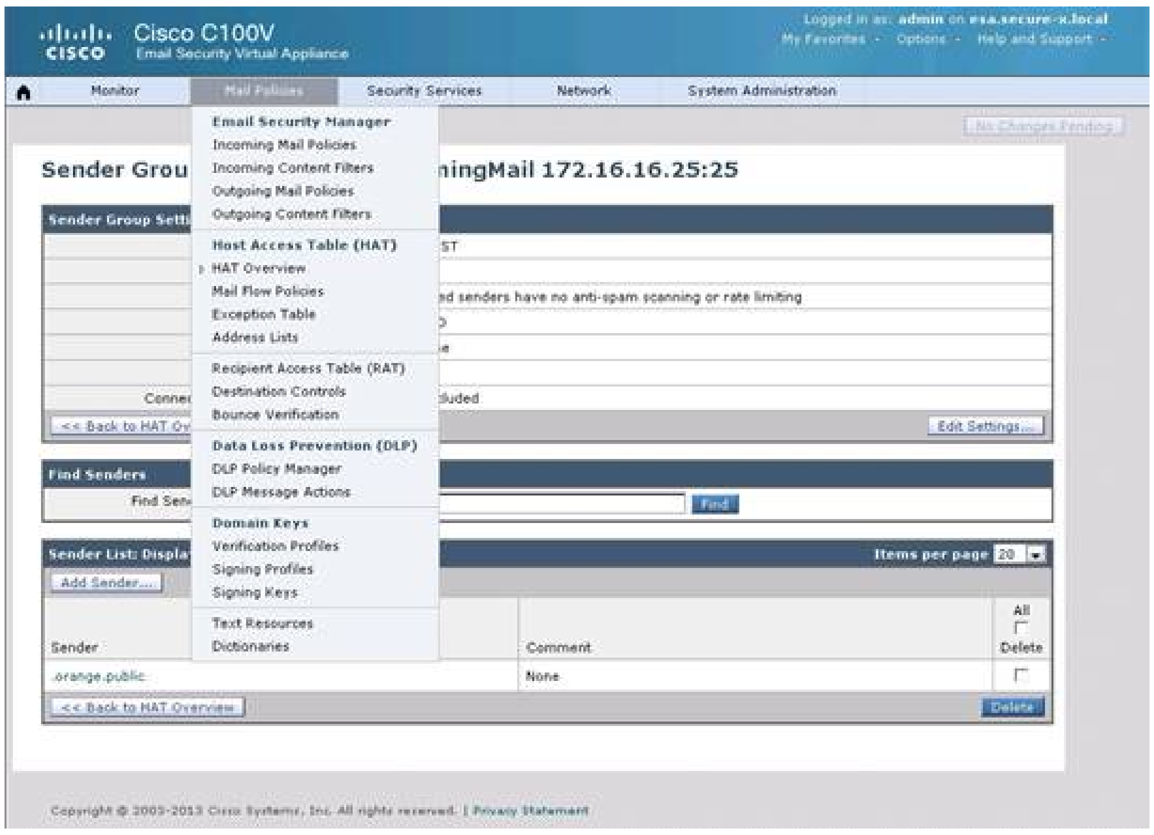
Find Senders

Find Senders that Contain this Text:

Sender List: Display All Items in List — Items per page 20

Sender	Comment	All □ Delete
.orange.public	None	□

<< Back to HAT Overview
Delete
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement



