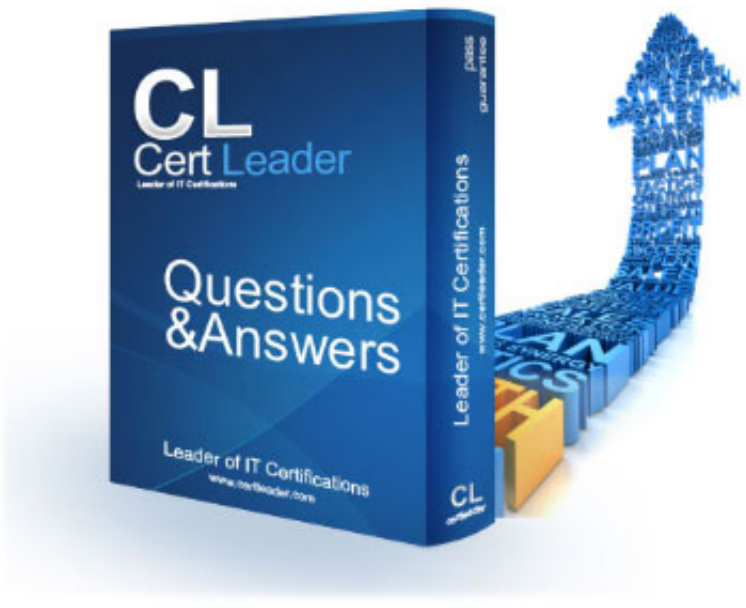
300-210 Dumps

Implementing Cisco Threat Control Solutions (SITCS)

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



NEW QUESTION 1
Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?

A. cloud web services
B. network AMP
C. private cloud
D. public cloud

Answer: C

NEW QUESTION 2
Refer to exhibit.
Which configuration blow would result in this output of the show service-policy sfr command?

A. policy-map global_policy Class inspection_default Class sfrSfr
B. Policy-map global_policy Class inspection-default Class sfrSfr fail-close
C. policy-map global_policy Class inspection_default Class sfrSfr fail-open monitor-only
D. policy-map global_policy Class inspection_default Class sfrSfr fail-close monitor-only

Answer: C

NEW QUESTION 3
Where in the Cisco ASA appliance CLI are Active/Active Failover configuration parameters configured?

A. admin context
B. customer context
C. system execution space
D. within the system execution space and admin context
E. within each customer context and admin context

Answer: C

NEW QUESTION 4
over which two ports does the ISR G2 connector for CWS support redirection of HTTP traffic? (choose tw0)

A. TCP port 65535
B. UDP port 8080
C. TCP port 88
D. TCP port 80 E,.UDP port 80

Answer: AD

NEW QUESTION 5
Which SSL traffic decryption feature is used when decrypting traffic from an external host to a server on your network?

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

Answer: B

NEW QUESTION 6
A network administrator noticed all traffic that is redirected to the cisco WSA from ASA firewall is unable to get to the internet in a transparent proxy environment using WCCP.

A. Ping the WCCP device
B. Explicity point to the browser to the proxy
C. Disable WCCP
D. Check WCCP logs in debug mode to check there are no pending HIA or ISY request

Answer: D

NEW QUESTION 7
An engineer must deploy AMP with cloud protection. Which machine learning engine uses active heuristics?

A. Spero
B. IOCs
C. 1to1
D. Ethos

Answer: A

NEW QUESTION 8
In cisco firePOWER 5.x and 6.0, which type of traffic causes a web page to be displayed by the appliance when Block or Interactive Block is selected as an access control action?

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

Answer: D

NEW QUESTION 9
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 10
A network engineer wants to deploy a virtual cisco ESA and wants protection against email-based threats, email encryption, and clustering. Which software license bundle must the network engineer purchase to access these components?

A. cisco email security Premium
B. cisco email security Hybrid Essential
C. cisco email security advansed
D. cisco email security Gateway

Answer: A

Explanation: Email Security Premium Boundle: Antispam scanning, Sophos Antivirus solution, Virus Outbreack filtres,DLP Compliance, Email encryption, CLustering

NEW QUESTION 10
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 15
With Cisco AMP for Endpoints, which option shows a list of all files that have been executed in your environment?

A. vulnerable software
B. file analysis
C. detections
D. prevalence
E. threat root cause

Answer: C

NEW QUESTION 17
How does the WSA policy trace tool make a request to the Proxy to emulate a client request?

A. explicitly
B. transparently
C. via WCCP
D. via policy-based routing

Answer: D

NEW QUESTION 18
In WSA , which two pieces of information are required to implement transparent user identification using Context Directory Agent? (Choose two.)

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

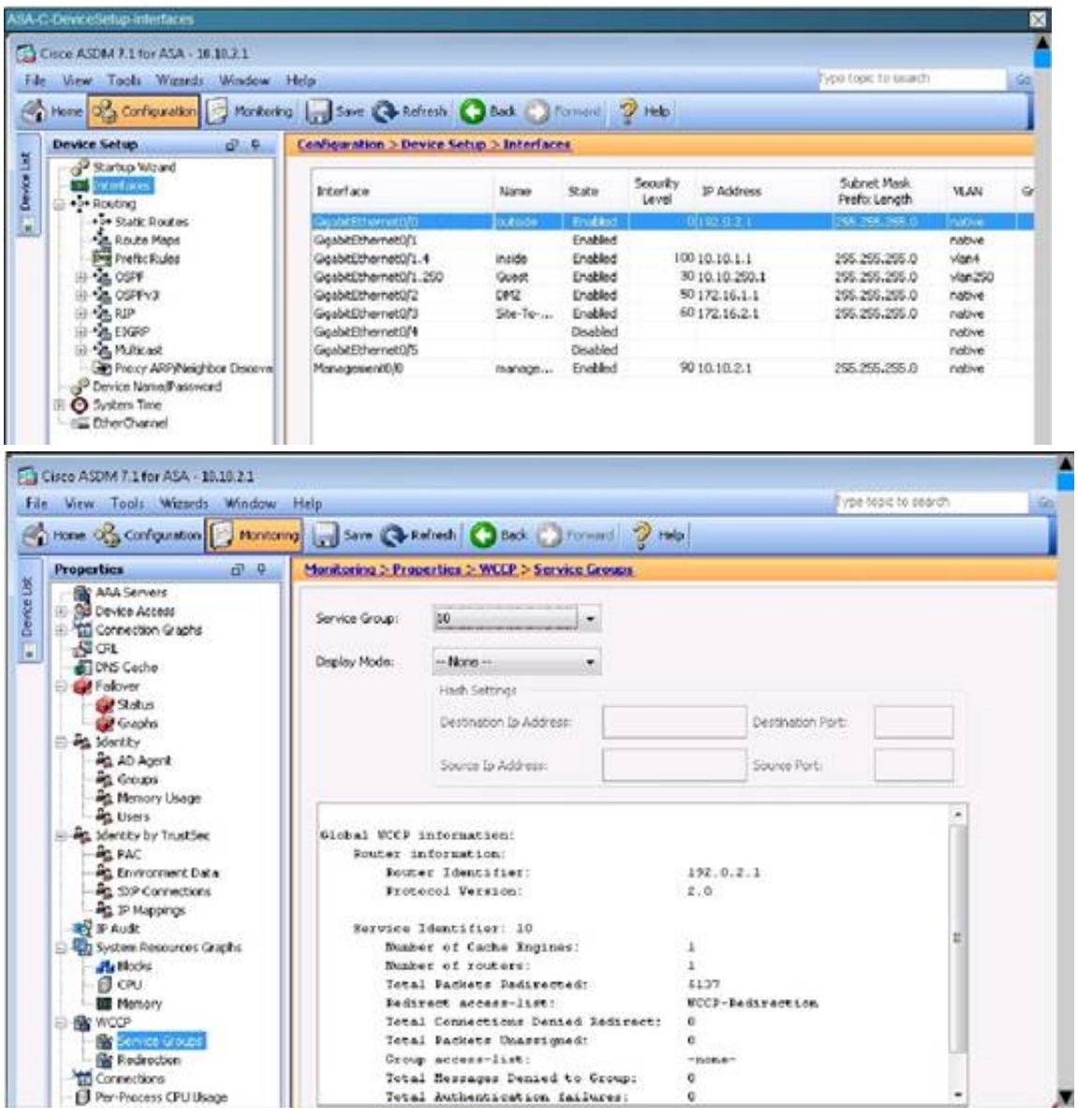
Answer: AE

NEW QUESTION 22
How many interfaces can a Cisco ASA bridge group support and how many bridge groups can a Cisco ASA appliance support?

A. up to 2 interfaces per bridge group and up to 4 bridge groups per Cisco ASA appliance
B. up to 2 interfaces per bridge group and up to 8 bridge groups per Cisco ASA appliance
C. up to 4 interfaces per bridge group and up to 4 bridge groups per Cisco ASA appliance
D. up to 4 interfaces per bridge group and up to 8 bridge groups per Cisco ASA appliance
E. up to 8 interfaces per bridge group and up to 4 bridge groups per Cisco ASA appliance
F. up to 8 interfaces per bridge group and up to 8 bridge groups per Cisco ASA appliance

Answer: D

NEW QUESTION 26
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.



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

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

Answer: A

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

NEW QUESTION 31
Which two statement about Cisco Firepower file and intrusion inspection under control policies are true? (Choose two.)

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

Answer: AE

NEW QUESTION 36
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 39
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 43
In the predefined URL category filtering configuration page in a cisco WSA, which two actions are valid?

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

Answer: AD

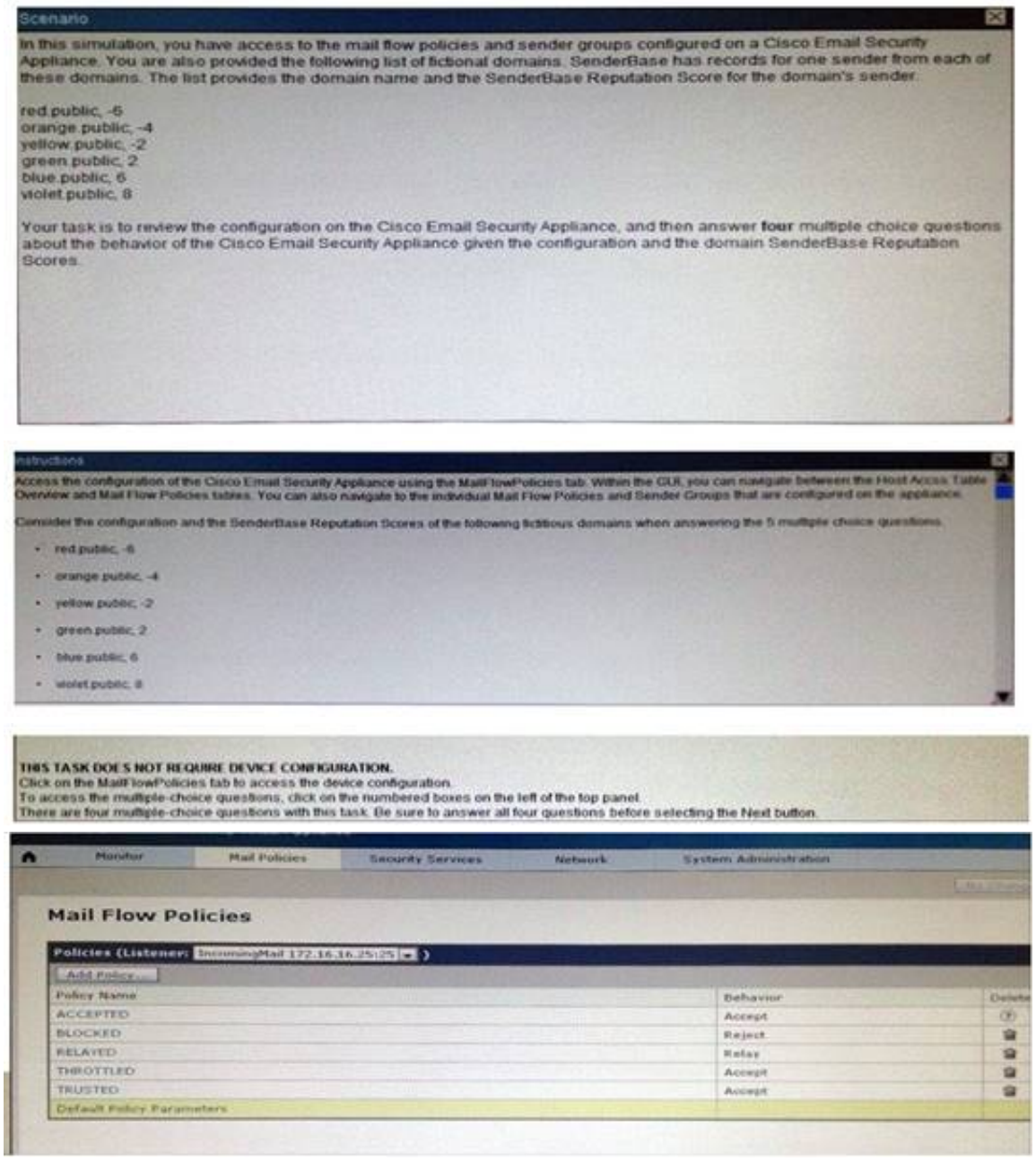
NEW QUESTION 45
Which Cisco Firepower rule action displays a HTTP warning page and resets the connection of HTTP traffic specified in the access control rule ?

A. Interactive Block with Reset
B. Block
C. Allow with Warning
D. Interactive Block

Answer: D

Explanation: http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html

NEW QUESTION 50



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

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

Answer: C

NEW QUESTION 53
With Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two.)

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

E. EtherChannel

Answer: AB

NEW QUESTION 55
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 56
Which protocols can be specified in a Snort rule header for analysis?

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

Answer: A

NEW QUESTION 61
Which cloud-based malware detection engine uses machine-learning detection techniques in the Cisco Advanced Malware Protection cloud?

A. third-party detections
B. Spero
C. Ethos
D. Memcache

Answer: B

NEW QUESTION 66
Which statement about Cisco ASA multicast routing support is true?

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

Answer: D

NEW QUESTION 69
Using the default modular policy framework global configuration on the Cisco ASA, how does the Cisco ASA process outbound HTTP traffic?

A. HTTP flows are not permitted through the Cisco ASA, because HTTP is not inspected by default.
B. HTTP flows match the inspection_default traffic class and are inspected using HTTP inspection.
C. HTTP outbound traffic is permitted, but all return HTTP traffic is denied.
D. HTTP flows are statefully inspected using TCP stateful inspection.

Answer: D

NEW QUESTION 73
When you configure the Cisco ESA to perform blacklisting, what are two items you can disable to enhance performance? (Choose two.)

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

Answer: BD

NEW QUESTION 78
What are two arguments that can be used with the show content-scan command in Cisco IOS software? (Choose two.)

A. data
B. session
C. buffer

D. statistics
E. verbose

Answer: BD

NEW QUESTION 82
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

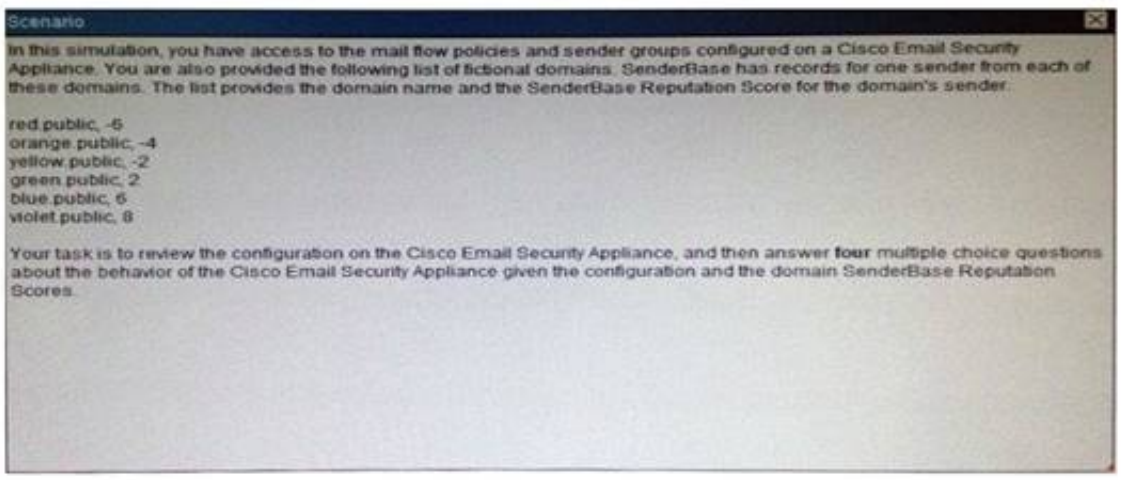
NEW QUESTION 87
Which three access control actions permit traffic to pass through the device when using Cisco FirePOWER? (Choose three.)

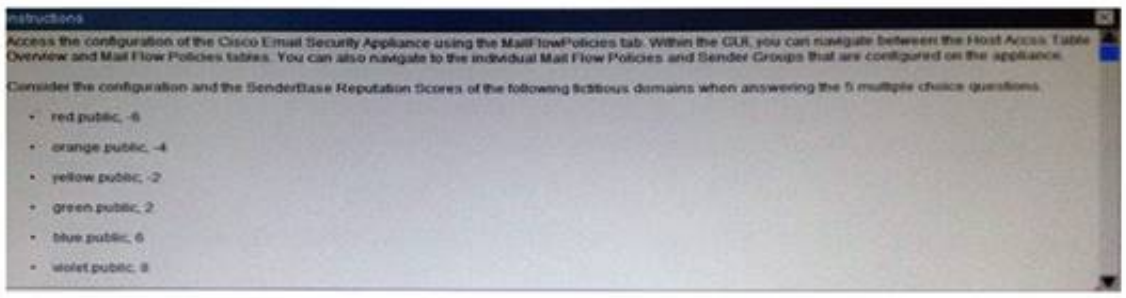
A. pass
B. trust
C. monitor
D. allow
E. permit
F. inspect

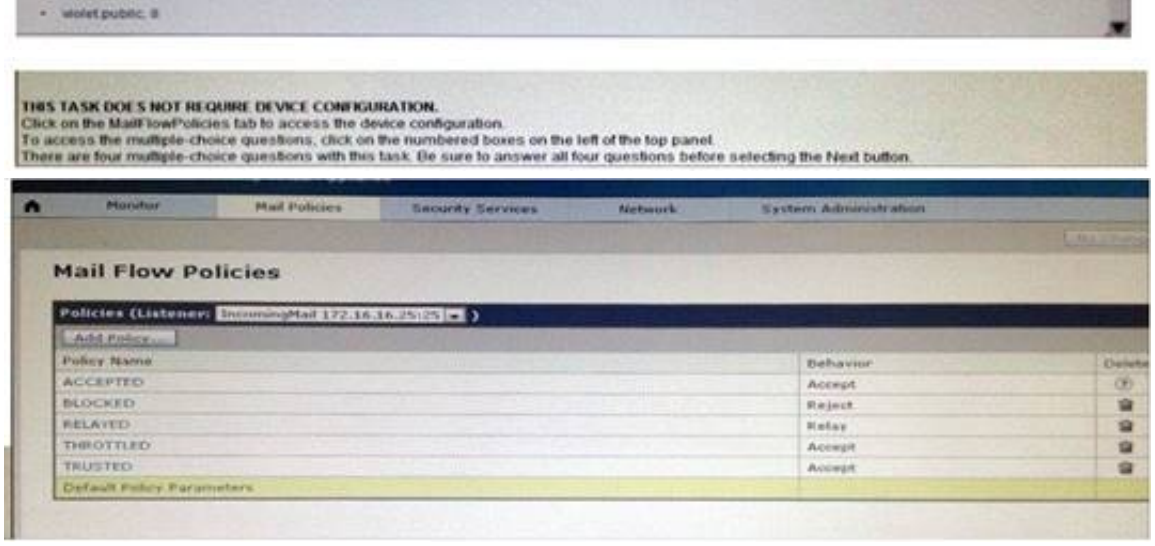
Answer: BCD

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

NEW QUESTION 92





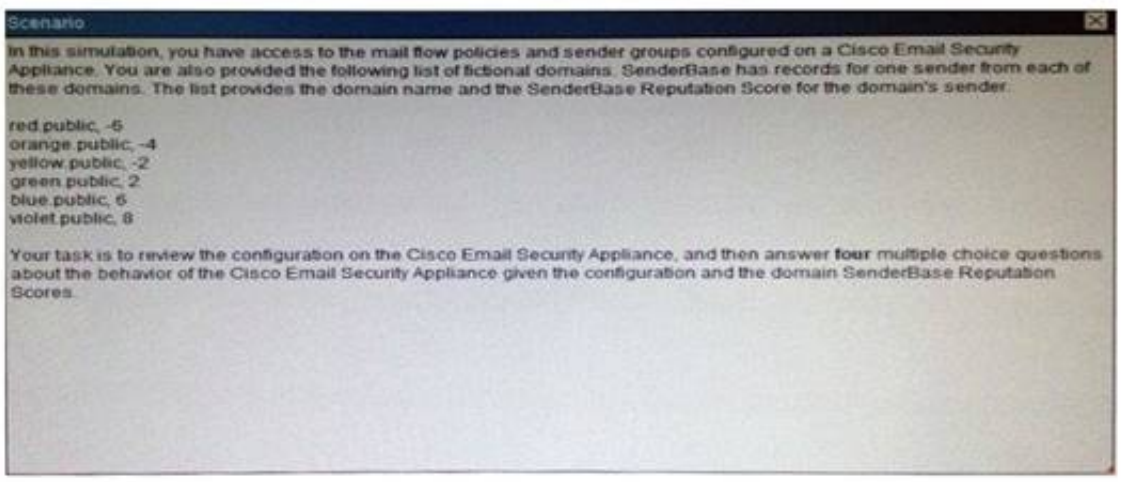


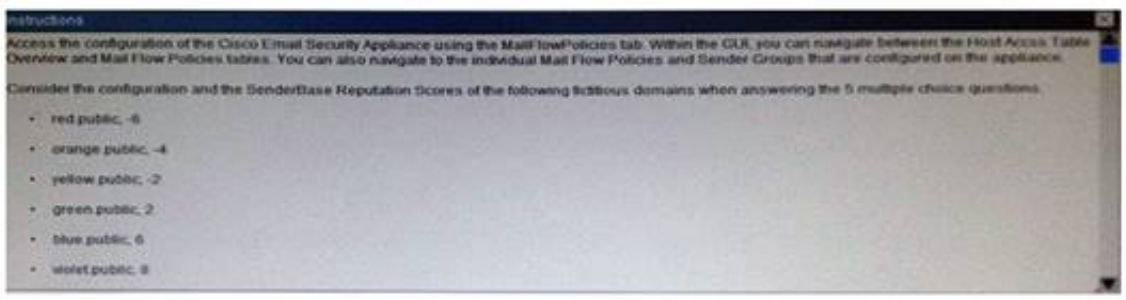
What is the maximum message size that the Cisco Email Security Appliance will accept from the violet.public domain?

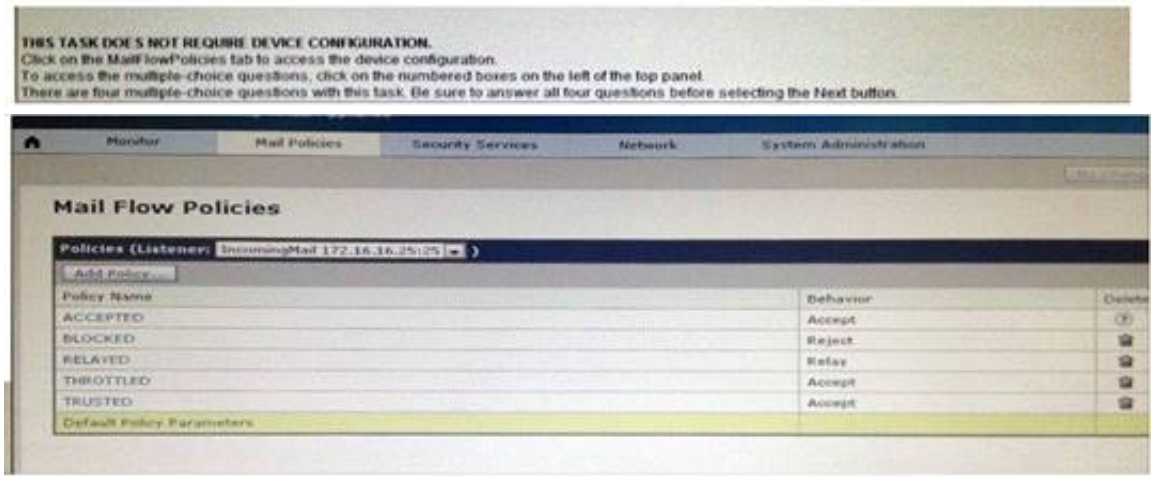
A. 1 KB
B. 100 KB
C. 1 MB
D. 10 MB
E. 100 MB
F. Unlimited

Answer: D

NEW QUESTION 96







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 97
Which website can be used to validate group information about connections that flow through Cisco CWS?

