Cisco

Exam Questions 300-210

Implementing Cisco Threat Control Solutions (SITCS)

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

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

Answer: B

NEW QUESTION 2
- (Exam Topic 1)
A university policy has to allow open access to resources on the Internet for research, but internal workstations have been exposed to malware. Which AMP feature allows the engineering team to determine whether a file is installed on a selected few workstations?

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

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

A. clean
B. disconnected
C. unavailable
D. unknown

Answer: C

NEW QUESTION 4
- (Exam Topic 1)
An engineer is configuring a Cisco Email Security Appliance (ESA) and chooses "Preferred" as the settings for TLS on a HAT Mail Flow Policy. Which result occurs?.

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

Answer: D

NEW QUESTION 5
- (Exam Topic 1)
Which two dynamic routing protocols are supported in FirePower Threat Defense v6.0? (Choose Two)

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

Answer: BC

NEW QUESTION 6
- (Exam Topic 1)
An enginner manages a Cisco Intrusion Prevention System via IME. A new user must be able to tune signatures, but must not be able to create new users. Which role for the new user is correct?

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

Answer: C

NEW QUESTION 7

- (Exam Topic 1)
Which Cisco Advanced Matware Protection event is generated when a file disposition changes because more information is gathered and evaluated about the file?

A. quarantine event
B. threat detected event
C. policy update event
D. retrospective event

Answer: D

NEW QUESTION 8
- (Exam Topic 1)
A web security appliance is inspecting inbound traffic. In which sequence is inbound https traffic inspected?

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

Answer: B

NEW QUESTION 9
- (Exam Topic 1)
which two tasks can the network discovery feature perform? (choose two)

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

Answer: AC

NEW QUESTION 10
- (Exam Topic 1)
What is difference between a Cisco Content Security Management virtual appliance and a physical appliance?

A. Migration between virtual appliance of varying sizes is possible, but physical appliances must be of equal size.
B. The virtual appliance requires an additional license to run on a host.
C. The virtual appliance requires an additional license to activate its adapters.
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: B

NEW QUESTION 10
- (Exam Topic 1)
Which type of policy is used to define the scope for applications that are running on hosts?

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

Answer: C

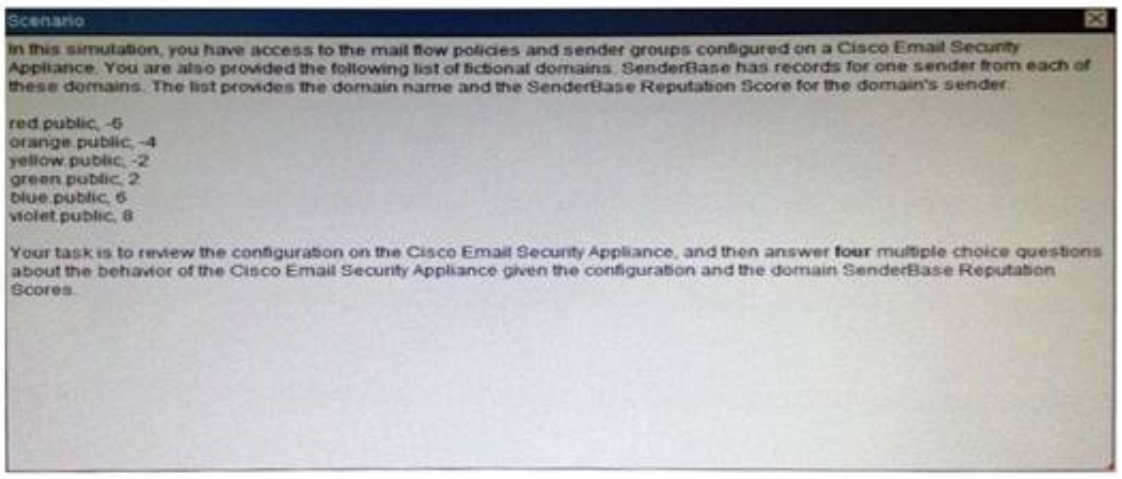
NEW QUESTION 15
- (Exam Topic 1)
Which three access control actions permit traffic to pass through the device when using Cisco FirePOWER? (Choose three.)

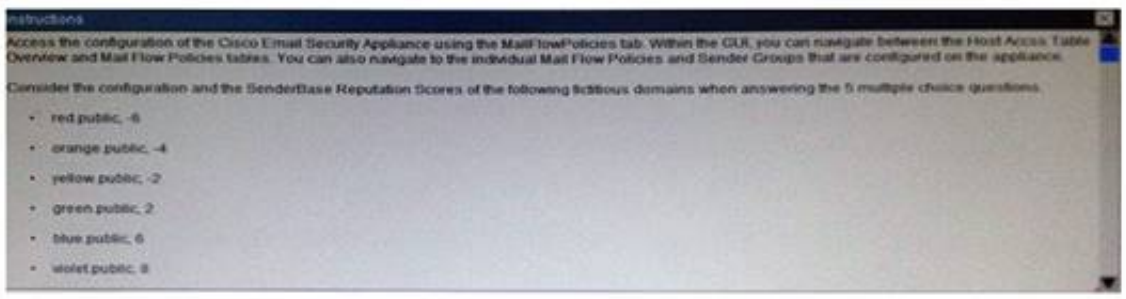
A. pass
B. trust
C. monitor
D. allow
E. permit
F. inspect

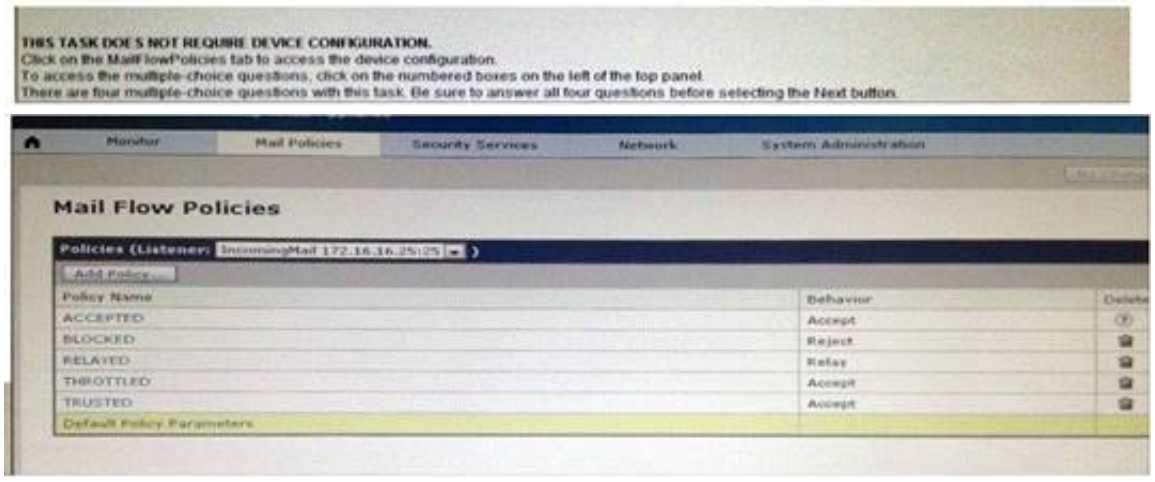
Answer: BCD

Explanation:
http://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/A

NEW QUESTION 18
- (Exam Topic 1)







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 23
- (Exam Topic 1)
With Cisco AMP for Endpoints on Windows, which three engines are available in the connector? (Choose three.)

A. Ethos
B. Tetra
C. Annos
D. Spero
E. Talos
F. ClamAV

Answer: ABD

Explanation:
http://www.cisco.com/c/en/us/products/collateral/security/fireamp-private-cloud-virtual-appliance/datasheet-c780.html

NEW QUESTION 28
- (Exam Topic 1)

Your organization has subscribed to the Cisco Cloud Web Security (CWS) service. You have been assigned the task of configuring the CWS connector on the ISR-G2 router at a branch office. Detail of the configuration requirement include:
. Content scanning should be enabled for traffic outbound from FastEthernet0/1
. Explicitly specify 8080 for both the http and the https ports
. The primary CWS proxy server is proxy-a.scansafe.net
. The secondary CWS proxy server is proxy-b.scansafe.net
. The unencrypted license key is 0123456789abcdef
. If the CWS proxy servers are not available, web traffic from the branch office should be denied
. After configuration, use show commands to verify connectivity with the CWS service and scan activity
You can access the console of the ISR at the branch office using the icon on the topology display. The enable password is Cisco!23.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Pending

NEW QUESTION 31
- (Exam Topic 1)
A system administrator wants to know if the email traffic from a remote partner will active special treatment message filters that are created just for them. Which tool on the Cisco Email Security gateway can you use to debug and emulate the flow that a message takes through the work queue?

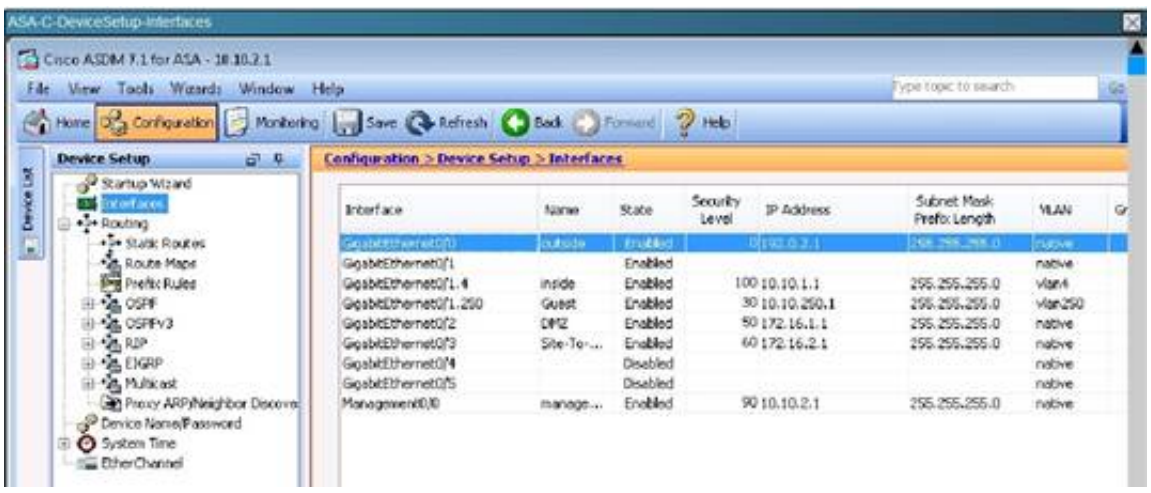
A. the trace tool
B. centralized or local message tracking
C. the CLI findevent command
D. the CLI grep command
E. the message tracker interface

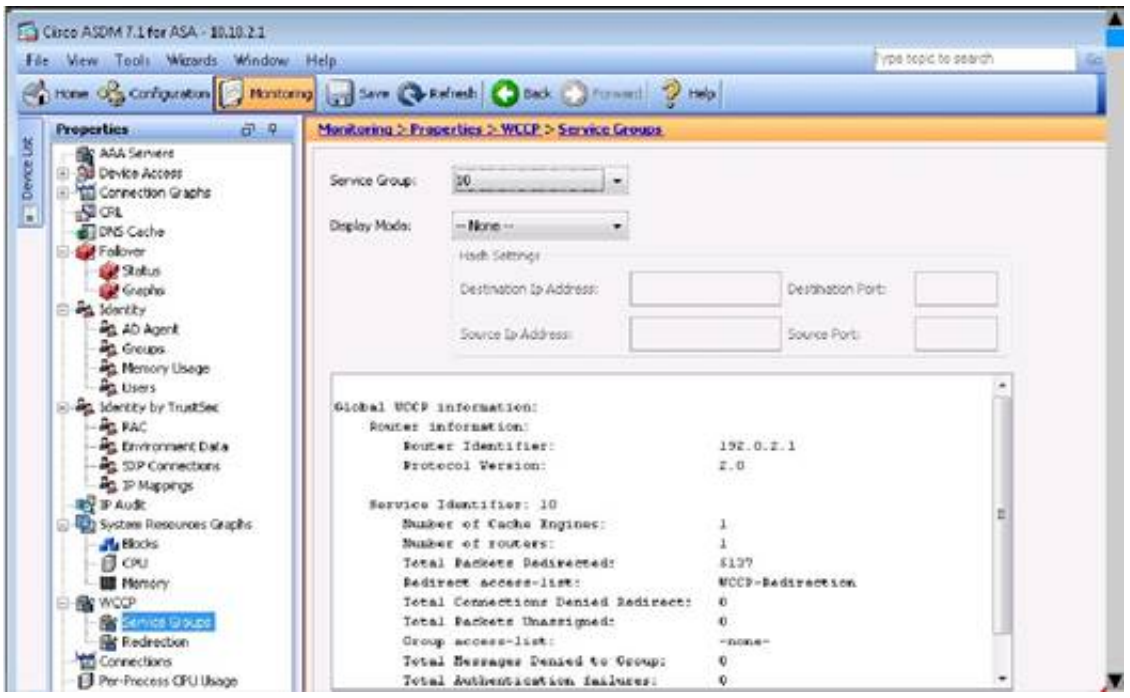
Answer: A

NEW QUESTION 33
- (Exam Topic 1)
The Web Cache Communication Protocol (WCCP) is a content-routing protocol that can facilitate the redirection of traffic flows in real time. Your organization has deployed WCCP to redirect web traffic that traverses their Cisco Adaptive Security Appliances (ASAs) to their Cisco Web Security Appliances (WSAs).
The simulator will provide access to the graphical user interfaces of one Cisco ASA and one Cisco WSA that are participating in a WCCP service. Not all aspects of the GUIs are implemented in the simulator. The options that have been implemented are sufficient to determine the best answer to each of the questions that are presented.
Your task is to examine the details available in the simulated graphical user interfaces and select the best answer.


Adaptive
Security Appliance

Web
Security Appliance



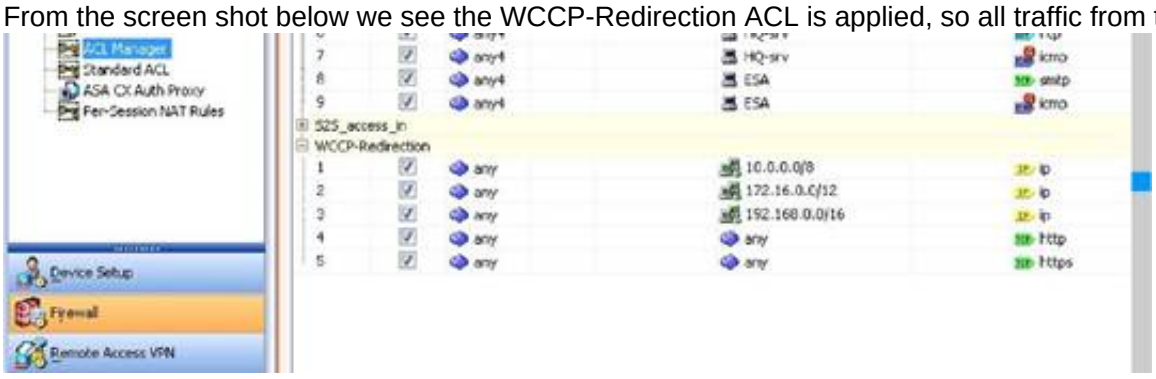


What traffic is not redirected by WCCP?