Sender Grou ningMail 172.16.16.25:25

Sender Group Setti

ST

ed senders have no anti-spam scanning or rate limiting

Conne luded

Find Senders

Find Sen

Sender List: Displa Items per page 20

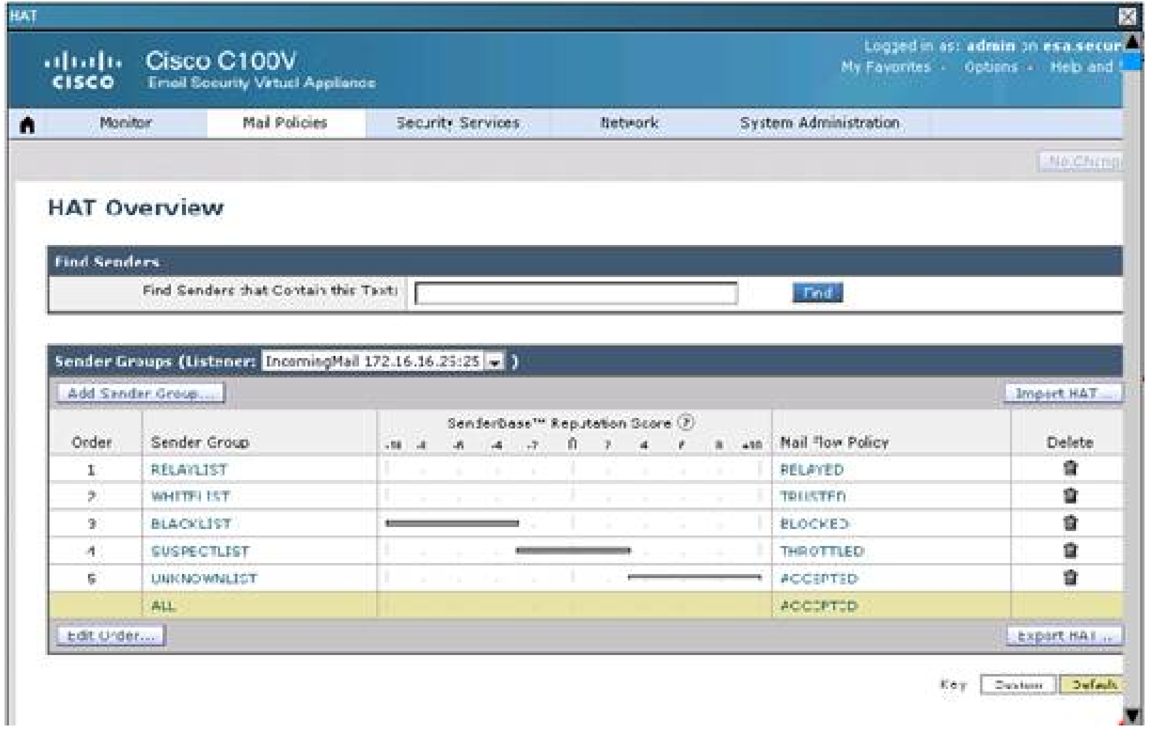
Sender	Comment	All □ Delete
.orange.public	None	□

What is the maximum number of recipients per hour that the Cisco Email Security Appliance will accept from the green.public domain?

A. 1
B. 20
C. 25
D. 50
E. 5000
F. Unlimited

Answer: C

Explanation:
From the instructions we know that the green.public domain has been assigned a reputation score of 2. From below we know that a reputation score of 2 belongs to the SUSPECTLIST, which has a policy of “THROTTLED”:
Capture