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

Answer: C

NEW QUESTION 100
When the WSA policy trace tool is used to make a request to the proxy, where is the request logged?

A. proxy logs
B. access logs
C. authentication logs
D. The request is not logged

Answer: B

NEW QUESTION 105
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 109
An engineer wants to improve web traffic performance by proxy caching. Which technology provides this improvement?

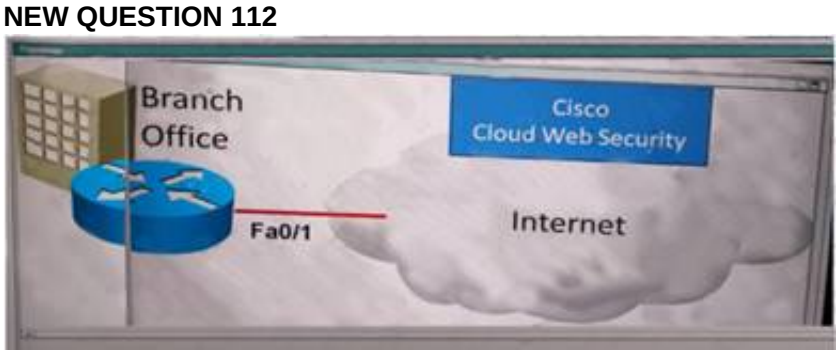
A. Firepower
B. FireSIGT
C. WSA
D. ASA

Answer: C

NEW QUESTION 111
Which two types of software can be installed on a cisco ASA-5545-X appliance? (choose two)

A. cisco ASAv
B. Cisco firePOWER Appliance
C. Cisco firePOWER services
D. cisco ASA
E. ciscofirePOWER management Center

Answer: CD

NEW QUESTION 112


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.

Answer:

Explanation: Pending

NEW QUESTION 115
An engineer is troubleshooting ARP cache on the ESA. Which command accomplishes this task?

A. diagnostic -> network -> arpshow
B. show ip arpshow
C. diagnostic -> ip -> arpshow
D. show network arpshow

Answer: A

NEW QUESTION 120
What are two requirements for configuring a hybrid interface in FirePOWER? (Choose two)

A. virtual network
B. virtual router
C. virtual appliance
D. virtual switch

E. virtual context

Answer: BD

Explanation: http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Hybrid

NEW QUESTION 123
Which option is a benefit of Cisco Email Security virtual appliance over the Cisco ESA appliance?

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

Answer: B

NEW QUESTION 125
Which Cisco FirePOWER setting is used to reduce the number of events received in a period of time and avoid being overwhelmed?

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

Answer: D

NEW QUESTION 127
An engineer is configuring a cisco ESA and wants to control whether to accept or reject email messages to a messages to a recipient address. Which list contains the allowed recipient addresses?

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

Answer: B

NEW QUESTION 128
Which CLI command is used to register a Cisco FirePOWER sensor to Firepower Management Center?

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

Answer: A

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

NEW QUESTION 130
In the cisco email security appliance, which tool be used to send a test email to a user can follow the flow of messages in configuration?

A. Message filter
B. Policy trace
C. Recipient access table
D. Content filter

Answer: B

NEW QUESTION 135
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 137
A customer's mobile clients now require content scanning, yet there is not an ASA on the network. Which deployment method is required for the Cisco AnyConnect Web Security Module?

A. standalone component
B. enterprise connection enforcement
C. roaming umbrella component
D. APEX enforcement

Answer: A

NEW QUESTION 139
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 144
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 145
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 147
Which option lists the minimum requirements to deploy a managed device inline?

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

Answer: A

NEW QUESTION 150
Which Cisco AMP file disposition valid?

A. pristine
B. malware
C. dirty
D. nonmalicios

Answer: B

Explanation: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Refere

NEW QUESTION 152
Which Cisco AMP for Endpoints, what, is meant by simple custom detection?

A. It is a rule for identifying a file that should be whitelisted by Cisco AMP.
B. It is a method for identifying and quarantining a specific file by its SHA-256 hash.
C. It is a feature for configuring a personal firewall.
D. It is a method for identifying and quarantining a set of files by regular expression language.

Answer: A

NEW QUESTION 154
Remote clients have reported application slowness. The remote site has one circuit that is highly utilized and a second circuit with nearly zero utilization. The business unit has asked to have applications load shared over two WAN links. An engineer has decided to deploy cisco Application Visibility and Control to better utilize the existing WAN links and to understand the traffic flows. Which configuration provides application deep packet inspection?

A. IP accounting
B. NBAR2
C. RMON
D. SNMP

Answer: B

NEW QUESTION 156
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 158

```
S*    0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C        1.1.1.0 255.255.255.0 is directly connect, outside
S        172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C        192.168.100.0 255.255.255.0 is directly connected, inside
C        172.16.10.0 255.255.255.0 is directly connected, dmz
S         10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz

access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
 match access-list redirect-acl

policy-map inside-policy
 class redirect-class
  sfr fail-open

service-policy inside-policy inside
```

Refer to the exhibit. Which option is a result of this configuration?

A. All ingress traffic on the inside interface that matches the access list is redirected.
B. All egress traffic on the outside interface that matches the access list is redirected.
C. All TCP traffic that arrives on the inside interface is redirected.
D. All ingress and egress traffic is redirected to the Cisco FirePOWER module.

Answer: C

NEW QUESTION 160
An engineer is configuring cisco ESA with a multilayer approach to fight virus and malware. Which two features can be used to fulfill that task?

A. Outbreak filters
B. White list
C. RAT
D. DLP
E. Sophos engine

Answer: AE

NEW QUESTION 165
Which option describes device trajectory on Cisco Advanced Matware Protection for Endpoints?

A. It shows the file path on a host.
B. It shows a full packet capture of the file.
C. It shows which devices on the network received the file.
D. It shows what a file did on a host.

Answer: C

NEW QUESTION 169
When you create a new server profile on the Cisco ESA, which subcommand of the ldapconfig command configures spam quarantine end-user authentication?

A. server
B. test
C. isqalias
D. isqauth

Answer: D

NEW QUESTION 170
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 175
Which Cisco ESA predefined sender group uses parameter-matching to reject senders?

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

Answer: B

NEW QUESTION 180
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 185
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 190
Which type of policy do you configure if you want to look for a combination of events using Boolean logic?

A. correlation
B. application detector
C. traffic profile
D. access control
E. intrusion

Answer: A

NEW QUESTION 191
A customer has recently purchased Cisco Application Visibility and Control and requires an AVC application profile to control a recognized application. Which two actions can be defined when creating an application profile? (Choose two.)

A. drop
B. tag
C. mark
D. alert
E. allow

Answer: AC

NEW QUESTION 192
Which information does whoami command display in a WSA?

A. Full name, group and location
B. Username, fullname and groups

C. Username only
D. Username and groups

Answer: B

NEW QUESTION 193
Which three protocols are required when considering firewall rules email services using a Cisco Email Security Appliance?

A. HTTP
B. SMTP
C. TFTP
D. FTP
E. DNS
F. SNMP

Answer: ABE

NEW QUESTION 195
Which object can be used on a Cisco FirePOWER appliance, but not in an access control policy rule on Cisco FirePOWER services running on a Cisco ASA?

A. URL
B. security intelligence
C. VLAN
D. geolocation

Answer: C

NEW QUESTION 196
On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed devices?

A. health policy
B. system policy
C. correlation policy
D. access control policy
E. health awareness policy

Answer: A

NEW QUESTION 197
An engineer must deploy email security to a large enterprise with multiple offices. Each office cannot support its own ESA appliance. What technology best supports email security across the organization?

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

Answer: C

NEW QUESTION 200
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 202
In a Cisco FirePOWER instrusion policy, which two event actions can be configured on a rule? (Choose two.)

A. drop packet
B. drop and generate
C. drop connection
D. capture trigger packet
E. generate events

Answer: B

Explanation: Topic 2, Exam Set 2

NEW QUESTION 207

Cisco's ASACX includes which two URL categories? (Choose two.)

A. Proxy Avoidance
B. Dropbox
C. Hate Speech
D. Facebook
E. Social Networking
F. Instant Messaging and Video Messaging

Answer: CE

NEW QUESTION 211
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 212
Which three search parameters are supported by the Email Security Monitor? (Choose three.)

A. Destination domain
B. Network owner
C. MAC address
D. Policy requirements
E. Internal sender IP address
F. Originating domain

Answer: ABE

NEW QUESTION 214
Which five system management protocols are supported by the Intrusion Prevention System? (Choose five.)

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

Answer: ABCFG

NEW QUESTION 219

Instructions

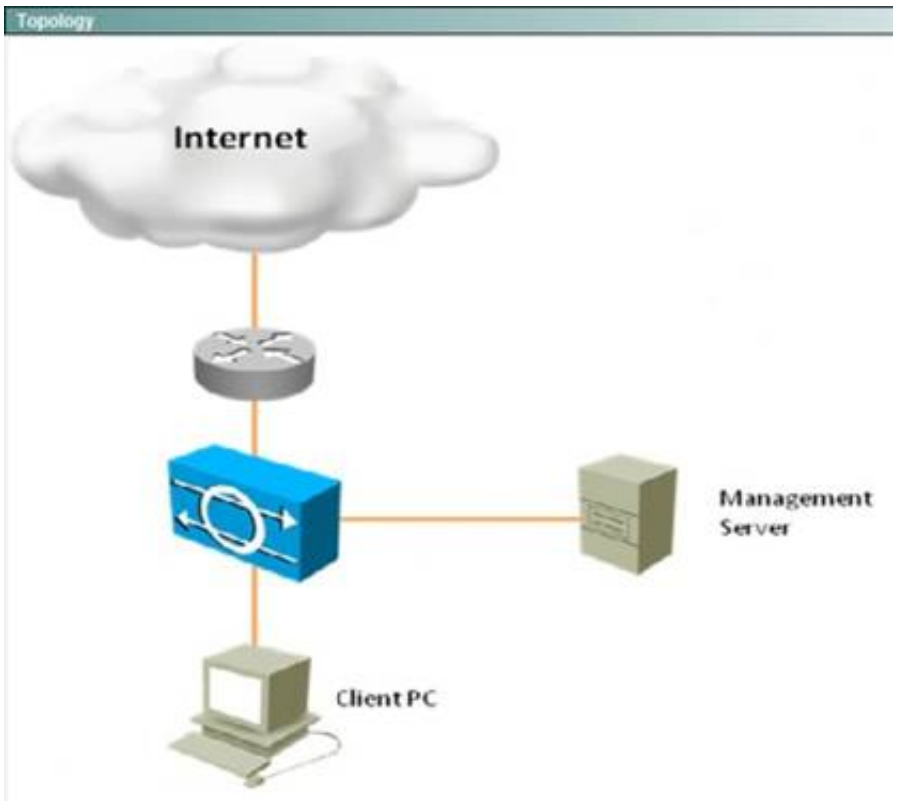
You can click the grey buttons at the bottom of this frame to view the different windows.

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 220
An ASA with an IPS module must be configured to drop traffic matching IPS signatures and block all traffic if the module fails. Which describes the correct configuration?

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

Answer: B

NEW QUESTION 224
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 229
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 230
Which four statements are correct regarding management access to a Cisco Intrusion Prevention System? (Choose four.)

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

Answer: BDEG

NEW QUESTION 234
Which Cisco technology is a customizable web-based alerting service designed to report threats and vulnerabilities?

A. Cisco Security Intelligence Operations
B. Cisco Security IntelliShield Alert Manager Service
C. Cisco Security Optimization Service
D. Cisco Software Application Support Service

Answer: B

NEW QUESTION 236
Which Cisco WSA is intended for deployment in organizations of up to 1500 users?

A. WSA S370
B. WSA S670
C. WSA S370-2RU
D. WSA S170

Answer: D

NEW QUESTION 240

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.

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 245
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 246
What is the default CX Management 0/0 IP address on a Cisco ASA 5512-X appliance?

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

Answer: F

NEW QUESTION 250
Which Cisco IPS CLI command shows the most fired signature?

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

Answer: A

NEW QUESTION 253
What three alert notification options are available in Cisco IntelliShield Alert Manager? (Choose three.)

A. Alert Summary as Text
B. Complete Alert as an HTML Attachment
C. Complete Alert as HTML
D. Complete Alert as RSS
E. Alert Summary as Plain Text
F. Alert Summary as MMS

Answer: ABC

NEW QUESTION 256
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 261
Which three functions can Cisco Application Visibility and Control perform? (Choose three.)

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

Answer: BDE

NEW QUESTION 265
What is the default antispam policy for positively identified messages within the Cisco Email Security Appliance?

A. Drop
B. Deliver and Append with [SPAM]
C. Deliver and Prepend with [SPAM]
D. Deliver and Alternate Mailbox

Answer: C

NEW QUESTION 267
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 268
Which two practices are recommended for implementing NIPS at enterprise Internet edges? (Choose two.)

A. Integrate sensors primarily on the more trusted side of the firewall (inside or DMZ interfaces).
B. Integrate sensors primarily on the less trusted side of the firewall (outside interfaces).
C. Implement redundant IPS and make data paths symmetrical.
D. Implement redundant IPS and make data paths asymmetrical.

E. Use NIPS only for small implementations.

Answer: AC

NEW QUESTION 271
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 274
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 275

Instructions

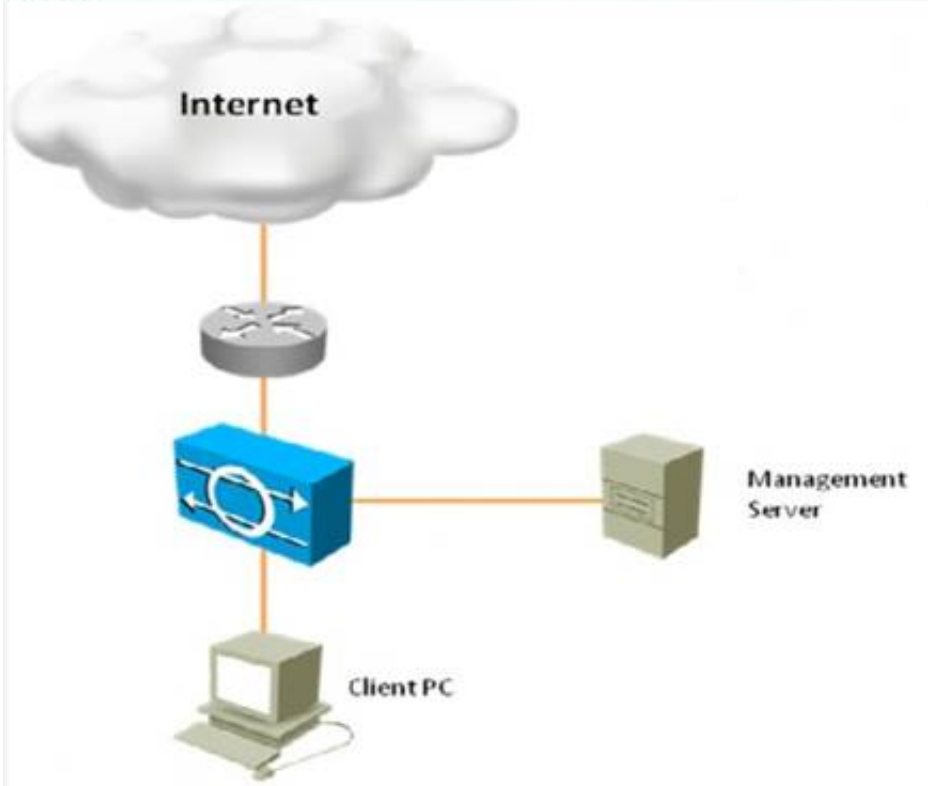
You can click the grey buttons at the bottom of this frame to view the different windows.

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

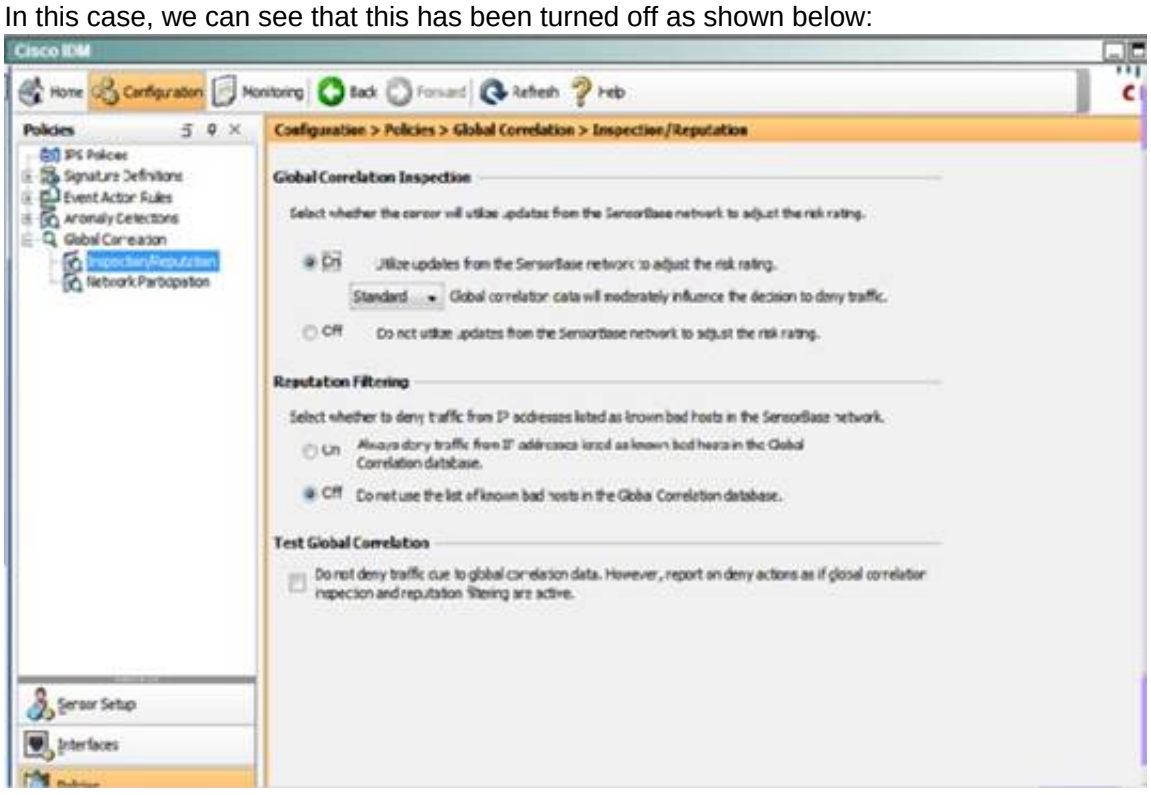


To what extent will the Cisco IPS sensor contribute data to the Cisco SensorBase network?

A. It will not contribute to the SensorBase network.
B. It will contribute to the SensorBase network, but will withhold some sensitive information
C. It will contribute the victim IP address and port to the SensorBase network.
D. It will not contribute to Risk Rating adjustments that use information from the SensorBase network.

Answer: B

Explanation: To configure network participation, follow these steps:
Step 1: Log in to IDM using an account with administrator privileges.
Step 2: Choose Configuration > Policies > Global Correlation > Network Participation. Step 3: To turn on network participation, click the Partial or Full radio button:
•Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
•Full—All data is contributed to the SensorBase Network
In this case, we can see that this has been turned off as shown below:



NEW QUESTION 279
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 283
Which Cisco WSA is intended for deployment in organizations of more than 6000 users?

A. WSA S370
B. WSA S670
C. WSA S370-2RU
D. WSA S170

Answer: B

NEW QUESTION 288
Which Cisco monitoring solution displays information and important statistics for the security devices in a network?

A. Cisco Prime LAN Management
B. Cisco ASDM Version 5.2
C. Cisco Threat Defense Solution
D. Syslog Server
E. TACACS+

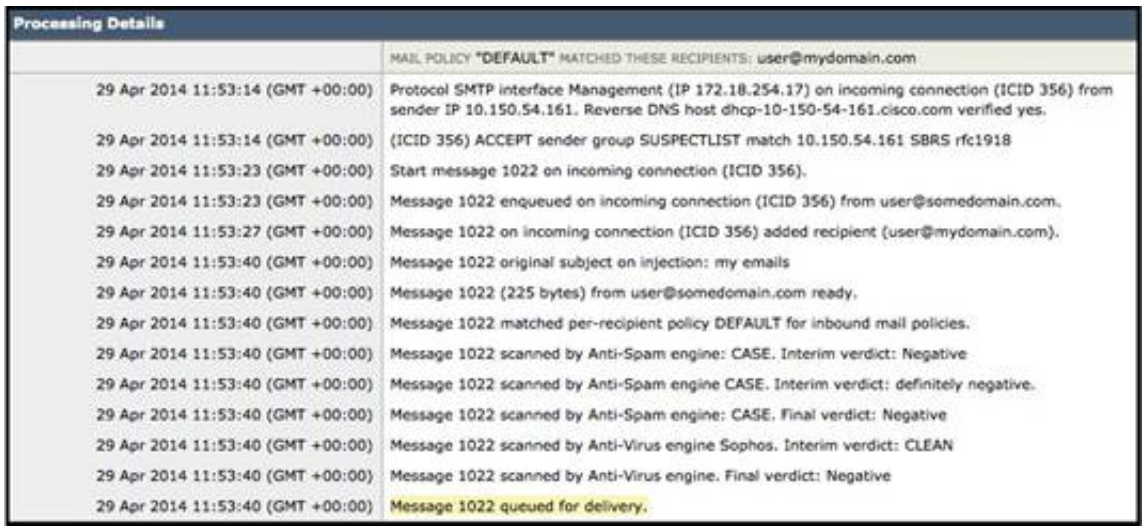
Answer: B

NEW QUESTION 290
What can Cisco Prime Security Manager (PRSM) be used to achieve?

A. Configure and Monitor Cisco CX Application Visibility and Control, web filtering, access and decryption policies
B. Configure Cisco ASA connection limits
C. Configure TCP state bypass in Cisco ASA and IOS
D. Configure Cisco IPS signature and monitor signature alerts
E. Cisco Cloud Security on Cisco ASA

Answer: A

NEW QUESTION 291
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 SBRS 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 292
When a Cisco Email Security Appliance joins a cluster, which four settings are inherited? (Choose four.)

A. IP address
B. DNS settings
C. SMTP routes
D. HAT
E. RAT
F. hostname
G. certificates

Answer: BCDE

NEW QUESTION 293
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 298
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 299
Which three user roles are partially defined by default in Prime Security Manager? (Choose three.)

A. networkoperator
B. admin
C. helpdesk
D. securityoperator
E. monitoringadmin
F. systemadmin

Answer: BCF

NEW QUESTION 302
The Web Security Appliance has identities defined for faculty and staff, students, and default access. The faculty and staff identity identifies users based on the source network and authenticated credentials. The identity for students identifies users based on the source network along with successful authentication credentials. The global identity is for guest users not authenticated against the domain.
Recently, a change was made to the organization's security policy to allow faculty and staff access to a social network website, and the security group changed the access policy for faculty and staff to allow the social networking category.
Which are the two most likely reasons that the category is still being blocked for a faculty and staff user? (Choose two.)

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

Answer: CE

NEW QUESTION 303
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 308
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 312
What is the CLI command to create a new Message Filter in a Cisco Email Security Appliance?

A. filterconfig
B. filters new
C. messagefilters
D. policyconfig-- inbound or outbound-- filters

Answer: B

NEW QUESTION 317
Which two options are features of the Cisco Email Security Appliance? (Choose two.)

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

Answer: CD

NEW QUESTION 318
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 322
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 324
The helpdesk was asked to provide a record of delivery for an important email message that a customer claims it did not receive. Which feature of the Cisco Email Security Appliance provides this record?

