

300-207 Dumps

Implementing Cisco Threat Control Solutions (SITCS)

<https://www.certleader.com/300-207-dumps.html>



NEW QUESTION 1

Which Cisco technology prevents targeted malware attacks, provides data loss prevention and spam protection, and encrypts email?

- A. SBA
- B. secure mobile access
- C. IPv6 DMZ web service
- D. ESA

Answer: D

NEW QUESTION 2

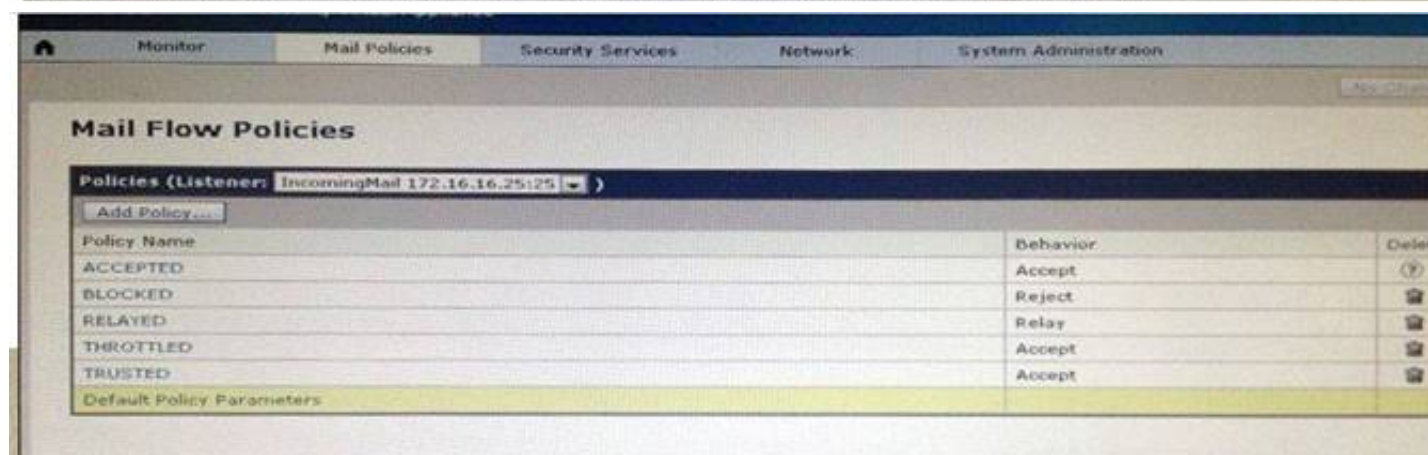
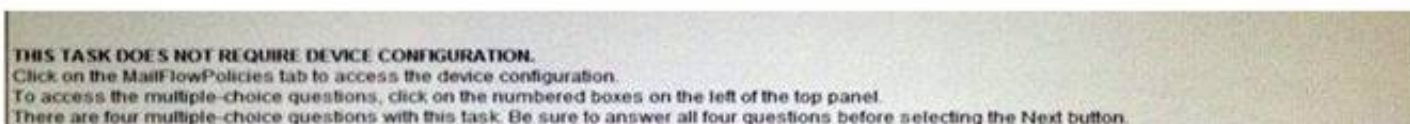
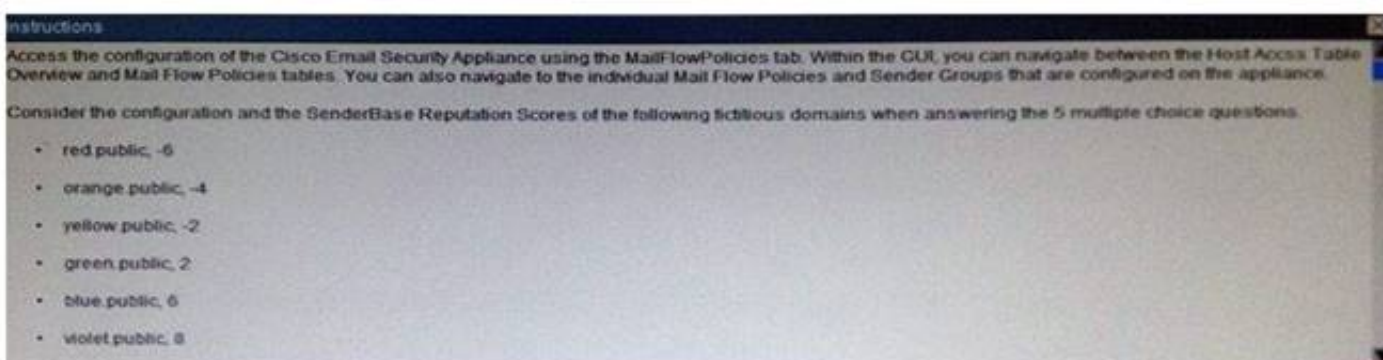
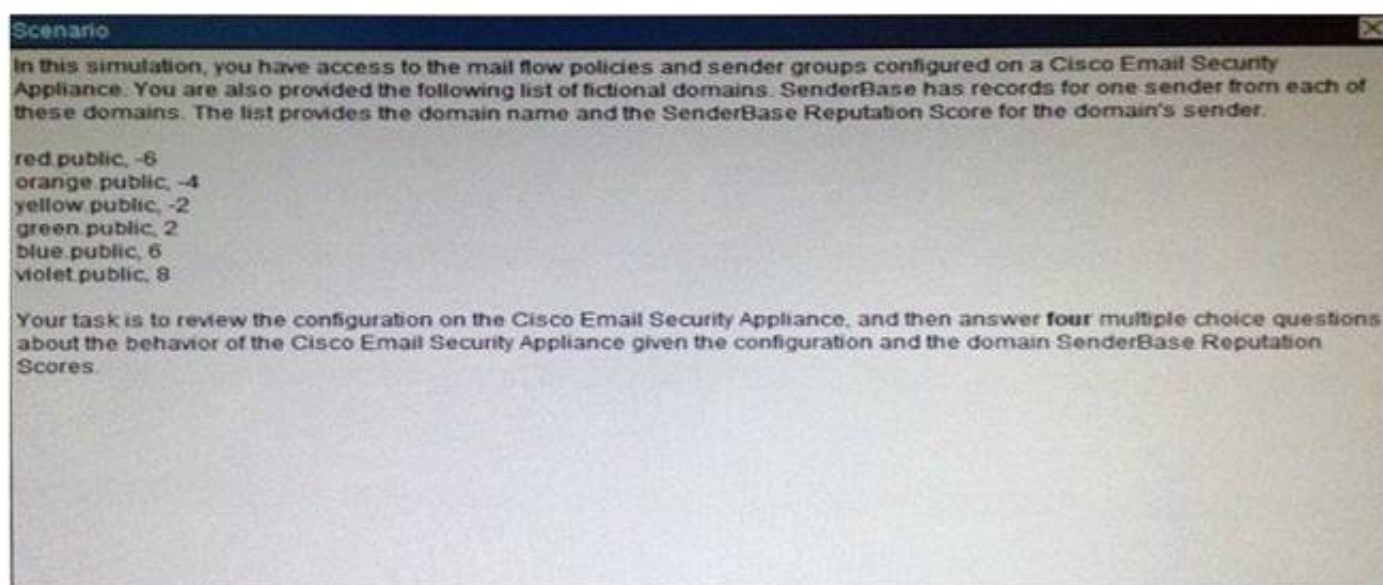
Which command verifies that CWS redirection is working on a Cisco IOS router?

- A. show content-scan session active
- B. show content-scan summary
- C. show interfaces stats
- D. show sessions

Answer: A

NEW QUESTION 3

Refer to the exhibit.



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

- A. viole
- B. public
- C. viole
- D. public and blu
- E. public
- F. viole
- G. Public, blu
- H. Public and green.public

- I. re
- J. public orang
- K. publicre
- L. public and orang
- M. public

Answer: B

NEW QUESTION 4

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 5

On which platforms can you run CWS connector? (Choose two)

- A. Cisco ASA Firewall
- B. Cisco IPS module
- C. Standalone deployment
- D. Cisco ISR router
- E. Cisco Firepower NGIPS

Answer: AD

NEW QUESTION 6

What are three arguments that can be used with the show content-scan command in Cisco IOS software? (Choose three)

- A. session
- B. data
- C. verbose
- D. buffer
- E. summary
- F. statistics

Answer: AEF

NEW QUESTION 7

Which piece of information is required to perform a policy trace for the Cisco WSA?

- A. the URL to trace
- B. the source IP address of the trace
- C. authentication credentials to make the request
- D. the destination IP address of the trace

Answer: A

NEW QUESTION 8

Which three zones are used for anomaly detection in a Cisco IPS? (Choose three.)

- A. internal zone
- B. external zone
- C. illegal zone
- D. inside zone
- E. outside zone
- F. DMZ zone

Answer: ABC

NEW QUESTION 9

When you deploy a sensor to send connection termination requests, which additional traffic-monitoring function can you configure the sensor to perform?

- A. Monitor traffic as it flows to the sensor.
- B. Monitor traffic as it flows through the sensor.
- C. Monitor traffic from the Internet only.
- D. Monitor traffic from both the Internet and the intranet.

Answer: B

NEW QUESTION 10

Which five system management and reporting 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 10

Refer to the following:

```
R01(config)#ip wccp web-cache redirect-list 80 password-local
```

- A. Traffic denied in prefix-list 80 is redirected to the Cisco WSA
- B. The default "cisco" password is configured on the Cisco WSA
- C. Traffic permitted in access-list 80 is redirected to the Cisco WSA
- D. Traffic using TCP port 80 is redirected to the Cisco WSA

Answer: C

NEW QUESTION 13

When centralized message tracking is enabled on the Cisco ESA, over which port does the communication to the SMA occur by default?

- A. port 2222/TCP
- B. port 443/TCP
- C. port 25/TCP
- D. port 22/TCP

Answer: D

NEW QUESTION 17

CORRECT TEXT

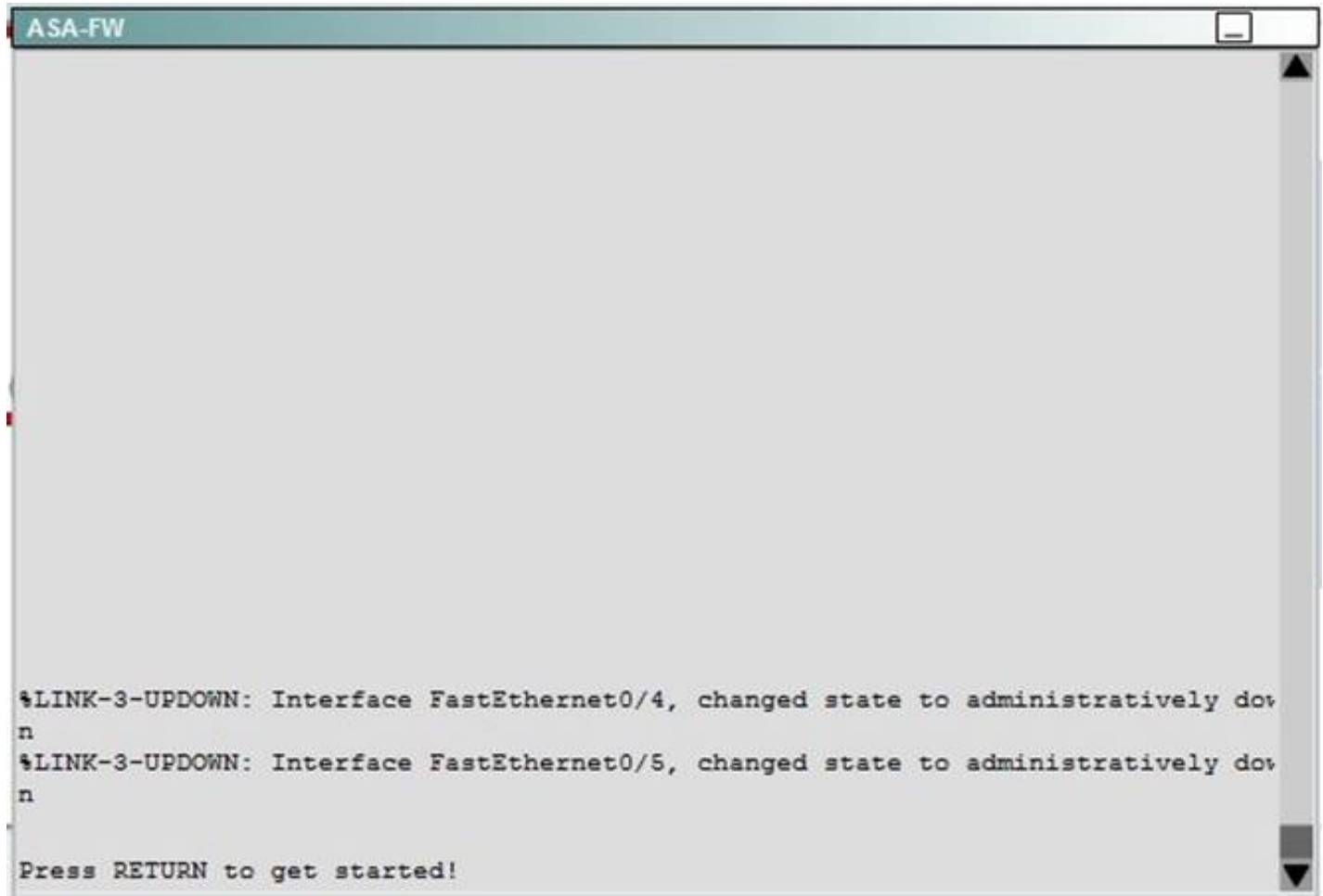
Scenario
Your organization is deploying the ASA CX software module in the ASA which connects the organization's internal network to the Internet. A colleague has configured the policy on the CX module itself. Your task is to configure the ASA to forward the appropriate traffic to the CX module for processing.