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

Answer: B

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



NEW QUESTION 36
- (Exam Topic 1)
which two options are the basic parts of a Snort rule? (Choose two)

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

Answer: BD

NEW QUESTION 40
- (Exam Topic 1)
Which three routing options are valid with Cisco FirePOWER version 5.4? (Choose three.)

A. Layer 3 routing with EIGRP
B. Layer 3 routing with OSPF not-so-stubby area
C. Layer 3 routing with RiPv2
D. Layer 3 routing with RIPvl

E. Layer 3 routing with OSPF stub area
F. Layer 3 routing with static routes

Answer: DEF

Explanation:
http://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/Inhtml

NEW QUESTION 44
- (Exam Topic 1)
After configuring an ISR with the Cisco Cloud Web security connector, which command does a network engineer run to verify connectivity to the CVV proxy?

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

Answer: A

NEW QUESTION 46
- (Exam Topic 1)
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 49
- (Exam Topic 1)
Which CLI command is used to generate firewall debug messages on a Cisco FirePOWER sensor?

A. system support ssl-debug
B. system support firewall-engine-debug
C. system support capture-traffic
D. system support platform

Answer: C

NEW QUESTION 53
- (Exam Topic 1)
Which two appliances support logical routed interfaces? (Choose two.)

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

Answer: D

NEW QUESTION 58
- (Exam Topic 1)
Which two routing options are valid with cisco firePOWER threat Defense version 6.0?(choose two)

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

Answer: AD

NEW QUESTION 61
- (Exam Topic 1)
Which piece of information is required to perform a policy trace for the Cisco WSA?

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

Answer:

C

NEW QUESTION 63
- (Exam Topic 1)
ACisco ASA requires an additional feature license to enable which feature?

A. transparent firewall
B. cut-thru proxy
C. threat detection
D. botnet traffic filtering
E. TCP normalizer

Answer: D

NEW QUESTION 64
- (Exam Topic 1)
User wants to deploy your managed device in Layer 3 routed mode and must configure a virtual router and a routed interface. Which managed shows this configuration?

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

Answer: C

NEW QUESTION 69
- (Exam Topic 1)
When using Cisco FirePOWFR Services for ASA, how is traffic directed form based Cisco ASA to the CiscoPOWER Services?

A. SPAN port on a Cisco Catalyst switch.
B. WCCP on the ASA.
C. inline interface pair on the Cisco FirePOWER module.
D. service policy on the ASA.

Answer: A

NEW QUESTION 70
- (Exam Topic 1)
Which type of server is required to communicate with a third-party DLP solution?

A. an ICAP-capable proxy server
B. a PKI certificate server
C. an HTTP server
D. an HTTPS server

Answer: A

NEW QUESTION 71
- (Exam Topic 1)
Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the Host Access Table Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance. Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the four multiple choice questions.

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

Answer: D

NEW QUESTION 72
- (Exam Topic 1)
Which detection method is also known as machine learning on Network-based Cisco Advanced Malware Protection?

A. custom file detection
B. hashing
C. Spero engine
D. dynamic analysis

Answer: D

NEW QUESTION 77

- (Exam Topic 1)
Which statement about the Cisco ASA botnet traffic filter is true?

A. The four threat levels are low, moderate, high, and very high.
B. By default, the dynamic-filter drop blacklist interface outside command drops traffic with a threat level of high or very high.
C. Static blacklist entries always have a very high threat level.
D. A static or dynamic blacklist entry always takes precedence over the static whitelist entry.

Answer: C

NEW QUESTION 79
- (Exam Topic 1)
After adding a remote-access IPsec tunnel via the VPN wizard, an administrator needs to tune the IPsec policy parameters. Where is the correct place to tune the IPsec policy parameters in Cisco ASDM?

A. IPsec user profile
B. Crypto Map
C. Group Policy
D. IPsec policy
E. IKE policy

Answer: D

NEW QUESTION 84
- (Exam Topic 2)
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 86
- (Exam Topic 2)

Instructions

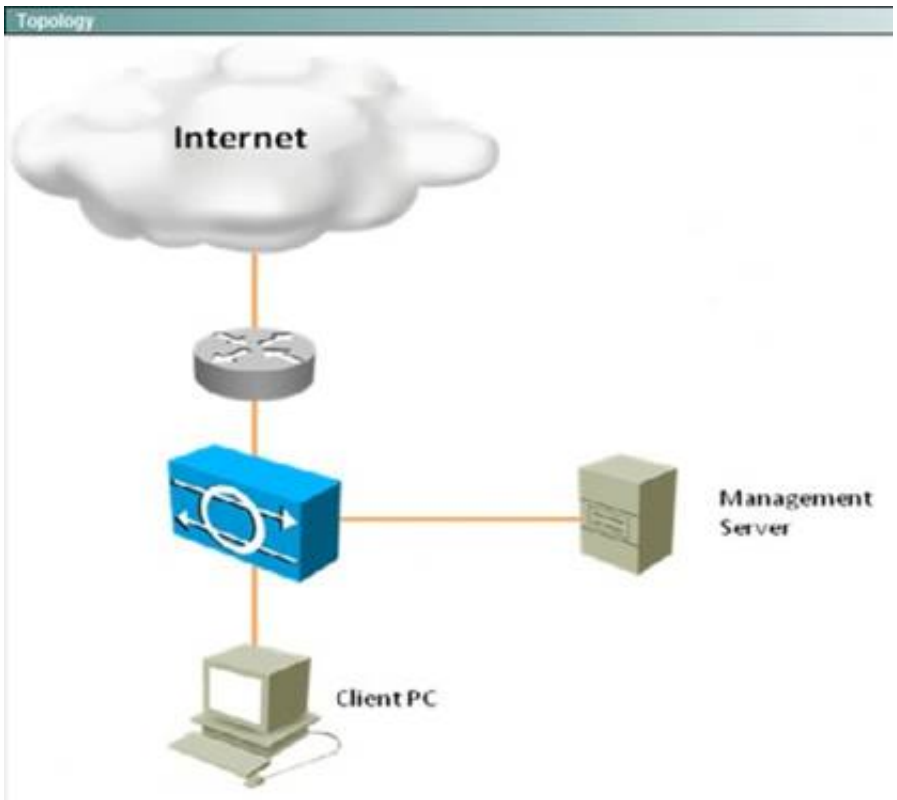
You can click the grey buttons at the bottom of this frame to view the different windows.

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

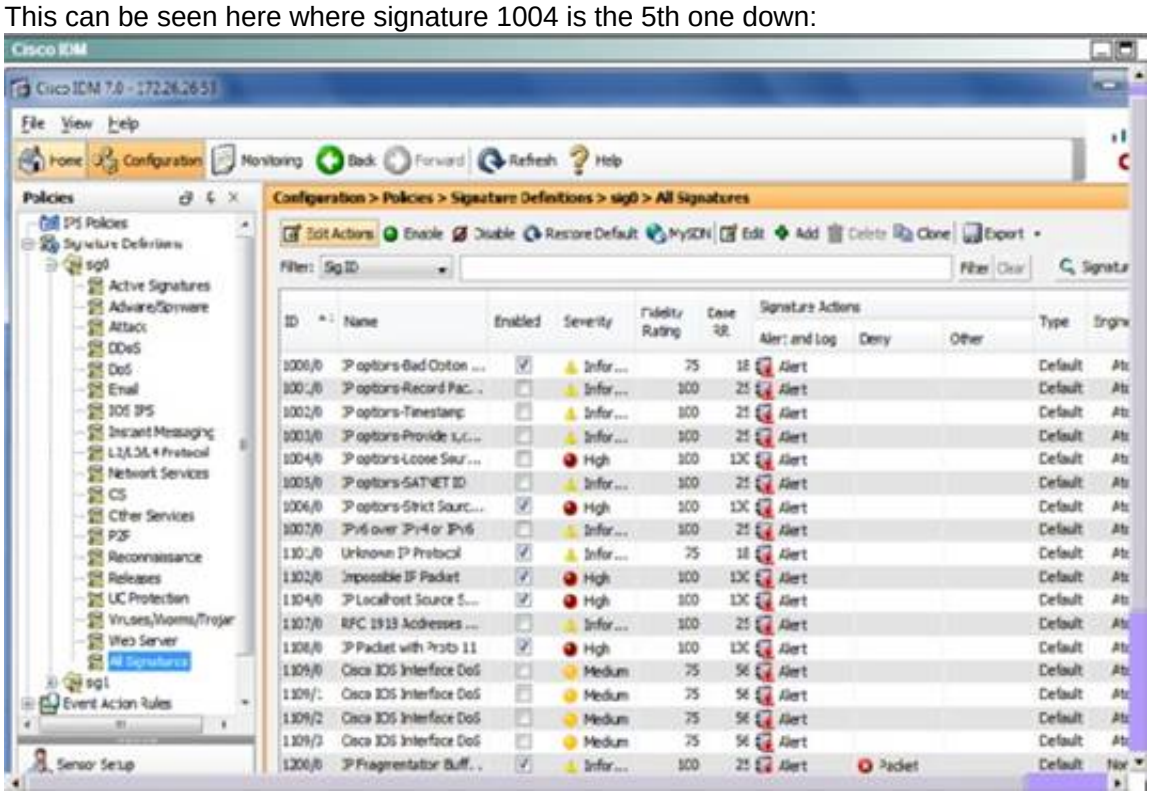


Which two statements about Signature 1104 are true? (Choose two.)

A. This is a custom signature.
B. The severity level is High.
C. This signature has triggered as indicated by the red severity icon.
D. Produce Alert is the only action defined.
E. This signature is enabled, but inactive, as indicated bythe/0 to that follows the signature number.

Answer: BD

Explanation:
This can be seen here where signature 1004 is the 5th one down:



NEW QUESTION 91
- (Exam Topic 2)
Which Cisco Web Security Appliance design requires minimal change to endpoint devices?

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

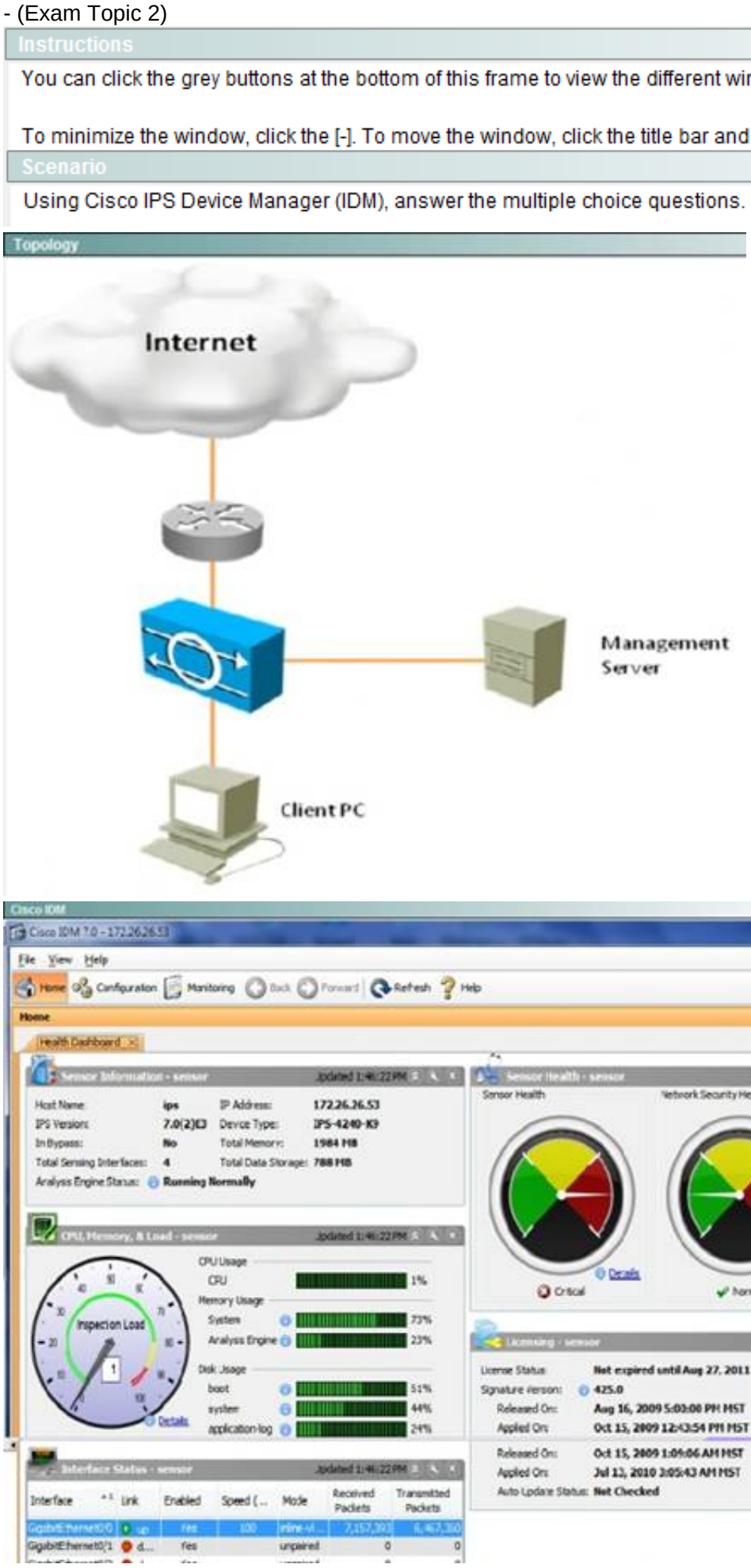
Answer: A

NEW QUESTION 96
- (Exam Topic 2)
During initial configuration, the Cisco ASA can be configured to drop all traffic if the ASACX SSP fails by using which command in a policy-map?

A. cxsc fail
B. cxsc fail-close
C. cxsc fail-open
D. cxssp fail-close

Answer: B

NEW QUESTION 100
- (Exam Topic 2)



Which three statements about the Cisco IPS appliance configurations are true? (Choose three.)

A. The maximum number of denied attackers is set to 10000.
B. The block action duraton is set to 3600 seconds.
C. The Meta Event Generator is globally enabled.
D. Events Summarization is globally disabled.
E. Threat Rating Adjustment is globally disabled.

Answer: ABC

NEW QUESTION 103
- (Exam Topic 2)
Which three zones are used for anomaly detection? (Choose three.)

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

Answer: ABC

NEW QUESTION 105
- (Exam Topic 2)
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 109
- (Exam Topic 2)
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 111
- (Exam Topic 2)
Which port is used for CLI Secure shell access?

A. Port 23
B. Port 25
C. Port 22
D. Port 443

Answer: C

NEW QUESTION 112
- (Exam Topic 2)
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 113
- (Exam Topic 2)
Which five system management protocols are supported by the Cisco Intrusion Prevention System? (Choose five.)

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

Answer: ABCFG

NEW QUESTION 114
- (Exam Topic 2)
What are two benefits of using SPAN with promiscuous mode deployment? (Choose two.)

A. SPAN does not introduce latency to network traffic.
B. SPAN can perform granular scanning on captures of per-IP-address or per-port monitoring.
C. Promiscuous Mode can silently block traffic flows on the IDS.
D. SPAN can analyze network traffic from multiple points.

Answer: AD

NEW QUESTION 119

- (Exam Topic 2)
Which two GUI options display users' activity in Cisco Web Security Appliance? (Choose two.)

A. Web Security Manager Identity Identity Name
B. Security Services Reporting
C. Reporting Users
D. Reporting Reports by User Location

Answer: CD

NEW QUESTION 120
- (Exam Topic 2)
Which two Cisco IPS events will generate an IP log? (Choose two.)