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

Answer: C

NEW QUESTION 328
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 333
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 338
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 339
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 341
Which two statements about Cisco Cloud Web Security functionality are true? (Choose two.)

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

Answer: AD

NEW QUESTION 345
What command alters the SSL ciphers used by the Cisco Email Security Appliance for TLS sessions and HTTPS access?

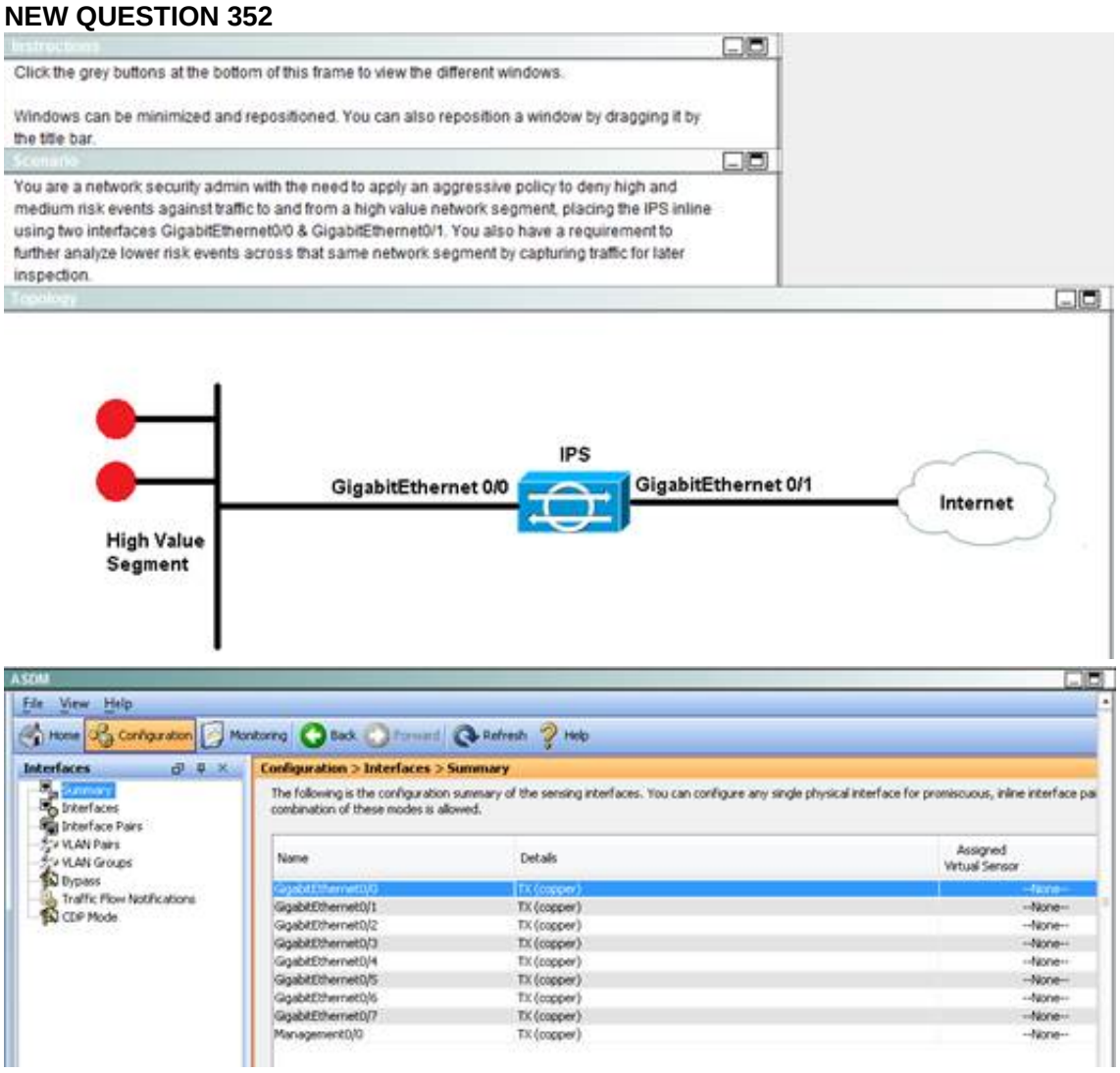
A. sslconfig
B. sslciphers
C. tlsconifg
D. certconfig

Answer: A

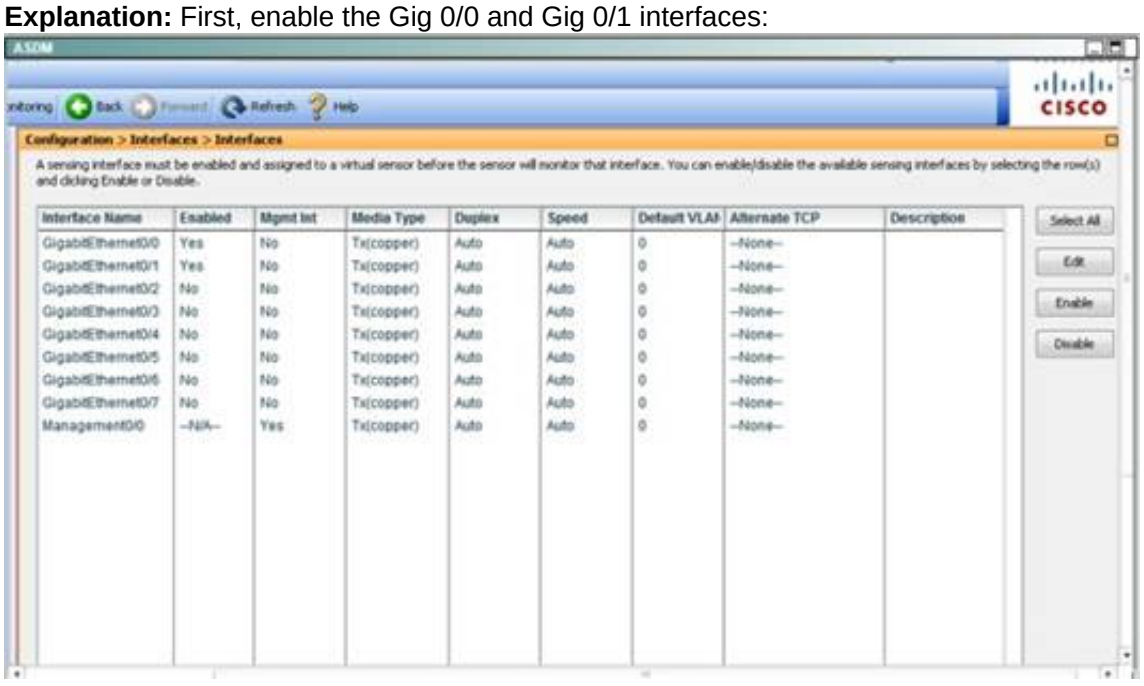
NEW QUESTION 348
Which version of AsyncOS for web is required to deploy the Web Security Appliance as a CWS connector?

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

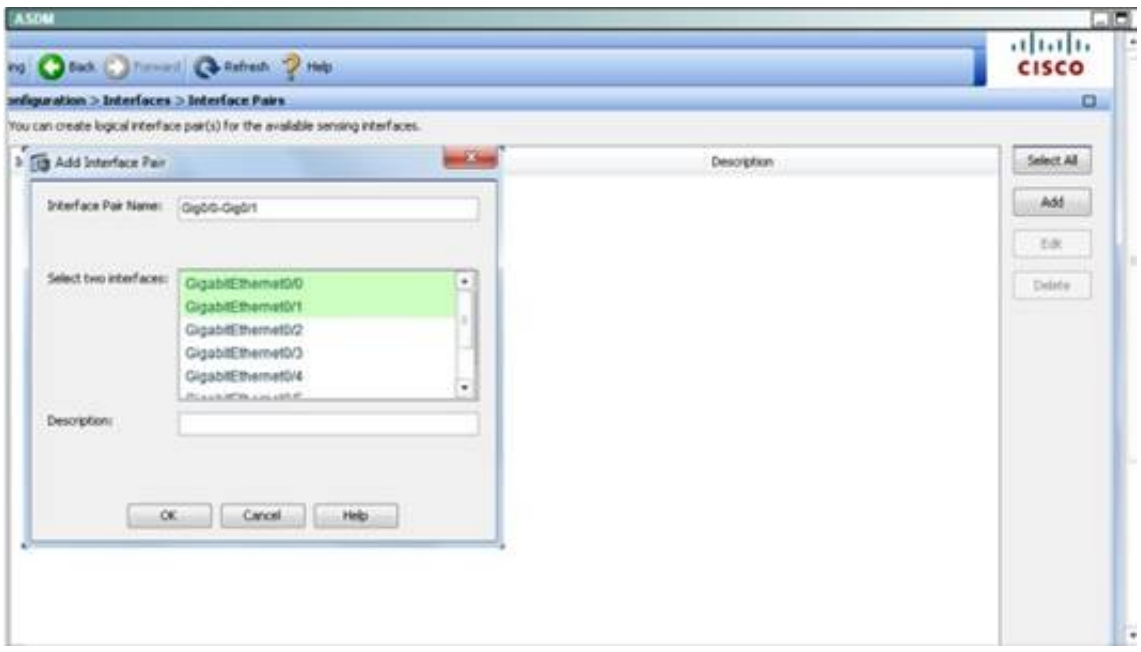
Answer: C

NEW QUESTION 352


Answer:

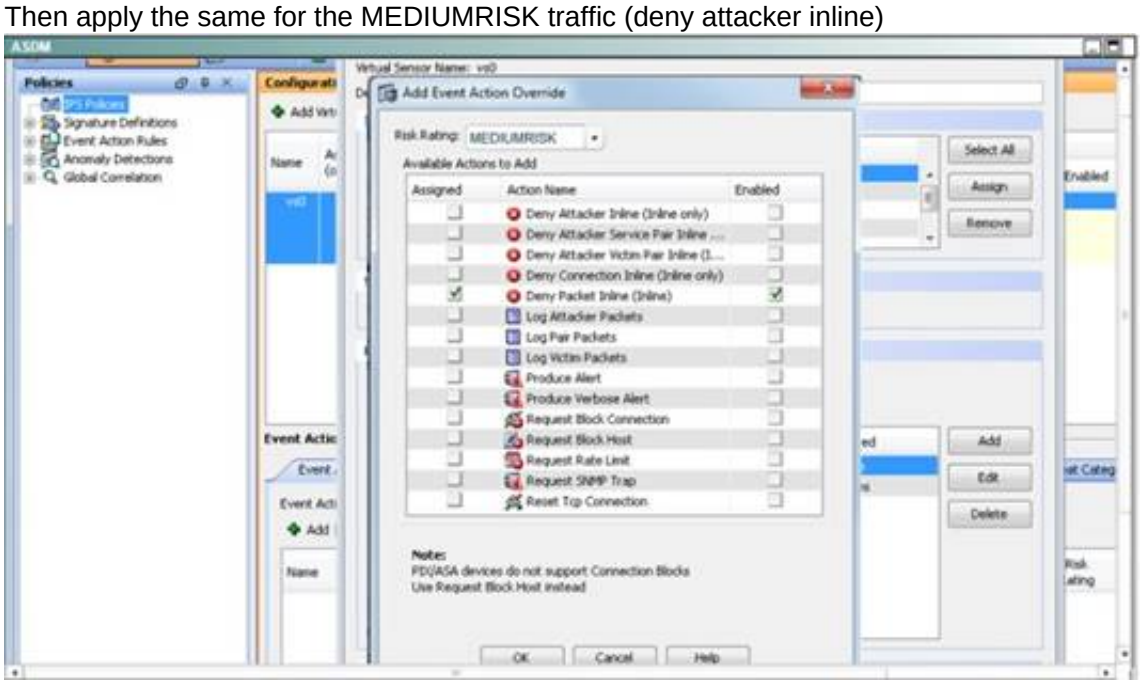
Explanation: First, enable the Gig 0/0 and Gig 0/1 interfaces:


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

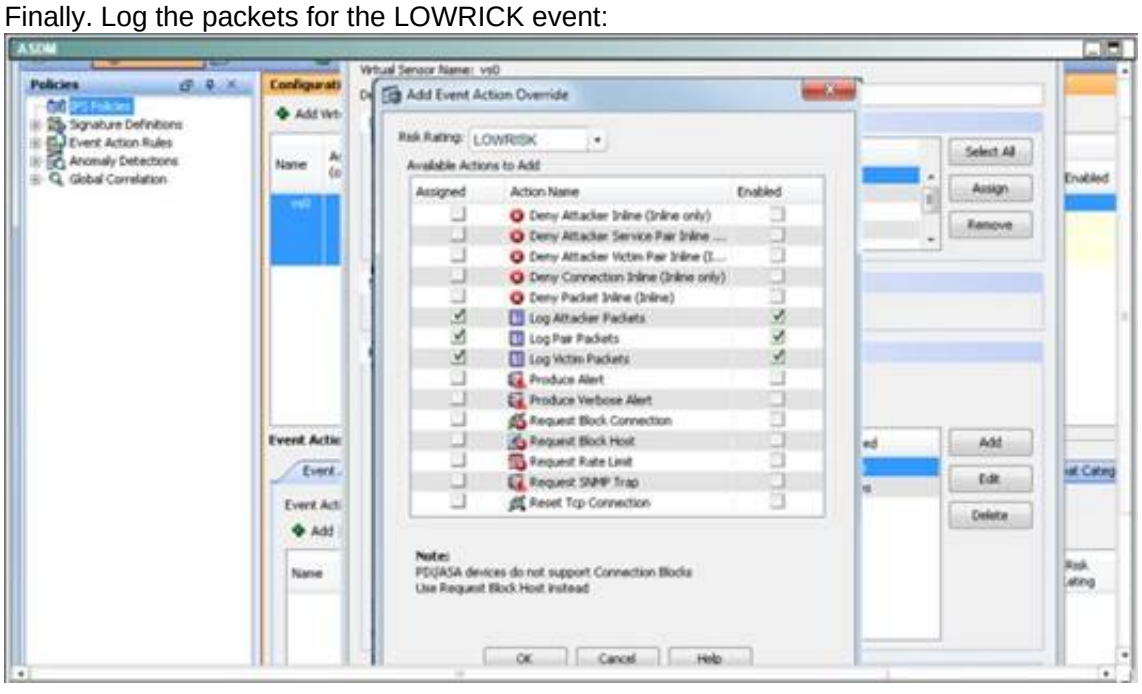


Then, apply the HIGHRISK action rule to the newly created interface pair:

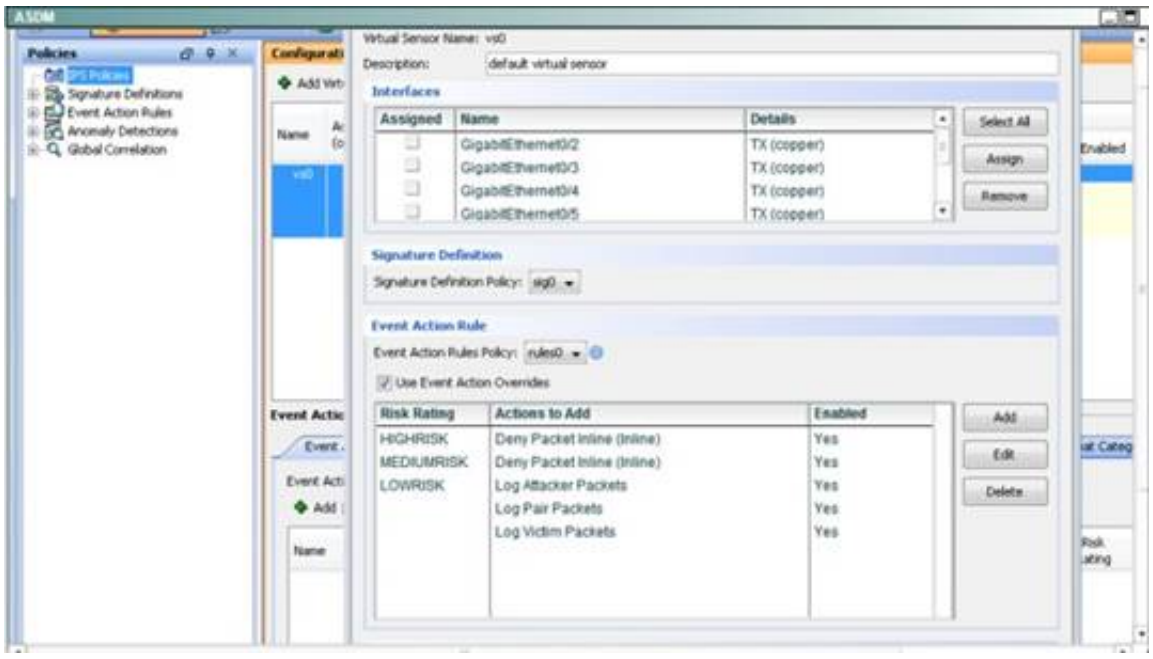
Then apply the same for the MEDIUMRISK traffic (deny attacker inline)

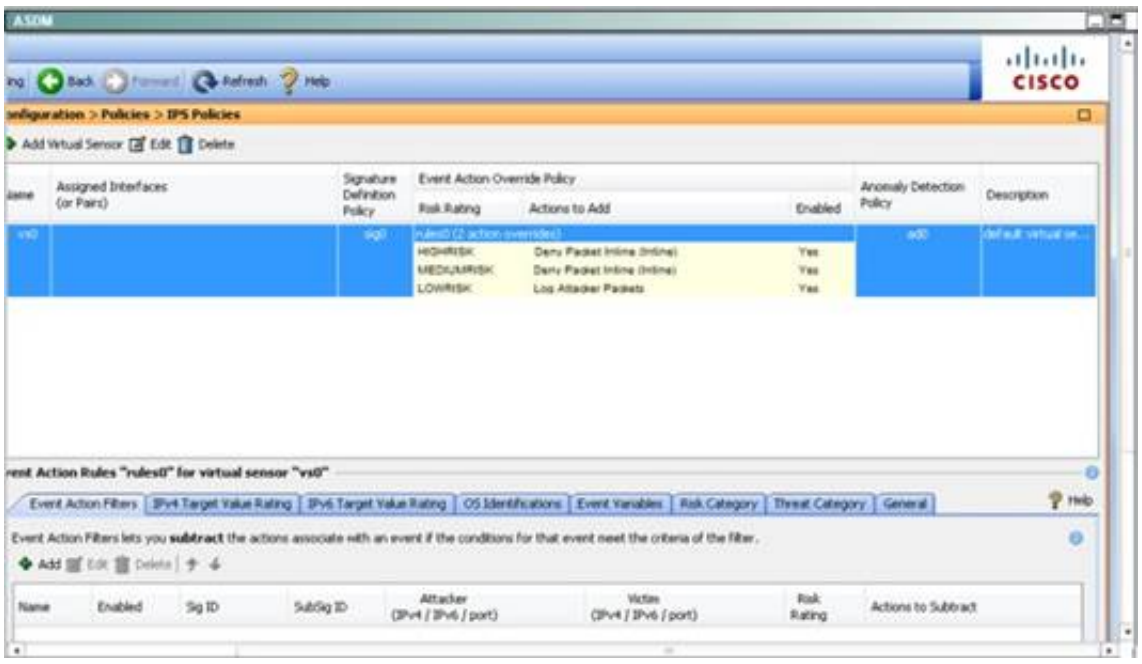


Finally. Log the packets for the LOWRICK event:



When done it should look like this:





NEW QUESTION 354
How does a user access a Cisco Web Security Appliance for initial setup?

A. Connect the console cable and use the terminal at 9600 baud to run the setup wizard.
B. Connect the console cable and use the terminal at 115200 baud to run the setup wizard.
C. Open the web browser at 192.168.42.42:8443 for the setup wizard over https.
D. Open the web browser at 192.168.42.42:443 for the setup wizard over https.

Answer: C

NEW QUESTION 358
Which IPS engine detects ARP spoofing?

A. Atomic ARP Engine
B. Service Generic Engine
C. ARP Inspection Engine
D. AICEngine

Answer: A

NEW QUESTION 363
Cisco AVC allows control of which three of the following? (Choose three.)

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

Answer: ADE

NEW QUESTION 364
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 369
Refer to the exhibit.

```
Status as of:                  Wed May 22 16:05:13 2013 GMT
Hosts marked with '*' were down as of the last delivery attempt.

                                Active  Conn.    Deliv.      Soft       Hard
#   Recipient Host              Recip.   Out     Recip.    Bounced    Bounced

1   example.com                   1      11       10078        0          1
2   acme.com                      0      3        34021        0          0
3   biology.acme.com              0      9        64026        0          0
4   *chemistry.acme.com           0      2        94091        0          0
5   pluto.acme.com                0      6        75021        0          0
5   *venus.acme.com               100    0          0          0          0
7   the.encryption.queue          0      0        90649        0          0
8   the.euq.queue                 0      0          1          0          0
9   the.euq.release.queue         0      0        4531         0          0

email.example.com>
```

What CLI command generated the output?

A. smtproutes
B. tophosts
C. hoststatus
D. workqueuestatus

Answer: B

NEW QUESTION 373
ACisco Web Security Appliance's policy can provide visibility and control of which two elements? (Choose two.)

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

Answer: CD

NEW QUESTION 376
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 381
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 386
ACisco Email Security Appliance uses which message filter to drop all executable attachments entering and leaving the Cisco Email Security Appliance?

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

Answer: A

NEW QUESTION 389
Which three statements about Cisco ASACX 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 393
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 398
An ASA with an IPS module must be configured to drop traffic matching IPS signatures and block all traffic if the module fails. Which describes the correct configuration?

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

Answer: B

NEW QUESTION 400
What is the default antispam policy for positively identified messages?

A. Drop
B. Deliver and Append with [SPAM]
C. Deliver and Prepend with [SPAM]
D. Deliver and Alternate Mailbox

Answer: C

NEW QUESTION 404
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

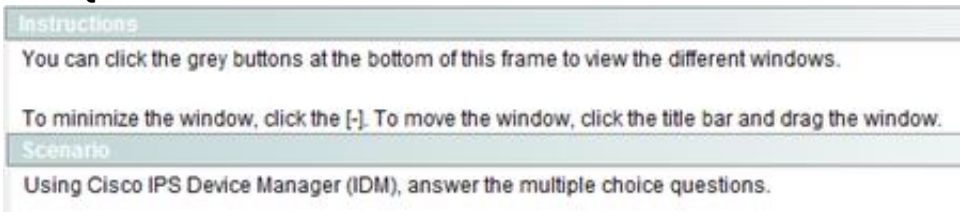
Answer: A

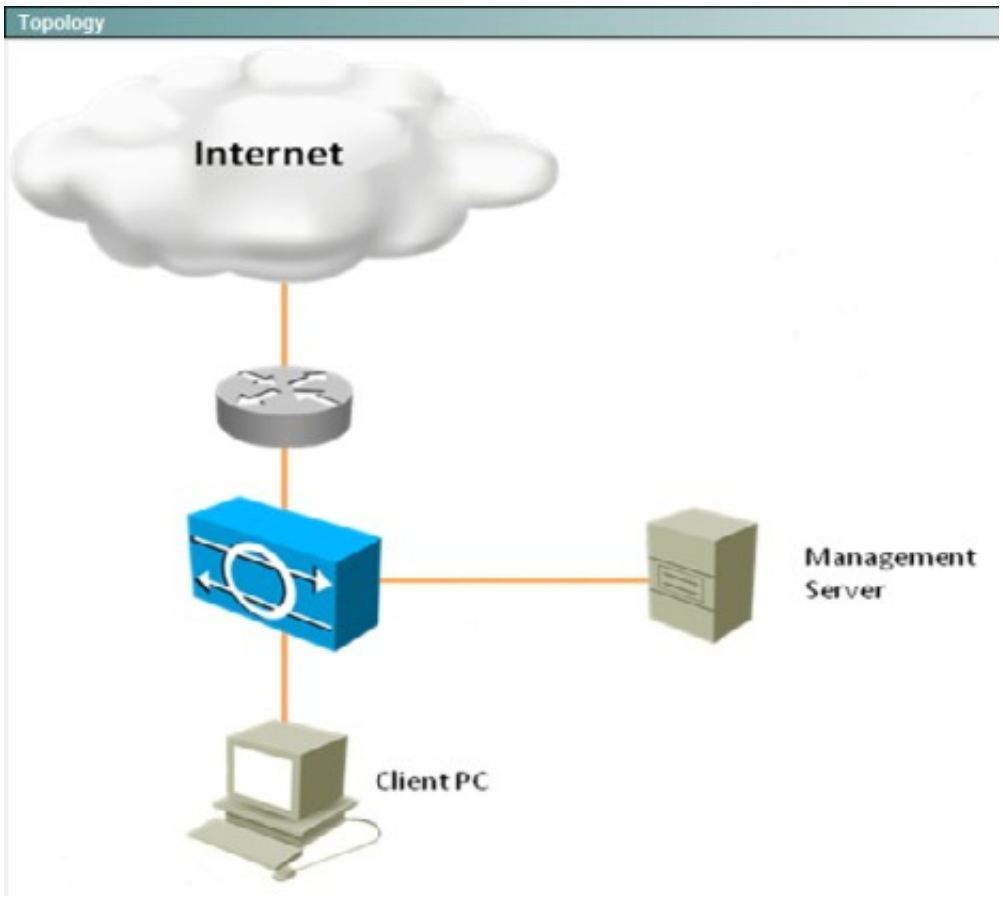
NEW QUESTION 408
What is the default IP range of the external zone?