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.

Topology

The diagram illustrates a network topology. On the left, a red vertical line represents the internal network. A horizontal red line connects this to the 'inside' interface of a blue cube representing the ASA. The cube has a magnifying glass icon. Above the cube is a red line labeled 'dmz'. To the right of the cube is a blue cloud labeled 'Internet'. A horizontal red line connects the 'outside' interface of the cube to the cloud. The word 'outside' is written below the line connecting the cube to the cloud.



Answer:

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:

NEW QUESTION 22

Which three pieces of information are required to implement transparent user identification using Context Directory Agent? (Choose three.)

- A. the server name of the global catalog domain controller
- B. the server name where Context Directory Agent is installed
- C. the backup Context Directory Agent
- D. the primary Context Directory Agent
- E. the shared secret
- F. the syslog server IP address

Answer: BDE

NEW QUESTION 26

Refer to the exhibit.

Processing Details	
	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: user@mydomain.com
29 Apr 2014 11:53:14 (GMT +00:00)	Protocol SMTP interface Management (IP 172.18.254.17) on incoming connection (ICID 356) from sender IP 10.150.54.161. Reverse DNS host dhcp-10-150-54-161.cisco.com verified yes.
29 Apr 2014 11:53:14 (GMT +00:00)	(ICID 356) ACCEPT sender group SUSPECTLIST match 10.150.54.161 SBR5 rfc1918
29 Apr 2014 11:53:23 (GMT +00:00)	Start message 1022 on incoming connection (ICID 356).
29 Apr 2014 11:53:23 (GMT +00:00)	Message 1022 enqueued on incoming connection (ICID 356) from user@somedomain.com.
29 Apr 2014 11:53:27 (GMT +00:00)	Message 1022 on incoming connection (ICID 356) added recipient (user@mydomain.com).
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 original subject on injection: my emails
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 (225 bytes) from user@somedomain.com ready.
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 matched per-recipient policy DEFAULT for inbound mail policies.
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 scanned by Anti-Spam engine: CASE. Final verdict: Negative
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 scanned by Anti-Virus engine. Final verdict: Negative
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 queued for delivery.

The system administrator of mydomain.com received complaints that some messages that were sent from sender user@somedomain.com were delayed.

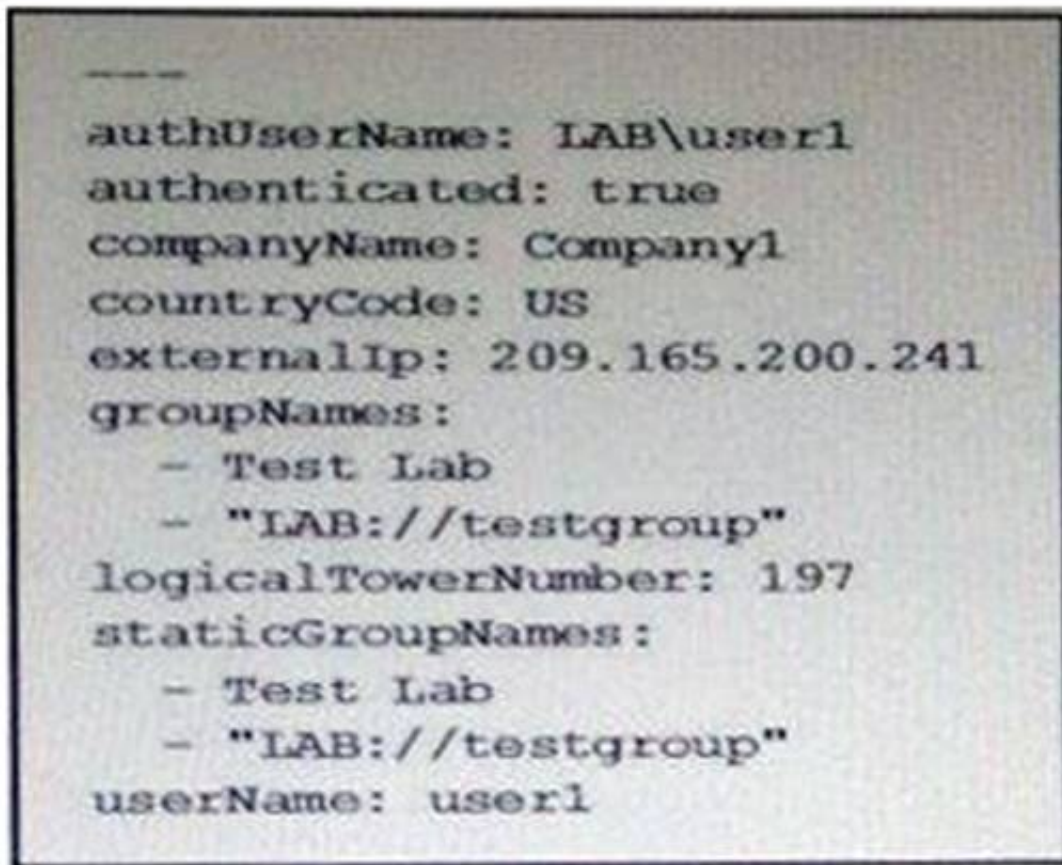
Message tracking data on the sender shows that an email sample that was received was clean and properly delivered. What is the likely cause of the intermittent delays?

- A. The remote MTA has a SenderBase Reputation Score of -1.0.
- B. The remote MTA is sending emails from RFC 1918 IP addresses.
- C. The remote MTA has activated the SUSPECTLIST sender group.
- D. The remote MTA has activated the default inbound mail policy.

Answer: C

NEW QUESTION 29

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 33

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 37

Which is the default IP address and admin port setting for https in the Cisco Web Security Appliance?

- A. http://192.168.42.42:8080
- B. http://192.168.42.42:80
- C. https://192.168.42.42:443
- D. https://192.168.42.42:8443

Answer: D

NEW QUESTION 41

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 46

Which solution must a customer deploy to prioritize traffic to a cloud-based contact management application while still allowing employees access to the Internet for business and personal use?

- A. Cisco Application Visibility and Control
- B. Cisco Intrusion Prevention Services
- C. Cisco NetFlow
- D. policy-based routing

Answer: A

NEW QUESTION 47

When https traffic is scanned, which component of the full URL does CWS log?

- A. not log
- B. only host host and query path and query

Answer: B

NEW QUESTION 51

Which three options are IPS signature classifications? (Choose three.)

- A. tuned signatures
- B. response signatures
- C. default signatures
- D. custom signatures
- E. preloaded signatures
- F. designated signatures

Answer: ACD

NEW QUESTION 52

Refer to the exhibit.

Instructions

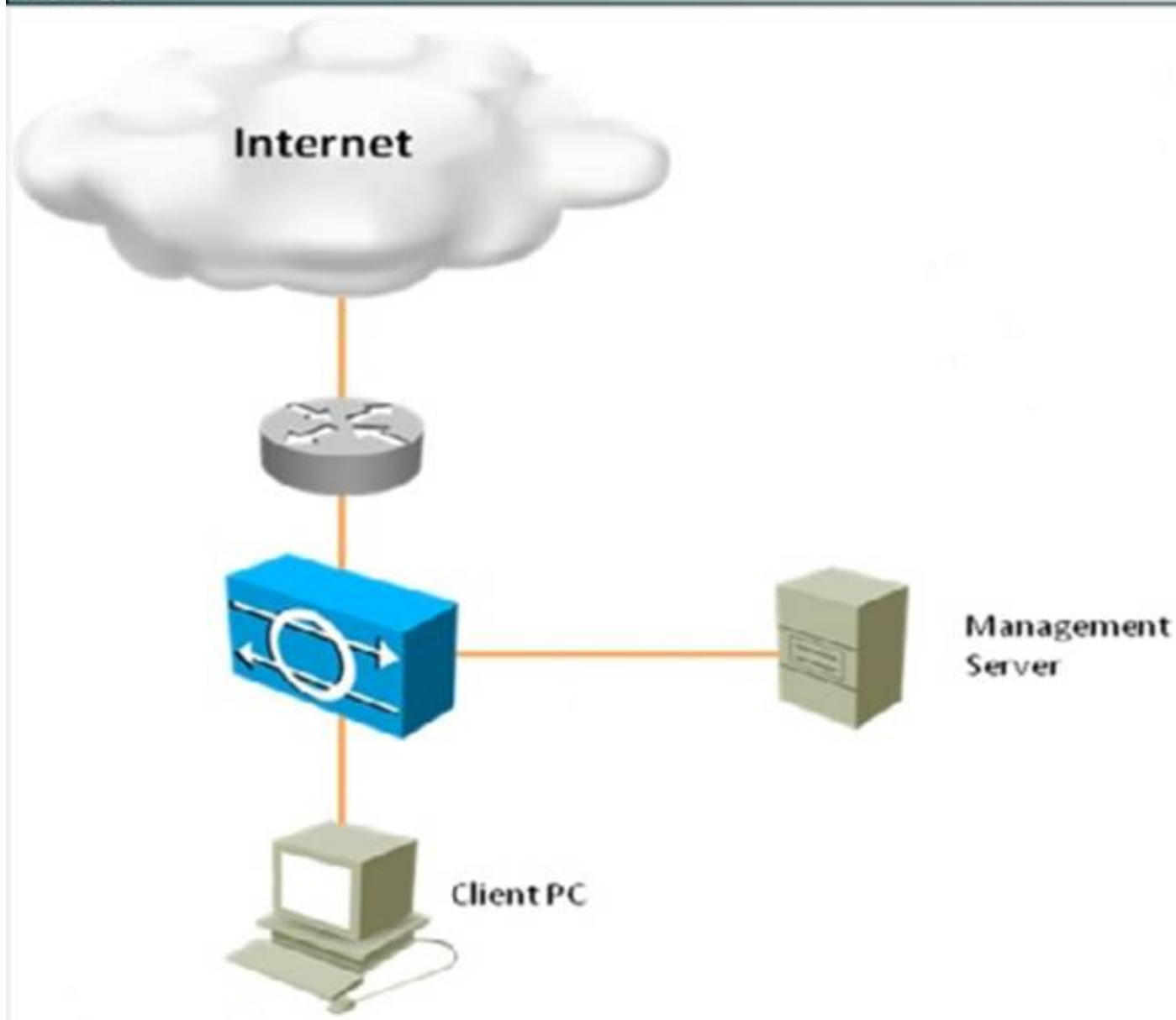
You can click the grey buttons at the bottom of this frame to view the different windows.

To minimize the window, click the [-]. To move the window, click the title bar and drag the window.

Scenario

Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.

Topology





What is the status of OS Identification?

- A. It is only enabled to identify "Cisco IOS" OS using statically mapped OS fingerprinting
- B. OS mapping information will not be used for Risk Rating calculations.
- C. It is configured to enable OS mapping and ARR only for the 10.0.0.0/24 network.
- D. It is enabled for passive OS fingerprinting for all networks.