A. A signature had an event action that was configured with log packets.
B. A statically configured IP or IP network criterion was matched.
C. A dynamically configured IP address or IP network was matched.
D. An attack produced a response action.

Answer: AB

NEW QUESTION 122
- (Exam Topic 2)
Which two options are characteristics of router-based IPS? (Choose two.)

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

Answer: CE

NEW QUESTION 123
- (Exam Topic 2)
Which two benefits are provided by the dynamic dashboard in Cisco ASDM Version 5.2? (Choose two.)

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

Answer: CE

NEW QUESTION 124
- (Exam Topic 2)
What is the authentication method for an encryption envelope that is set to medium security?

A. The recipient must always enter a password, even if credentials are cached.
B. A password is required, but cached credentials are permitted.
C. The recipient must acknowledge the sensitivity of the message before it opens.
D. The recipient can open the message without authentication.

Answer: B

NEW QUESTION 127
- (Exam Topic 2)
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 130
- (Exam Topic 2)
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 131
- (Exam Topic 2)
Which command is used to enable strong ciphers on the Cisco Web Security Appliance?

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

Answer: B

NEW QUESTION 134
- (Exam Topic 2)
Which set of commands changes the FTP client timeout when the sensor is communicating with an FTP server?

A. sensor# configure terminal sensor(config)# service sensor sensor(config-hos)# network-settings sensor(config-hos-net)# ftp-timeout 500
B. sensor# configure terminal sensor(config)# service hostsensor(config-hos)# network-settings parameter ftp sensor(config-hos-net)# ftp-timeout 500
C. sensor# configure terminal sensor(config)# service host sensor(config-hos)# network-settings sensor(config-hos-net)# ftp-timeout 500
D. sensor# configure terminalsensor(config)# service network sensor(config-hos)# network-settings sensor(config-hos-net)# ftp-timeout 500

Answer: C

NEW QUESTION 138
- (Exam Topic 2)
What is the default IP range of the external zone?

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

Answer: B

NEW QUESTION 142
- (Exam Topic 2)
A new Cisco IPS device has been placed on the network without prior analysis. Which CLI command shows the most fired signature?

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

Answer: A

NEW QUESTION 144
- (Exam Topic 2)
A network engineer may use which three types of certificates when implementing HTTPS decryption services on the ASACX? (Choose three.)

A. Self Signed Server Certificate
B. Self Signed Root Certificate
C. Microsoft CA Server Certificate
D. Microsoft CA Subordinate Root Certificate
E. LDAP CA Server Certificate
F. LDAP CA Root Certificate
G. Public Certificate Authority Server Certificate
H. Public Certificate Authority Root Certificate

Answer: BDF

NEW QUESTION 148
- (Exam Topic 2)
What is the correct deployment for an IPS appliance in a network where traffic identified as threat traffic should be blocked and all traffic is blocked if the IPS fails?

A. Inline; fail open
B. Inline; fail closed
C. Promiscuous; fail open
D. Promiscuous; fail closed

Answer: B

NEW QUESTION 152
- (Exam Topic 2)
Which Cisco technology is a modular security service that combines a stateful inspection firewall with next-generation application awareness, providing near real-

time threat protection?

A. Cisco ASA 5500 series appliances
B. Cisco ASACX Context-Aware Security
C. WSA
D. Internet Edge Firewall / IPS

Answer: B

NEW QUESTION 155
- (Exam Topic 2)
Which Cisco technology combats viruses and malware with virus outbreak filters that are downloaded from Cisco SenderBase?

A. ASA
B. WSA
C. Secure mobile access
D. IronPort ESA
E. SBA

Answer: D

NEW QUESTION 156
- (Exam Topic 3)
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 158
- (Exam Topic 3)
Which option describes a customer benefit of the Cisco Security IntelliShield Alert Manager?

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

Answer: C

NEW QUESTION 162
- (Exam Topic 3)
A user is deploying a Cisco IPS appliance in a data center to mitigate most attacks, including atomic attacks. Which two modes does Cisco recommend using to configure for this? (Choose two.)

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

Answer: AD

NEW QUESTION 165
- (Exam Topic 3)
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 166
- (Exam Topic 3)
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

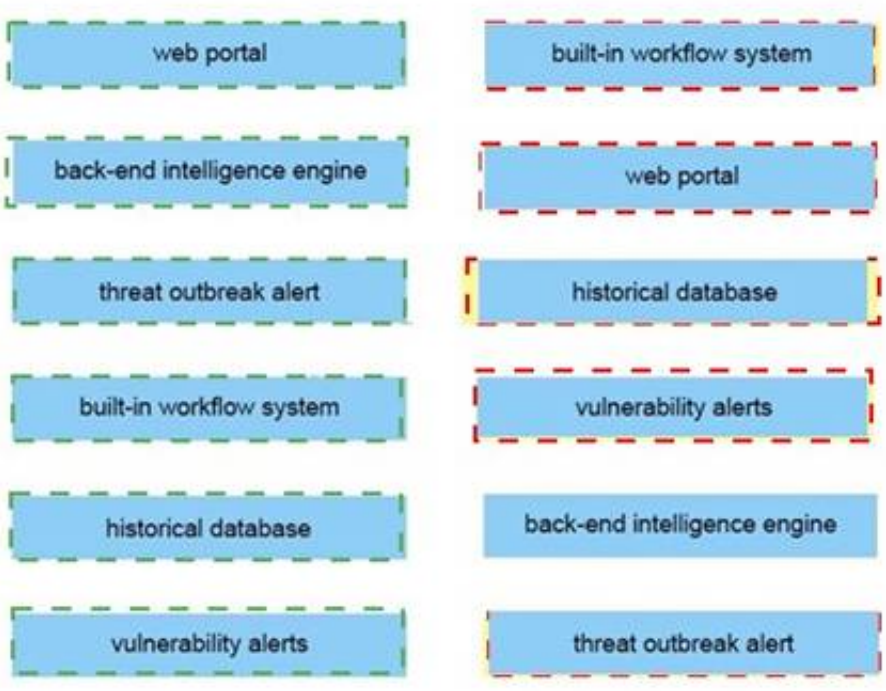
Answer: A

NEW QUESTION 168
- (Exam Topic 3)
Drag and drop the Cisco Security IntelliShield Alert Manager Service components on the left onto the corresponding description on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 171
- (Exam Topic 3)
Which sensor deployment mode does Cisco recommend when interface capacity is limited and you need to increase sensor functionality?

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

Answer: C

NEW QUESTION 173
- (Exam Topic 3)
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
- (Exam Topic 3)
Which Cisco Web Security Appliance feature enables the appliance to block suspicious traffic on all of its ports and IP addresses?

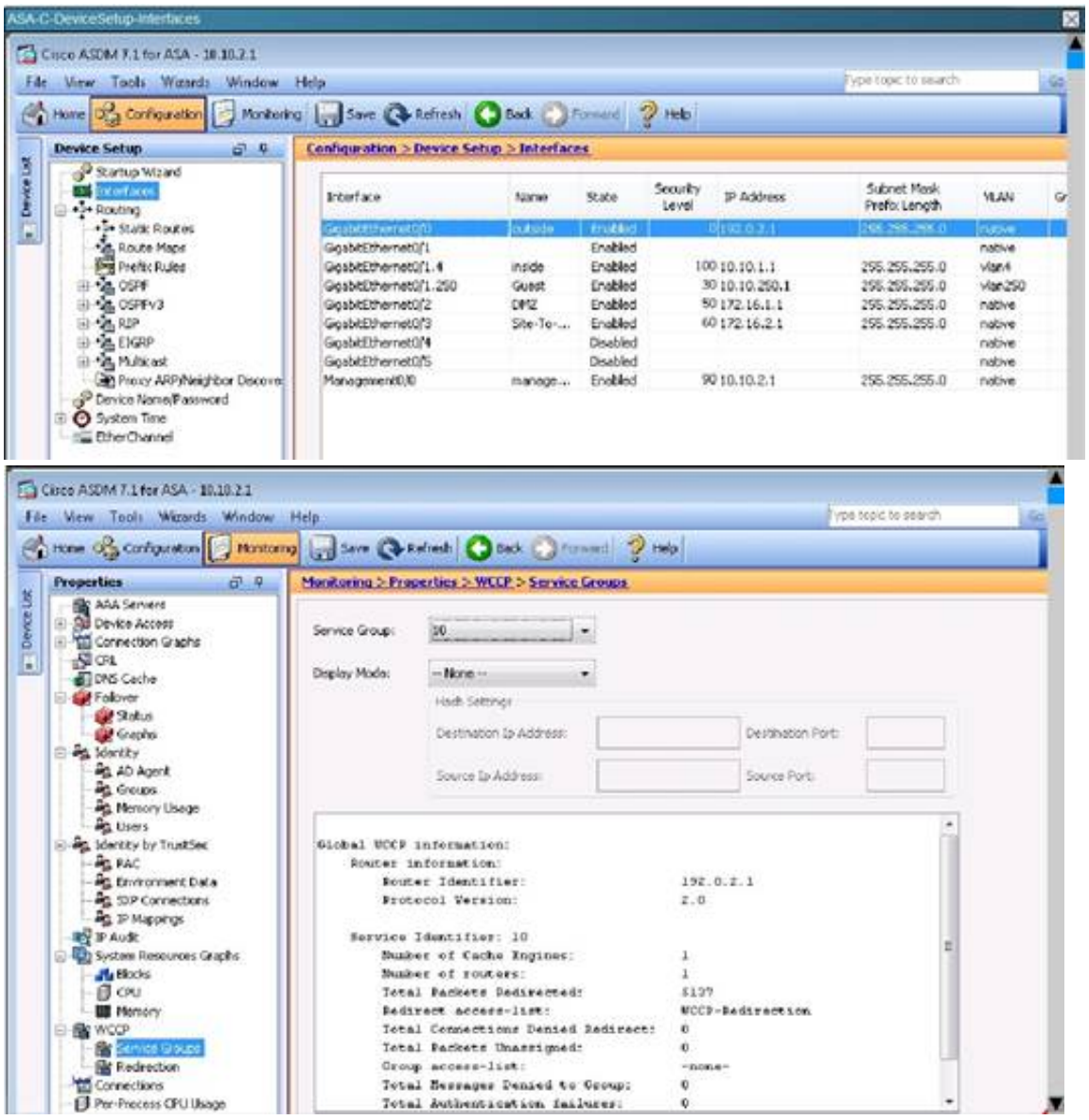
A. Layer 4 Traffic Monitor
B. Secure Web Proxy
C. explicit forward mode
D. transparent mode

Answer: A

NEW QUESTION 180
- (Exam Topic 3)
The Web Cache Communication Protocol (WCCP) is a content-routing protocol that can facilitate the redirection of traffic flows in real time. Your organization has deployed WCCP to redirect web traffic that traverses their Cisco Adaptive Security Appliances (ASAs) to their Cisco Web Security Appliances (WSAs).
The simulator will provide access to the graphical user interfaces of one Cisco ASA and one Cisco WSA that are participating in a WCCP service. Not all aspects of the GUIs are implemented in the simulator. The options that have been implemented are sufficient to determine the best answer to each of the questions that are presented.
Your task is to examine the details available in the simulated graphical user interfaces and select the best answer.

Adaptive
Security Appliance

Web
Security Appliance

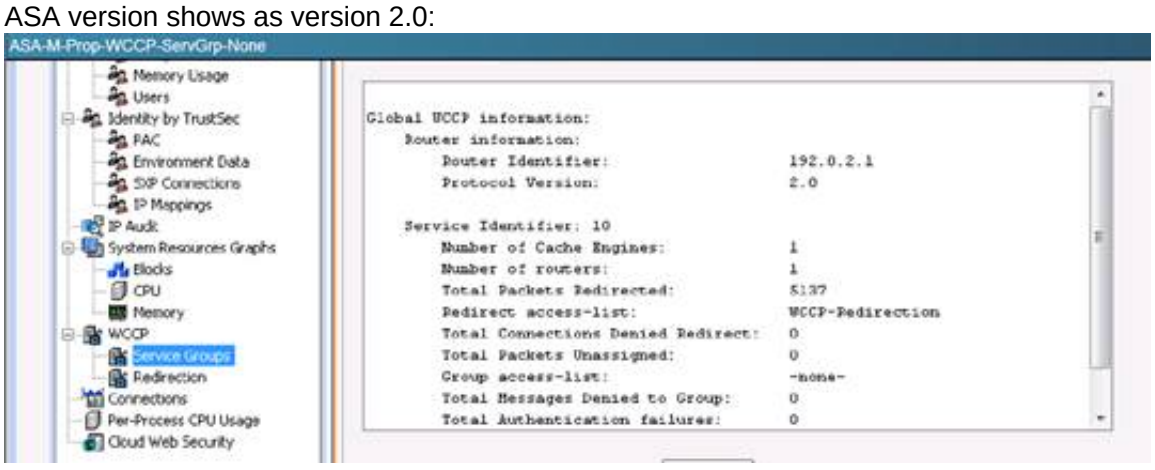


Which of the following is true with respect to the version of WCCP configured on the Cisco ASA and the Cisco WSA?

A. Both are configured for WCCP v1.
B. Both are configured for WCCP v2.
C. Both are configured for WCCP v3.
D. There is a WCCP version mismatch between the Cisco WSA and the Cisco ASA.

Answer: B

Explanation:
ASA version shows as version 2.0:



WSA also shows version 2 is being used:

NEW QUESTION 185
- (Exam Topic 3)
Which settings are required when deploying Cisco IPS in high-availability mode using EtherChannel load balancy?

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

Answer: C

Explanation:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_example09186 a0080671a8d.shtml

NEW QUESTION 189
- (Exam Topic 3)
Refer to the following.

Router (config) #username admin secret cisco Router (config) #no service password-encryption
How is the “cisco” password stored?

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

Answer: A

NEW QUESTION 193
- (Exam Topic 3)
Which option describes how the native VLAN is set up on an IPS sensor when VLAN groups are used in an inline deployment of the sensor?

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

Answer: C

NEW QUESTION 194
- (Exam Topic 3)
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 197
- (Exam Topic 3)
Which command allows the administrator to access the Cisco WSA on a secure channel on port 8443?

A. strictssl
B. adminaccessconfig
C. ssl
D. ssh

Answer: A

NEW QUESTION 200
- (Exam Topic 3)
Elliptic curve cryptography is a stronger more efficient cryptography method meant to replace which current encryption technology?

A. RSA
B. DES
C. AES
D. 3DES

Answer: A

NEW QUESTION 205
- (Exam Topic 3)
You have configured a VLAN pair that is connected to a switch that is unable to pass traffic. If the IPS is configured correctly, which additional configuration must you perform to enable the switch to pass traffic?

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

Answer: A

NEW QUESTION 206
- (Exam Topic 3)
What is the function of the Web Proxy Auto-Discovery protocol?

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

Answer: A

NEW QUESTION 209
- (Exam Topic 3)
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 211
- (Exam Topic 3)
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 212
- (Exam Topic 3)
Which two commands are used to verify that CWS redirection is working on a Cisco ASA appliance? (Choose two.)