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 411



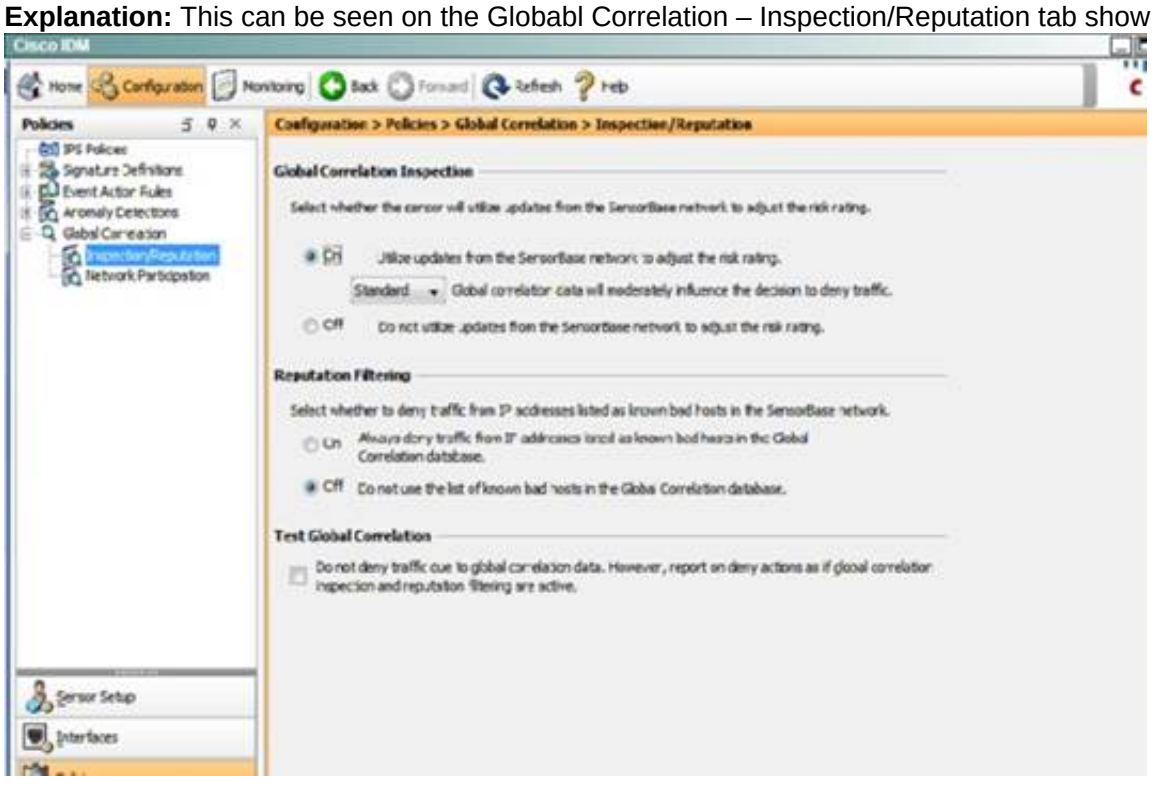


What action will the sensor take regarding IP addresses listed as known bad hosts in the Cisco SensorBase network?

A. Global correlation is configured in Audit mode fortesting 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 Globabl Correlation – Inspection/Reputation tab show below:



NEW QUESTION 413
What are the initial actions that can be performed on an incoming SMTP session by the workqueue of a Cisco Email Security Appliance?

A. Accept, Reject, Relay, TCPRefuse
B. LDAP Verification, Envelope Sender Verification, Bounce Verification, Alias Table Verification
C. Recipient Access Table Verification, Host DNS Verification, Masquerading, Spam Payload Check
D. SMTP Authentication, SBRS Verification, Sendergroup matching, DNS host verification

Answer: A

NEW QUESTION 415
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 417
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 419
At which value do custom signatures begin?

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

Answer: D

NEW QUESTION 421
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 426
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 428
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 433
The security team needs to limit the number of e-mails they receive from the Intellishield Alert Service. Which three parameters can they adjust to restrict alerts to specific product sets? (Choose three.)

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

Answer: AEF

NEW QUESTION 434
Which Cisco Cloud Web Security tool provides URL categorization?

A. Cisco Dynamic Content Analysis Engine
B. Cisco ScanSafe
C. ASA Firewall Proxy
D. Cisco Web Usage Control

Answer: D

NEW QUESTION 435
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 436
Which three features does Cisco CX provide? (Choose three.)

A. HTTPS traffic decryption and inspection
B. Application Visibility and Control
C. Category or reputation-based URL filtering
D. Email virus scanning
E. Application optimization and acceleration
F. VPN authentication

Answer: ABC

Explanation: Topic 3, Exam Set 3

NEW QUESTION 441
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 443
What is the function of the Cisco Context Adaptive Scanning Engine in Cisco Hybrid Email Security services?

A. It uses real-time traffic threat assessment to identify suspicious email senders and messages.
B. It provides a preventive defense against viruses by scanning messages before they enter the network.
C. It analyzes message content and attachments to protect an organization's intellectual property.
D. It protects against blended threats by using human-like logic to review and evaluate traffic.

Answer: D

NEW QUESTION 445
An IPS is configured to fail-closed and you observe that all packets are dropped. What is a possible reason for this behavior?

A. Mainapp is unresponsive.
B. The global correlation update failed.

C. The IPS span session failed.
D. The attack drop file is misconfigured.

Answer: A

NEW QUESTION 450
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

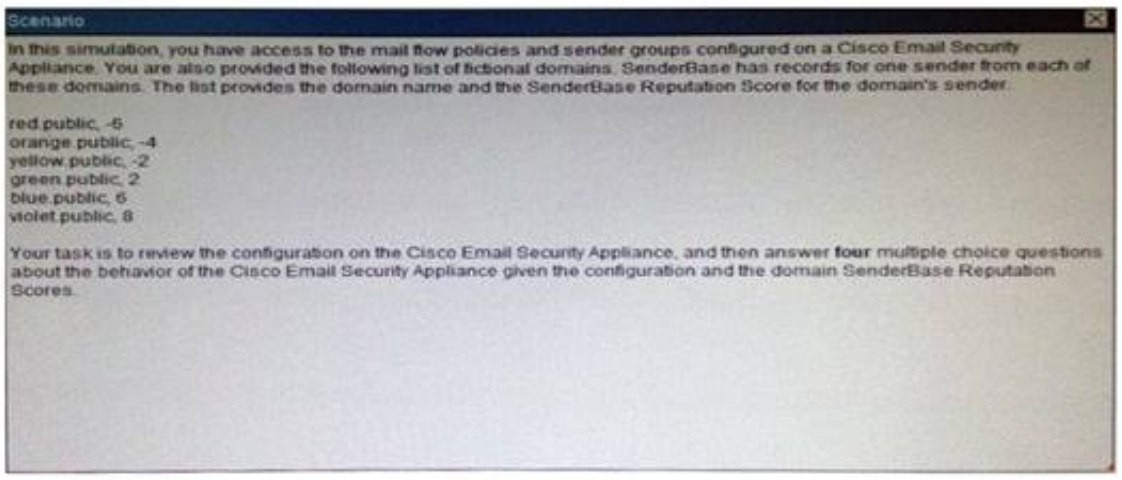
Answer: D

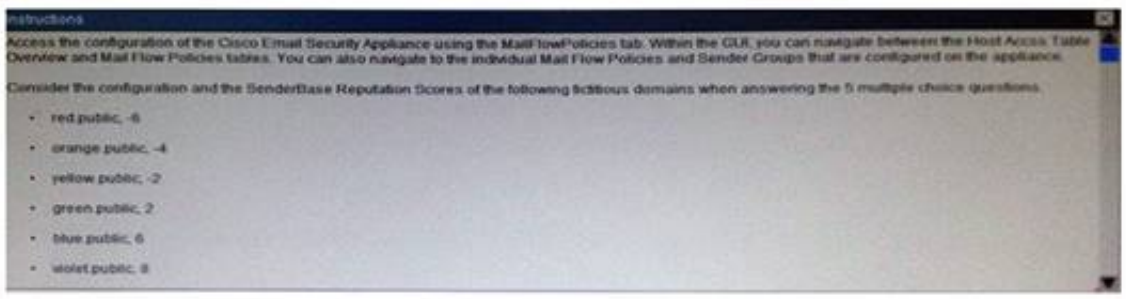
NEW QUESTION 451
Which three protocols are required when considering firewall rules for email services using a Cisco Email Security Appliance? (Choose three.)

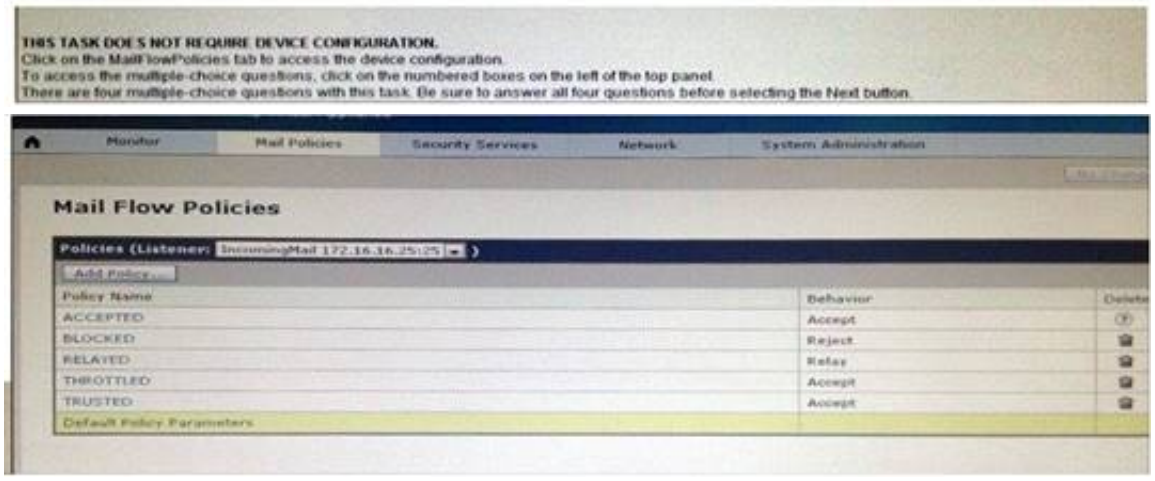
A. SMTP
B. HTTP
C. DNS
D. SNMP
E. FTP

Answer: ABC

NEW QUESTION 456







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

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

Answer: C

NEW QUESTION 458
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 461
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 463
Refer to the Following. Which option describe the result of this configuration on a Cisco ASA firewall?
asafwl (config) #http server enable asafw1(config)#http 10.10.10.1 255.255.255.255 inside

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

Answer: B

NEW QUESTION 466
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 469
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 473
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 477
Which command sets the number of packets to log on a Cisco IPS sensor?

A. ip-log-count number
B. ip-log-packets number
C. ip-log-bytes number
D. ip-log number

Answer: B

NEW QUESTION 478
Which command verifies that CWS redirection is working on a Cisco IOS router?

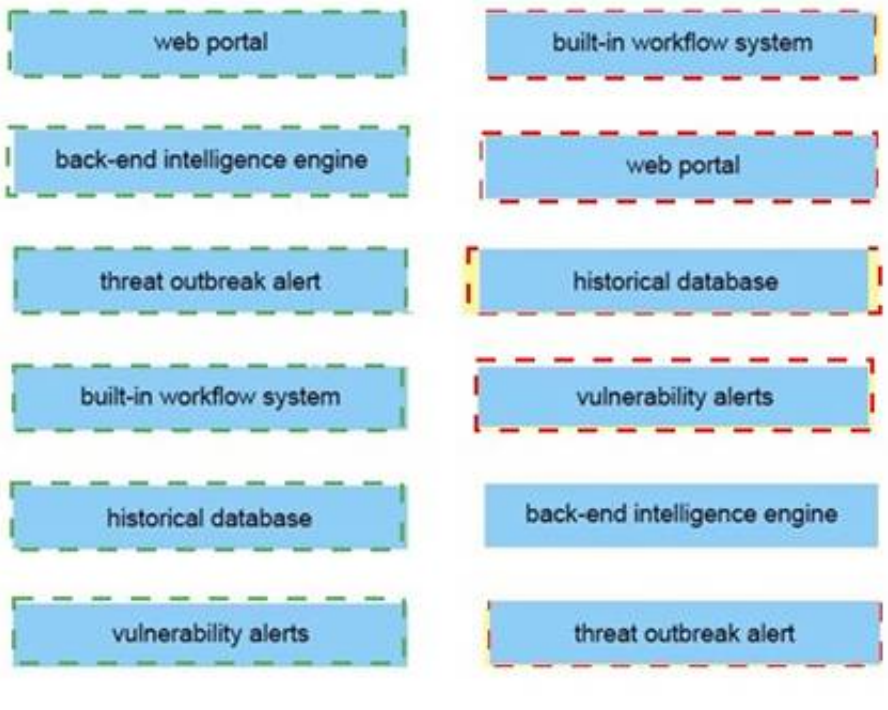
A. show content-scan session active
B. show content-scan summary
C. show interfaces stats
D. show sessions

Answer: A

NEW QUESTION 482
Drag and drop the Cisco Security IntelliShield Alert Manager Service components on the left onto the corresponding description on the right.

Answer:

Explanation:

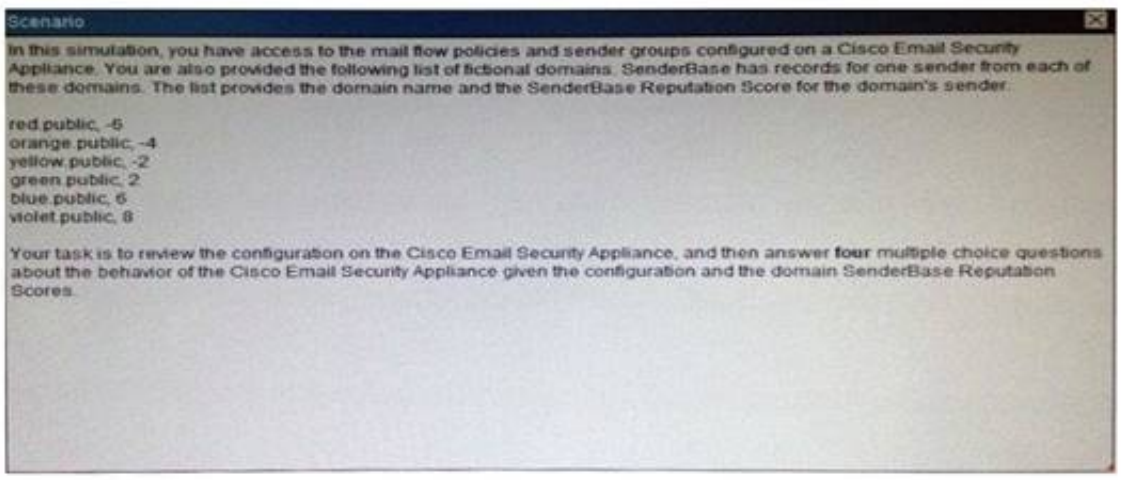


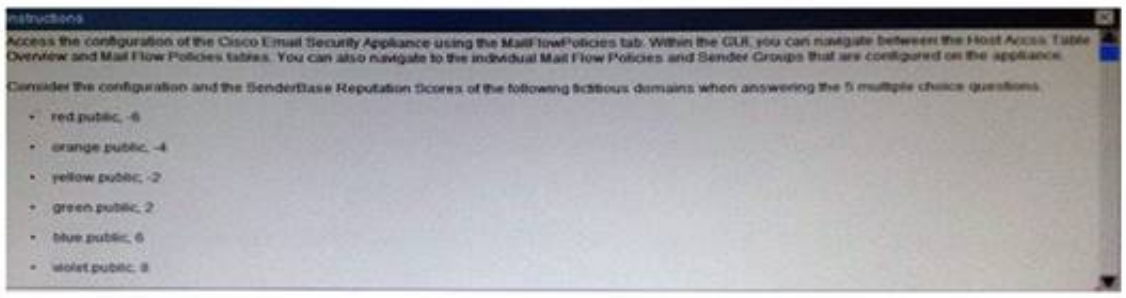
NEW QUESTION 487
Which sensor deployment mode does Cisco recommend when interface capacity is limited and you need to increase sensor functionality?

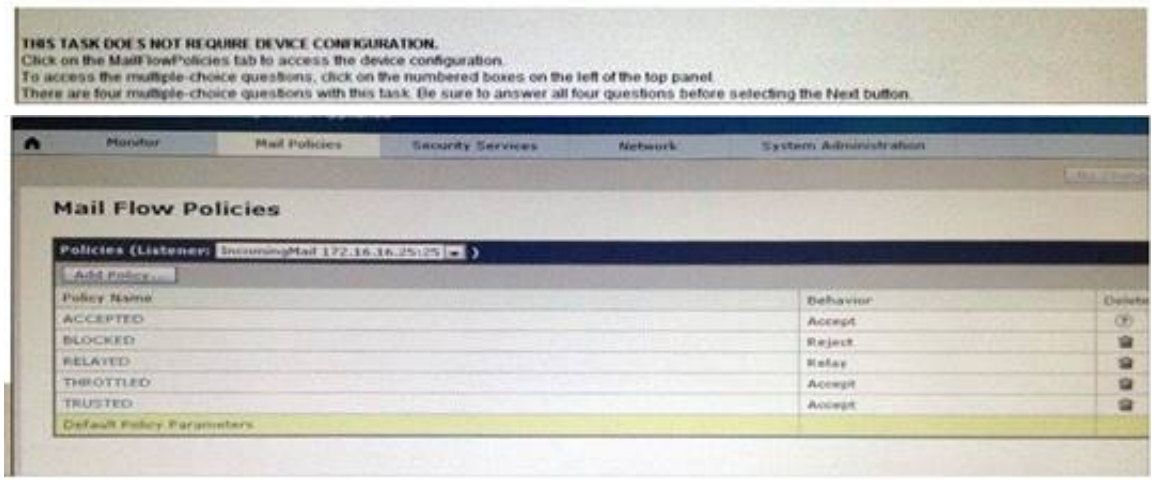
A. inline interface pair mode
B. inline VLAN pair mode
C. inline VLAN group mode
D. VLAN group mode

Answer: C

NEW QUESTION 489







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 493
Which technology is used to improve business-critical application performance?

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

Answer: A

NEW QUESTION 495
Which description of an advantage of utilizing IPS virtual sensors is true?

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

Answer: A

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

NEW QUESTION 499
How are HTTP requests handled by the Cisco WSA?

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

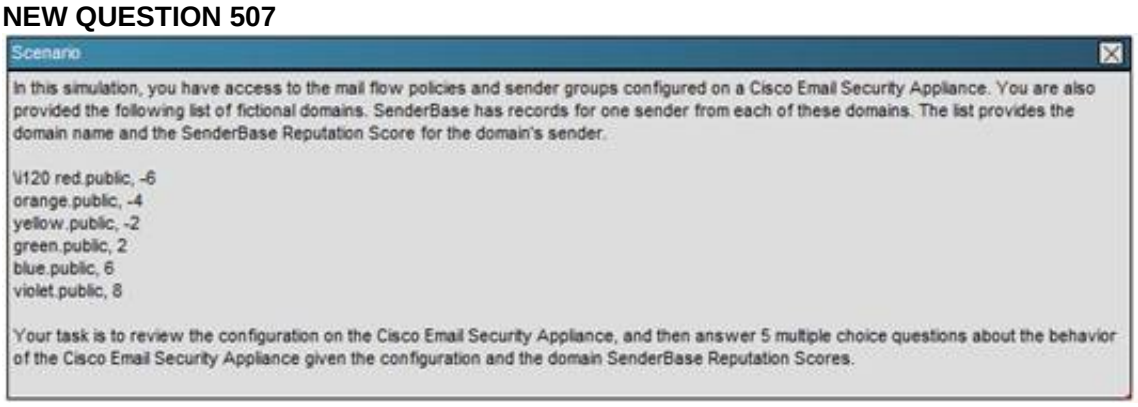
Answer: D

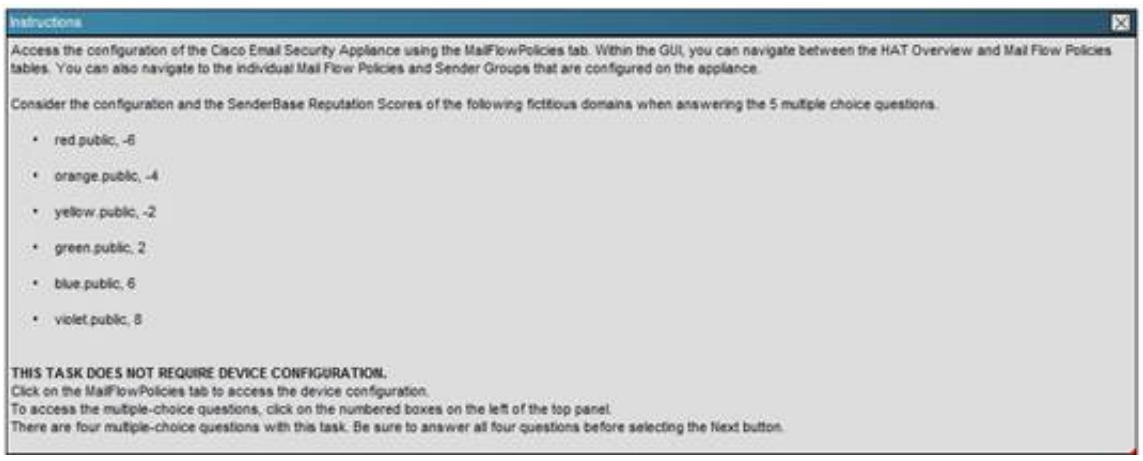
NEW QUESTION 504
Which feature does Acceptable Use Controls use to implement Cisco AVC?