Answer: D

Explanation: Understanding Passive OS Fingerprinting

Passive OS fingerprinting lets the sensor determine the OS that hosts are running. The sensor analyzes network traffic between hosts and stores the OS of these hosts with their IP addresses. The sensor inspects TCP SYN and SYNACK packets exchanged on the network to determine the OS type.

The sensor then uses the OS of the target host OS to determine the relevance of the attack to the victim by computing the attack relevance rating component of the risk rating. Based on the relevance of the attack, the sensor may alter the risk rating of the alert for the attack and/or the sensor may filter the alert for the attack. You can then use the risk rating to reduce the number of false positive alerts (a benefit in IDS mode) or definitively drop suspicious packets (a benefit in IPS mode). Passive OS fingerprinting also enhances the alert output by reporting the victim OS, the source of the OS identification, and the relevance to the victim OS in the alert.

Passive OS fingerprinting consists of three components:

- Passive OS learning

Passive OS learning occurs as the sensor observes traffic on the network. Based on the characteristics of TCP SYN and SYNACK packets, the sensor makes a determination of the OS running on the host of the source IP address.

- User-configurable OS identification

You can configure OS host mappings, which take precedence over learned OS mappings.

- Computation of attack relevance rating and risk rating.

NEW QUESTION 53

An engineer 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. service
- B. operator
- C. administrator

Answer: C

Explanation: <http://www.cisco.com/c/en/us/td/docs/security/ips/7-0/command/reference/cmdref/crIntro.html>

NEW QUESTION 55

Which command can change the HTTPS SSL method on the Cisco ESA?

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

Answer: A

NEW QUESTION 58

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 60

Which IPS engine detects ARP spoofing?

- A. Atomic ARP Engine
- B. Service Generic Engine
- C. ARP Inspection Engine
- D. AIC Engine

Answer: A

NEW QUESTION 61

Which two statements regarding the basic setup of the Cisco CX for services are correct? (Choose two.)

- A. The Packet capture feature is available for either permitted or dropped packets by default.
- B. Public Certificates can be used for HTTPS Decryption policies.
- C. Public Certificates cannot be used for HTTPS Decryption policies.
- D. When adding a standard LDAP realm, the group attribute will be UniqueMember.
- E. The Packet capture features is available for permitted packets by default.

Answer: CE

NEW QUESTION 62

Which Cisco Web Security Appliance deployment mode requires minimal change to endpoint devices?

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

Answer: A

NEW QUESTION 67

What can you use to access the Cisco IPS secure command and control channel to make configuration changes?

- A. SDEE
- B. the management interface
- C. an HTTP server
- D. Telnet

Answer: B

NEW QUESTION 70

Who or what calculates the signature fidelity rating in a Cisco IPS?

- A. the signature author
- B. Cisco Professional Services
- C. the administrator
- D. the security policy

Answer: A

NEW QUESTION 73

What CLI command configures IP-based access to restrict GUI and CLI access to a Cisco Email Security appliance's administrative interface?

- A. adminaccessconfig
- B. sshconfig
- C. sslconfig
- D. ipaccessconfig

Answer: A

NEW QUESTION 74

Which two options are known limitations in deploying an IPS sensor in promiscuous mode versus inline mode? (Choose two).

- A. It is less effective in stopping email viruses and automated attackers such as worms.

- B. It requires less of an operational response because the attacks are blocked automatically without operational team support.
- C. Sensors in this deployment cannot stop the trigger packet and are not guaranteed to stop a connection.
- D. A sensor failure affects network functionality.
- E. It does not see the same traffic.

Answer: AC

NEW QUESTION 76

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 80

What are two features of the Cisco ASA NGFW? (Choose two.)

- A. It can restrict access based on qualitative analysis.
- B. It can restrict access based on reputation.
- C. It can reactively protect against Internet threats.
- D. It can proactively protect against Internet threats.

Answer: BD

NEW QUESTION 84

A system administrator wants to know if the email traffic from a remote partner will activate special treatment message filters that are created just for them. Which tool on the Cisco Email Security gateway can you use to debug or emulate the flow that a message takes through the work queue?

- A. the message tracker interface
- B. centralized or local message tracking
- C. the CLI findevent command
- D. the trace tool
- E. the CLI grep command

Answer: D

NEW QUESTION 86

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. A Cisco 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 89

You ran the ssh generate-key command on the Cisco IPS and now administrators are unable to connect. Which action can be taken to correct the problem?

- A. Replace the old key with a new key on the client.
- B. Run the ssh host-key command.
- C. Add the administrator IP addresses to the trusted TLS host list on the IPS.
- D. Run the ssh authorized-keys command.

Answer: A

NEW QUESTION 92

When learning accept mode is set to auto, and the action is set to rotate, when is the KB created and used?

- A. It is created every 24 hours and used for 24 hours.

- B. It is created every 24 hours, but the current KB is used.
- C. It is created every 1 hour and used for 24 hours.
- D. A KB is created only in manual mode.

Answer: A

NEW QUESTION 97

Which two conditions must you configure in an event action override to implement a risk rating of 70 or higher and terminate the connection on the IPS? (Choose two.)

- A. Configure the event action override to send a TCP reset.
- B. Set the risk rating range to 70 to 100.
- C. Configure the event action override to send a block-connection request.
- D. Set the risk rating range to 0 to 100.
- E. Configure the event action override to send a block-host request.

Answer: AB

NEW QUESTION 102

Which statement about the Cisco ASA CX role in inspecting SSL traffic is true?

- A. To decrypt traffic, the Cisco ASA CX must accept the websites' certificates as Trusted Root Cas.
- B. If the administrator elects to decrypt traffic, the Cisco ASA CX acts as a man-in—me- middle.
- C. Either all traffic is decrypted, or no traffic is decrypted by the Cisco ASA CX.
- D. The traffic is encrypted, so the Cisco ASA CX cannot determine the content of the traffic.

Answer: B

NEW QUESTION 107

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 110

Which Cisco ESA predefined sender group uses parameter-matching to reject senders?

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

Answer: A

NEW QUESTION 111

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 112

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 114

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 118

Which three administrator actions are used to configure IP logging in Cisco IME? (Choose three.)

- A. Select a virtual sensor.
- B. Enable IP logging.
- C. Specify the host IP address.
- D. Set the logging duration.
- E. Set the number of packets to capture.
- F. Set the number of bytes to capture.

Answer: ACD

NEW QUESTION 121

Which role does Passive Identity Management play in the Cisco Cloud Web Security architecture?

- A. It provides user-level information that is received from Active Directory.
- B. It enables the administrator to control web access for users and user groups.
- C. It defines a standard for exchanging authentication and authorization data.
- D. It controls content that passes into and out of the network.

Answer: A

NEW QUESTION 122

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 126

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 127

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 129

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 130

Which configuration mode enables a virtual sensor to monitor the session state for unidirectional traffic?

- A. asymmetric mode
- B. symmetric mode
- C. loose mode
- D. strict mode

Answer: A

NEW QUESTION 131

A Cisco 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 135

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 140

Refer to the exhibit.

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.

V120 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

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...

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

Import HAT... 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

HAT Overview

Find Senders

Find Senders that Contain this Text: Find

Sender Groups (Listener: IncomingMail 172.16.16.25:25)

Add Sender Group...

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	

Import HAT... 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

Mail Flow Policy

Policies (Listeners):

- Add Policy...
- Policy Name
- ACCEPTED
- BLOCKED
- RELAYED
- THROTTLED
- TRUSTED
- Default Policy Parameters

Email Security Manager

- Incoming Mail Policies
- Incoming Content Filters
- Outgoing Mail Policies
- Outgoing Content Filters

Host Access Table (HAT)

- HAT Overview
- Mail Flow Policies
- Exception Table
- Address Lists

Recipient Access Table (RAT)

- Destination Controls
- Bounce Verification

Data Loss Prevention (DLP)

- DLP Policy Manager
- DLP Message Actions

Domain Keys

- Verification Profiles
- Signing Profiles
- Signing Keys

Text Resources

- Dictionaries

No Changes Pending...

Behavior	Delete
Accept	?
Reject	🗑️
Relay	🗑️
Accept	🗑️
Accept	🗑️

Copyright © 2003-2010 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: ACCEPTED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name:

Connection Behavior:

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)

Monitor

Mail Policies

Security Services

Network

System Administration

Home

Monitor

Mail Policies

Security Services

Network

System Administration

Cisco C100V

Email Security Virtual Appliance

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

Mail Flow Policies

Host Access Table (HAT)

Host Access Table (HAT) Overview

Mail Flow Policies

Exception Table

Address Lists

Recipient Access Table (RAT)

Destination Controls

Bounce Verification

Data Loss Prevention (DLP)

DLP Policy Manager

DLP Message Actions

Domain Keys

Verification Profiles

Signing Profiles

Signing Keys

Text Resources

Dictionaries

IncomingMail 172.16.16.25:25

Messages Per Connection: ☒ Use Default (10) ☐

Recipients Per Message: ☒ Use Default (50) ☐

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

Messages From a Single IP: ☒ Use Default (10) ☐

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: ☒ Use Default (Unlimited) ☐ Unlimited

Max. Recipients Per Hour: ☒ Use Default (452) ☐

Max. Recipients Per Hour Code: ☒ Use Default (Too many recipients received this hour) ☐

Monitor

Mail Policies

Security Services

Network

System Administration

Cisco C100V

Email Security Virtual Appliance

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

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

<< Back to HAT Overview

Edit Settings...

Find Senders

Find Senders that Contain this Text:

Sender List: Display All Items in List

Add Sender...

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

Sender Group Settings

Host Access Table (HAT)

HAT Overview

Mail Flow Policies

Exception Table

Address Lists

Recipient Access Table (RAT)

Destination Controls

Bounce Verification

Data Loss Prevention (DLP)

DLP Policy Manager

DLP Message Actions

Domain Keys

Verification Profiles

Signing Profiles

Signing Keys

Text Resources

Dictionaries

IncomingMail 172.16.16.25:25

ST

rs are rejected

D

-3.0

cluded

Edit Settings...

Find

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

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) ☐

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)

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

Monitor Mail Policies Security Services Network System Administration

Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25

Edit Policy Settings

- Email Security Manager
 - Incoming Mail Policies
 - Incoming Content Filters
 - Outgoing Mail Policies
 - Outgoing Content Filters
- Host Access Table (HAT)
 - HAT Overview
 - Mail Flow Policies
 - Exception Table
 - Address Lists
- Recipient Access Table (RAT)
 - Destination Controls
 - Bounce Verification
- Data Loss Prevention (DLP)
 - DLP Policy Manager
 - DLP Message Actions
- Domain Keys
 - Verification Profiles
 - Signing Profiles
 - Signing Keys
- Text Resources
 - Dictionaries

Mail Flow Limits

Rate Limit for Hosts:	Max. Recipients Per Hour:	<input checked="" type="radio"/> Use Default (Unlimited) <input type="radio"/> Unlimited <input type="text"/>
	Max. Recipients Per Hour Code:	<input checked="" type="radio"/> Use Default (452) <input type="text"/>
	Max. Recipients Per Hour Text:	<input checked="" type="radio"/> Use Default (Too many recipients received this hour) <input type="text"/>

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

Monitor Mail Policies Security Services Network System Administration

Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name: RELAYED

Connection Behavior: Relay

Connections:

Max. Messages Per Connection:	<input checked="" type="radio"/> Use Default (10) <input type="text"/>
Max. Recipients Per Message:	<input checked="" type="radio"/> Use Default (50) <input type="text"/>
Max. Message Size:	<input checked="" type="radio"/> Use Default (10M) <input type="text"/> <small>(add a trailing K for kilobytes; M for megabytes)</small>
Max. Concurrent Connections From a Single IP:	<input checked="" type="radio"/> Use Default (10) <input type="text"/>

SMTP:

Custom SMTP Banner Code:	<input checked="" type="radio"/> Use Default (220) <input type="text"/>
Custom SMTP Banner Text:	<input checked="" type="radio"/> Use Default () <input type="text"/>
Override SMTP Banner Hostname:	<input checked="" type="radio"/> Use Default (Use Hostname from Interface) <input type="radio"/> Use Hostname from Interface <input type="text"/>

Mail Flow Limits

Rate Limit for Hosts:	Max. Recipients Per Hour:	<input checked="" type="radio"/> Use Default (Unlimited) <input type="radio"/> Unlimited <input type="text"/>
	Max. Recipients Per Hour Code:	<input checked="" type="radio"/> Use Default (452) <input type="text"/>
	Max. Recipients Per Hour Text:	<input checked="" type="radio"/> Use Default (Too many recipients received this hour) <input type="text"/>

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

Mail Flow Policies

Mail Flow Policy Settings

Host Access Table (HAT)

HAT Overview

Mail Flow Policies

Exception Table

Address Lists

Recipient Access Table (RAT)

Destination Controls

Bounce Verification

Data Loss Prevention (DLP)

DLP Policy Manager

DLP Message Actions

Domain Keys

Verification Profiles

Signing Profiles

Signing Keys

Text Resources

Dictionaries

IncomingMail 172.16.16.25:25

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

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

<< 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
hq-mail.maroon.public	None	<input type="checkbox"/>

<< Back to HAT Overview Delete

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

Sender Group

Sender Group Settings

Find Senders

Sender List: Display

Add Sender...