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

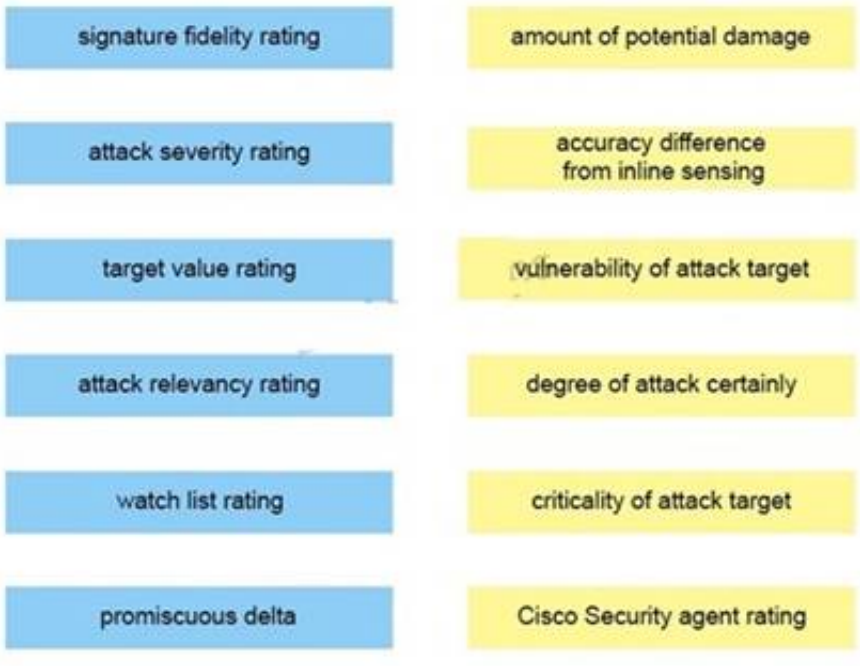
Answer: AC

NEW QUESTION 217
- (Exam Topic 3)
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 220
- (Exam Topic 3)
Drag and drop the terms on the left onto the correct definition for the promiscuous IPS risk rating calculation on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
http://www.cisco.com/c/en/us/products/collateral/security/ips-4200-seriessensors/prod_white_paper0
900aecd806e7299.html

NEW QUESTION 223
- (Exam Topic 3)
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 224
- (Exam Topic 3)
For which task can PRSM be used?

A. To configure Cisco ASACX firewalls
B. To monitor Cisco intelliShield
C. To monitor CWS traffic
D. To configure Cisco ESA

Answer: A

NEW QUESTION 227
- (Exam Topic 3)
What are the two policy types that can use a web reputation profile to perform reputation-based processing? (Choose two.)

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

Answer: CD

NEW QUESTION 228
- (Exam Topic 3)
Which option represents the cisco event aggregation product?

A. CVSS system
B. IntelliShield
C. ASACX Event Viewer
D. ASDM 7

Answer: C

NEW QUESTION 233
- (Exam Topic 3)
When you configure the Cisco ESA to perform blacklisting, what are two items you can disable to enhance performance? (Choose two.)

A. spam scanning
B. antivirus scanning
C. APT detection
D. rootkit detection

Answer: AB

NEW QUESTION 234
- (Exam Topic 3)
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 236
- (Exam Topic 3)
Over the period of one day, several Atomic ARP engine alerts fired on the same IP address. You observe that each time an alert fired, requests on the IP address exceeded replies by the same number. Which configuration could cause this behavior?

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

Answer: A

NEW QUESTION 241
- (Exam Topic 3)
A network security design engineer is considering using a Cisco Intrusion Detection System in the DMZ of the network. Which option is the drawback to using IDS in the DMZ as opposed to using
Intrusion Prevention System?

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

Answer: B

NEW QUESTION 243
- (Exam Topic 3)
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 244
- (Exam Topic 3)
Which option is a benefit of deploying Cisco Application Visibility and Control?

A. It ensures bandwidth availability and performance of mission-critical applications in a data- and media-rich environment.
B. It performs deep packet inspection of mission-critical applications in a data- and media-rich environment.
C. It encrypts mission-critical applications in a data- and media-rich environment.
D. It securely tunnels mission-critical applications in a data- and media-rich environment.

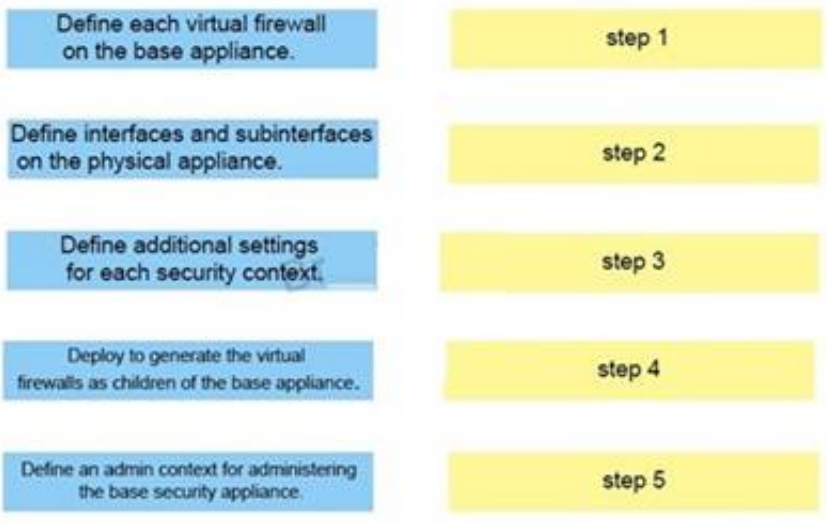
Answer: A

NEW QUESTION 248
- (Exam Topic 3)
Which IPS signature engine inspects the IP protocol packets and the Layer TCP?

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

Answer: D

NEW QUESTION 251
- (Exam Topic 3)
Drag and drop the steps on the left into the correct order on the right to configure a Cisco ASA NGFW with multiple security contexts.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 253
- (Exam Topic 3)
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 258
- (Exam Topic 3)
Which Cisco technology provides spam filtering and email protection?

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

Answer: B

NEW QUESTION 261
- (Exam Topic 3)
Which step is required when you configure URL filtering to Cisco Cloud Web Security?

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

Answer: A

NEW QUESTION 263
- (Exam Topic 3)
Refer to the exhibit.

Option	Redirect Method	Assignment Method	Ingress/Egress Redirection	Switching Result
1	L2	Hash	Ingress	Software Processing
2	L2 (Recommended)	Mask	Ingress	Full Hardware Processing with ACL TCAM
3	L2	Hash	Egress	Software Processing
4	L2	Mask	Egress	Software Processing of initial packet
5	GRE (PFC3 or newer)	Hash	Ingress	Software Processing of Initial packet with Netflow Partial-Flow
6	GRE (PFC3 or newer)	Mask	Ingress	Full Hardware Processing with Netflow Full-Flow
7	GRE	Hash	Egress	Software Processing
8	GRE (PFC3 or newer)	Mask	Egress	Software Processing of initial packet

When designing the network to redirect web traffic utilizing the Catalyst 6500 to the Cisco Web Security Appliance, impact on the switch platform needs consideration. Which four rows identify the switch behavior in correlation to the redirect method? (Choose four.)

A. Row 1
B. Row 2
C. Row 3
D. Row 4
E. Row 5
F. Row 6
G. Row 7
H. Row 8

Answer: BCFG

NEW QUESTION 265
- (Exam Topic 3)
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 268
- (Exam Topic 3)
Which type of signature is generated by copying a default signature and modifying its behavior?

A. meta
B. custom
C. atomic
D. normalized

Answer: B

NEW QUESTION 272
- (Exam Topic 3)
Which Cisco ASA configuration command drops traffic if the Cisco ASACX module fails?

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

Answer: B

NEW QUESTION 274
- (Exam Topic 3)
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 275
- (Exam Topic 3)

Scenario

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

\i120 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.

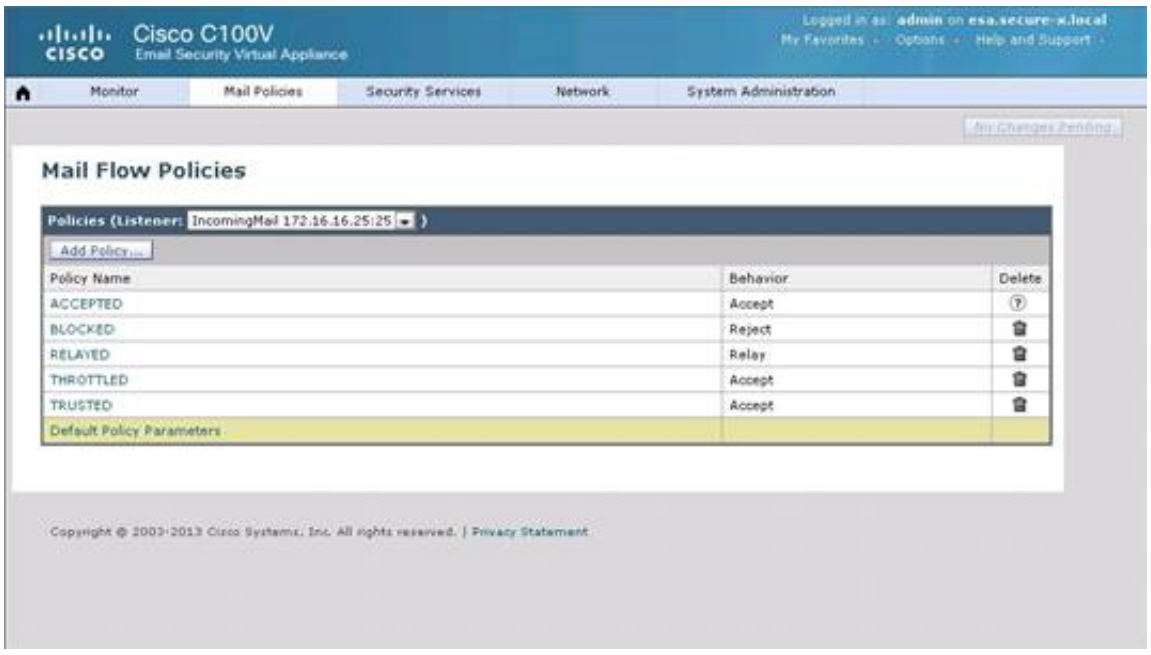
Instructions

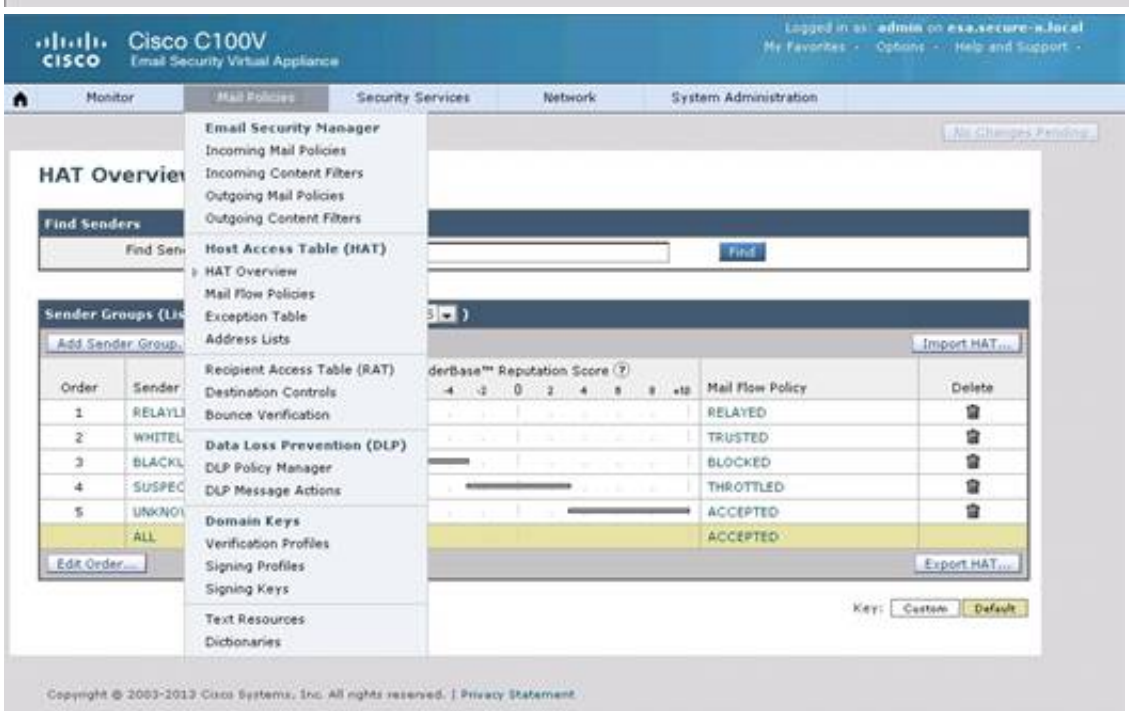
Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the HAT Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance.

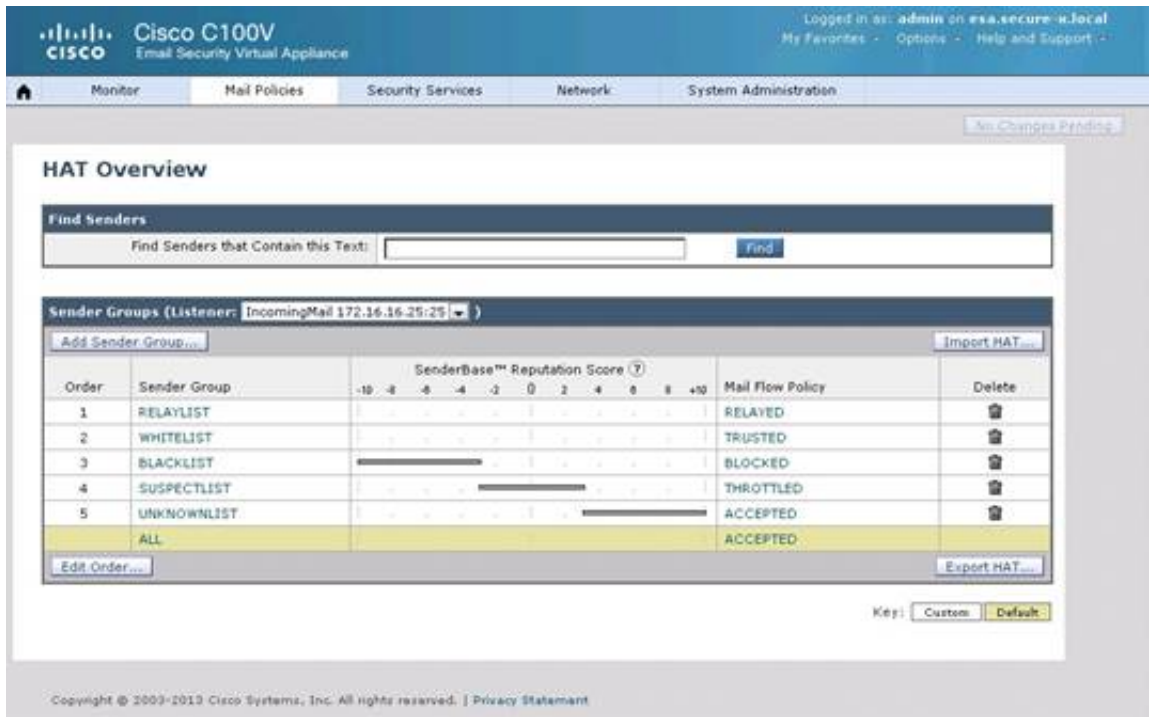
Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the 5 multiple choice questions.