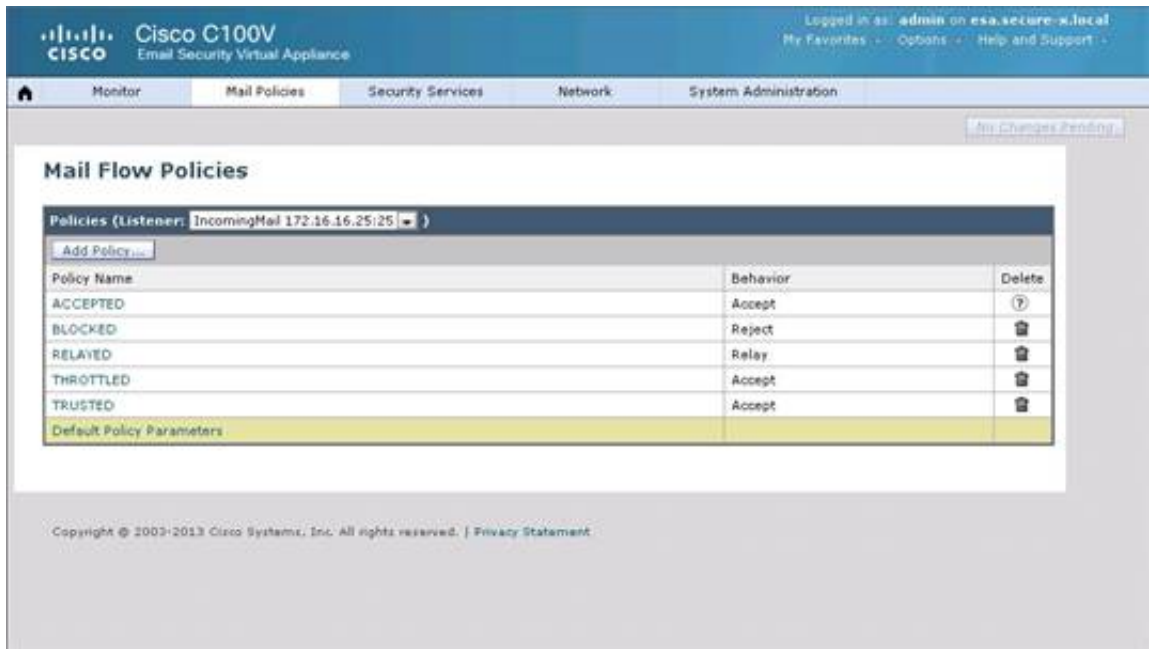
A. ISA
B. Cisco Web Usage Controls
C. Cisco WSA
D. Cisco ESA

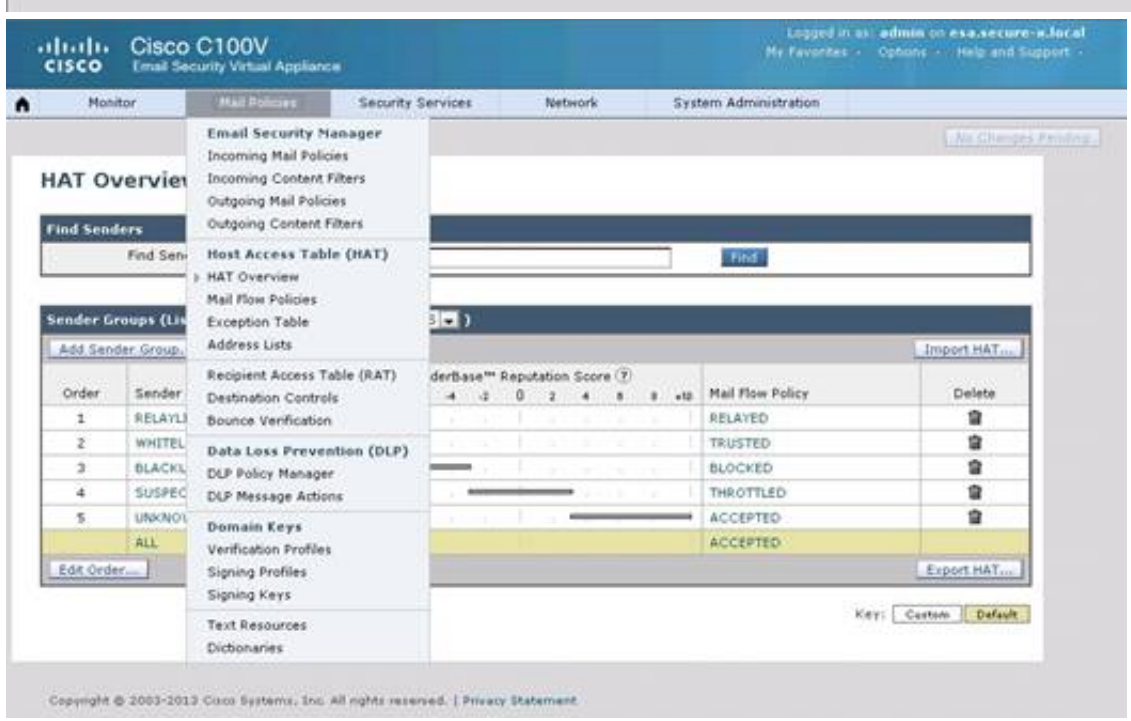
Answer: B

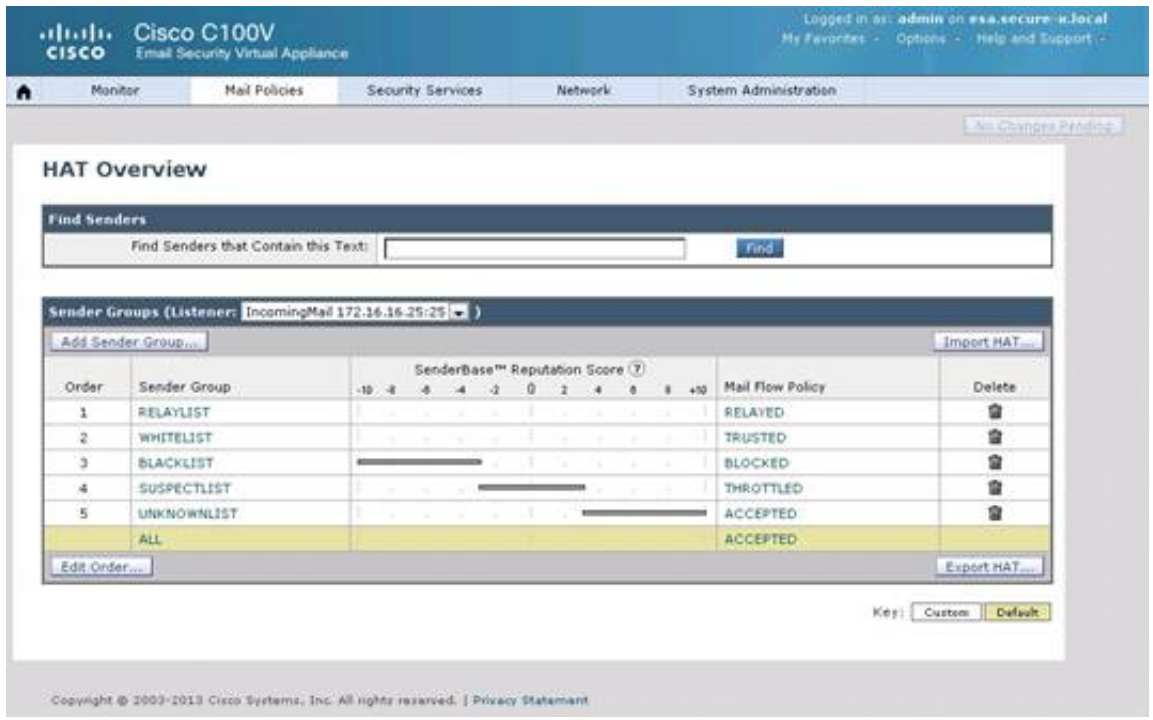
NEW QUESTION 507

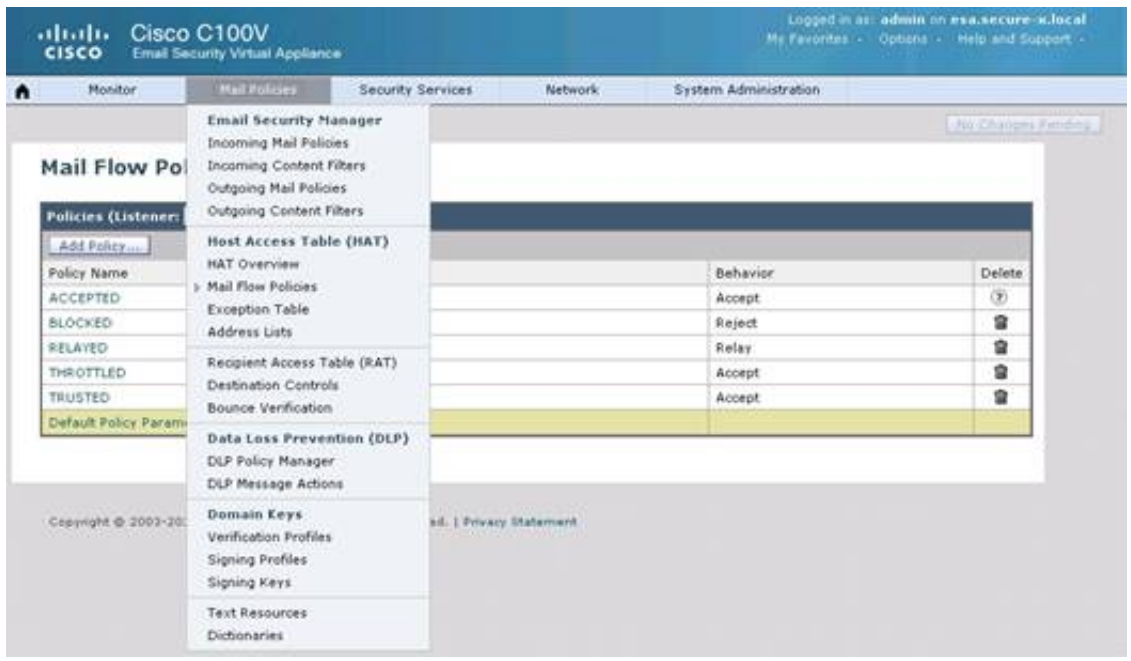


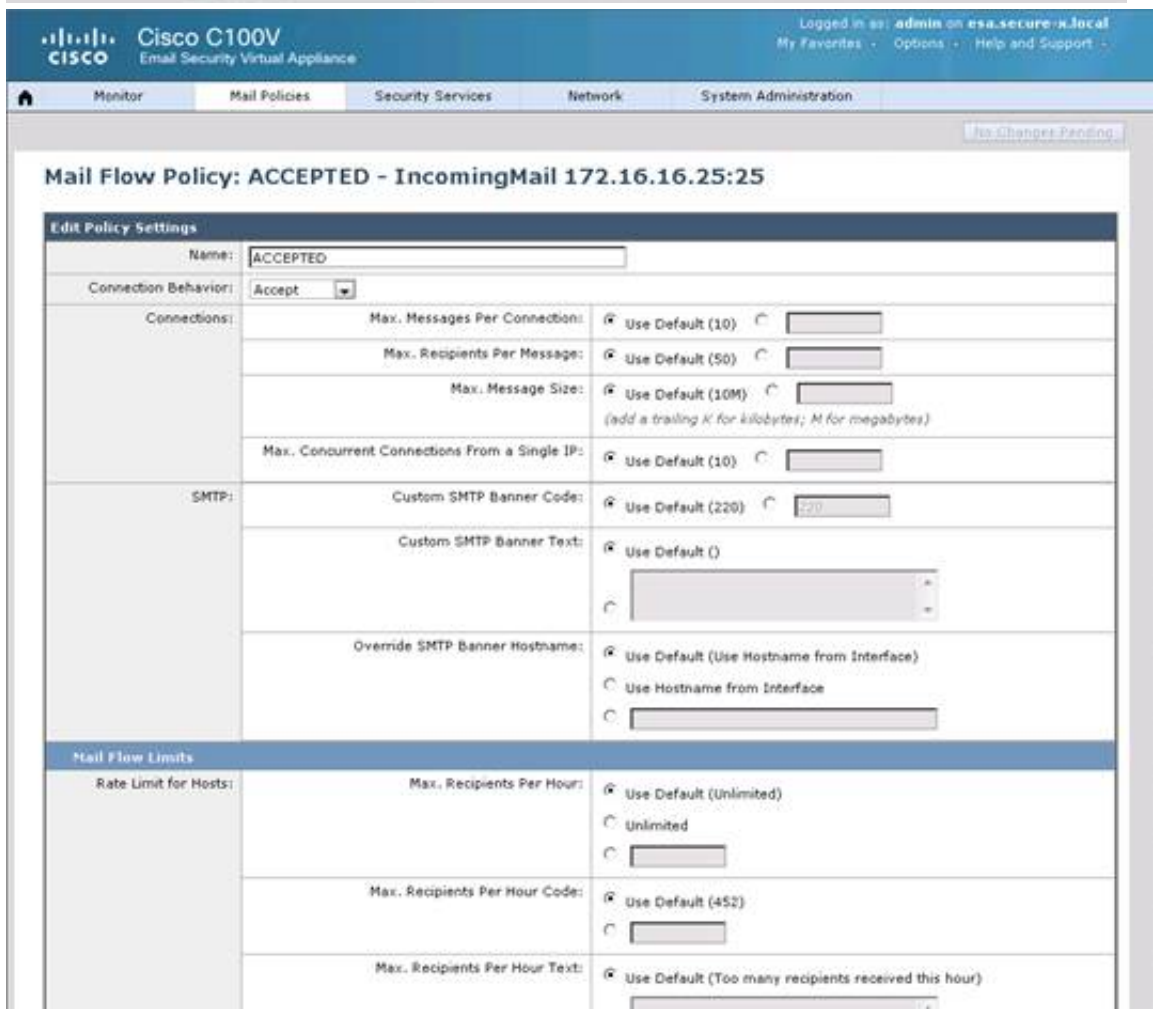






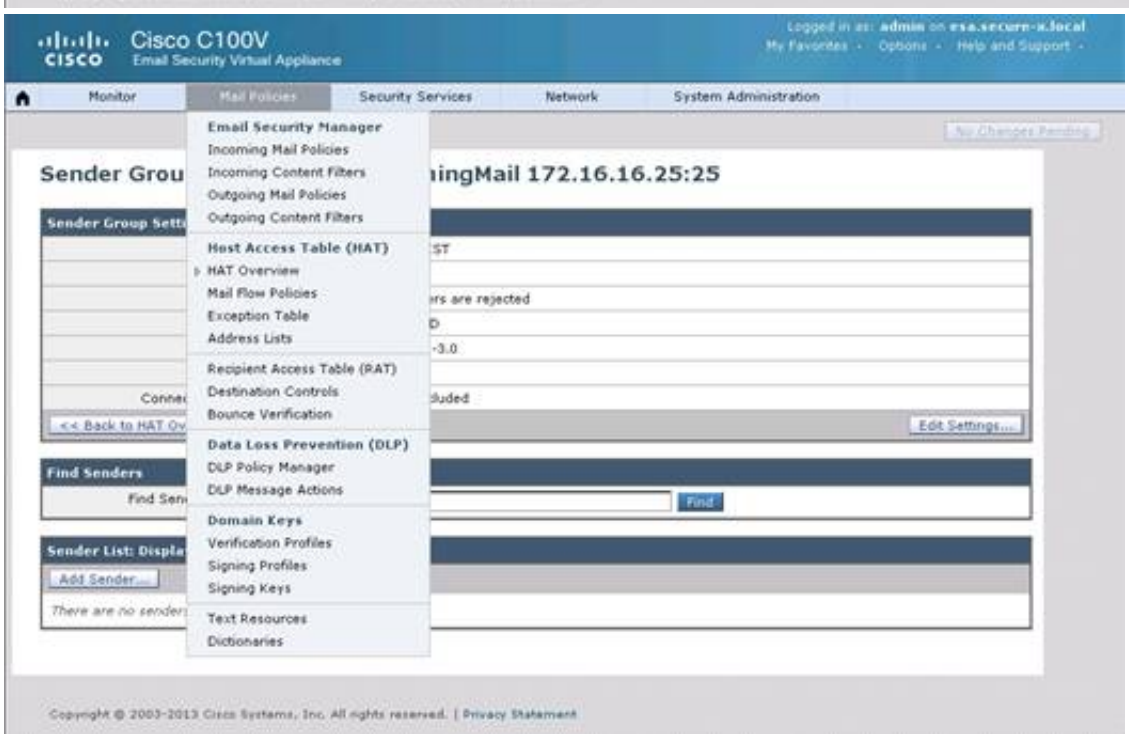

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
HAT Overview
Find Senders
Find Senders that Contain this Text:
Find
Sender Groups (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

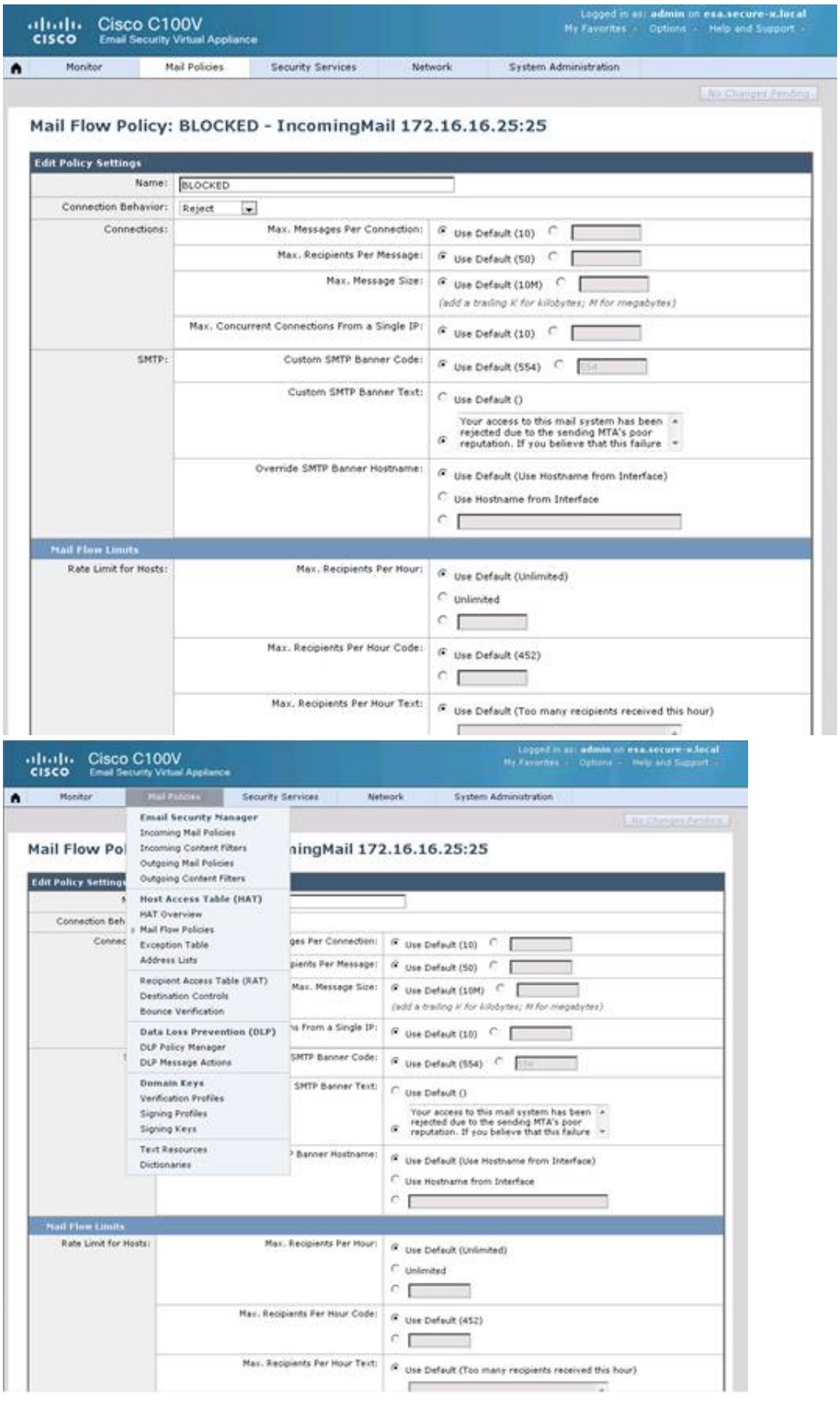

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail 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 Po
Policies (Listener:
Add Policy...
Policy Name
Behavior
Delete
ACCEPTED Accept
BLOCKED Reject
RELAYED Relay
THROTTLED Accept
TRUSTED Accept
Default Policy Param
Copyright © 2003-20
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)

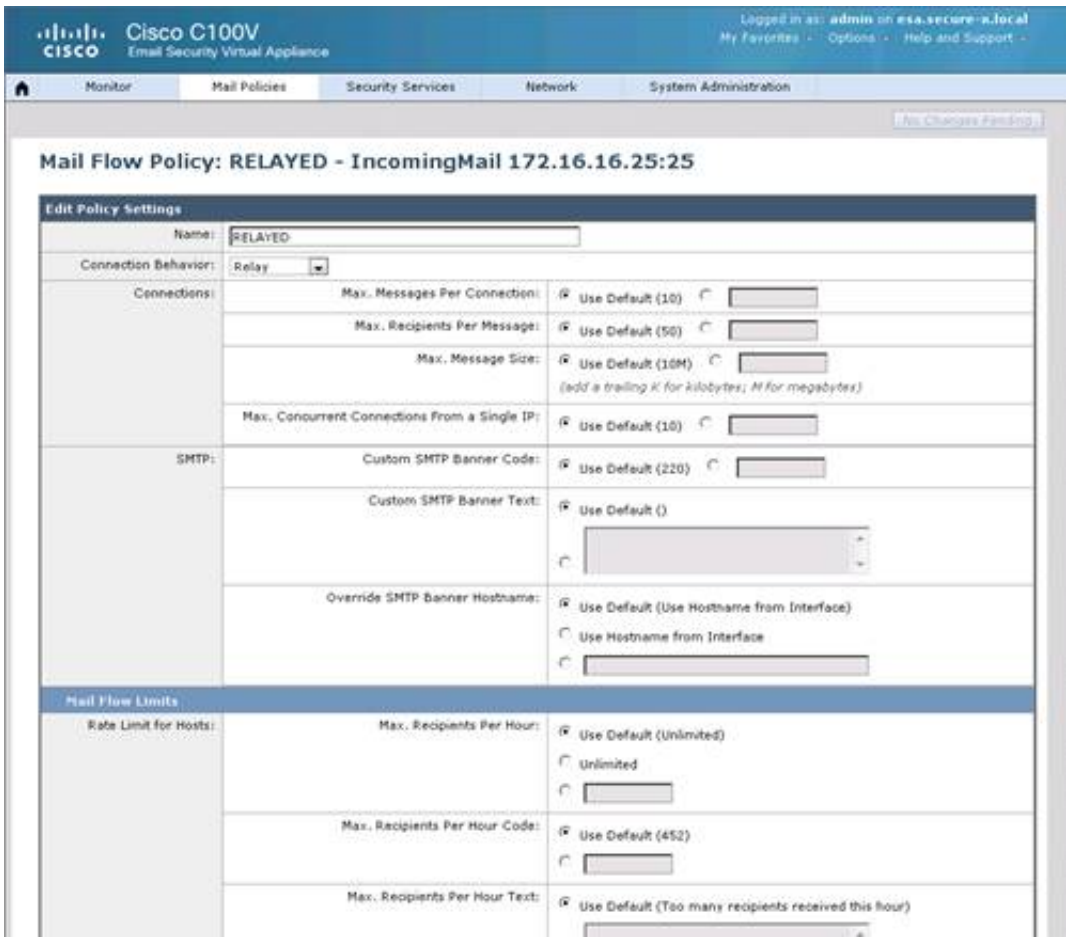

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing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