HAT Overview

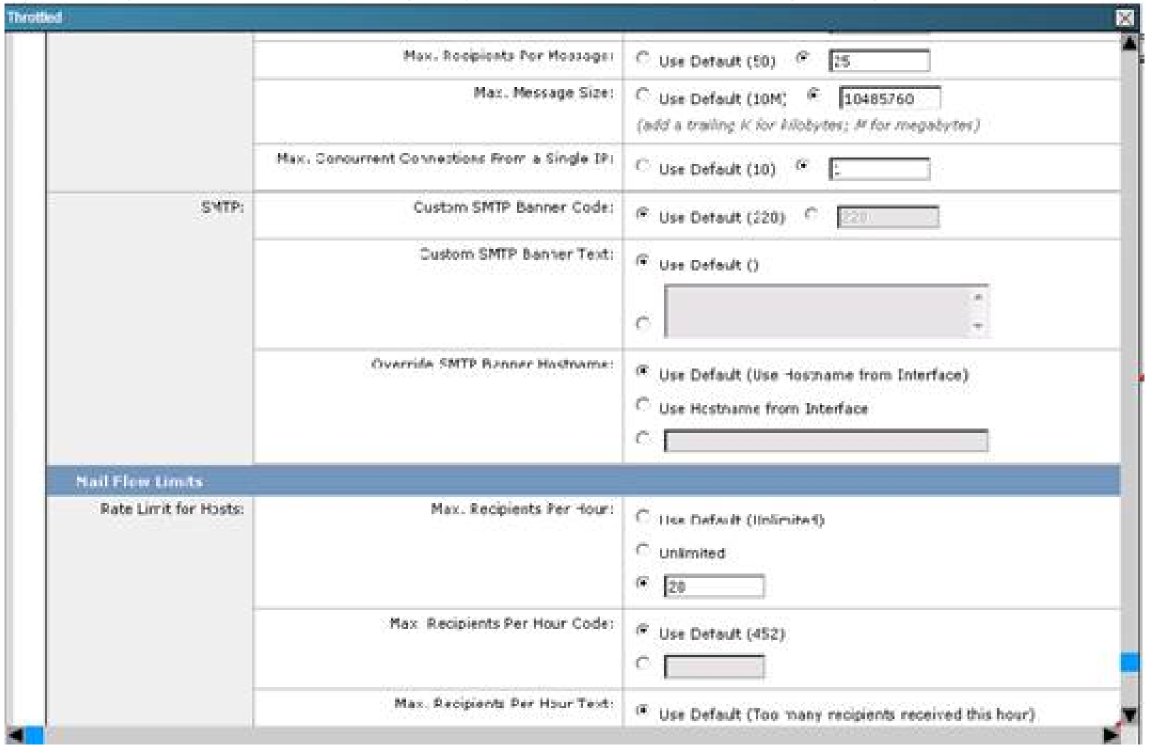
Find Senders

Find Senders that Contain this Text:

Sender Groups (Listener: IncomingMail 172.16.16.25:25)

Order	Sender Group	SenderBase™ Reputation Score	Mail Flow Policy	Delete
1	RELAYLIST		RELAYED	🗑
2	WHITELIST		TRUSTED	🗑
3	BLACKLIST		BLOCKED	🗑
4	SUSPECTLIST		THROTTLED	🗑
5	UNKNOWNLIST		ACCEPTED	🗑
	ALL		ACCEPTED	

By clicking on the THROTTLED policy we see that the max recipients per hour has been set to 20: Capture



	Max. Recipients Per Message:	○ Use Default (50) ● 25
	Max. Message Size:	○ Use Default (10M) ● 10485760 (add a trailing K for kilobytes; M for megabytes)
	Max. Concurrent Connections From a Single IP:	○ Use Default (10) ● 1
SMTP:	Custom SMTP Banner Code:	● Use Default (220) ○ 220
	Custom SMTP Banner Text:	● Use Default () ○
	Override SMTP Banner Hostname:	● Use Default (Use Hostname from Interface) ○ Use Hostname from Interface ○
Mail Flow Limits		
Rate Limit for Hosts:	Max. Recipients Per Hour:	○ Use Default (Unlimited) ○ Unlimited ● 20
	Max. Recipients Per Hour Code:	● Use Default (452) ○
	Max. Recipients Per Hour Text:	● Use Default (Too many recipients received this hour)

NEW QUESTION 375
- (Exam Topic 4)
When attempting to tunnel FTP traffic through a stateful firewall that may be performing NAT or PAT, which type of VPN tunneling should be used to allow the VPN traffic through the stateful firewall?

A. clientless SSL VPN
B. IPsec over TCP
C. Smart Tunnel
D. SSL VPN plug-ins

Answer: B

NEW QUESTION 378
- (Exam Topic 4)
Which option describes device trajectory on Cisco Advanced Malware protection for End[points? It show which devices on the network receive the file.

A. it shows a full packet capture of the file.
B. it show the file path on a host.
C. it shows the file path on a host.
D. it show what a file did on a host.

Answer: B

NEW QUESTION 381
- (Exam Topic 4)
Which three webtype ACL statements are correct? (Choose three.)

A. are assigned per-Connection Profile
B. are assigned per-user or per-Group Policy
C. can be defined in the Cisco AnyConnect Profile Editor
D. supports URL pattern matching
E. supports implicit deny all at the end of the ACL
F. supports standard and extended webtype ACLs

Answer: BDE

NEW QUESTION 382
- (Exam Topic 4)
An engineer is used the reporting feature on a WSA. Which option must they consider about the reporting capabilities?

A. Reports can be viewed for a particular domain, user or category.
B. Detail reports require a separate license.
C. Reports to view system activity over a specific period of time do not exist.
D. report must be scheduled manually.

Answer: D

NEW QUESTION 387
- (Exam Topic 4)
Which two Snort actions are available by default creating Snort rules, regardless of deployment mode? (Choose two)

A. activate
B. sdrop
C. drop
D. pass
E. reject

Answer: AD

NEW QUESTION 390
- (Exam Topic 4)
Which statement regarding hashing is correct?

A. MD5 produces a 64-bit message digest
B. SHA-1 produces a 160-bit message digest
C. MD5 takes more CPU cycles to compute than SHA-1.
D. Changing 1 bit of the input to SHA-1 can change up to 5 bits in the output.

Answer: B

NEW QUESTION 394
- (Exam Topic 4)
Which option is omitted from a query on a ESA virtual appliance?

A. raidrable
B. FailoverHealthy

C. keyExpiration
D. CPUUtilizationExceeded

Answer: A

NEW QUESTION 397
- (Exam Topic 4)
Which action inspects packets in IPS?