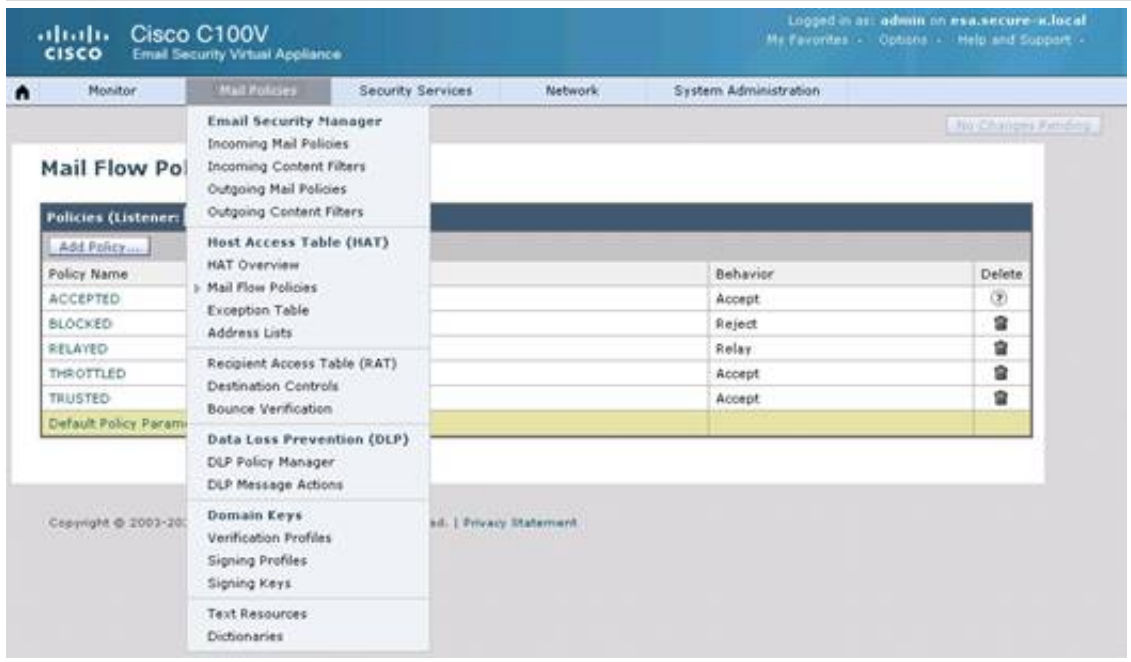
- red.public, -6
- orange.public, -4
- yellow.public, -2
- green.public, 2
- blue.public, 6
- violet.public, 8

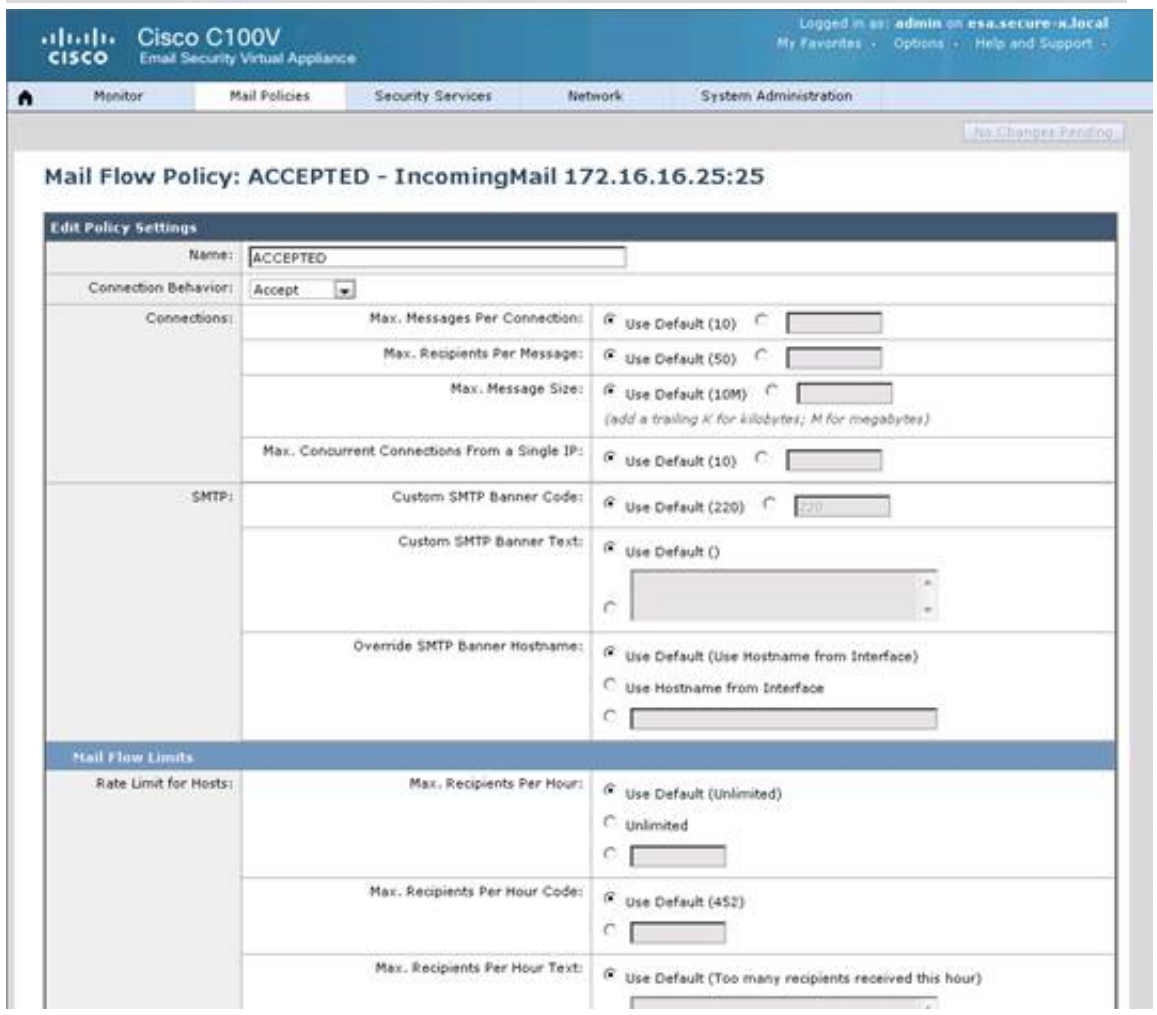
THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
Click on the MailFlowPolicies tab to access the device configuration.
To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
There are four multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.



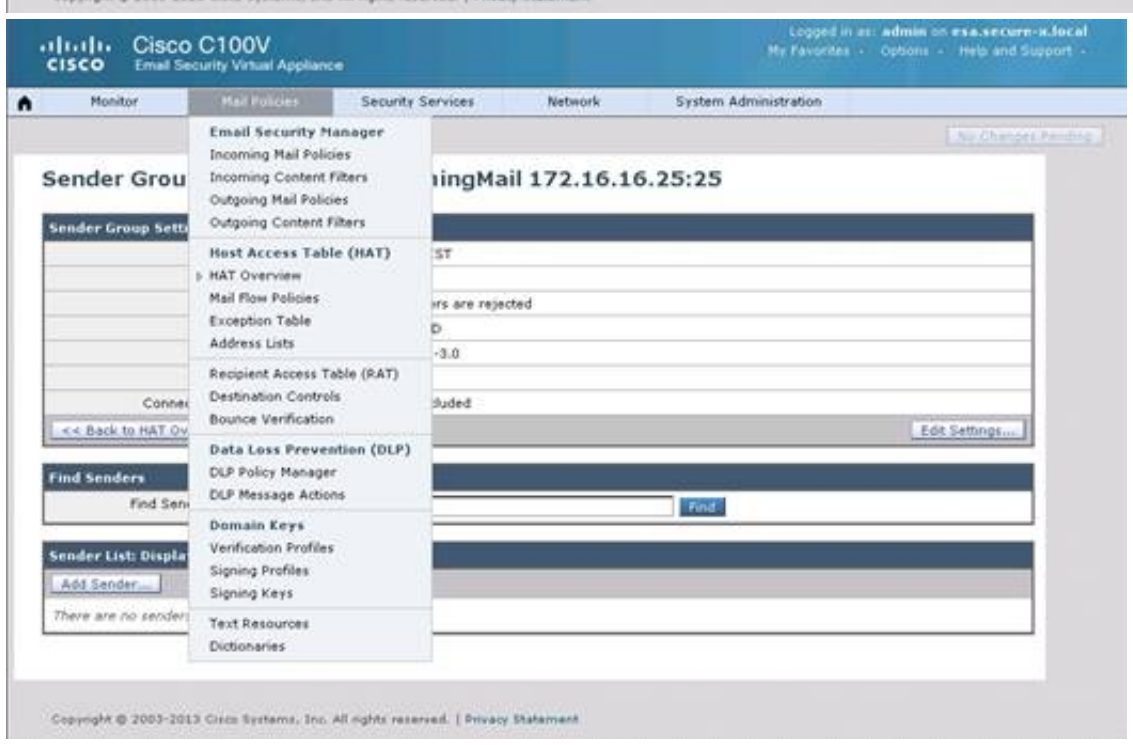


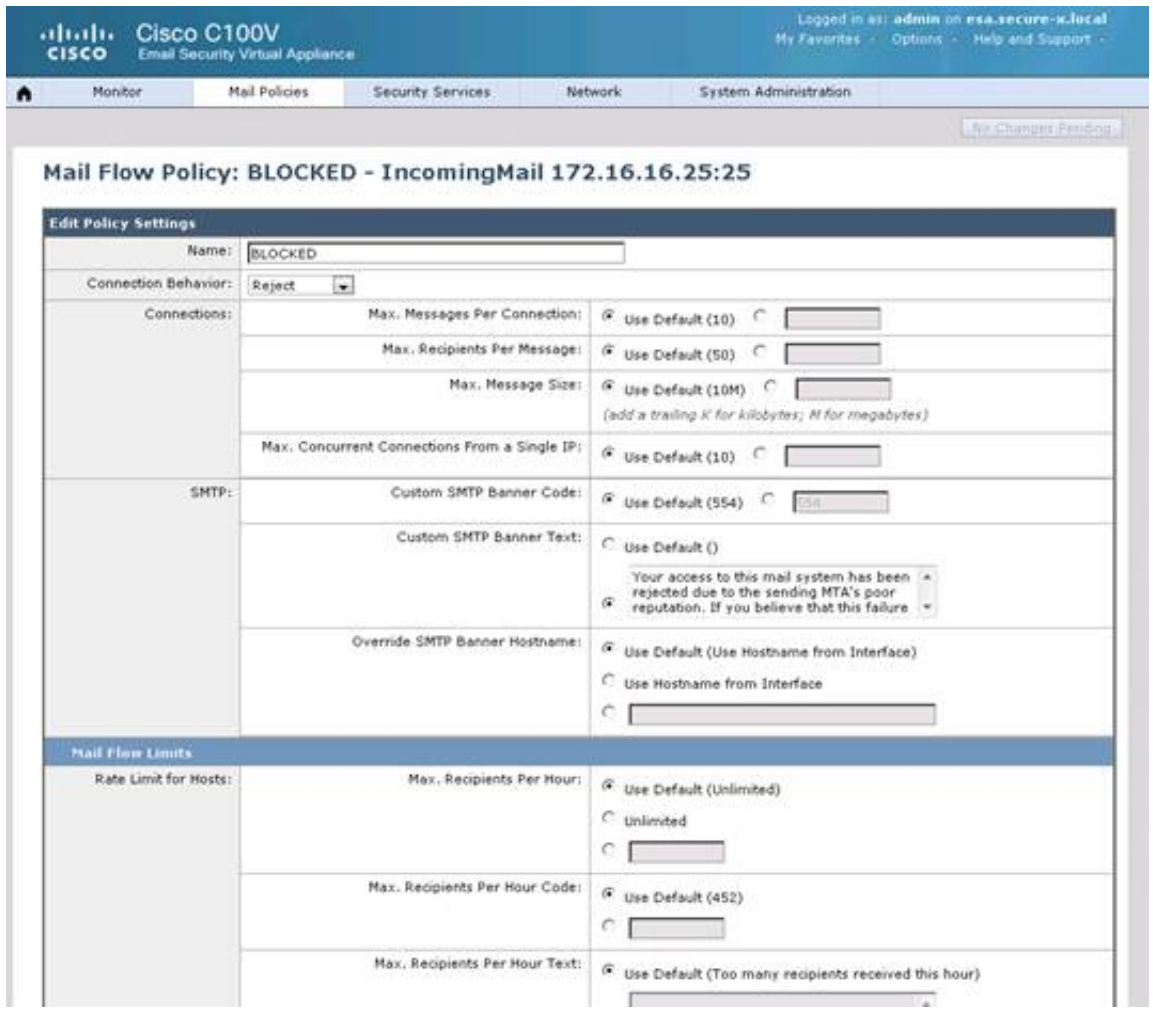

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
HAT Overview
Find Senders
Find Senders that Contain this Text:
Find
Sender Groups (Listener: IncomingMail 172.16.16.25:25)
Add Sender Group...
Import HAT...
Order
Sender Group
SenderBase™ Reputation Score
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

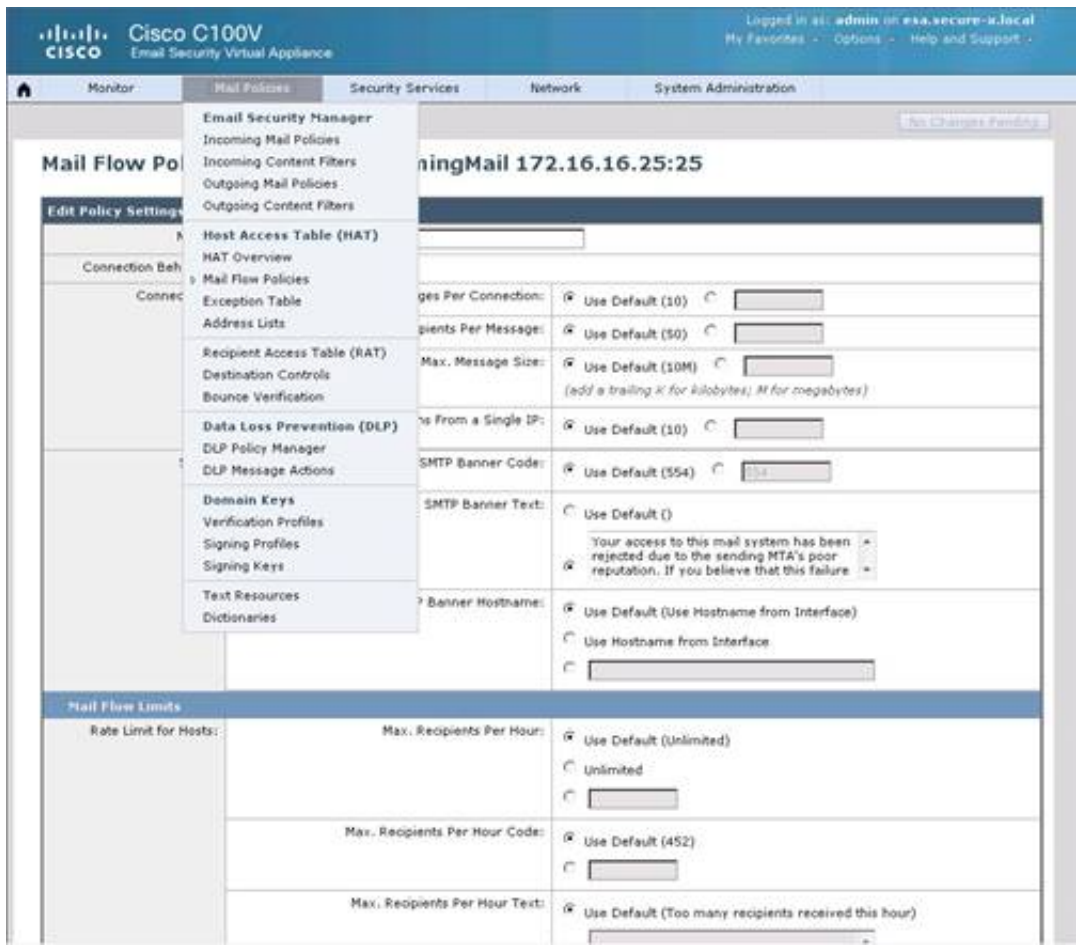

Cisco C100V
Email Security Virtual Appliance
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing Content Filters
Host Access Table (HAT)
HAT Overview
Mail Flow Policies
Exception Table
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
Policies (Listener:
Add Policy...
Policy Name
Behavior
Delete
ACCEPTED Accept
BLOCKED Reject
RELAYED Relay
THROTTLED Accept
TRUSTED Accept
Default Policy Param