Sender

hq-mail.maroon.public

<< Back to HAT Overview

Host Access Table (HAT)

Incoming Mail 172.16.16.25:25

ST

ect hosts can relay from this box.

cluded

Edit Settings...

Find

Items per page 20

All

Delete

Delete

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

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

<< Back to HAT Overview

Edit Settings...

Find Senders

Find Senders that Contain this Text:

Find

Sender List: Display All Items in List

Add Sender...

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

Sender Group

Sender Group Settings

Find Senders

Sender List: Display

Add Sender...

There are no senders.

Host Access Table (HAT)

Incoming Mail 172.16.16.25:25

TLIST

us senders are throttled

LED

.0

cluded

Edit Settings...

Find

Items per page 20

All

Delete

Delete

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

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:

Connection Behavior:

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) ☐

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:

Connection Behavior:

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) ☐

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:

Connection Behavior:

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)
☐

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:

Connection Behavior:

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)
☐

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

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text: Find

Sender List: Display All Items in List

Add Sender...

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

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

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text: Find

Sender List: Display All Items in List

Add Sender...

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

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

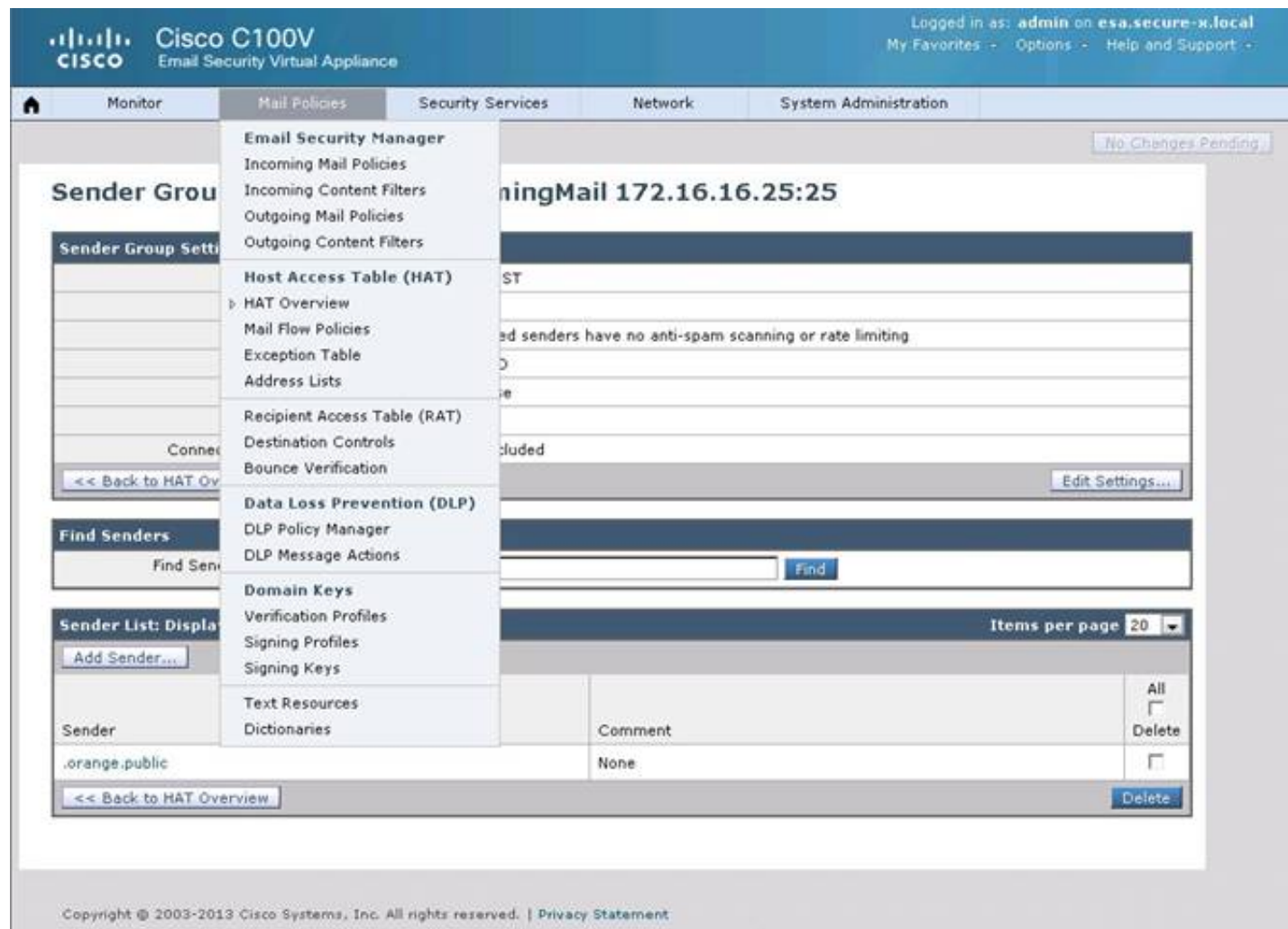
Sender List: Display All Items in List Items per page: 20

Add Sender...

Sender	Comment	All Delete
.orange.public	None	<input type="checkbox"/>

<< Back to HAT Overview Delete

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

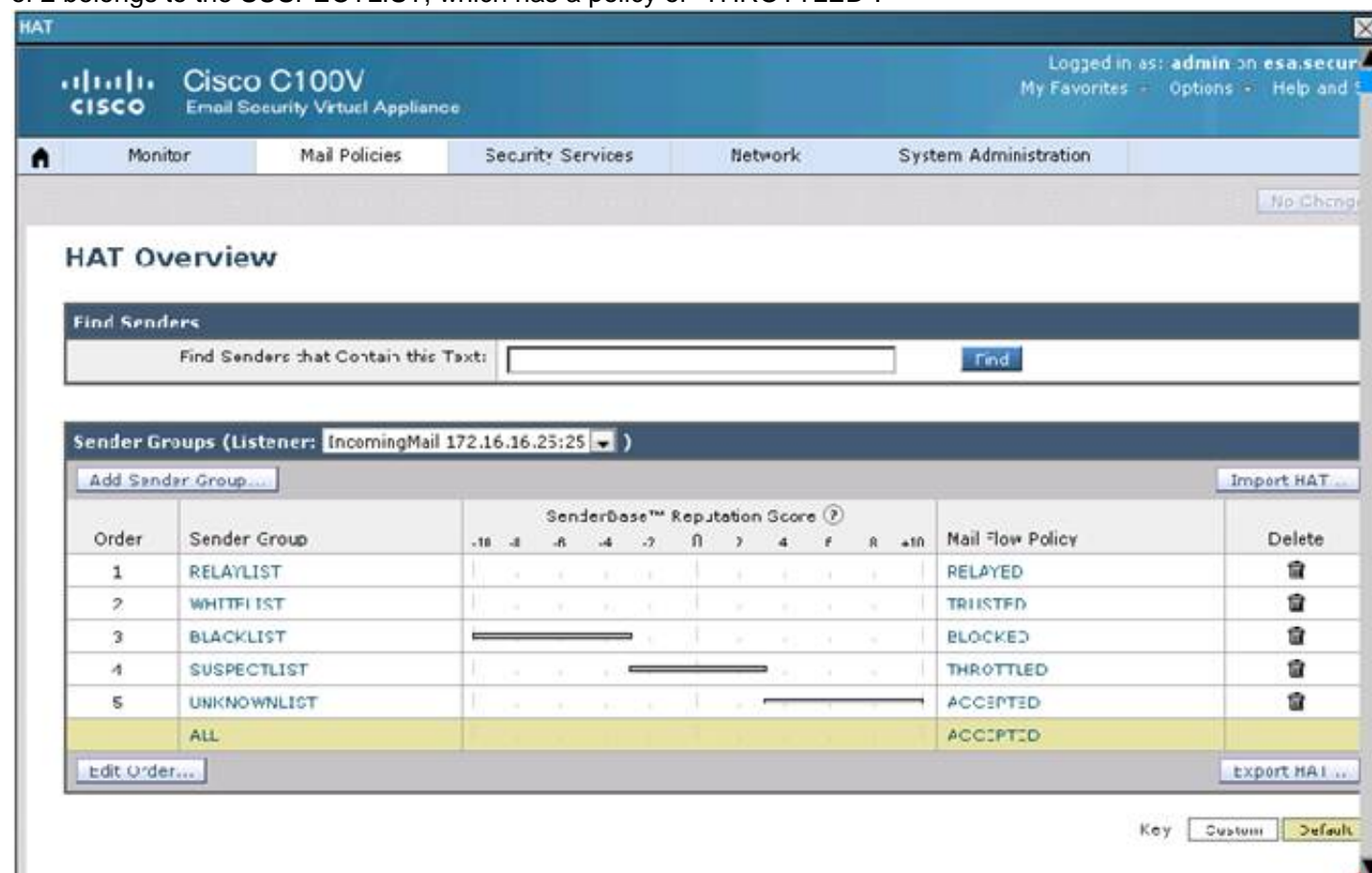


What is the maximum number of recipients per hour that the Cisco Email Security Appliance will accept from the green.public domain?

- 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

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

The screenshot shows the 'Throttled' configuration window for a Cisco ESA. It contains several settings for mail flow limits and SMTP banner codes. The 'Mail Flow Limits' section is highlighted in blue.

Section	Parameter	Options	Selected Value
General	Max. Recipients Per Message:	<input type="radio"/> Use Default (50) <input checked="" type="radio"/> [25]	25
	Max. Message Size:	<input type="radio"/> Use Default (10M) <input checked="" type="radio"/> [10485760]	10485760 <small>(add a trailing K for kilobytes; M for megabytes)</small>
	Max. Concurrent Connections From a Single IP:	<input type="radio"/> Use Default (10) <input checked="" type="radio"/> []	
SMTP	Custom SMTP Banner Code:	<input checked="" type="radio"/> Use Default (220) <input type="radio"/> [220]	220
	Custom SMTP Banner Text:	<input checked="" type="radio"/> Use Default () <input type="radio"/> []	
	Override SMTP Banner Hostname:	<input checked="" type="radio"/> Use Default (Use -hostname from Interface) <input type="radio"/> Use Hcstname from Interface <input type="radio"/> []	
Mail Flow Limits	Rate Limit for Hosts:	<input type="radio"/> Use Default (Unlimited) <input type="radio"/> Unlimited <input checked="" type="radio"/> [20]	20
	Max. Recipients Per Hour:	<input type="radio"/> Use Default (Unlimited) <input type="radio"/> Unlimited <input checked="" type="radio"/> [20]	20
	Max. Recipients Per Hour Code:	<input checked="" type="radio"/> Use Default (452) <input type="radio"/> []	
	Max. Recipients Per Hour Text:	<input checked="" type="radio"/> Use Default (Too many recipients received this hour) <input type="radio"/> []	

Capture

NEW QUESTION 143

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 146

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 151

Which two pieces of information are required to implement transparent user identification using context Directory Agent? (Choose two.)

- A. the shared secret
- B. the server name where Context Directory Agent is installed
- C. the server name of the global catalog domain controller
- D. the syslog server IP address

Answer: AB

NEW QUESTION 155

What is a valid search parameter for the Cisco ESA find event tool?