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

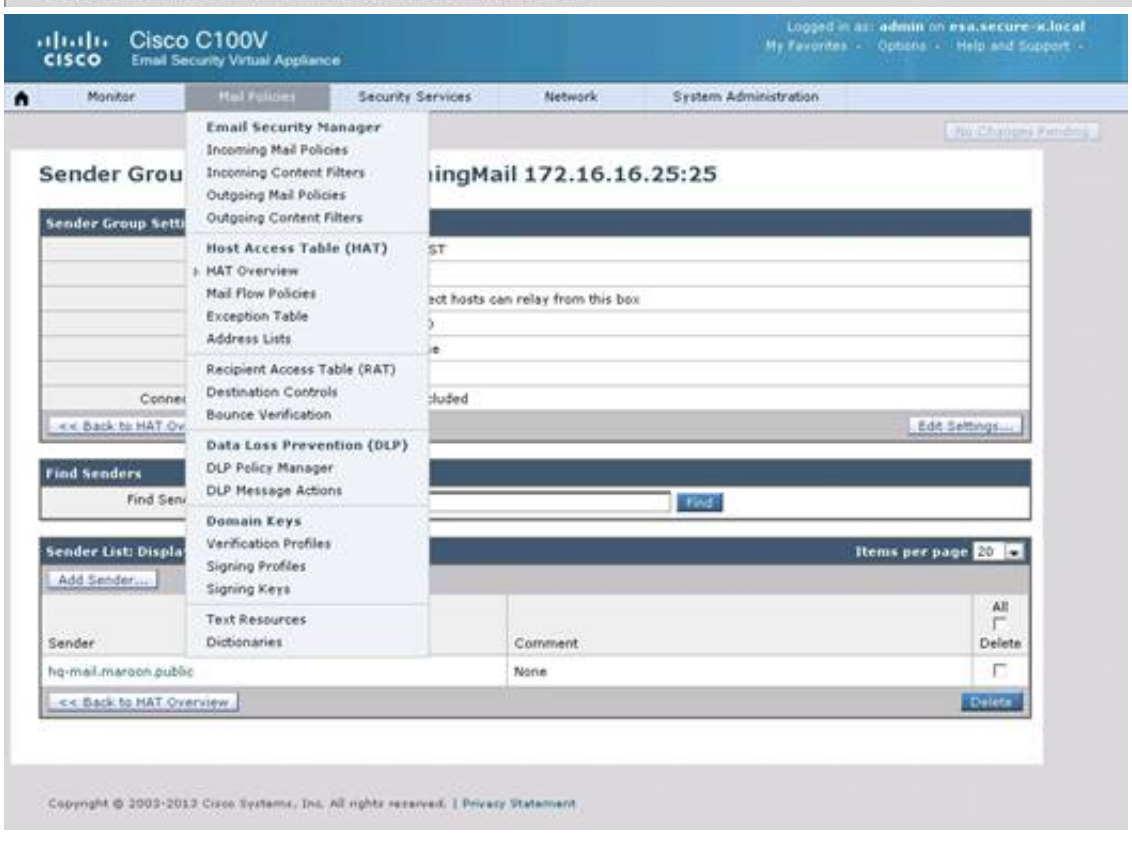

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: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

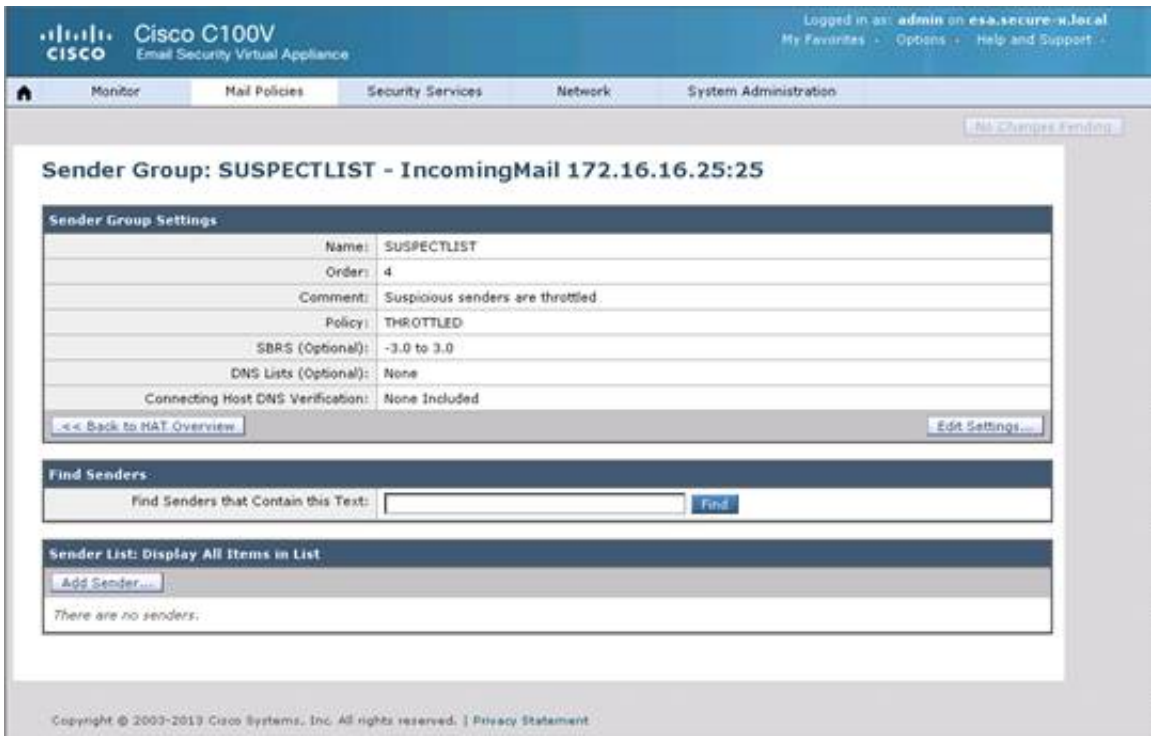
Cisco C100V
Email Security Virtual Appliance
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing Content Filters
Host Access Table (HAT)
HAT Overview
Mail Flow Policies
Exception Table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

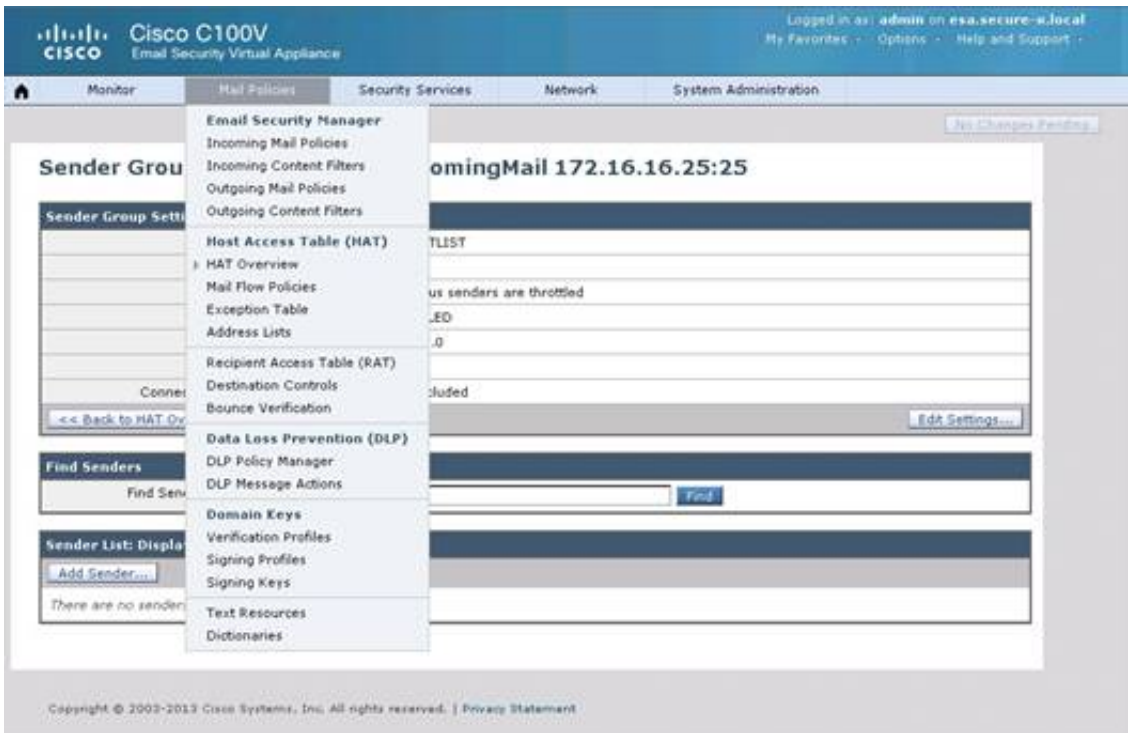

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: RELAYED
Connection 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)

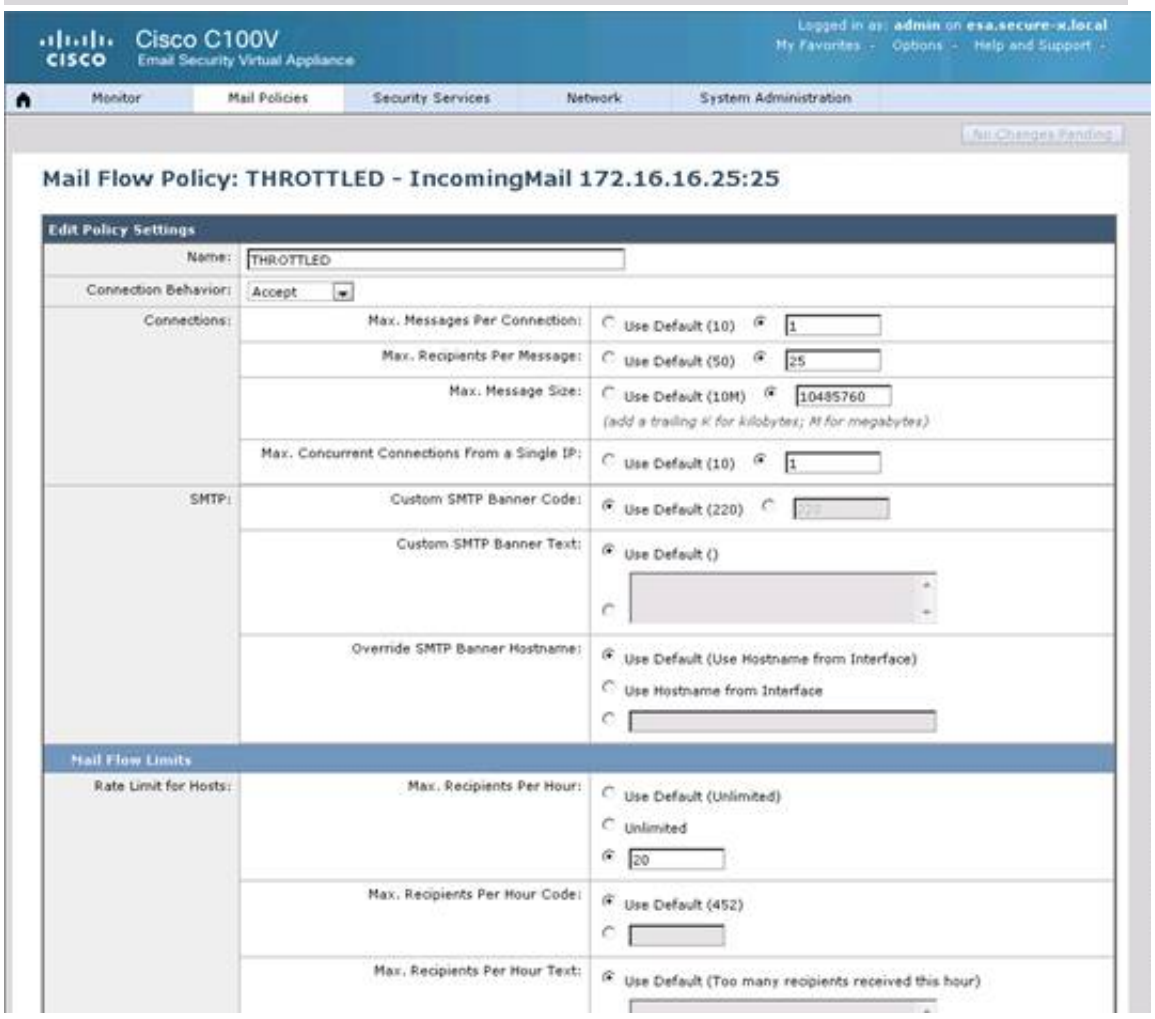

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing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

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

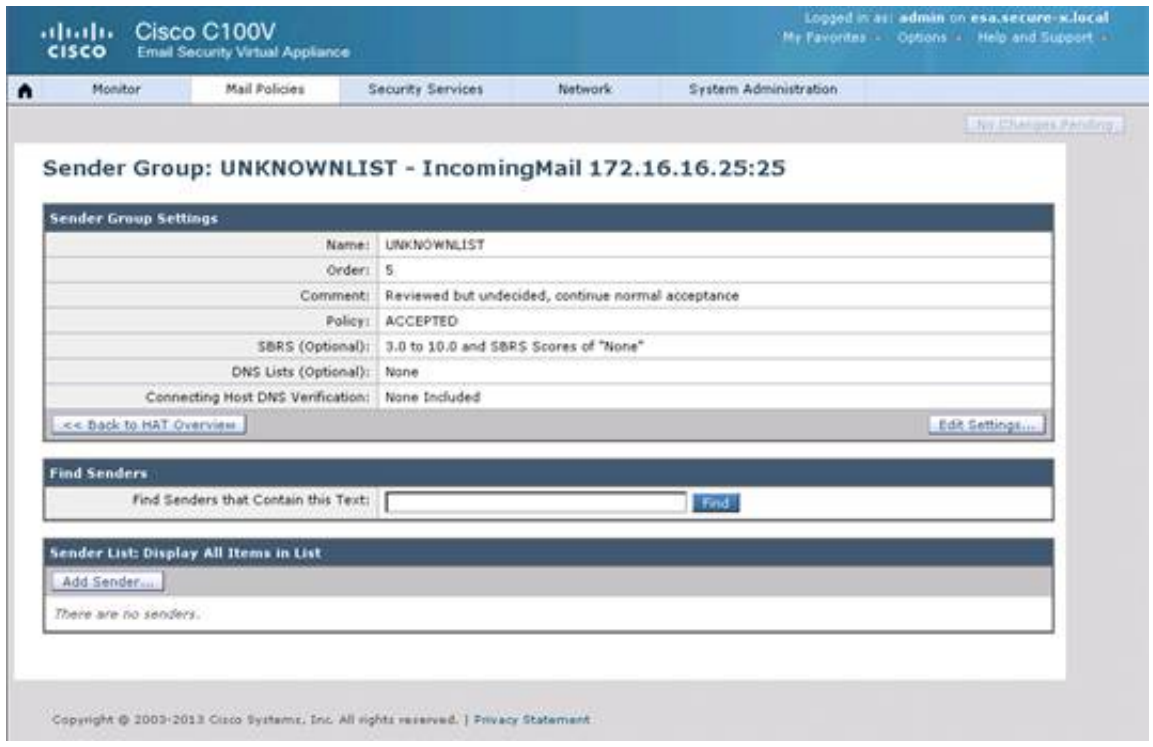

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing 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
Sender Grou
ingMail 172.16.16.25:25
Sender Group Setti
ST
ect hosts can relay from this box
cluded
Edit Settings...
Find Senders
Find
Sender List: Displa
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

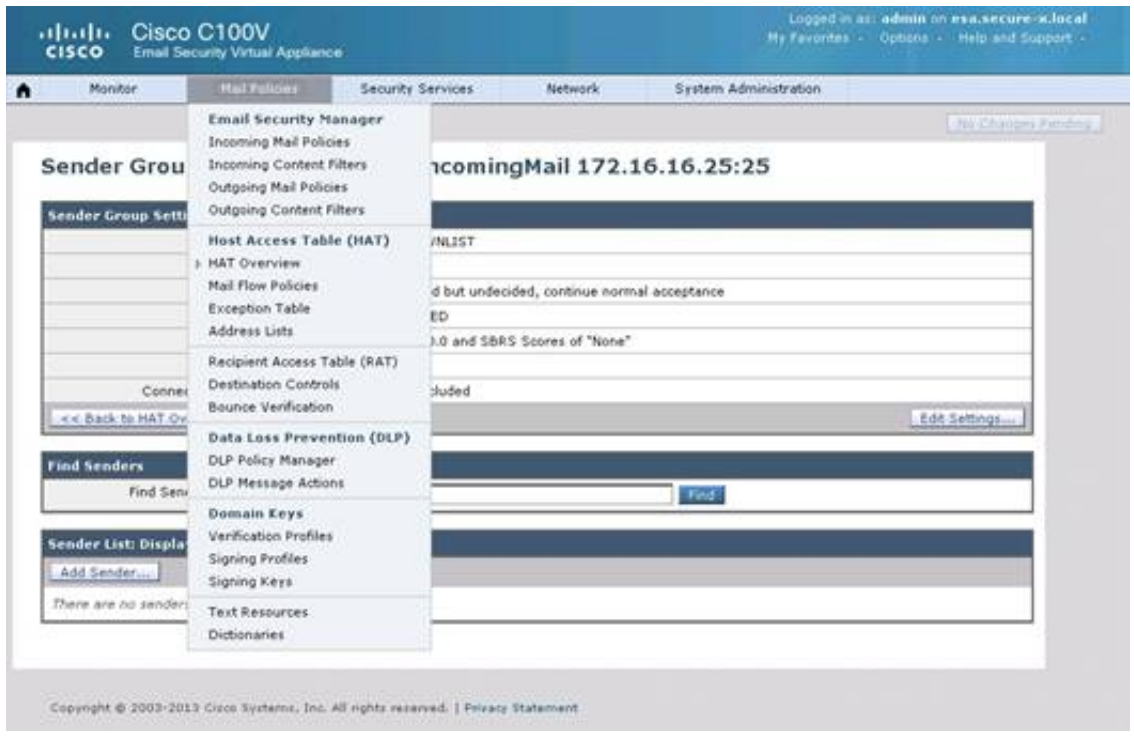

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Sender Group: SUSPECTLIST - IncomingMail 172.16.16.25:25
Sender Group Settings
Name: SUSPECTLIST
Order: 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

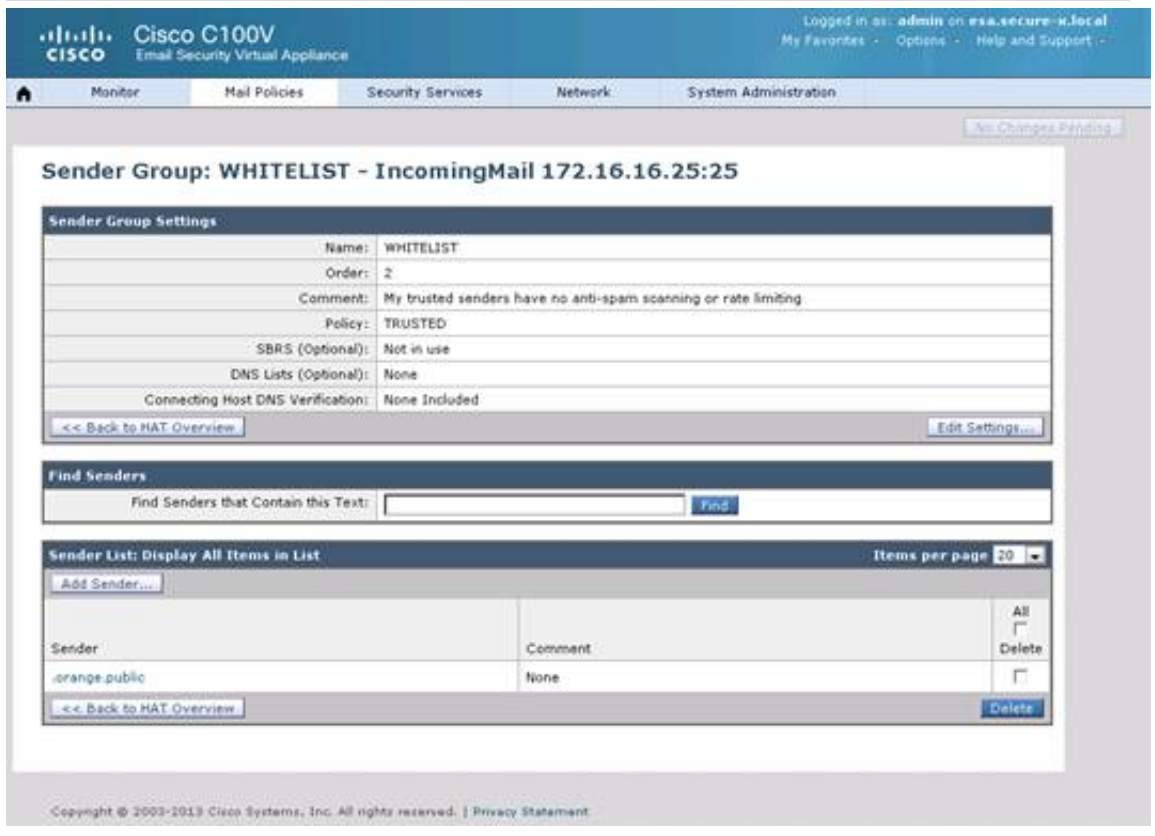

Cisco C100V
Email Security Virtual Appliance
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing Content Filters
Host Access Table (HAT)
HAT Overview
Mail Flow Policies
Exception Table
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
Edit Settings...
Find
Add Sender...
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

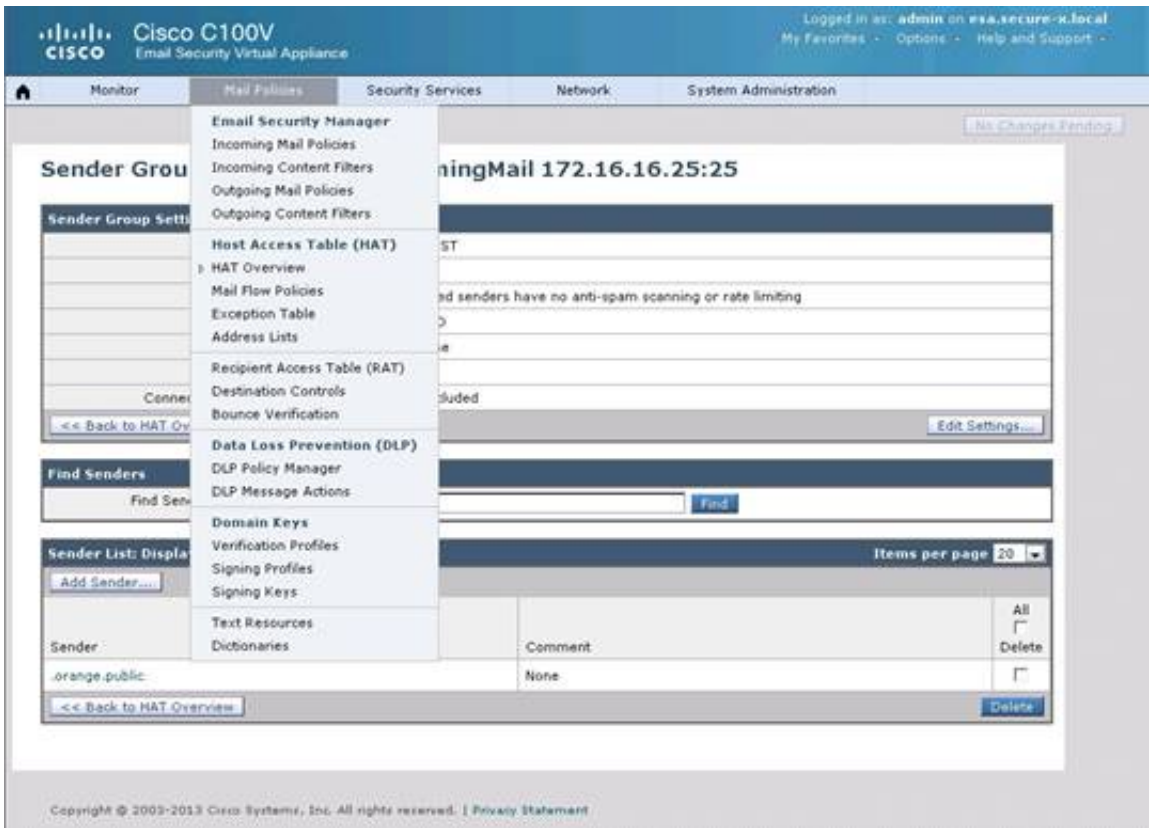

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Mail Flow Policy: THROTTLED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: THROTTLED
Connection 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
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

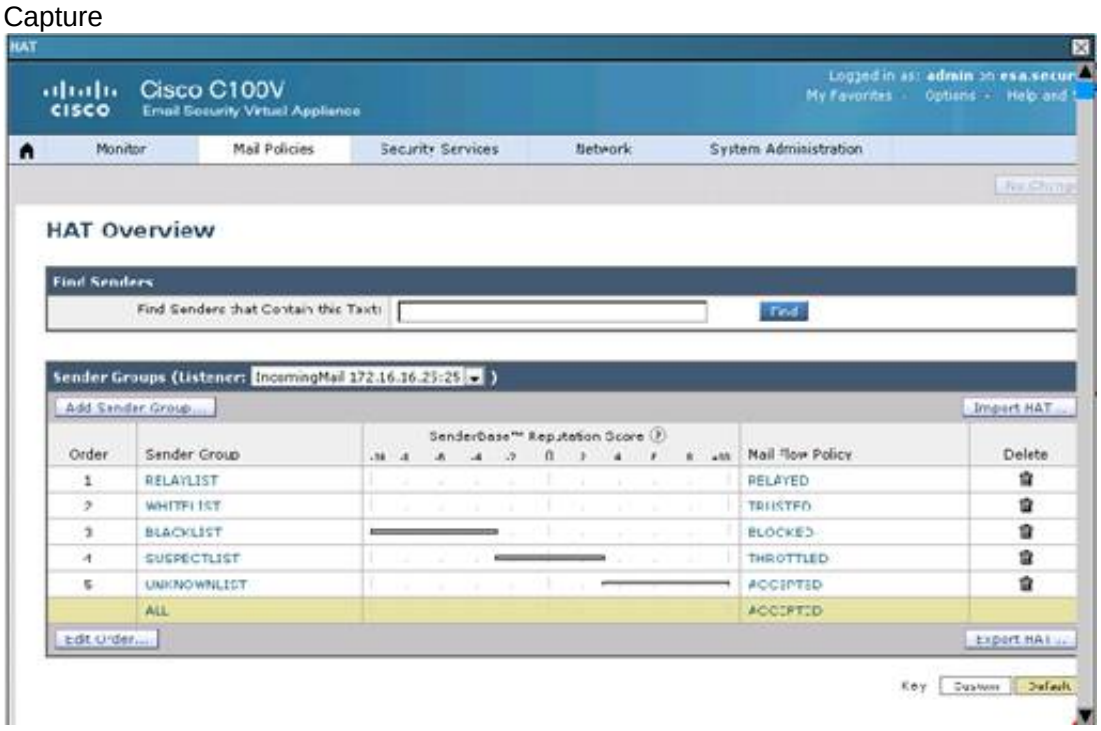


What is the maximum message size that the Cisco Email Security Appliance will accept from the violet.public domain?