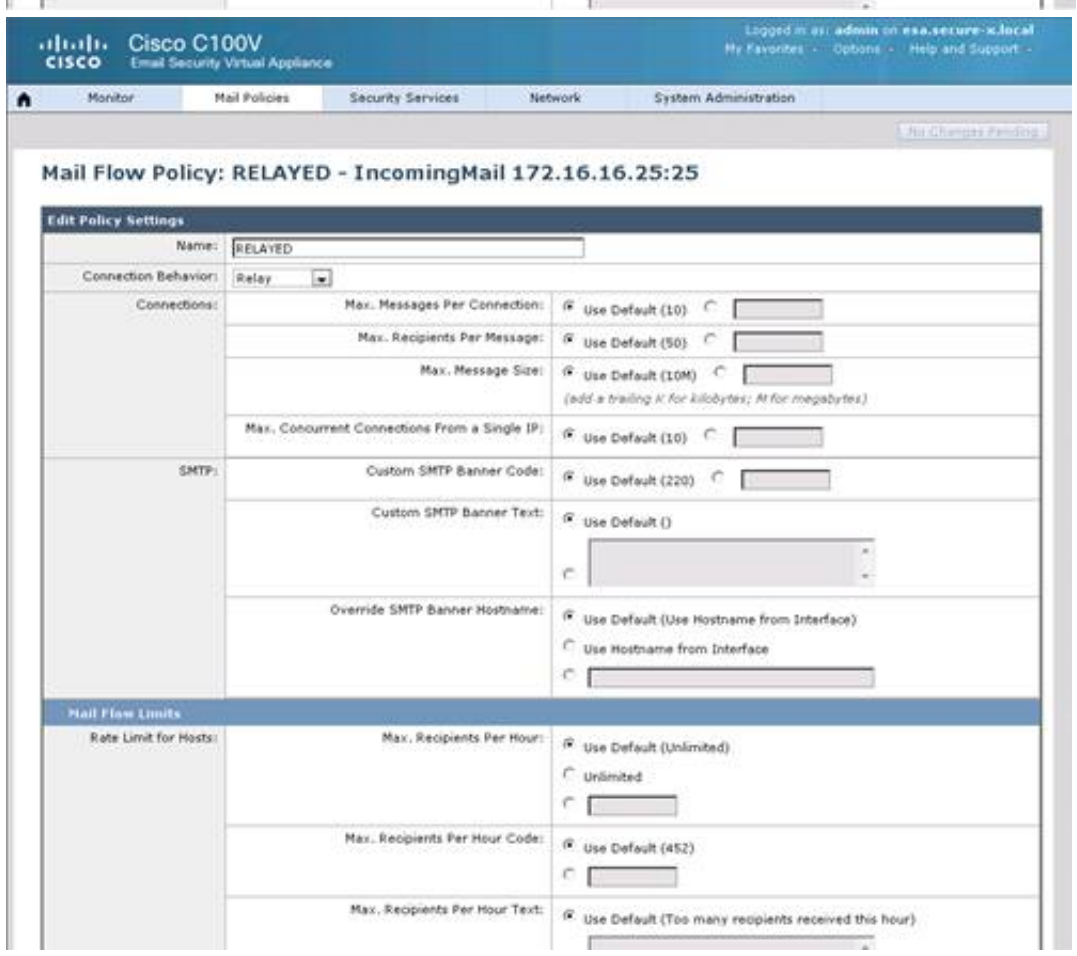

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Mail Flow Policy: ACCEPTED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: ACCEPTED
Connection Behavior: Accept
Connections:
Max. Messages Per Connection: Use Default (10)
Max. Recipients Per Message: Use Default (50)
Max. Message Size: Use Default (10M)
(add a trailing K for kilobytes, M for megabytes)
Max. Concurrent Connections From a Single IP: Use Default (10)
SMTP:
Custom SMTP Banner Code: Use Default (220)
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
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:
Use Default (Unlimited)
Unlimited
Max. Recipients Per Hour Code:
Use Default (452)
Max. Recipients Per Hour Text:
Use Default (Too many recipients received this hour)
Sender Group: 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

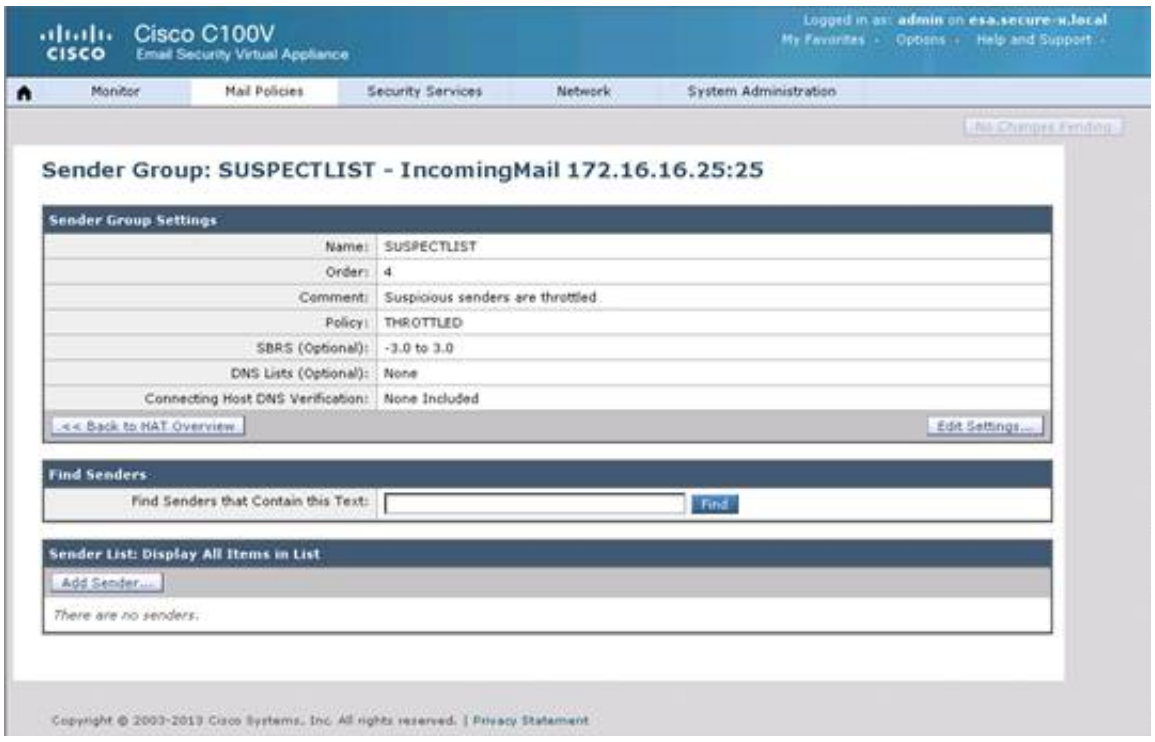

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing 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
Edit Settings...
Find
Add Sender...
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

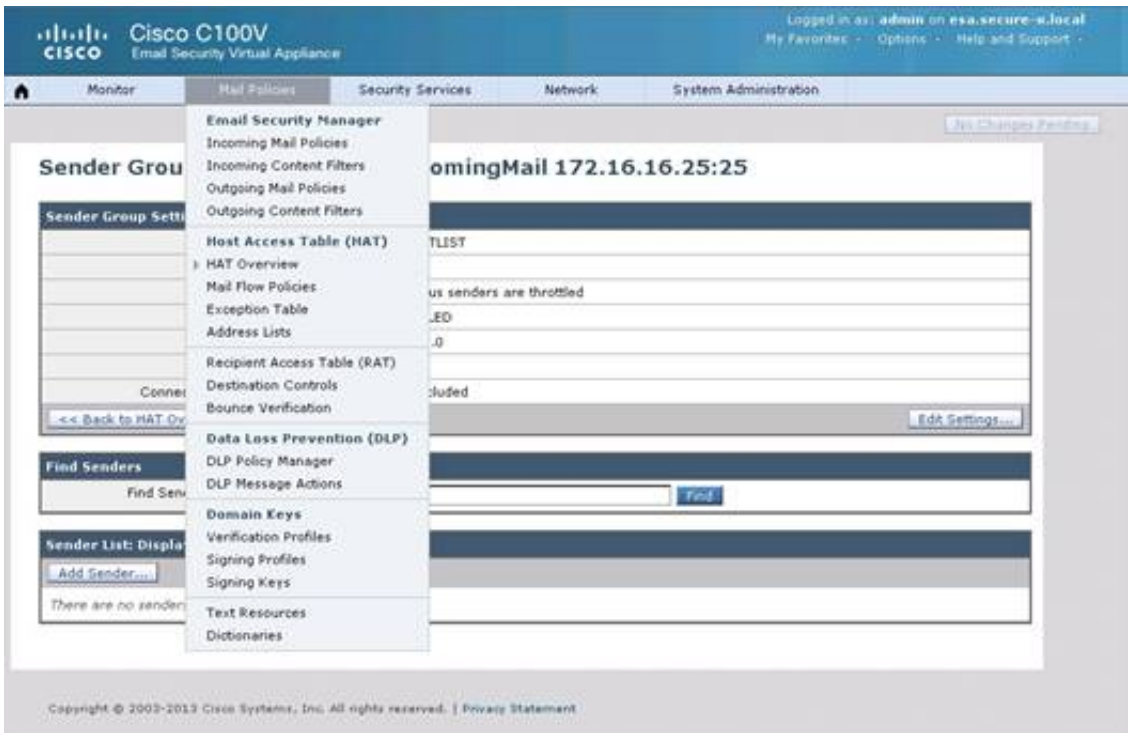

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: BLOCKED
Connection Behavior: Reject
Connections:
Max. Messages Per Connection: Use Default (10)
Max. Recipients Per Message: Use Default (50)
Max. Message Size: Use Default (10M)
(add a trailing K for kilobytes; M for megabytes)
Max. Concurrent Connections From a Single IP: Use Default (10)
SMTP:
Custom SMTP Banner Code: Use Default (554)
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)

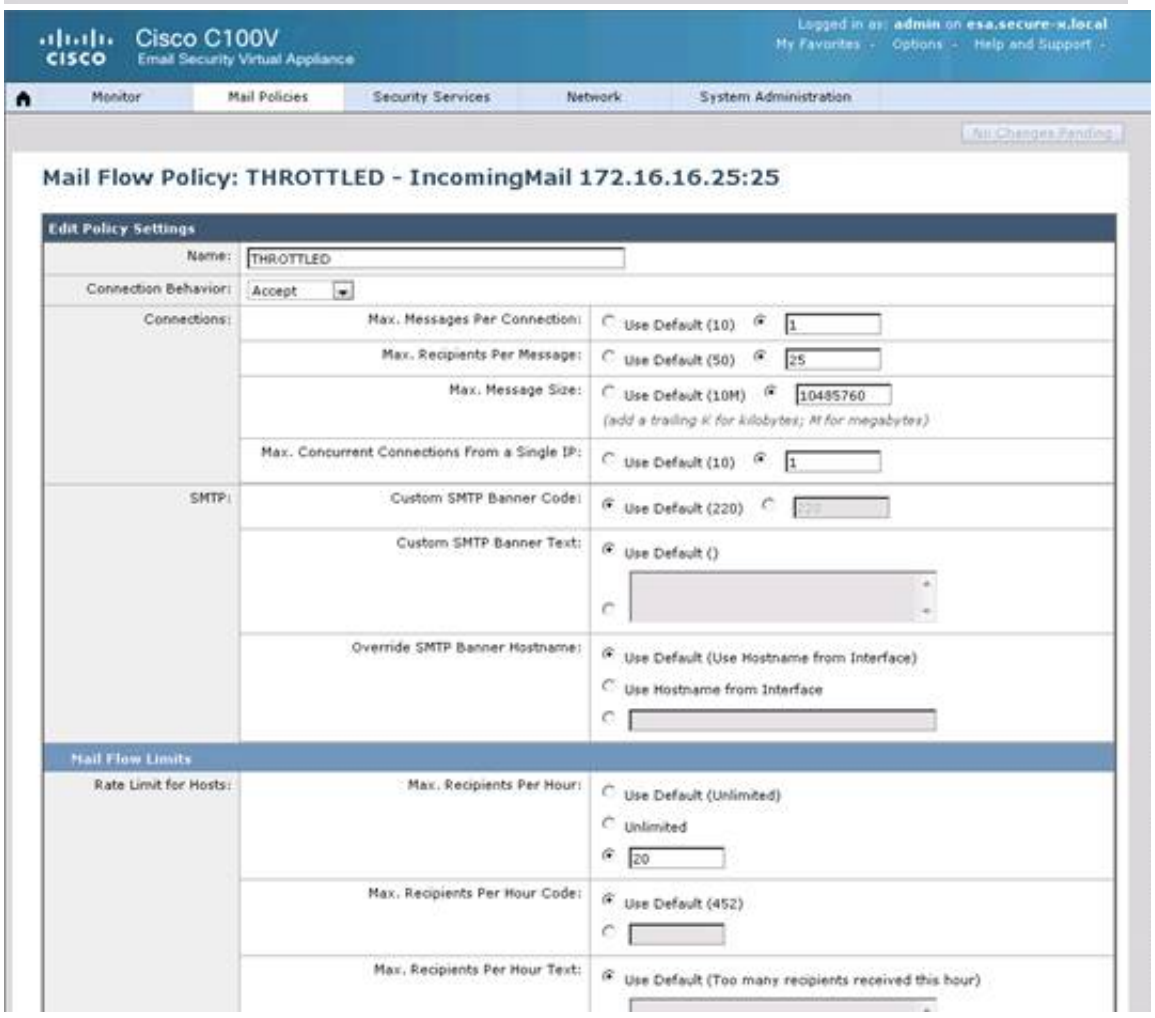

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing 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