- A. Envelope Origination
- B. Envelope Type
- C. Message ID
- D. Download Type

Answer: C

NEW QUESTION 159

Which three statements about threat ratings are true? (Choose three.)

- A. A threat rating is equivalent to a risk rating that has been lowered by an alert rating.
- B. The largest threat rating from all actioned events is added to the risk rating.

- C. The smallest threat rating from all actioned events is subtracted from the risk rating.
- D. The alert rating for deny-attacker-inline is 45.
- E. Unmitigated events do not cause a threat rating modification.
- F. The threat rating for deny-attacker-inline is 50.

Answer: ADE

NEW QUESTION 164

Which Cisco Cloud Web Security Connector feature allows access by all of an organization's users while applying Active Directory group policies?

- A. a company authentication key
- B. a group authentication key
- C. a PAC file
- D. proxy forwarding
- E. a user authentication key

Answer: A

NEW QUESTION 166

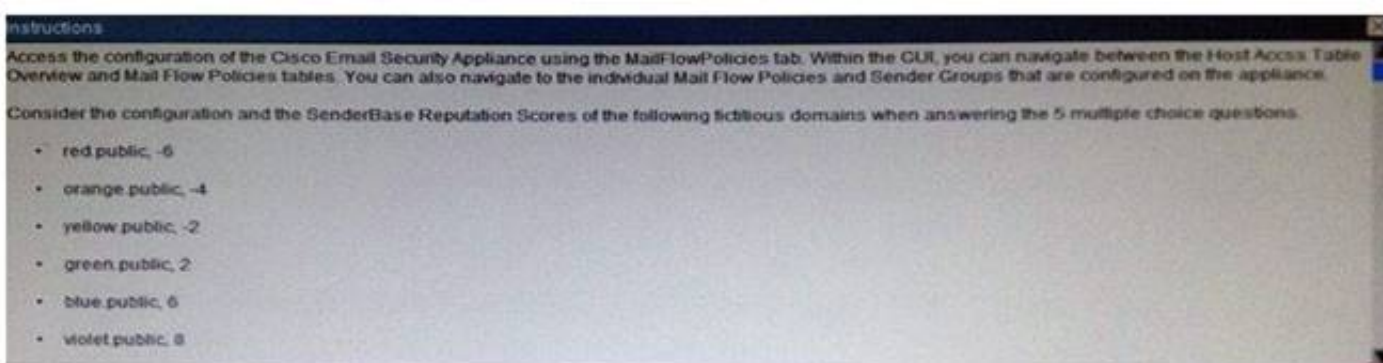
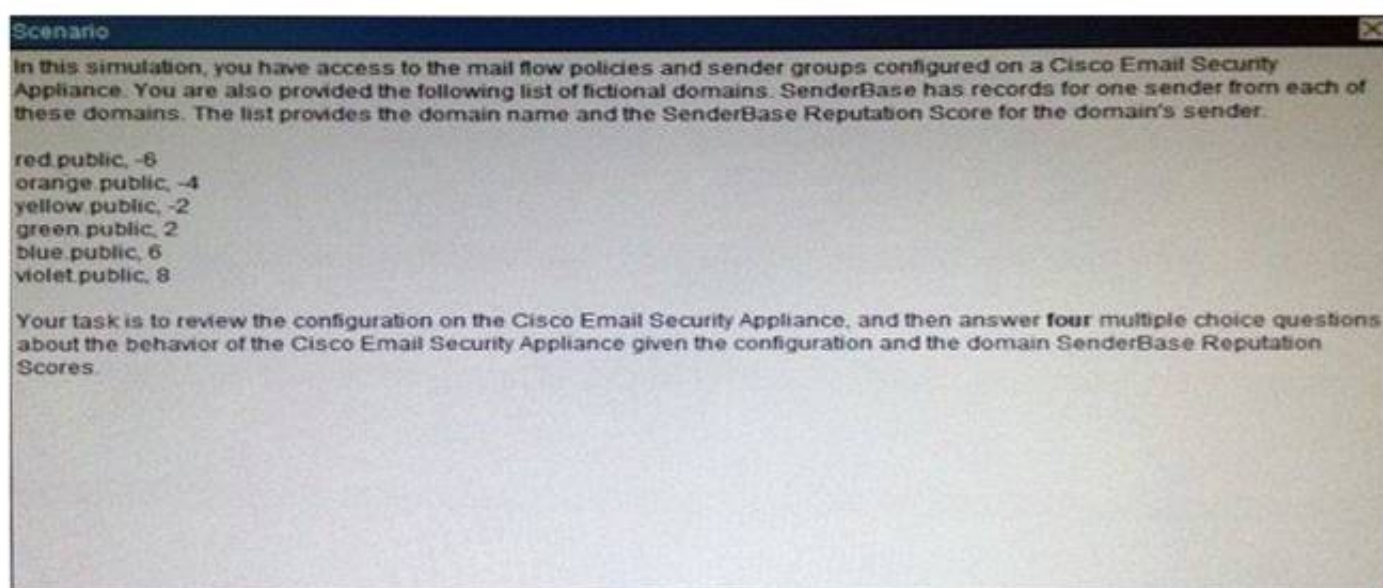
Which statement about Cisco IPS Manager Express is true?

- A. It provides basic device management for large-scale deployments.
- B. It provides a GUI for configuring IPS sensors and security modules.
- C. It enables communication with Cisco ASA devices that have no administrative access.
- D. It provides greater security than simple ACLs.

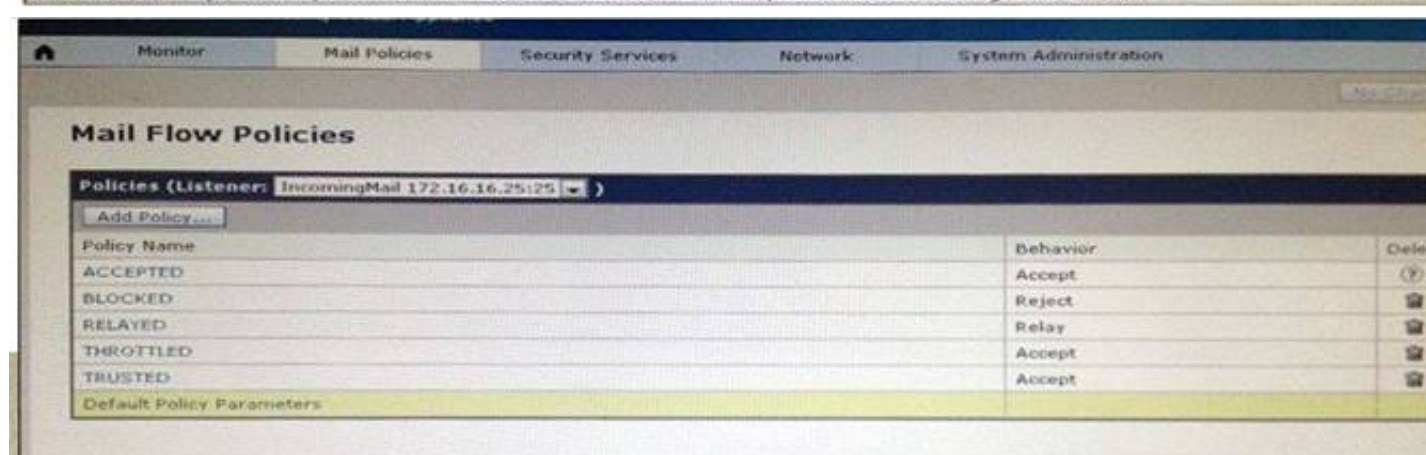
Answer: B

NEW QUESTION 170

Refer to the exhibit.



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.



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 174

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 178

With Cisco IDM, which rate limit option specifies the maximum bandwidth for rate-limited traffic?

- A. protocol
- B. rate
- C. bandwidth
- D. limit

Answer: B

NEW QUESTION 181

In addition to the CLI, what is another option to manage a Cisco IPS?

- A. SDEE
- B. Cisco SDM
- C. Cisco IDM
- D. Cisco ISE

Answer: C

NEW QUESTION 186

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 187

Refer to the Following. Which option describe the result of this configuration on a Cisco ASA firewall?

asafw1 (config) #http server enable
asafw1(config)#http 10.10.10.1 255.255.255.255 inside

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

Answer: A

NEW QUESTION 188

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

Which action is possible when a signature is triggered on the Cisco IOS IPS?

- A. Send an email via SMTP to the administrator
- B. Deny all packets with the same port destination
- C. Send an SNMP alert to a monitoring system

Answer: A

NEW QUESTION 196

Which three statements about Cisco ASA CX are true? (Choose three.)

- A. It groups multiple ASAs as a single logical device.
- B. It can perform context-aware inspection.
- C. It provides high-density security services with high availability.
- D. It uses policy-based interface controls to inspect and forward TCP- and UDP-based packets.
- E. It can make context-aware decisions.
- F. It uses four cooperative architectural constructs to build the firewall.

Answer: BEF

NEW QUESTION 197

What is a value that Cisco ESA can use for tracing mail flow?

- A. the FQDN of the source IP address
- B. the FQDN of the destination IP address
- C. the destination IP address
- D. the source IP address

Answer: A

NEW QUESTION 202

What step is required to enable HTTPS Proxy on the Cisco Web Security Appliance?

- A. Web Security Manager HTTPS Proxy click Enable
- B. Security Services HTTPS Proxy click Enable
- C. HTTPS Proxy is enabled by default
- D. System Administration HTTPS Proxy click Enable

Answer: B

NEW QUESTION 205

In order to set up HTTPS decryption on the Cisco Web Security Appliance, which two steps must be performed? (Choose two.)

- A. Enable and accept the EULA under Security Services > HTTPS Proxy.
- B. Upload a publicly signed server certificate.
- C. Configure or upload a certificate authority certificate.
- D. Enable HTTPS decryption in Web Security Manager > Access Policies.

Answer: AC

NEW QUESTION 206

Which command establishes a virtual console session to a CX module within a Cisco Adaptive Security Appliance?

- A. session 1 ip address
- B. session 2 ip address
- C. session 1
- D. session ips console
- E. session cxsc console

Answer: E

NEW QUESTION 211

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 213

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 214

Which Cisco IPS deployment mode is best suited for bridged interfaces?

- A. inline interface pair mode
- B. inline VLAN pair mode
- C. inline VLAN group mode
- D. inline pair mode

Answer: B

NEW QUESTION 219

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 224

Refer to the exhibit.