A. Monitor
B. Trust
C. Block
D. Allow
E. Default Action

Answer: AE

NEW QUESTION 402
- (Exam Topic 4)
What Software can be installed on the Cisco 4100 series appliance?

A. FTD
B. ASA
C. ASAv
D. FMC

Answer: A

NEW QUESTION 405
- (Exam Topic 4)
By default, which access rule is applied inbound to the inside interface?

A. All IP traffic is denied.
B. All IP traffic is permitted.
C. All IP traffic sourced from any source to any less secure network destinations is permitted.
D. All IP traffic sourced from any source to any more secure network destinations is permitted

Answer: C

NEW QUESTION 407
- (Exam Topic 4)
An engineer is troubleshooting authentication settings on a WSA. Which command accomplishes this action?

A. testauthconfig
B. testconfgauth
C. verifyconfigauth
D. verifyauth

Answer: A

NEW QUESTION 410
- (Exam Topic 4)
An engineer is using policy trace tool to debug how a message is processed by the ESA. Which option is the expected behavior from the tool?

A. The sections of configuration tested by the tool are performed in a random order.
B. A message body cannot be populated via an upload.
C. The test message created by the tool is distributed.
D. A message is emulated as being accepted by a listener

Answer: D

NEW QUESTION 412
- (Exam Topic 4)
Which two are valid suppression types on a Cisco Next Generation Intrusion Prevention System?

A. Port
B. Rule
C. Source
D. Application
E. Protocol

Answer: BC

NEW QUESTION 417
- (Exam Topic 4)

A Cisco AnyConnect user profile can be pushed to the PC of a remote user from a Cisco ASA. Which three user profile parameters are configurable? (Choose three.)

A. Backup Server list
B. DTLS Override
C. Auto Reconnect
D. Simultaneous Tunnels
E. Connection Profile Lock
F. Auto Update

Answer: ACF

NEW QUESTION 420
- (Exam Topic 4)
Which two types of digital certificate enrollment processes are available for the Cisco ASA security appliance? (Choose two.)

A. LDAP
B. FTP
C. TFTP
D. HTTP
E. SCEP
F. Manual

Answer: EF

NEW QUESTION 425
- (Exam Topic 4)
Which tools are used to analyze Endpoints for AMP file activity performed on endpoints?

A. File Trajectory
B. Device Trajectory
C. File Analysis
D. Prevalence

Answer: C

Explanation:
Explanation
Cisco AMP for Endpoints File Analysis (Figure 4), backed by the Talos Security Intelligence and Research Group and powered by AMP’s built-in sandboxing technology (Threat Grid), provides a safe, highly secure sandbox environment for you to analyze the behavior of malware and suspect files. File analysis produces detailed information on file behavior, including the severity of behaviors, the original filename, screenshots of the malware executing, and sample packet captures.Armed with this information, you’ll have a better understanding of what is necessary to contain the outbreak and block future attacks.

NEW QUESTION 426
- (Exam Topic 4)
Which of the following are Cisco FirePOWER Application Layer Preprocessors? (Choose 2).

A. SIP preprocessor
B. HTTP preprocessor
C. ICMP preprocessor
D. Modbus

Answer: AB

NEW QUESTION 430
- (Exam Topic 4)
Which access control policy action must be selected to inspect traffic for malware using cisco AMP for Networks?

A. monitor
B. inspect
C. trust
D. allow

Answer: D

NEW QUESTION 431
- (Exam Topic 4)
Upon receiving a digital certificate, what are three steps that a Cisco ASA will perform to authenticate the digital certificate? (Choose three.)

A. The identity certificate validity period is verified against the system clock of the Cisco ASA.
B. Identity certificates are exchanged during IPsec negotiations.
C. The identity certificate signature is validated by using the stored root certificate.
D. The signature is validated by using the stored identity certificate.
E. If enabled, the Cisco ASA locates the CRL and validates the identity certificate.

Answer: ACE

NEW QUESTION 432
- (Exam Topic 4)
What are 2 types or forms of suppression on a FirePower policy (or FTD)?

A. source
B. port
C. rule
D. protocol
E. application

Answer: AC

NEW QUESTION 433
- (Exam Topic 4)
Which Cisco ESA command is used to edit the ciphers that are used for GUI access?

A. interfaceconfig
B. etherconfig
C. certconfig
D. sslconfig

Answer: D

NEW QUESTION 434
......

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 300-210 Exam with Our Prep Materials Via below:

https://www.certleader.com/300-210-dumps.html