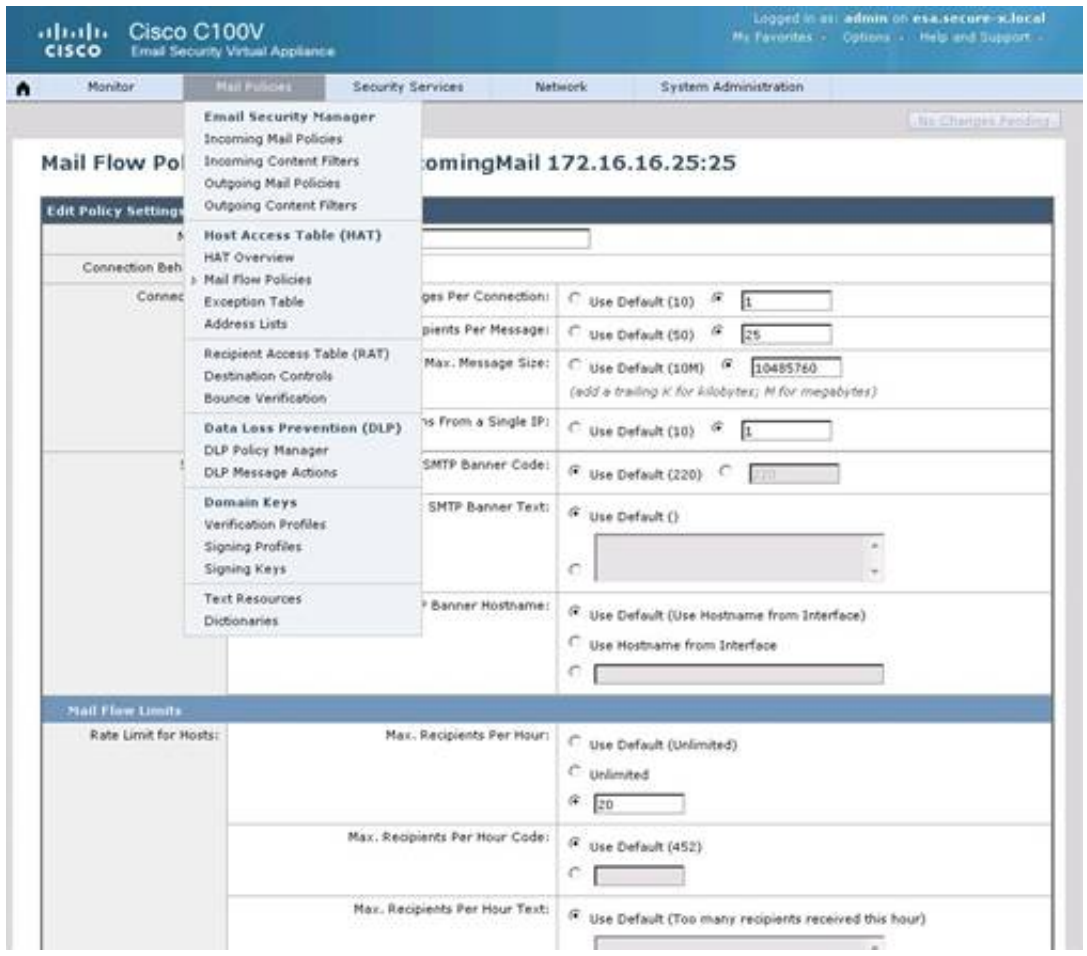

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: RELAYED
Connection Behavior: Relay
Connections:
Max. Messages Per Connection: Use Default (10)
Max. Recipients Per Message: Use Default (50)
Max. Message Size: Use Default (10M)
(add a trailing K for kilobytes; M for megabytes)
Max. Concurrent Connections From a Single IP: Use Default (10)
SMTP:
Custom SMTP Banner Code: Use Default (220)
Custom SMTP Banner Text: Use Default ()
Override SMTP Banner Hostname: Use Default (Use Hostname from Interface)
Use Hostname from Interface
Mail Flow Limits
Rate Limit for Hosts:
Max. Recipients Per Hour: Use Default (Unlimited)
Unlimited
Max. Recipients Per Hour Code: Use Default (452)
Max. Recipients Per Hour Text: Use Default (Too many recipients received this hour)

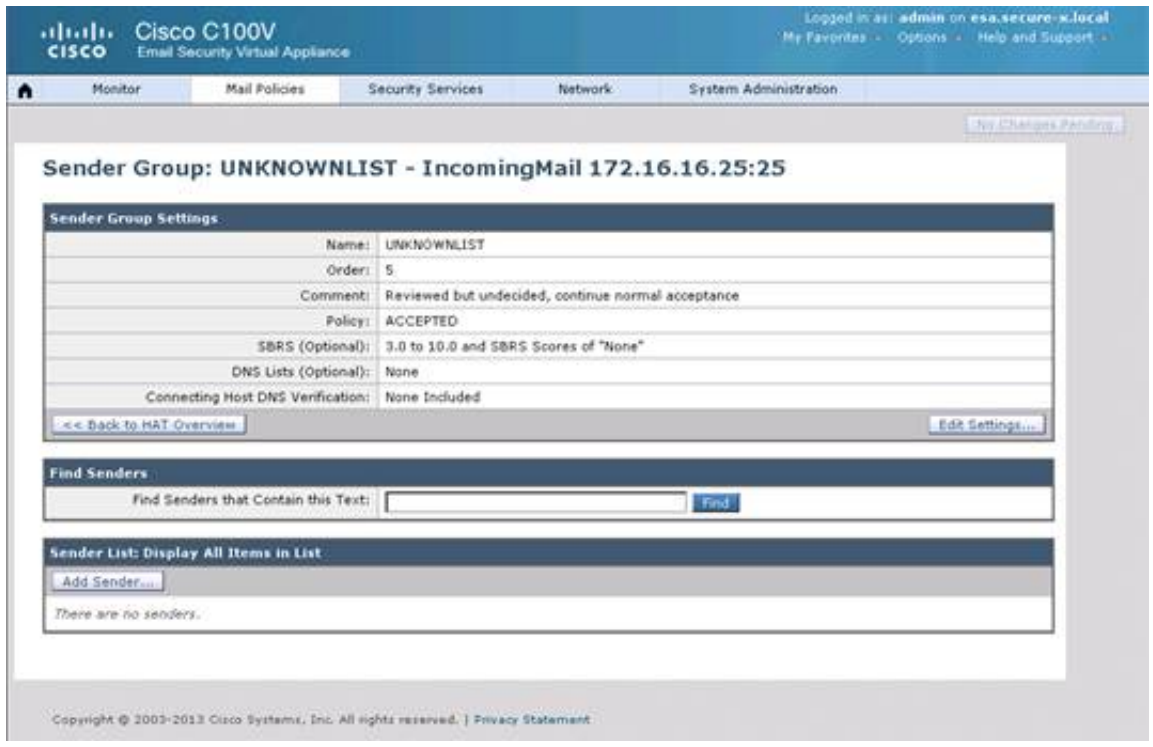

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing 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 Po
ingMail 172.16.16.25:25
Edit Policy Settings
Connection Beh
Connec
ges Per Connection:
Use Default (10)
pients Per Message:
Use Default (50)
Max. Message Size:
Use Default (10M)
(add a trailing k for kilobytes; M for megabytes)
s From a Single IP:
Use Default (10)
SMTP Banner Code:
Use Default (220)
SMTP Banner Text:
Use Default ()
Banner Hostname:
Use Default (Use Hostname from Interface)
Use Hostname from Interface
Mail Flow Limits
Rate Limit for Hosts:
Max. Recipients Per Hour:
Use Default (Unlimited)
Unlimited
Max. Recipients Per Hour Code:
Use Default (452)
Max. Recipients Per Hour Text:
Use Default (Too many recipients received this hour)
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
<< Back to HAT Overview
Delete
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

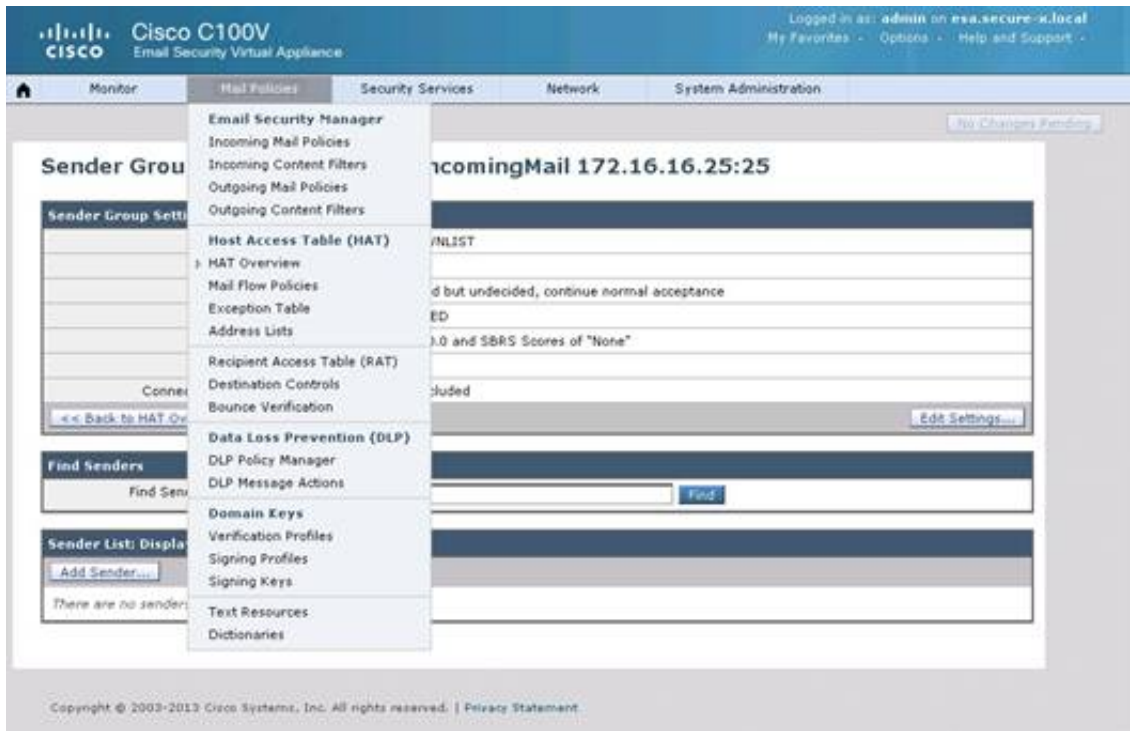

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Sender Group: SUSPECTLIST - IncomingMail 172.16.16.25:25
Sender Group Settings
Name: 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

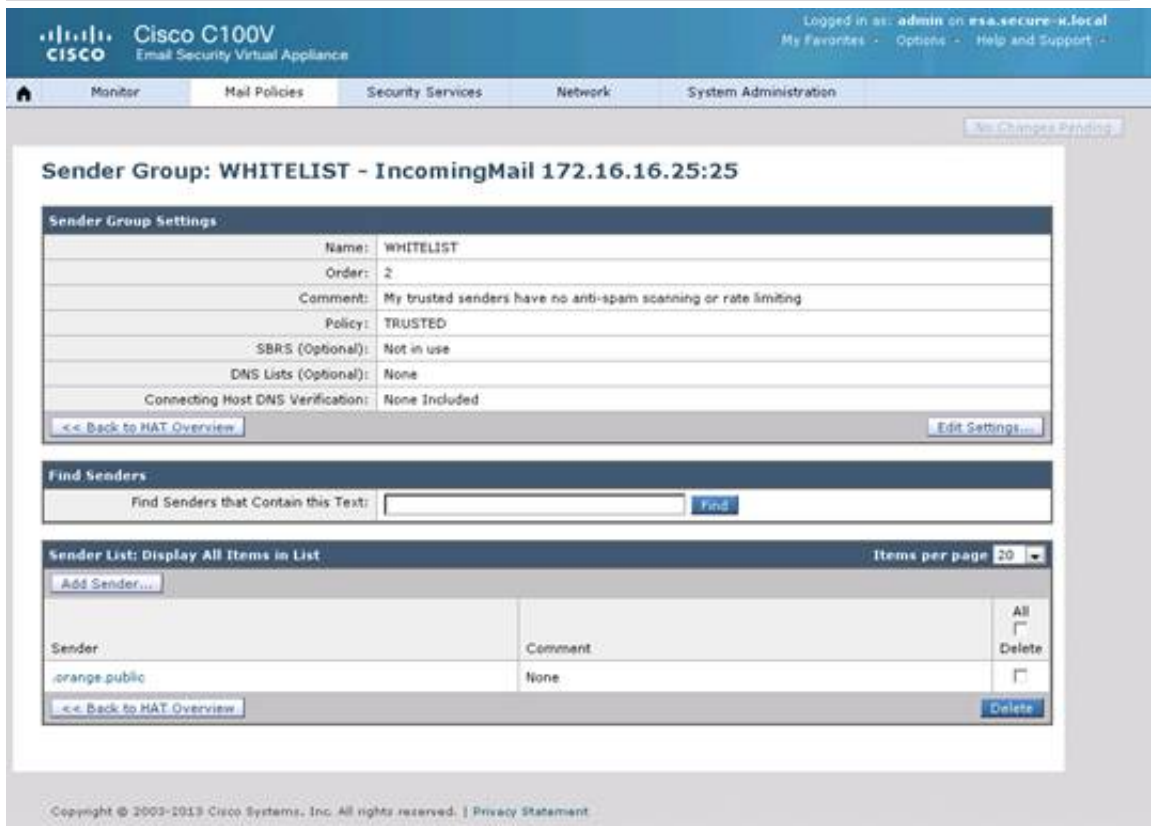

Cisco C100V
Email Security Virtual Appliance
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing Content Filters
Host Access Table (HAT)
HAT Overview
Mail Flow Policies
Exception Table
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

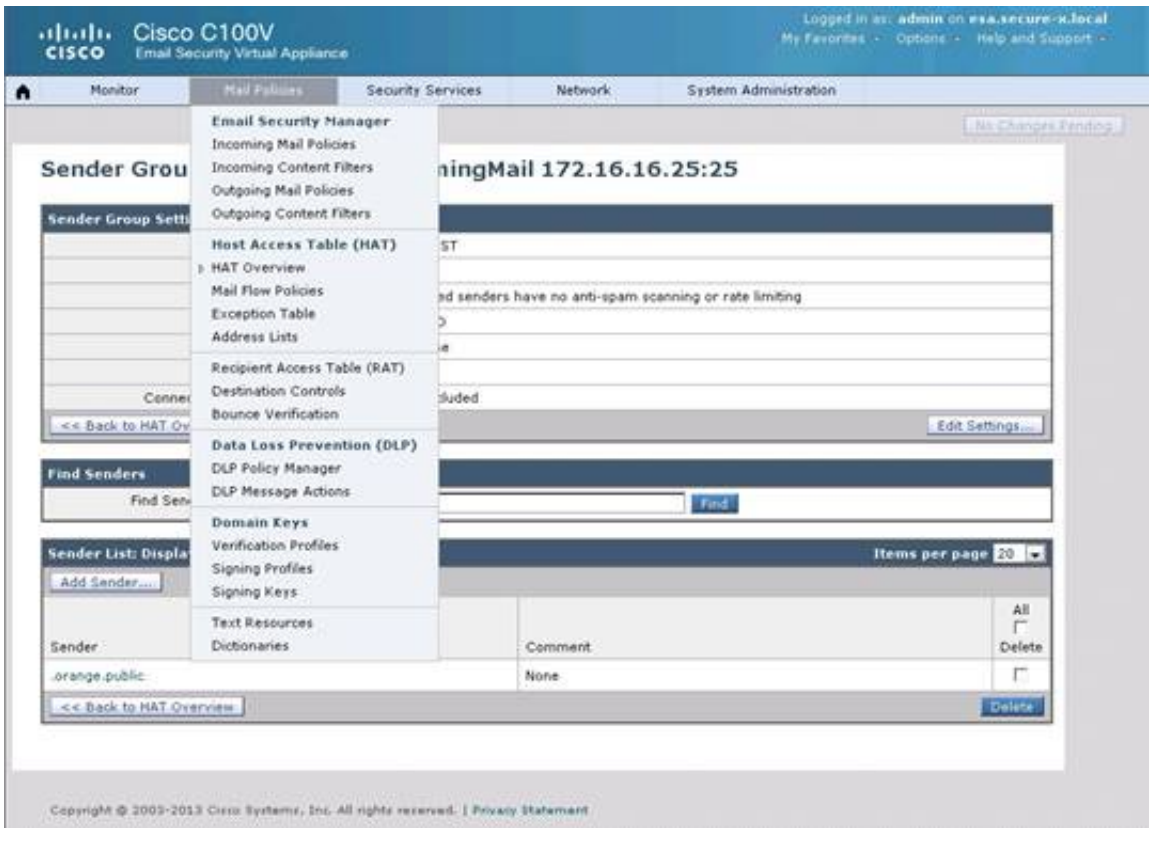

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Mail Flow Policy: THROTTLED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: THROTTLED
Connection Behavior: Accept
Connections:
Max. Messages Per Connection: Use Default (10) 1
Max. Recipients Per Message: Use Default (50) 25
Max. Message Size: Use Default (10M) 10485760
(add a trailing k for kilobytes; M for megabytes)
Max. Concurrent Connections From a Single IP: Use Default (10) 1
SMTP:
Custom SMTP Banner Code: Use Default (220)
Custom SMTP Banner Text: Use Default ()
Override SMTP Banner Hostname: Use Default (Use Hostname from Interface)
Use Hostname from Interface
Mail Flow Limits
Rate Limit for Hosts:
Max. Recipients Per Hour: Use Default (Unlimited)
Unlimited
20
Max. Recipients Per Hour Code: Use Default (452)
Max. Recipients Per Hour Text: Use Default (Too many recipients received this hour)