Instructions

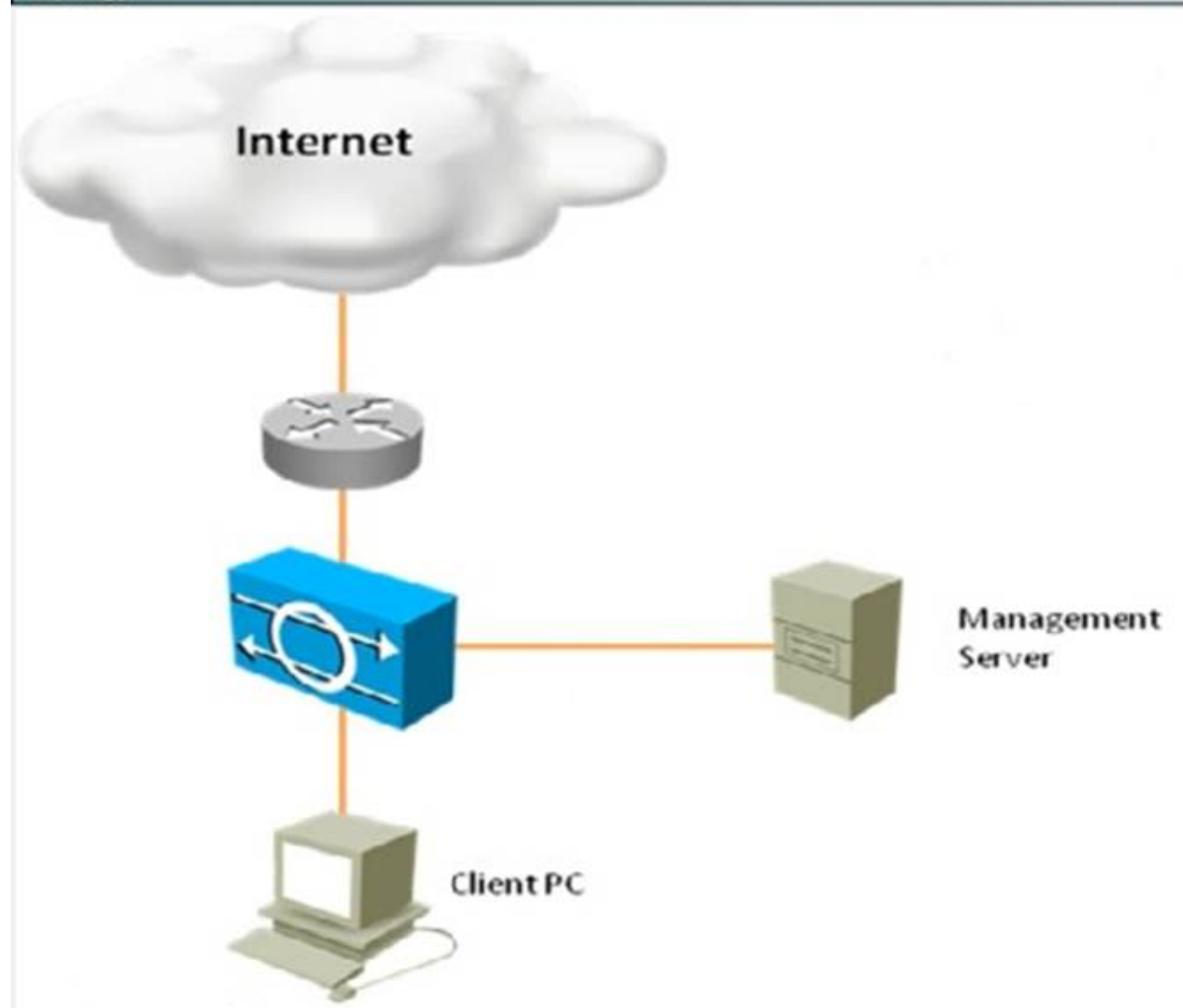
You can click the grey buttons at the bottom of this frame to view the different windows.

To minimize the window, click the [-]. To move the window, click the title bar and drag the window.

Scenario

Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.

Topology



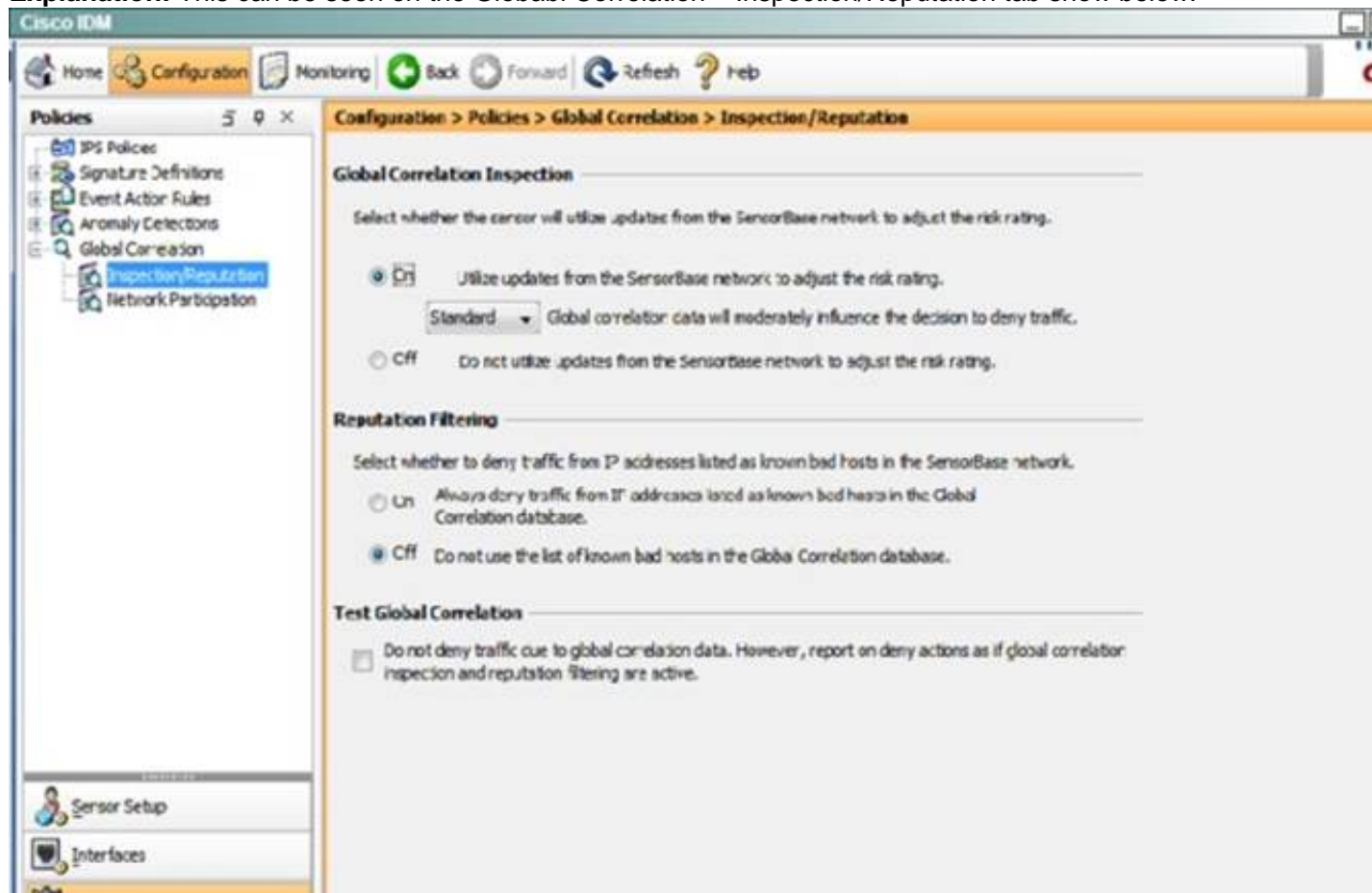


What action will the sensor take regarding IP addresses listed as known bad hosts in the Cisco SensorBase network?

- A. Global correlation is configured in Audit mode for testing the feature without actually denying any hosts.
- B. Global correlation is configured in Aggressive mode, which has a very aggressive effect on deny actions.
- C. It will not adjust risk rating values based on the known bad hosts list.
- D. Reputation filtering is disabled.

Answer: D

Explanation: This can be seen on the Global Correlation – Inspection/Reputation tab shown below:



NEW QUESTION 225

Which interface on the Cisco Email Security Appliance has HTTP and SSH enabled by default?

- A. data 1
- B. data 2
- C. management 1
- D. all interfaces

Answer: A

NEW QUESTION 226

Which three categories of the seven major risk management categories are covered in the Cyber Risk Reports? (Choose three.)

- A. vulnerability
- B. risk rating
- C. legal
- D. confidence level
- E. geopolitical
- F. global reputation

Answer: ACE

NEW QUESTION 231

Which information does the show scansafe statistics command provide?

- A. ESA message tracking
- B. PRSM events
- C. AV statistics
- D. Cisco CWS activity

Answer: D

NEW QUESTION 234

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 236

Which statement about the default configuration of an IPS sensor's management security settings is true?

- A. The web server port is TCP 80
- B. Telnet and SSH are enable
- C. User accounts lock after three attempts

Answer: A

NEW QUESTION 240

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 245

What is a difference between a Cisco Content Security Management virtual appliance and a physical appliance?

- A. The virtual appliance requires an additional license to run on a host.
- B. The physical appliance requires an additional license to activate its adapters.
- C. Migration between virtual appliances of varying sizes is possible, but physical appliances must be of equal size.
- D. The physical appliance is configured with a DHCP-enabled management port to receive an IP address automatically, but you must assign the virtual appliance an IP address manually in your management subnet.

Answer: A

NEW QUESTION 248

Which two options are the correct URL and credentials used to access the Cisco Web Security Appliance for the first time? (Choose two.)

- A. admin/password
- B. http://192.168.1.1:8080
- C. ironport/ironport
- D. http://192.168.42.42:8080
- E. admin/ironport
- F. http://192.168.42.42:8443

Answer: DE

NEW QUESTION 253

What are three features of the Cisco Security Intellishield Alert Manager Service? (Choose three.)

- A. validation of alerts by security analysts
- B. custom notifications
- C. complete threat and vulnerability remediation
- D. vendor-specific threat analysis
- E. workflow-management tools
- F. real-time threat and vulnerability mitigation

Answer: ABE

NEW QUESTION 258

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 262

A network engineer can assign IPS event action overrides to virtual sensors and configure which three modes? (Choose three.)

- A. Anomaly detection operational mode
- B. Inline TCP session tracking mode
- C. Normalizer mode
- D. Load-balancing mode
- E. Inline and Promiscuous mixed mode
- F. Fail-open and fail-close mode

Answer: ABC

NEW QUESTION 264

Which method does Cisco recommend for collecting streams of data on a sensor that has been virtualized?

- A. VACL capture
- B. SPAN
- C. the Wireshark utility
- D. packet capture

Answer: D

NEW QUESTION 269

When a user receives an encrypted email from a Cisco ESA, which technology is used to retrieve the key to open the email?

- A. trusted certificate authority
- B. private certificate authority
- C. Cisco Registered Envelope Service
- D. Simple Certificate Enrollment Protocol

Answer: C

NEW QUESTION 273

Which three options are characteristics of router-based IPS? (Choose three.)

- A. It is used for large networks.
- B. It is used for small networks.
- C. It supports virtual sensors.
- D. It supports multiple VRFs.
- E. It uses configurable anomaly detection.
- F. Signature definition files have been deprecated.

Answer: BDF

NEW QUESTION 278

At which value do custom signatures begin?

- A. 1024
- B. 10000
- C. 1
- D. 60000

Answer: D

NEW QUESTION 281

If inline-TCP-evasion-protection-mode on a Cisco IPS is set to asymmetric mode, what is a side effect?

- A. Packet flow is normal.
- B. TCP requests are throttled.
- C. Embryonic connections are ignored.
- D. Evasion may become possible.

Answer: D

NEW QUESTION 284

Which signature engine is responsible for ICMP inspection on Cisco IPS?

- A. AIC Engine
- B. Fixed Engine
- C. Service Engine
- D. Atomic IP Engine

Answer: D

NEW QUESTION 289

What is the access-list command on a Cisco IPS appliance used for?

- A. to permanently filter traffic coming to the Cisco IPS appliance via the sensing port
- B. to filter for traffic when the Cisco IPS appliance is in the inline mode
- C. to restrict management access to the sensor
- D. to create a filter that can be applied on the interface that is under attack

Answer: C

NEW QUESTION 294

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 298

Who or what calculates the signature fidelity rating?

- A. the signature author
- B. Cisco Professional Services
- C. the administrator
- D. the security policy

Answer: A

NEW QUESTION 299

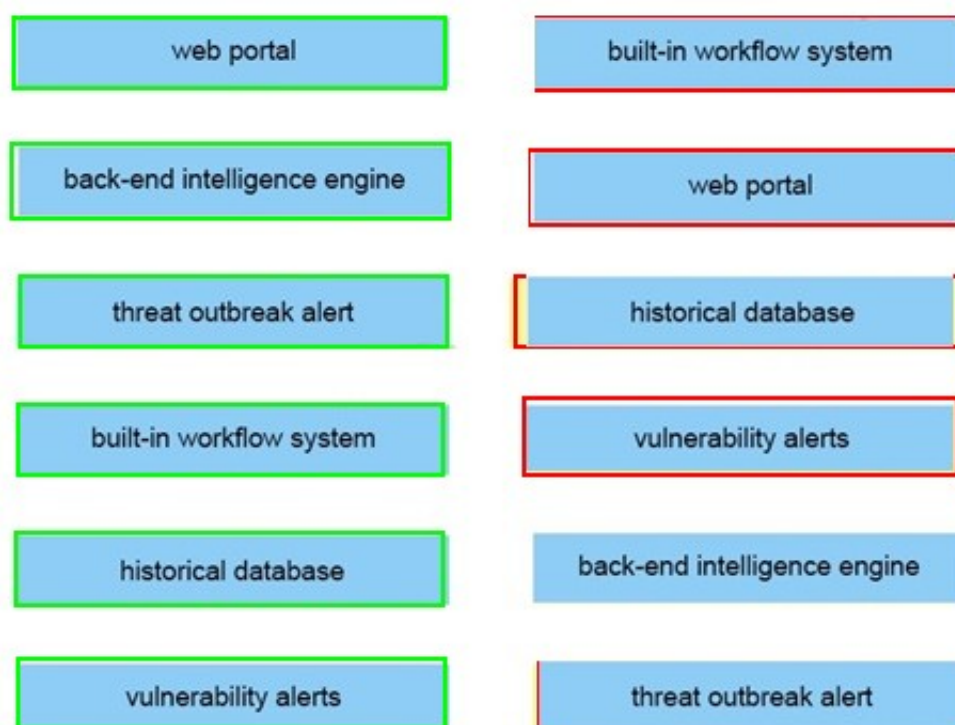
DRAG DROP

Drag and drop the Cisco Security IntelliShield Alert Manager Service components on the left onto the corresponding description on the right.