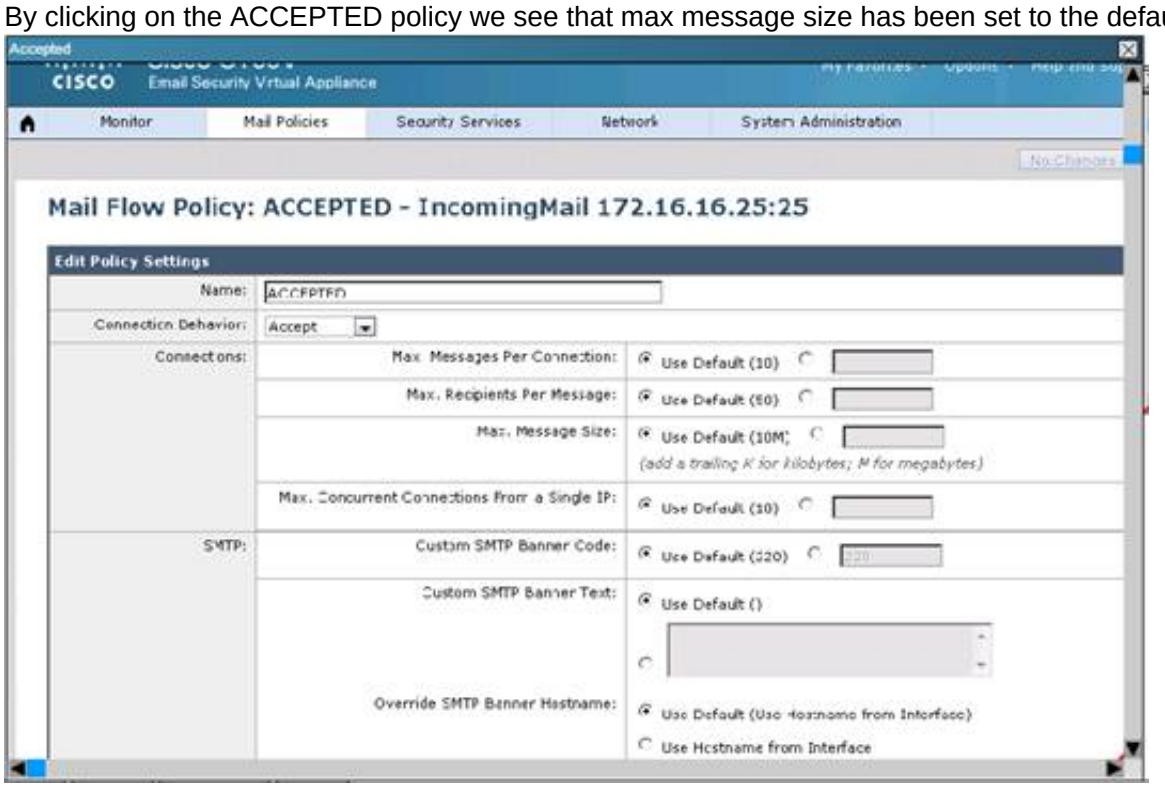
A. 1 KB
B. 100 KB
C. 1 MB
D. 10 MB
E. 100 MB
F. Unlimited

Answer: D

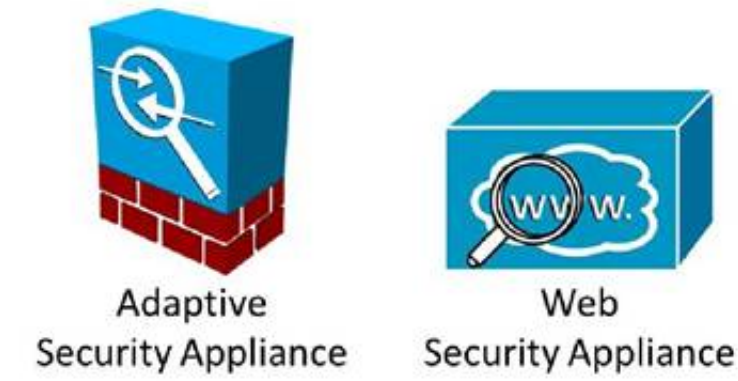
Explanation: From the instructions we know that the reputation score for the violet.public domain has been set to 8. From the HAT table shown below we know that a score of 8 belongs to the UNKNOWNLIST group, which is assigned the ACCEPTED policy.
Capture

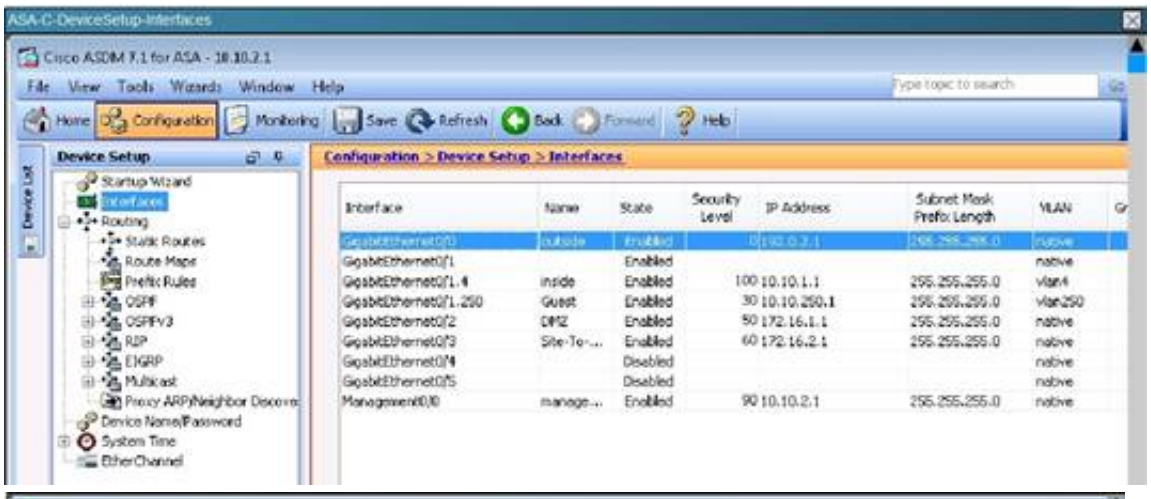


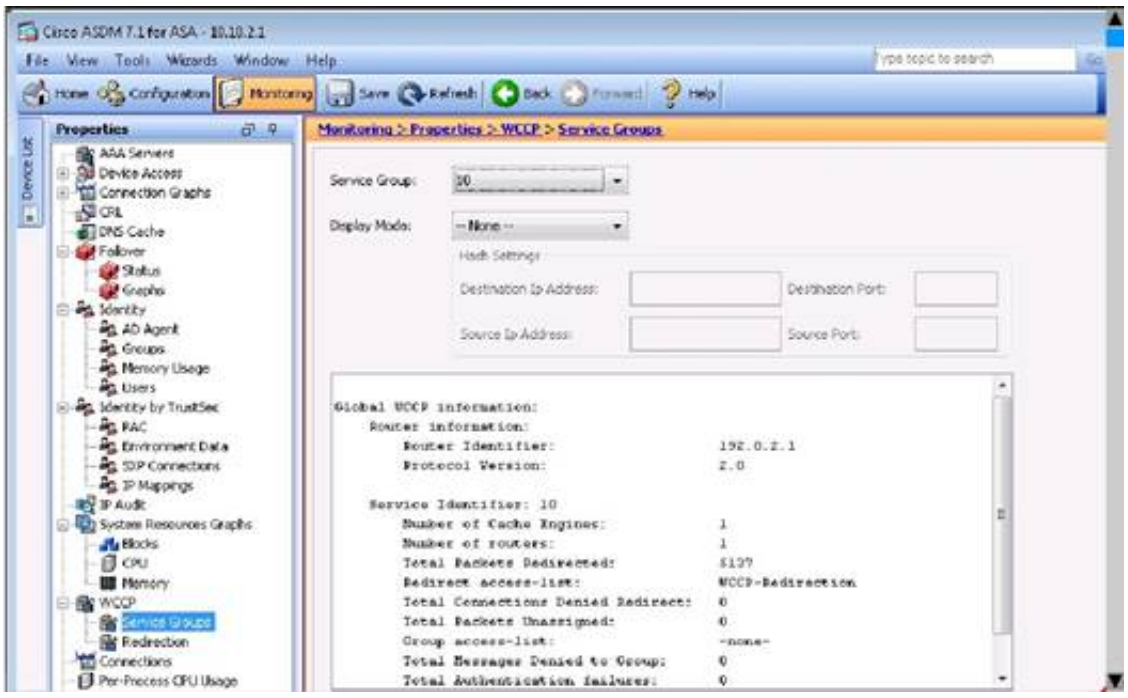
By clicking on the ACCEPTED policy we see that max message size has been set to the default value of 10M: Capture

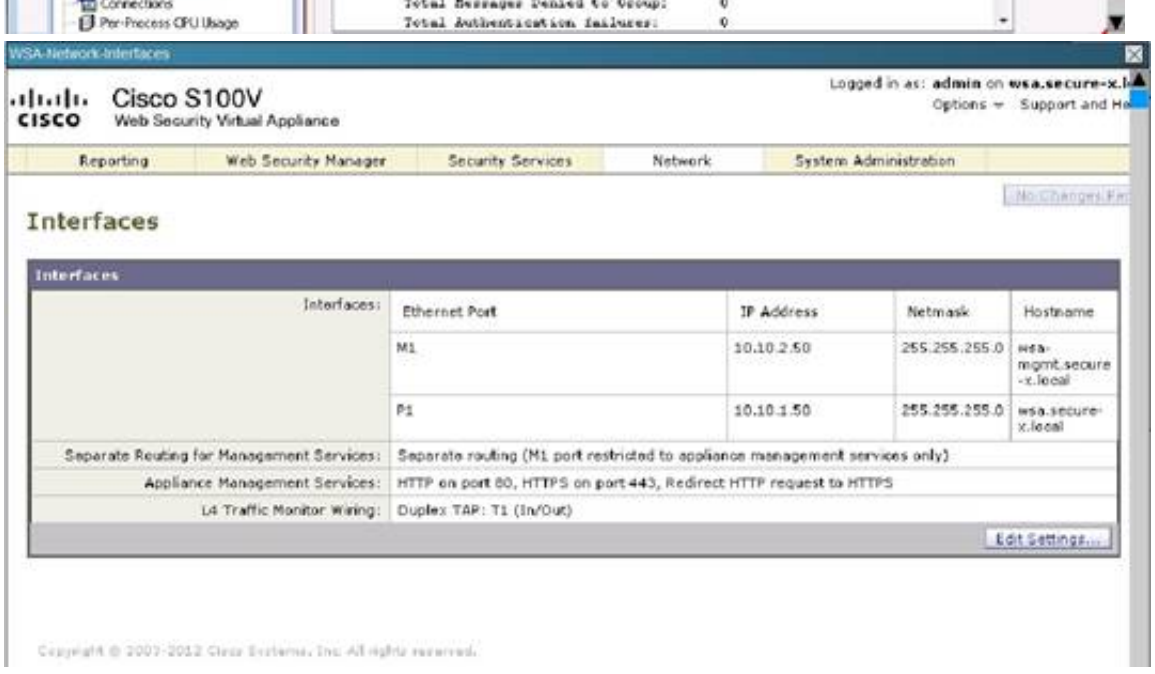


NEW QUESTION 509
The Web Cache Communication Protocol (WCCP) is a content-routing protocol that can facilitate the redirection of traffic flows in real time. Your organization has deployed WCCP to redirect web traffic that traverses their Cisco Adaptive Security Appliances (ASAs) to their Cisco Web Security 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.







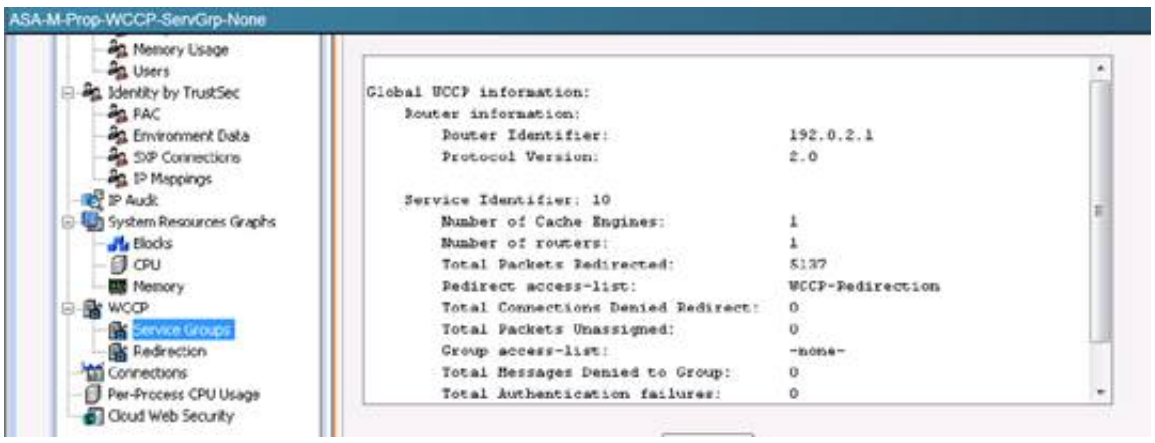


Which of the following is true with respect to the version of WCCP configured on the Cisco ASA and the Cisco WSA?

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 514
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 515
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 520
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 521
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 523
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 526
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 529
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 532
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. viewer
B. service
C. operator
D. administrator

Answer: C

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

NEW QUESTION 533
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 534
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.

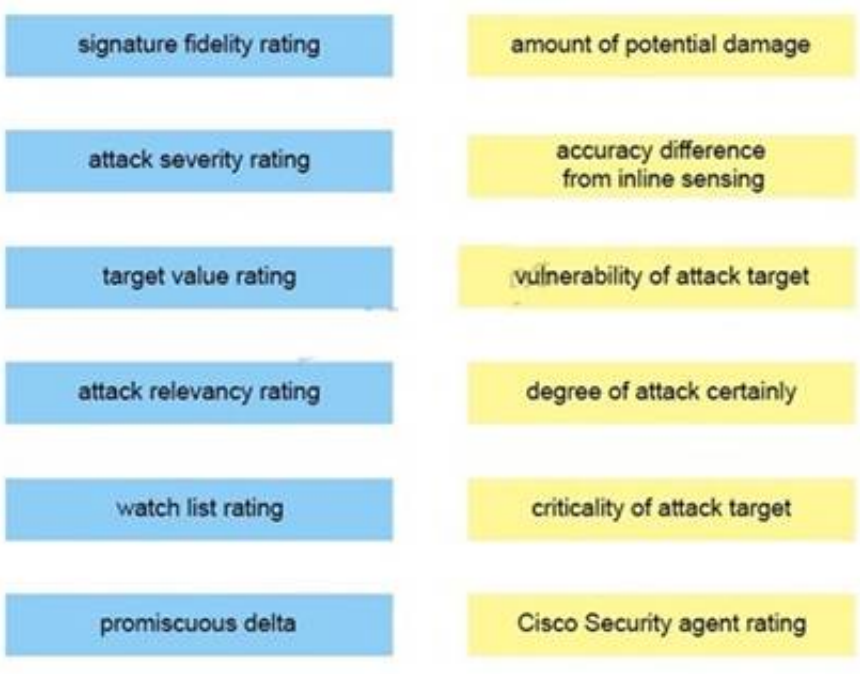
Answer: D

NEW QUESTION 539
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 542
Drag and drop the terms on the left onto the correct definition for the promiscuous IPS risk rating calculation on the right.



Answer:

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

NEW QUESTION 543
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 545
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 550
Refer to the following. What type of password is “cisco”? Router(config)#service password-encryption Router(config)#username admin password cisco

A. Enhanced
B. CHAP
C. Type 7
D. Type 0

Answer: C

NEW QUESTION 552
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 557
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 559
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 564
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.

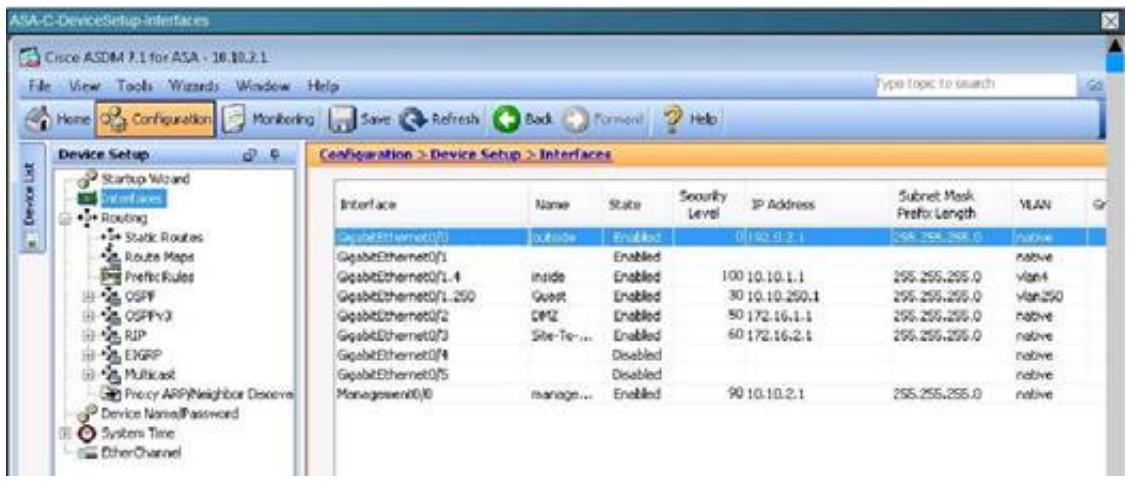
Answer: B

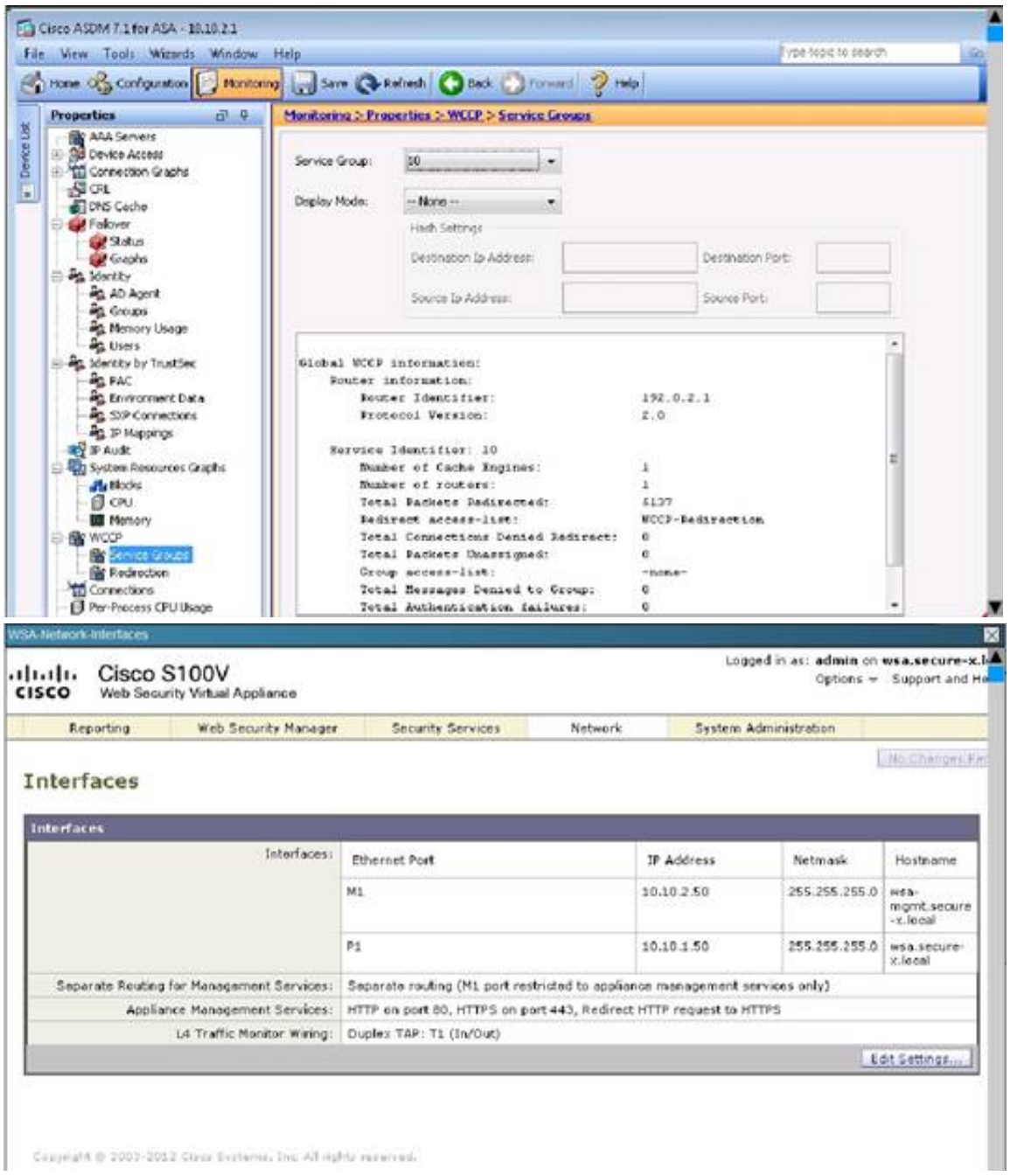
NEW QUESTION 569
Which option represents the cisco event aggregation product?

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

Answer: C

NEW QUESTION 572
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.