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
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 Policy: TRUSTED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: TRUSTED
Connection Behavior: Accept
Connections:
Max. Messages Per Connection: Use Default (10) 5000
Max. Recipients Per Message: Use Default (50) 5000
Max. Message Size: Use Default (10M) 104857600
(add a trailing K for kilobytes; M for megabytes)
Max. Concurrent Connections From a Single IP: Use Default (10) 300
SMTP:
Custom SMTP Banner Code: Use Default (220)
Custom SMTP Banner Text: Use Default ()
Override SMTP Banner Hostname: Use Default (Use Hostname from Interface)
Use Hostname from Interface
Mail Flow Limits
Rate Limit for Hosts:
Max. Recipients Per Hour: Use Default (Unlimited)
Unlimited
Max. Recipients Per Hour Code: Use Default (452)
Max. Recipients Per Hour Text: Use Default (Too many recipients received this hour)


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
Monitor
Mail Policies
Security Services
Network
System Administration
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
Sender Group: WHITELIST - IncomingMail 172.16.16.25:25
Sender Group Settings
Name: WHITELIST
Order: 2
Comment: My trusted senders have no anti-spam scanning or rate limiting
Policy: TRUSTED
SBRS (Optional): Not in use
DNS Lists (Optional): None
Connecting Host DNS Verification: None Included
<< Back to HAT Overview
Edit Settings...
Find Senders
Find Senders that Contain this Text:
Find
Sender List: Display All Items in List
Items per page 20
Add Sender...
Sender
Comment
All
Delete
.orange.public
None
<< Back to HAT Overview
Delete
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

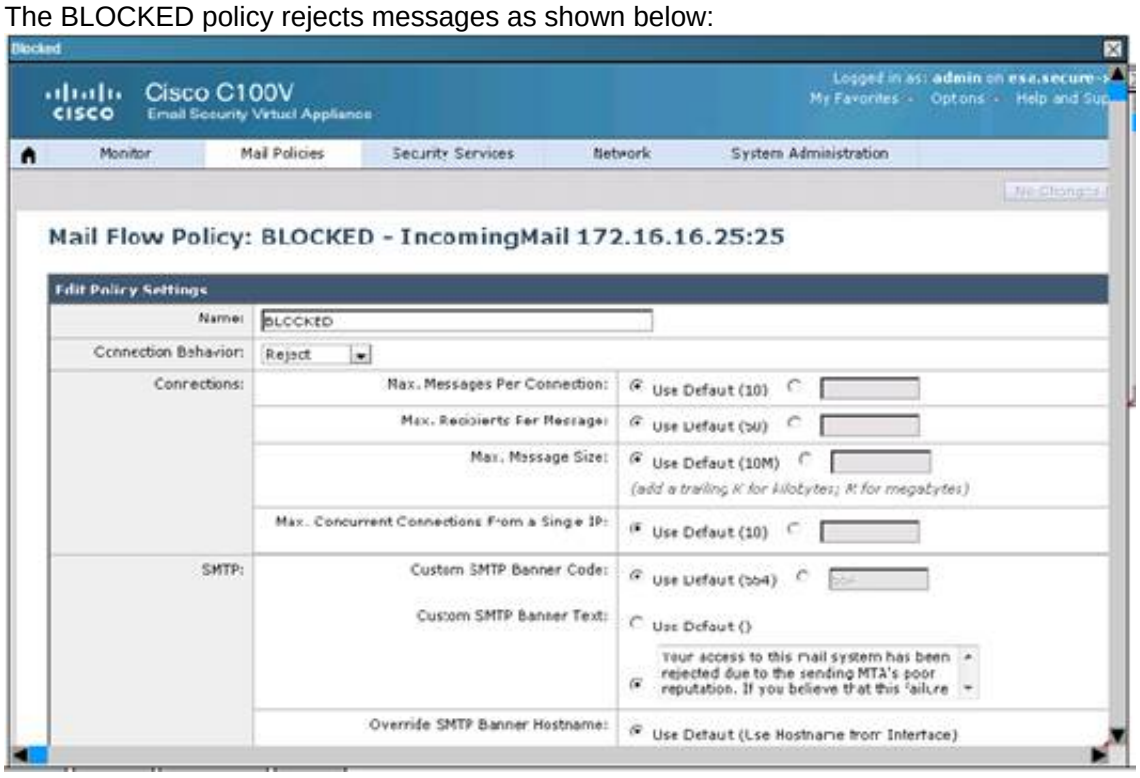


The Cisco Email Security Appliance will reject messages from which domains?

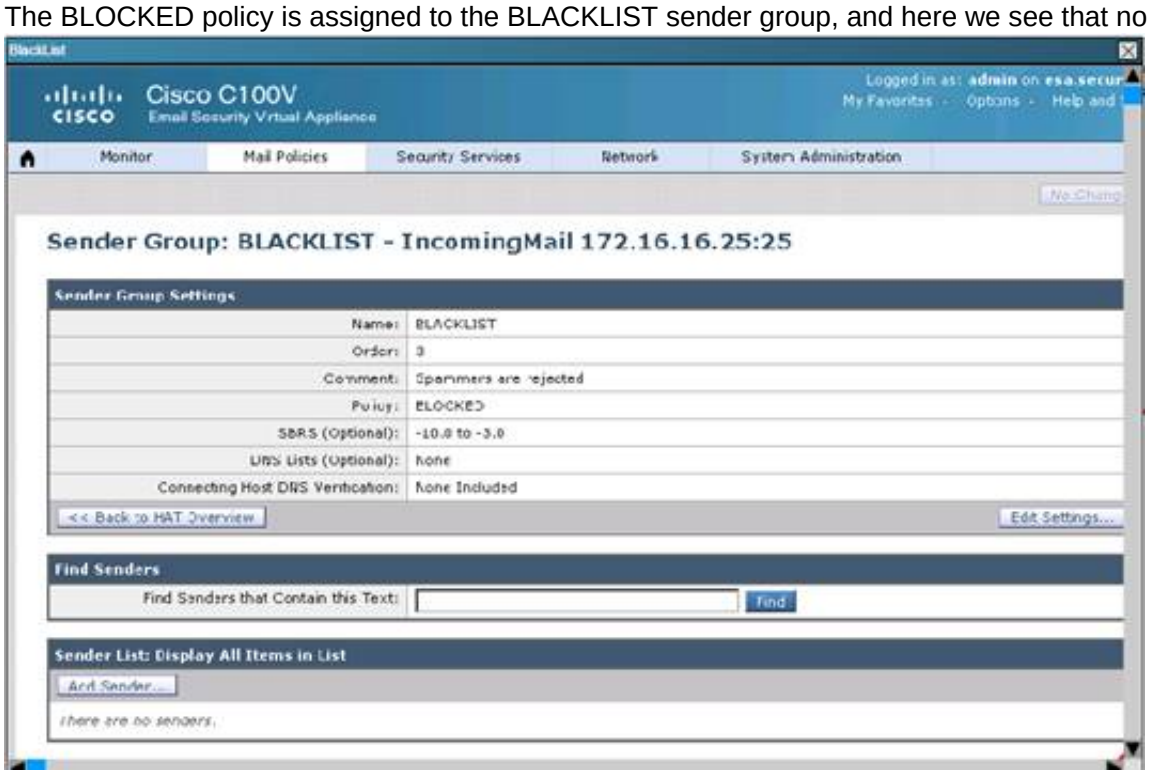
A. red.public
B. red.public and orange.public
C. red.public, orange.public and yellow.public
D. orange.public
E. violet.public
F. violet.public and blue.public
G. None of the listed domains

Answer: G

Explanation:
The BLOCKED policy rejects messages as shown below:



Capture
The BLOCKED policy is assigned to the BLACKLIST sender group, and here we see that no senders have been applied to this group:



Capture

NEW QUESTION 280
- (Exam Topic 4)
With Cisco ASA active/standby failover, what is needed to enable subsecond failover?

A. Use redundant interfaces.
B. Enable the stateful failover interface between the primary and secondary Cisco ASA.
C. Decrease the default unit failover polltime to 300 msec and the unit failover holdtime to 900 msec.
D. Decrease the default number of monitored interfaces to 1

Answer: C

NEW QUESTION 282
- (Exam Topic 4)
Which option describes device trajectory on Cisco Advanced Malware protection for End[points? It show which devices on the network receive the file.

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

Answer: B

NEW QUESTION 287
- (Exam Topic 4)
Which Cisco ASA platform should be selected if the requirements are to support 35,000 connections per second, 600,000 maximum connections, and traffic shaping?

A. A.5540B.5550C.5580-20D.5580-40

Answer: C

NEW QUESTION 289
- (Exam Topic 4)
Which three webtype ACL statements are correct? (Choose three.)

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

Answer: BDE

NEW QUESTION 292
- (Exam Topic 4)
What is retrospective alerting in Cisco Advanced Malware Protection for Endpoints?

A. alerts when a file changes disposition
B. alerts on events over a week old
C. alerts showing previously installed malware
D. alerts on previously blacklisted applications

Answer: C

NEW QUESTION 297
- (Exam Topic 4)
Which redundancy protocol is available for Cisco firepower but is a limitation for the WSA?

A. VVRP
B. HSRP
C. SFRP
D. GLBR

Answer: C

NEW QUESTION 298
- (Exam Topic 4)
What is a limitation of the AMP Threatgrid Sandbox?

A. delayed software updates
B. the requirement of fully assembled malware
C. single point of failure
D. complex setup

Answer: A

NEW QUESTION 299
- (Exam Topic 4)
Which action inspects packets in IPS?

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

Answer: AE

NEW QUESTION 303
- (Exam Topic 4)
What Software can be installed on the Cisco 4100 series appliance?

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

Answer: A

NEW QUESTION 307
- (Exam Topic 4)
Which Cisco ASA SSL VPN feature provides support for PCI compliance by allowing for the validation of two sets of username and password credentials on the SSL VPN login page?

A. Single Sign-On
B. Certificate to Profile Mapping
C. Double Authentication
D. RSA OTP

Answer: D

NEW QUESTION 312
- (Exam Topic 4)
Which standby protocol which works on NGIPS but not on CWS?

A. HSRP
B. GLBP
C. SFRP
D. VRRP

Answer: C

NEW QUESTION 314
- (Exam Topic 4)
Troubleshoot command for NGIPSv.

A. system generate-troubleshoot all
B. sudo sf_troubleshoot.pl

Answer: A

NEW QUESTION 318
- (Exam Topic 4)
Which four advanced endpoint assessment statements are correct? (Choose four.)

A. examines the remote computer for personnel firewalls applications
B. examines the remote computer for antivirus applications
C. examines the remote computer for antispyware applications
D. examines the remote computer for malware applications
E. does not perform any remediation but provides input that can be evaluated by DAP records
F. performs active remediation by applying rules, activating modules, and providing updates where applicable

Answer: ABCF

NEW QUESTION 319
- (Exam Topic 4)
A Cisco AnyConnect user profile can be pushed to the PC of a remote user from a Cisco ASA. Which three user profile parameters are configurable? (Choose three.)

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

Answer: ACF

NEW QUESTION 321
- (Exam Topic 4)
Your corporate finance department purchased a new non-web-based TCP application tool to run on one of its servers. The finance employees need remote access to the software during non- business hours. The employees do not have "admin" privileges to their PCs. How would you configure the SSL VPN tunnel to allow this application to run?

A. Configure a smart tunnel for the application.
B. Configure a "finance tool" VNC bookmark on the employee clientless SSL VPN portal.
C. Configure the plug-in that best fits the application.
D. Configure the Cisco ASA appliance to download the Cisco AnyConnect SSL VPN client to the financeemployee each time an SSL VPN tunnel is established

Answer: A

NEW QUESTION 325
- (Exam Topic 4)
Which command is used on the cisco firepower threat defense to send logs to cisco tac?

A. sudo_
B. tac

Answer: B

NEW QUESTION 329
- (Exam Topic 4)
Which two statements about Cisco Firepower file and intrusion inspection under control policies are true? (Choose two.)

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

Answer: AE

NEW QUESTION 331
- (Exam Topic 4)
Which two health modules are available within the Firepower solution?

A. AMP for Firepower Status
B. Policy Usage
C. Appliance heartbeat
D. SNMP Analysis
E. Connection Monitoring

Answer: AC

NEW QUESTION 332
- (Exam Topic 4)
Which tools are used to analyze Endpoints for AMP file activity performed on endpoints?

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

Answer: C

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

NEW QUESTION 334
- (Exam Topic 4)
Which of the following are Cisco FirePOWER Application Layer Preprocessors? (Choose 2).

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

Answer: AB

NEW QUESTION 338
- (Exam Topic 4)
A user wants to configure high availability with their Cisco Firepower deployment. Which platforms allow for clustering?

A. All platforms support clustering
B. Virtual NGIPS
C. FirePower Threat Defense for ISR
D. Cisco FirePower appliance

Answer: A

NEW QUESTION 343
- (Exam Topic 4)
Upon receiving a digital certificate, what are three steps that a Cisco ASA will perform to authenticate the digital certificate? (Choose three.)

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

Answer: ACE

NEW QUESTION 344
- (Exam Topic 4)
What are 2 types or forms of suppression on a FirePower policy (or FTD)?

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

Answer: AC

NEW QUESTION 348
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

300-210 Practice Exam Features:

* 300-210 Questions and Answers Updated Frequently

* 300-210 Practice Questions Verified by Expert Senior Certified Staff

* 300-210 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 300-210 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 300-210 Practice Test Here