Answer:

Explanation:



NEW QUESTION 304

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 309

Which Cisco technology secures the network through malware filtering, category-based control, and reputation-based control?

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

Answer: C

NEW QUESTION 310

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 315

DRAG DROP

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.	step 1
Define interfaces and subinterfaces on the physical appliance.	step 2
Define additional settings for each security context.	step 3
Deploy to generate the virtual firewalls as children of the base appliance.	step 4
Define an admin context for administering the base security appliance.	step 5

Answer:

Explanation:

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

NEW QUESTION 317

Refer to the exhibit.

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.

V120 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](#)

[Home](#)
[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](#)

Cisco C100V
Email Security Virtual Appliance

Logged in as: **admin** on **esa.secure-x.local**
[My Favorites](#) - [Options](#) - [Help and Support](#)

[Home](#)
[Monitor](#)
[Mail Policies](#)
[Security Services](#)
[Network](#)
[System Administration](#)

No Changes Pending

HAT Overview

Find Senders

[Find](#)

Sender Groups (List)
 [Add Sender Group...](#)

Order	Sender
1	RELAYLI
2	WHITEL
3	BLACKKL
4	SUSPEC
5	UNKNOW
	ALL

[Edit Order...](#)

Email Security Manager
 Incoming Mail Policies
 Incoming Content Filters
 Outgoing Mail Policies
 Outgoing Content Filters
 Host Access Table (HAT)
 HAT Overview
 Mail Flow Policies
 Exception Table
 Address Lists
 Recipient Access Table (RAT)
 Destination Controls
 Bounce Verification
 Data Loss Prevention (DLP)
 DLP Policy Manager
 DLP Message Actions
 Domain Keys
 Verification Profiles
 Signing Profiles
 Signing Keys
 Text Resources
 Dictionaries

[Find](#)

Policies (Listener: IncomingMail 172.16.16.25:25)
 [Import HAT...](#)

SenderBase™ Reputation Score	Mail Flow Policy	Delete
-4 -2 0 2 4 6 8 +10	RELAYED	
	TRUSTED	
	BLOCKED	
	THROTTLED	
	ACCEPTED	
	ACCEPTED	

[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...

HAT Overview

Find Senders

Find Senders that Contain this Text: **Find**

Sender Groups (Listeners: IncomingMail 172.16.16.25:25)

Add Sender Group... **Import HAT...**

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	

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...

Mail Flow Policy

Policies (Listeners: IncomingMail 172.16.16.25:25)

Add Policy...

Policy Name: **ACCEPTED**
Behavior: **Accept**
Delete:

Host Access Table (HAT)

HAT Overview
Mail Flow Policies
Exception Table
Address Lists

Recipient Access Table (RAT)

Destination Controls
Bounce Verification

Data Loss Prevention (DLP)

DLP Policy Manager
DLP Message Actions

Domain Keys

Verification Profiles
Signing Profiles
Signing Keys

Text Resources

Dictionaries

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: 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) ☐

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)

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

Mail Flow Policies

IncomingMail 172.16.16.25:25

Edit Policy Settings

Connection Behavior

Connection Behavior

Max. Recipients 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. Recipients From a Single IP: ☒ Use Default (10) ☐

SMTP Banner Code: ☒ Use Default (220) ☐

SMTP Banner Text: ☒ Use Default () ☐

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

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

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text: Find

Sender List: Display All Items in List

Add Sender...

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-k.local**
My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

Sender Group Settings

Sender Group Settings

Find Senders

Sender List: Display

There are no senders

Email Security Manager

- Incoming Mail Policies
- Incoming Content Filters
- Outgoing Mail Policies
- Outgoing Content Filters

Host Access Table (HAT)

- HAT Overview
- Mail Flow Policies
- Exception Table
- Address Lists

Recipient Access Table (RAT)

- Destination Controls
- Bounce Verification

Data Loss Prevention (DLP)

- DLP Policy Manager
- DLP Message Actions

Domain Keys

- Verification Profiles
- Signing Profiles
- Signing Keys

Text Resources

- Dictionaries

IncomingMail 172.16.16.25:25

ST

ers are rejected

D

+3.0

cluded

Edit Settings...

Find

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

Cisco C100V
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

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) ☐
- 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

Mail Flow Policy: IncomingMail 172.16.16.25:25

Edit Policy Settings

Connection Behavior

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 Banner Code: ☒ Use Default (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

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

Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name:

Connection Behavior:

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)

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

<< 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
hq-mail.maroon.public	None	<input type="checkbox"/>

<< Back to HAT Overview Delete

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: 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

<< 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
hq-mail.maroon.public	None	<input type="checkbox"/>

<< Back to HAT Overview Delete

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 -

MonitorMail PoliciesSecurity ServicesNetworkSystem 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

<< Back to HAT OverviewEdit Settings...


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 -

MonitorMail PoliciesSecurity ServicesNetworkSystem Administration

No Changes Pending

Sender Group: 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

<< Back to HAT OverviewEdit Settings...

Find Senders

Find Senders that Contain this Text:

Sender List: Display All Items in List

There are no senders.

Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing Content Filters
Host Access Table (HAT)
HAT Overview
Mail Flow Policies
Exception Table
Address Lists
Recipient Access Table (RAT)
Destination Controls
Bounce Verification
Data Loss Prevention (DLP)
DLP Policy Manager
DLP Message Actions
Domain Keys
Verification Profiles
Signing Profiles
Signing Keys
Text Resources
Dictionaries

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:

Connection Behavior:

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) ☐

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:

Connection Behavior:

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) ☐

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:

Connection Behavior:

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) ☐

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:

Connection Behavior:

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) ☐

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

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text: Find

Sender List: Display All Items in List

Add Sender...

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

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

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text: Find

Sender List: Display All Items in List

Add Sender...

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

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

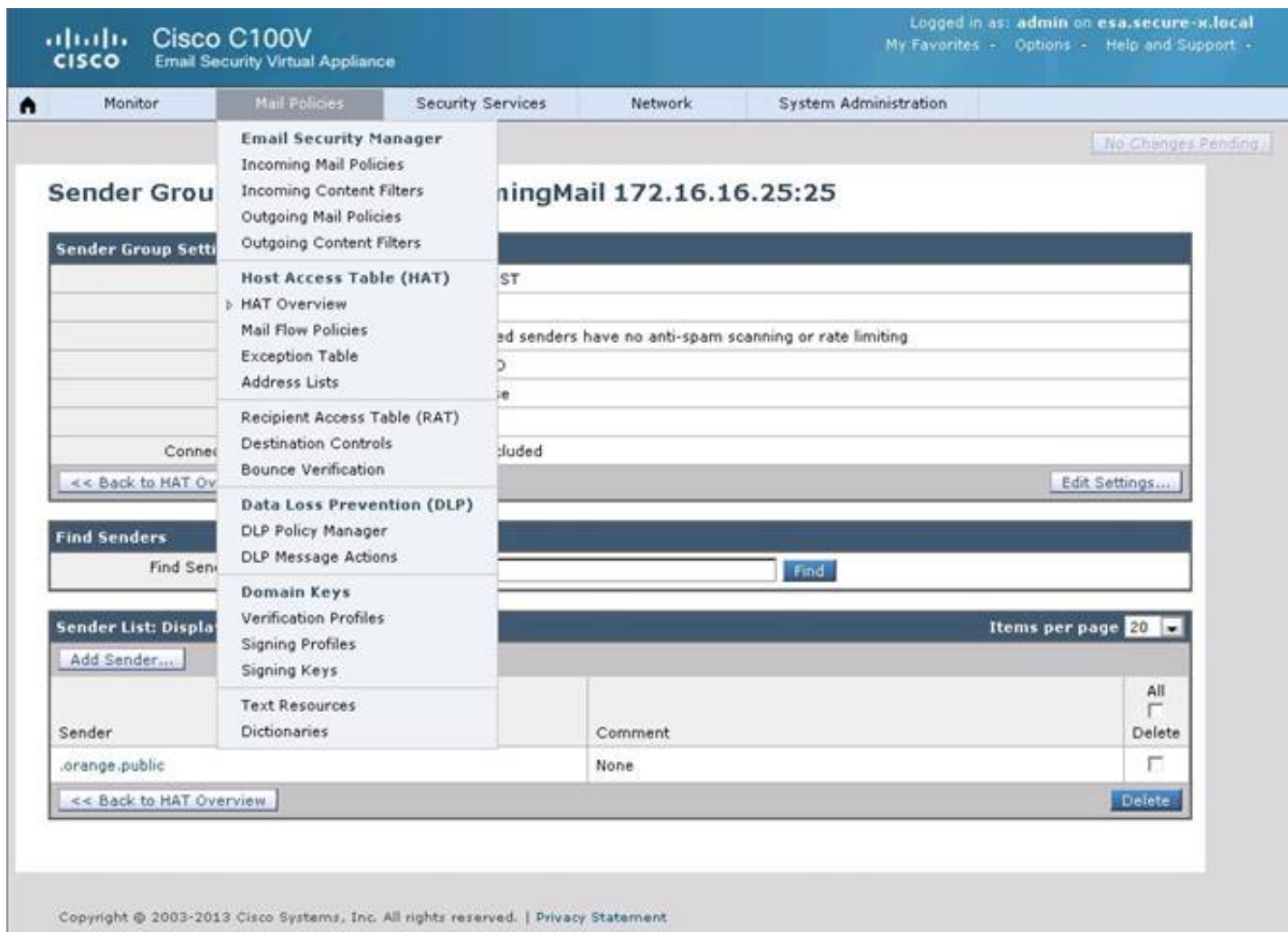
Sender List: Display All Items in List

Add Sender...

Sender	Comment	
.orange.public	None	<input type="checkbox"/> All <input type="checkbox"/> Delete

<< Back to HAT Overview Delete

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

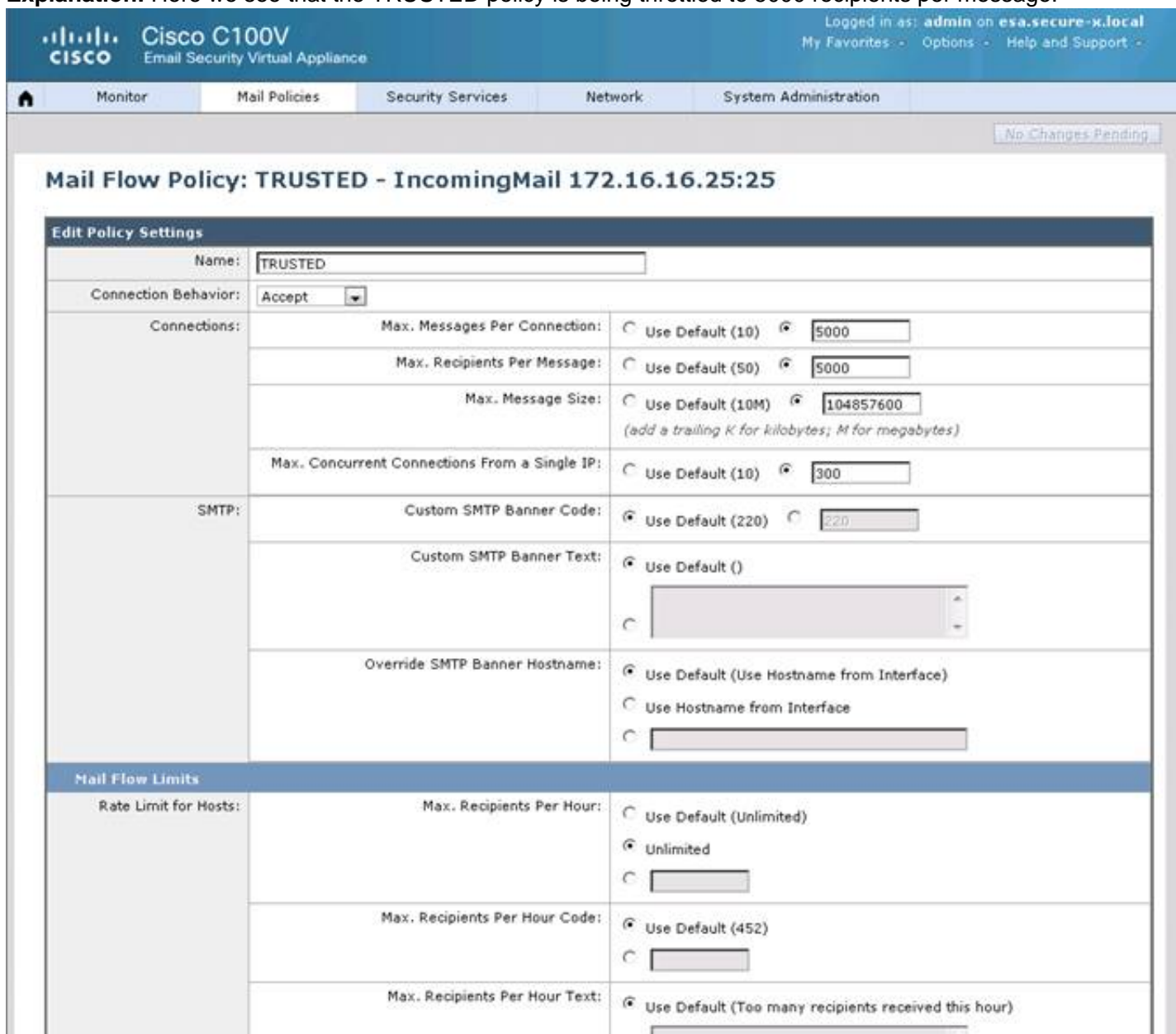


For which domains will the Cisco Email Security Appliance allow up to 5000 recipients per message?

- 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

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

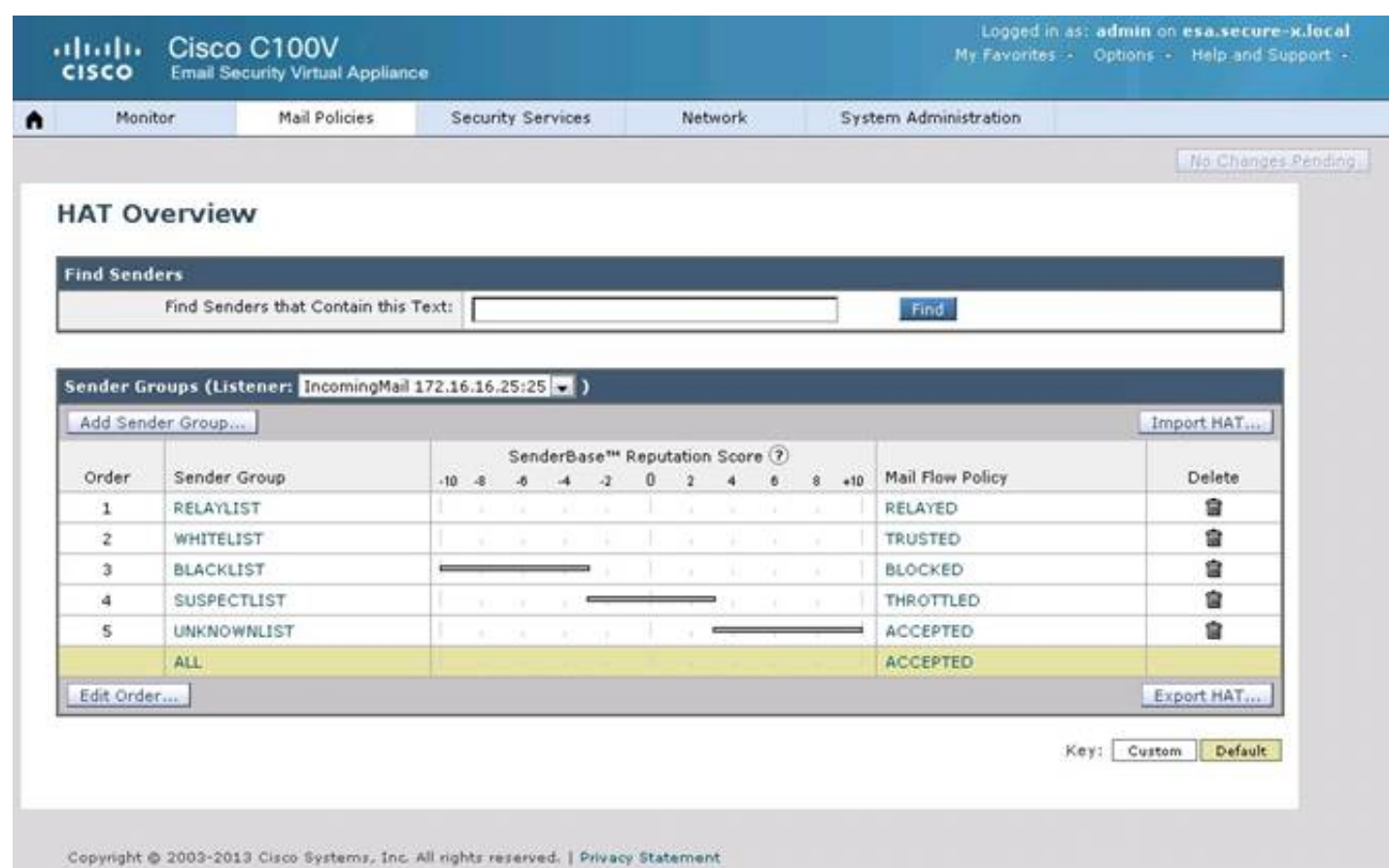
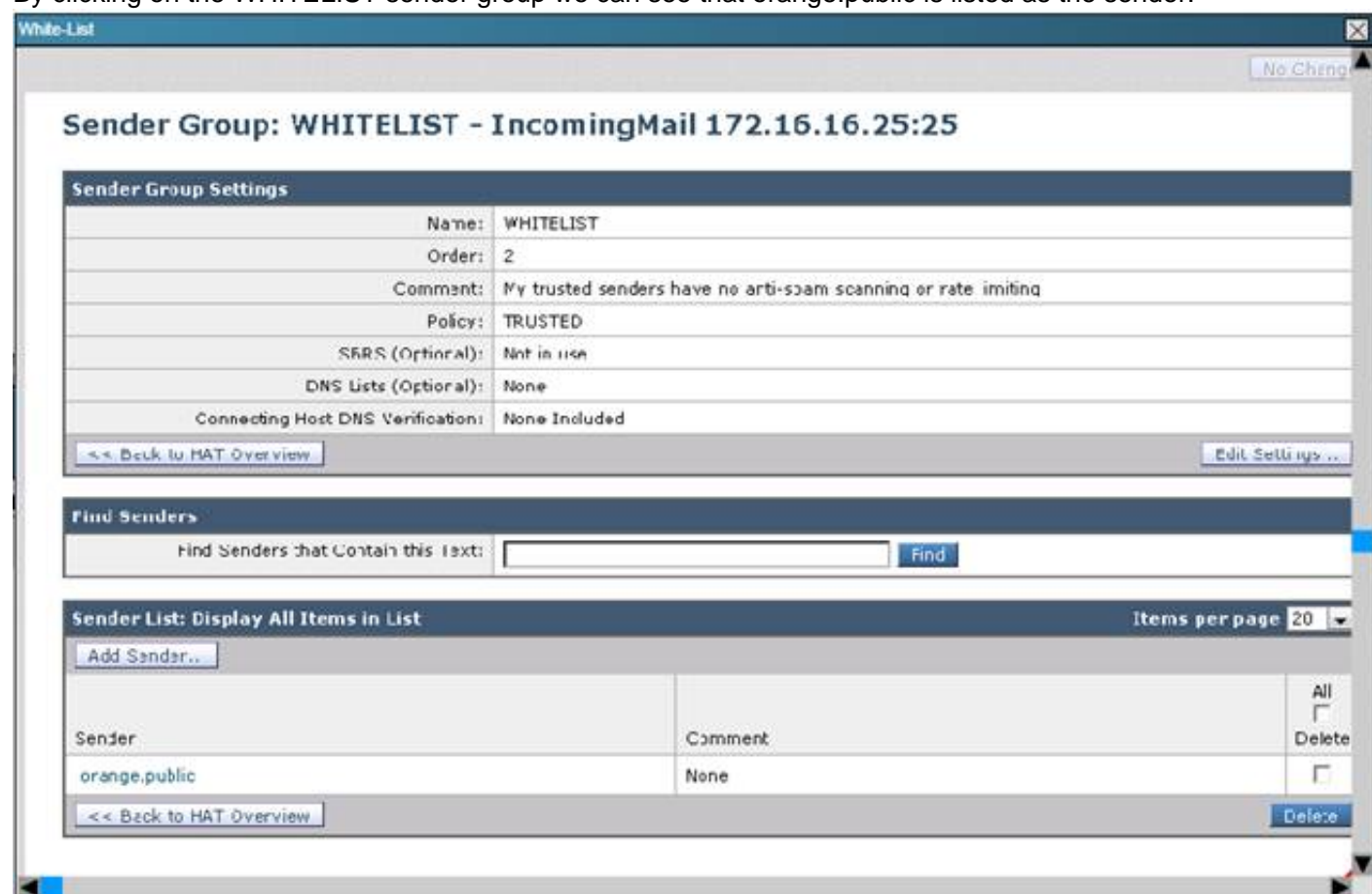


Image 27

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



Capture

NEW QUESTION 321

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 324

Which two commands are valid URL filtering commands? (Choose two.)

- A. url-server (DMZ) vendor smartfilter host 10.0.1.1
- B. url-server (DMZ) vendor url-filter host 10.0.1.1
- C. url-server (DMZ) vendor n2h2 host 10.0.1.1
- D. url-server (DMZ) vendor CISCO host 10.0.1.1
- E. url-server (DMZ) vendor web host 10.0.1.1

Answer: AC

NEW QUESTION 329

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 10.1.1.0.0.0.255 192.168.1.0.0.0.255hostname(config)# class-map inspection_defaulthostname(config-cmap)# match access-list inspect
- B. hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0 192.168.1.0255.255.255.0hostname(config-cmap)# match access-list inspect
- C. hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0 192.168.1.0255.255.255.0hostname(config)# class-map inspection_defaulthostname(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_overview.html

NEW QUESTION 332

Which Cisco ASA configuration command drops traffic if the Cisco ASA CX module fails?

- A. no fail-open
- B. fail-close
- C. fail-close auth-proxy
- D. auth-proxy

Answer: B

NEW QUESTION 337

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 338

What Event Action in an IPS signature is used to stop an attacker from communicating with a network using an access-list?

- A. Request Block Host
- B. Deny Attacker Inline
- C. Deny Connection Inline
- D. Deny Packet Inline
- E. Request Block Connection

Answer: A

NEW QUESTION 343

Which settings are required when deploying Cisco IPS in high-availability mode using EtherChannel load balancy?

- A. ECLB IPS appliances must not be in on-a-stick mode, ECLB IPS solution maintains state if asensor goes down, and TCP flow is forced through the same IPS appliance flow
- B. ECLB IPS appliances must be in on-a-stick mode, ECLB IPS solution does not maintain state ifa sensor goes down, and TCP flow is forced through a different IPS appliance.
- C. ECLB IPS appliances must not be in on-a-stick mode, ECLB IPS solution does not maintainstate if a sensor goes down, and TCP flow is forced through a different IPS appliance.

Answer: B

Explanation: http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_example_09186_a0080671a8d.shtml

NEW QUESTION 344

Which three functions can Cisco Application Visibility and Control perform within Cisco Cloud Web Security? (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 349

.....

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 300-207 Exam with Our Prep Materials Via below:

<https://www.certleader.com/300-207-dumps.html>