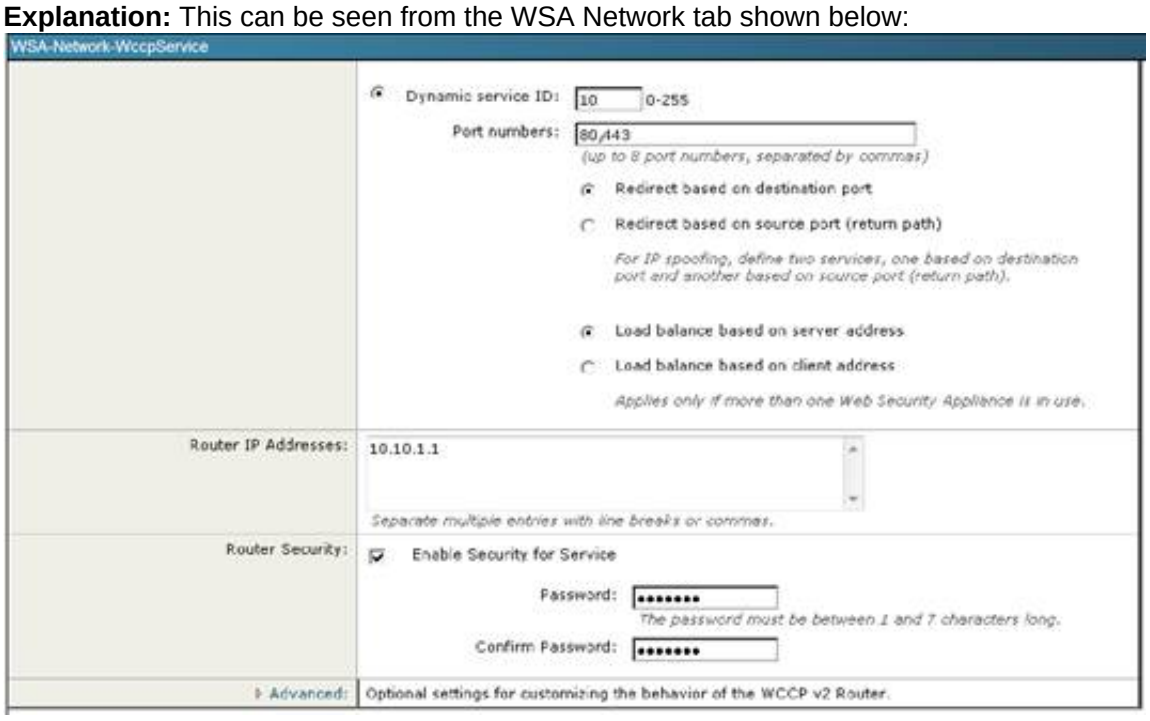


Between the Cisco ASA configuration and the Cisco WSA configuration, what is true with respect to redirected ports?

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

Answer: C

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



NEW QUESTION 574
Which command disables SSH access for administrators on the Cisco ESA?

A. interfaceconfig
B. sshconfig
C. sslconfig
D. systemsetup

Answer: A

NEW QUESTION 576
Which three administrator actions are used to configure IP logging in Cisco IME? (Choose three.)

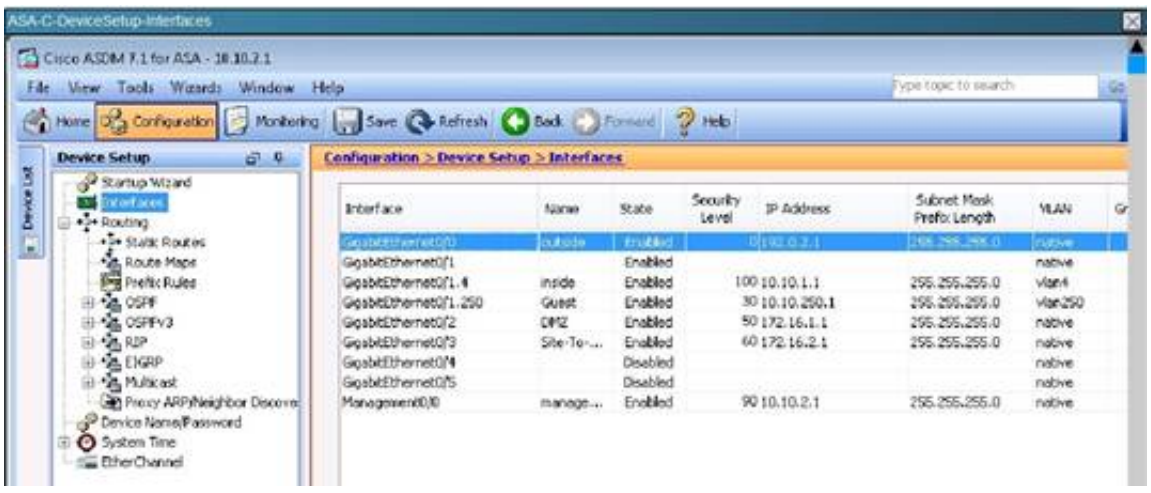
A. Select a virtual sensor.
B. Enable IP logging.
C. Specify the host IP address.
D. Set the logging duration.
E. Set the number of packets to capture.
F. Set the number of bytes to capture.

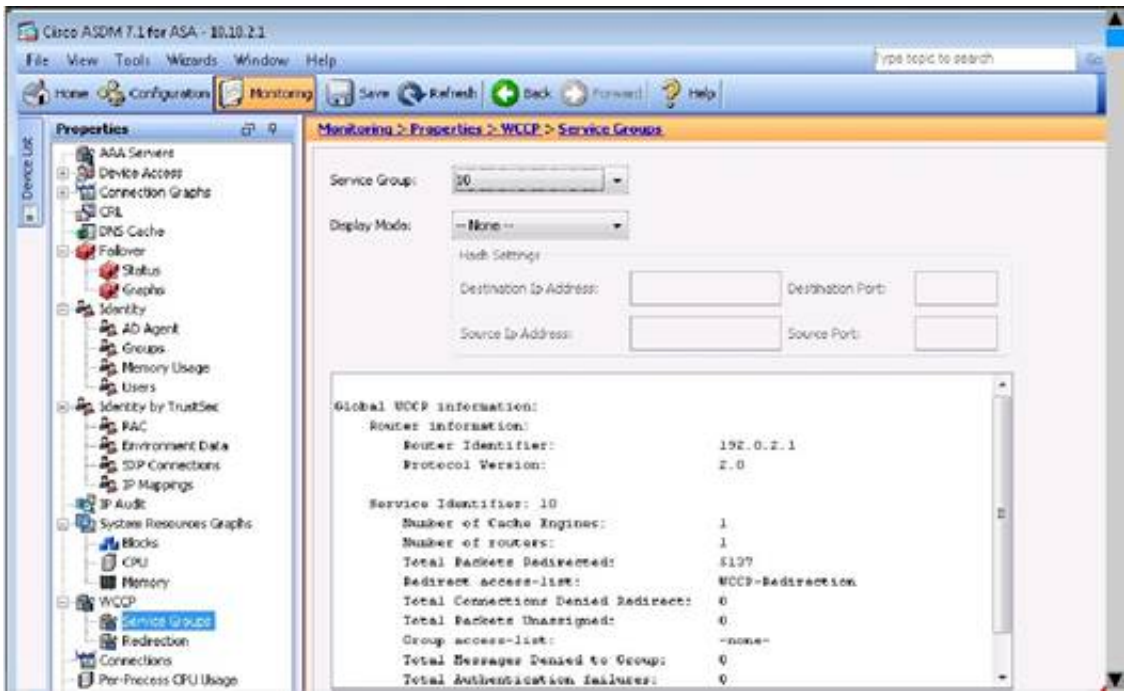
Answer: ACD

NEW QUESTION 577
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 580
Which statement about the default configuration of an IPS sensor's management security settings is true?

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

Answer: A

NEW QUESTION 584
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 587
Which commands are required to configure SSH on router? (Choose two.)

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

Answer: AB

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

NEW QUESTION 590
Which command can change the HTTPS SSL method on the Cisco ESA?

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

Answer: A

NEW QUESTION 595
When you create a new server profile on the Cisco ESA, which subcommand of the ldapconfig command configures spam quarantine end-user authentication?

A. isqauth
B. isqalias
C. test
D. server

Answer: A

NEW QUESTION 598
Using the Cisco WSA GUI, where should an operator navigate to determine the running software image on the Cisco WSA?

A. Systems Administration > System Upgrade
B. Systems Administration > Feature Keys
C. Systems Administration > General
D. Admin > System Info

Answer: A

NEW QUESTION 602
Which Cisco ESA predefined sender group uses parameter-matching to reject senders?

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

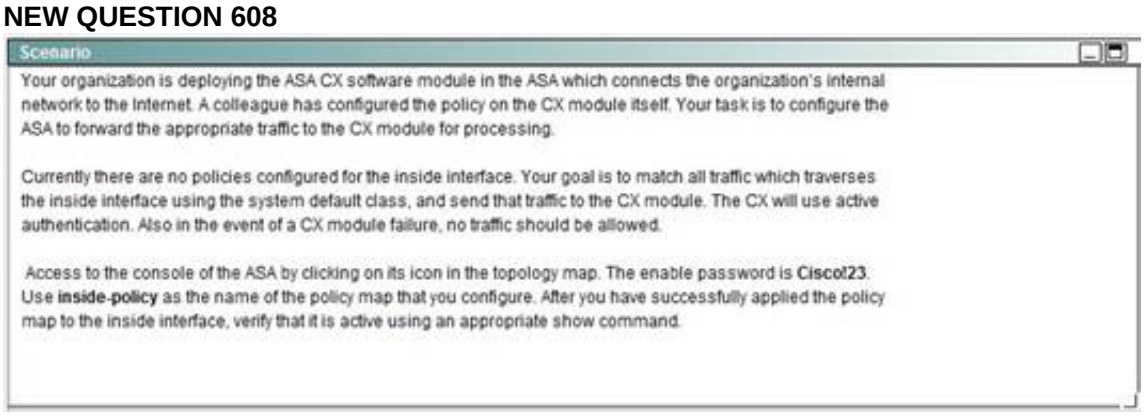
Answer: A

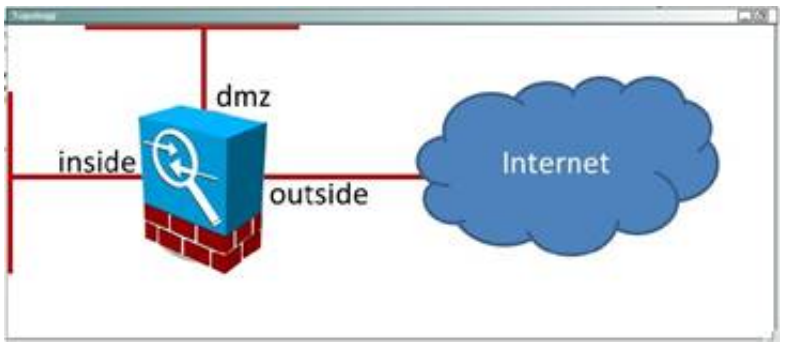
NEW QUESTION 604
Which option is a benefit of deploying Cisco Application Visibility and Control?

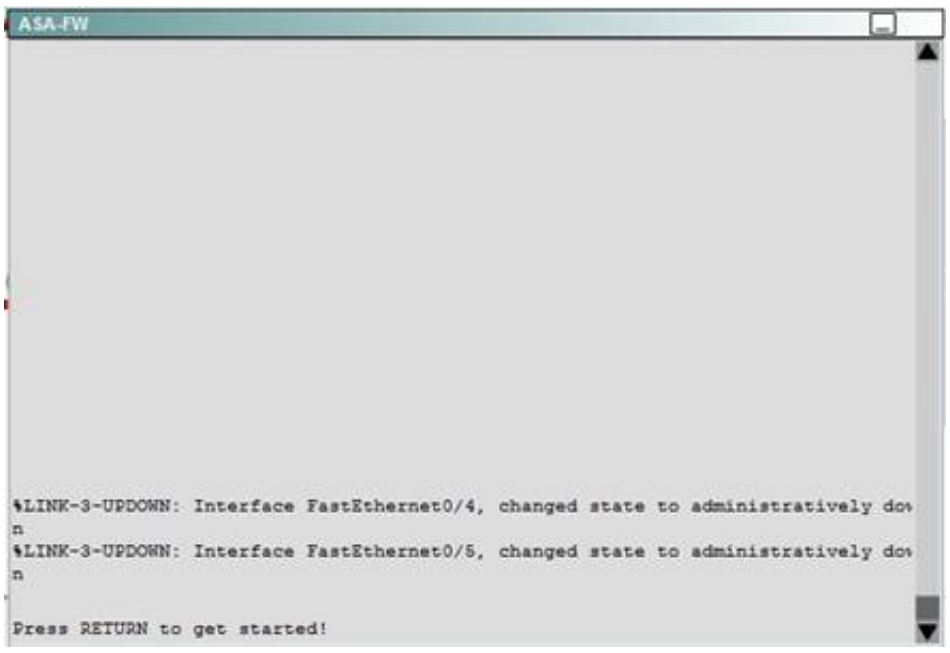
A. It ensures bandwidth availability and performance of mission-critical applications in a data- and media-rich environment.
B. It performs deep packet inspection of mission-critical applications in a data- and media-rich environment.
C. It encrypts mission-critical applications in a data- and media-rich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

Answer: A

NEW QUESTION 608







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:
Reference:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/modules_cx.pdf

NEW QUESTION 613
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 618
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 622
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 625
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 630
Which platform has message tracking enabled by default?

A. C670
B. C370
C. Virtual ESA
D. It is not enabled by default on any platform.

Answer: D

NEW QUESTION 634
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 637
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 640
r01(config)#ip wccp web-cache redirect-list 80 password local
Refer to the above. What can be determined from this router configuration command for Cisco WSA?

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

Answer: D

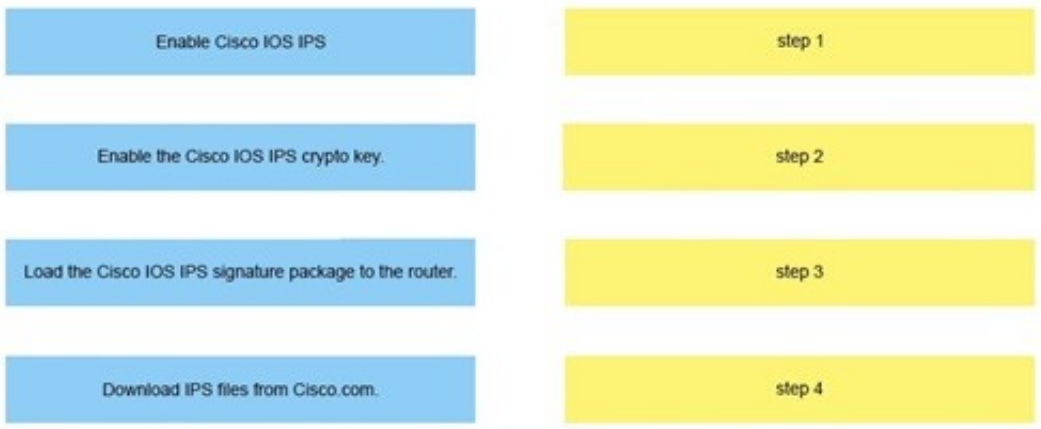
NEW QUESTION 645
Which option is a benefit of Cisco hybrid email security?

A. on-premises control of outbound data
B. advanced malware protection
C. email encryption
D. message tracking

Answer: A

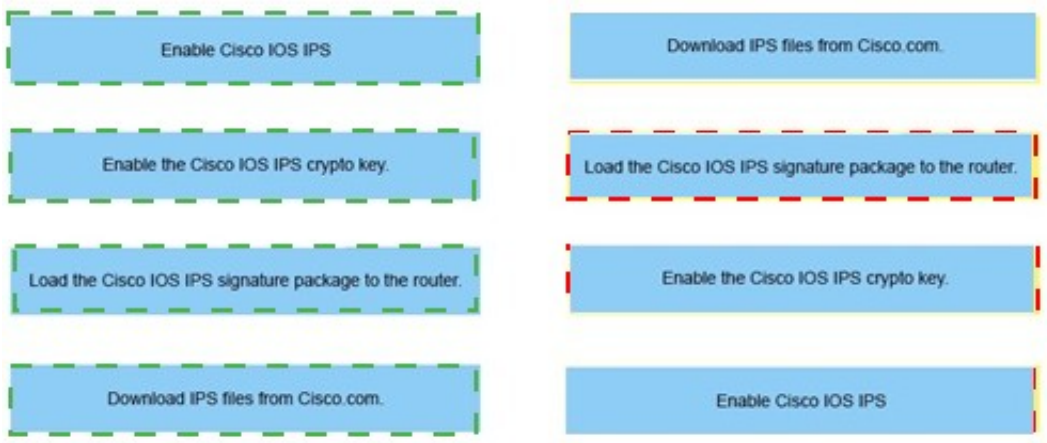
NEW QUESTION 646

Drag and drop the steps on the left into the correct order of initial Cisco IOS IPS configuration on the right.

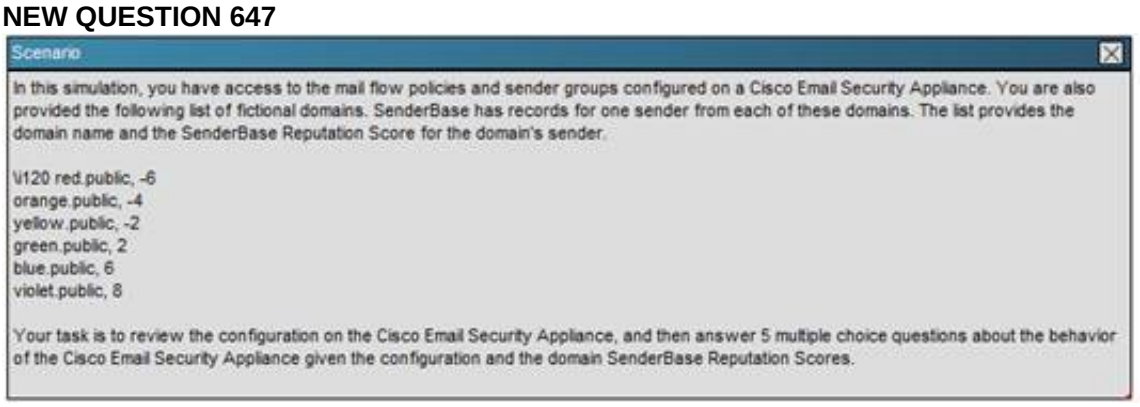


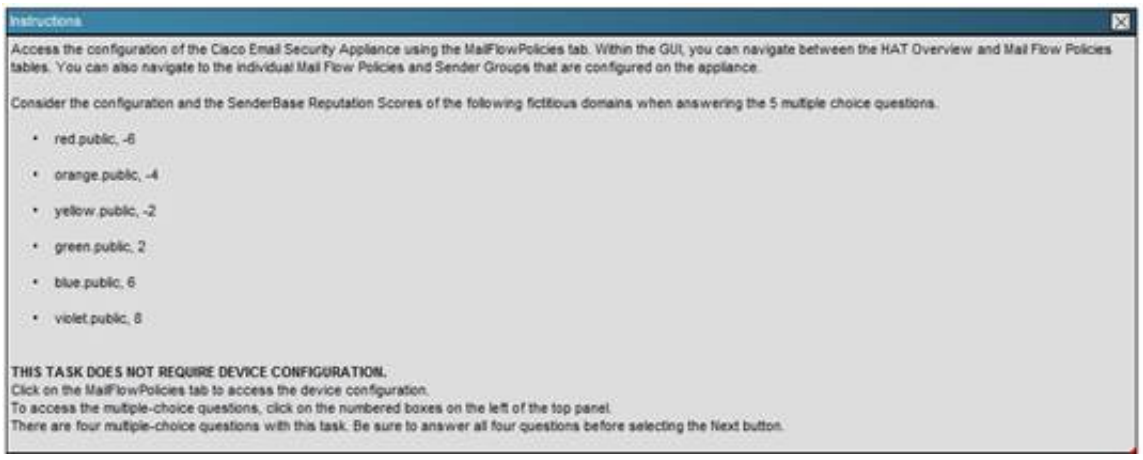
Answer:

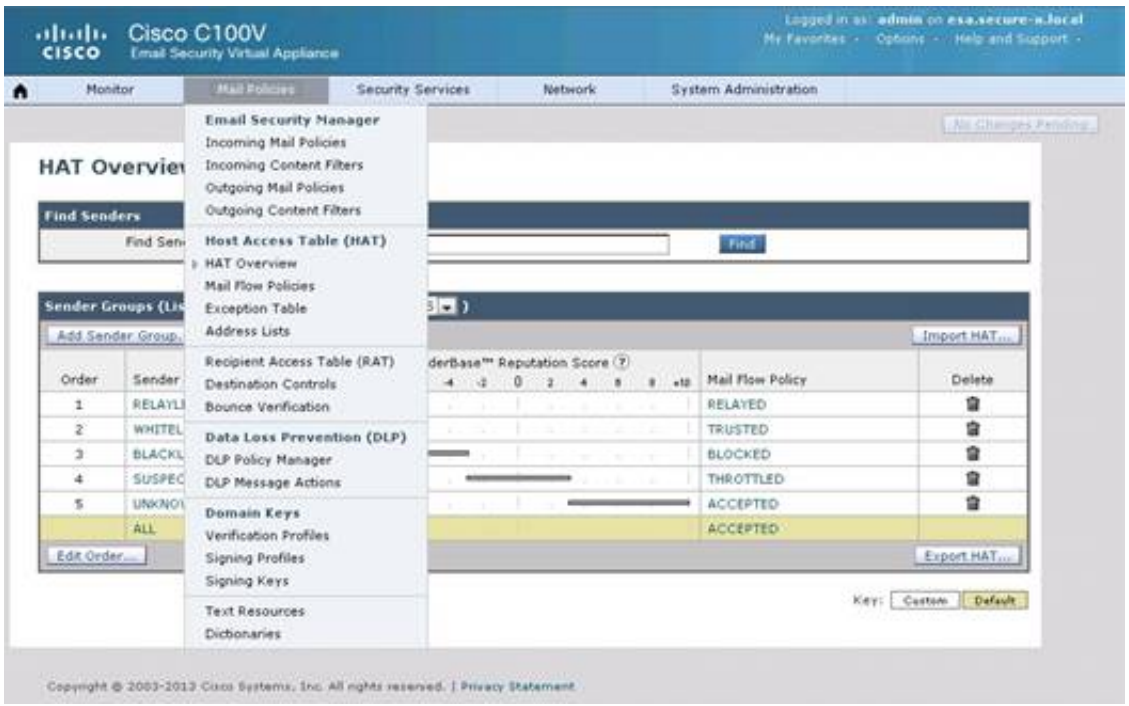
Explanation:

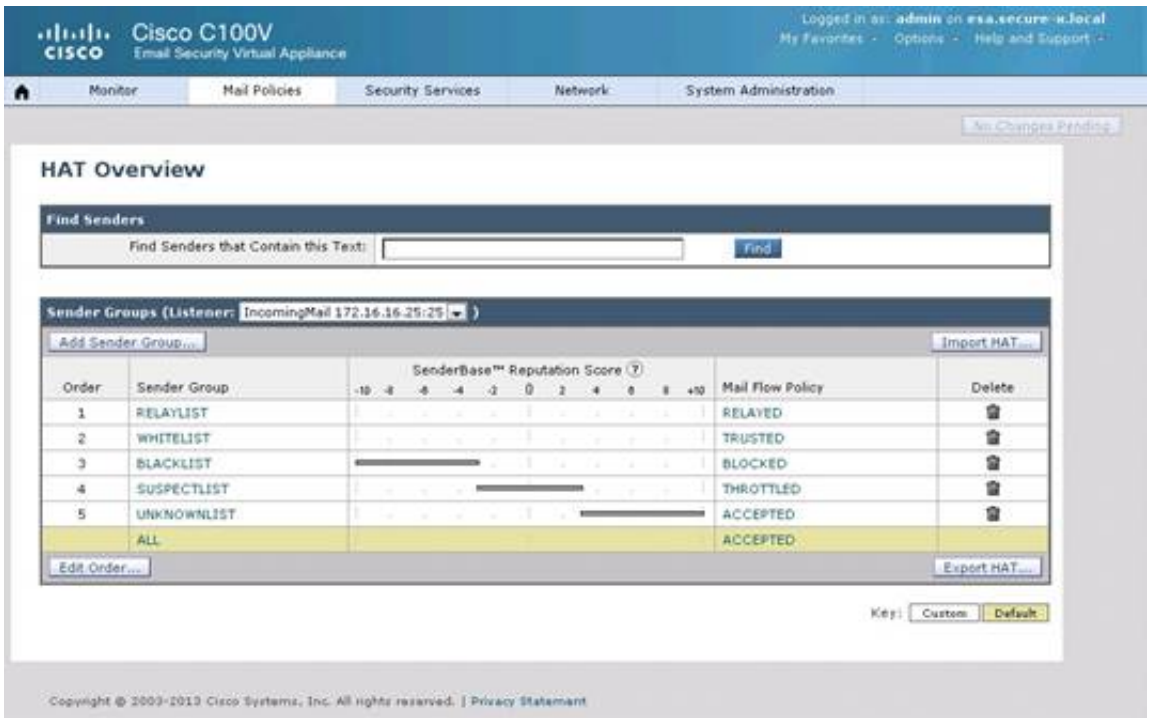


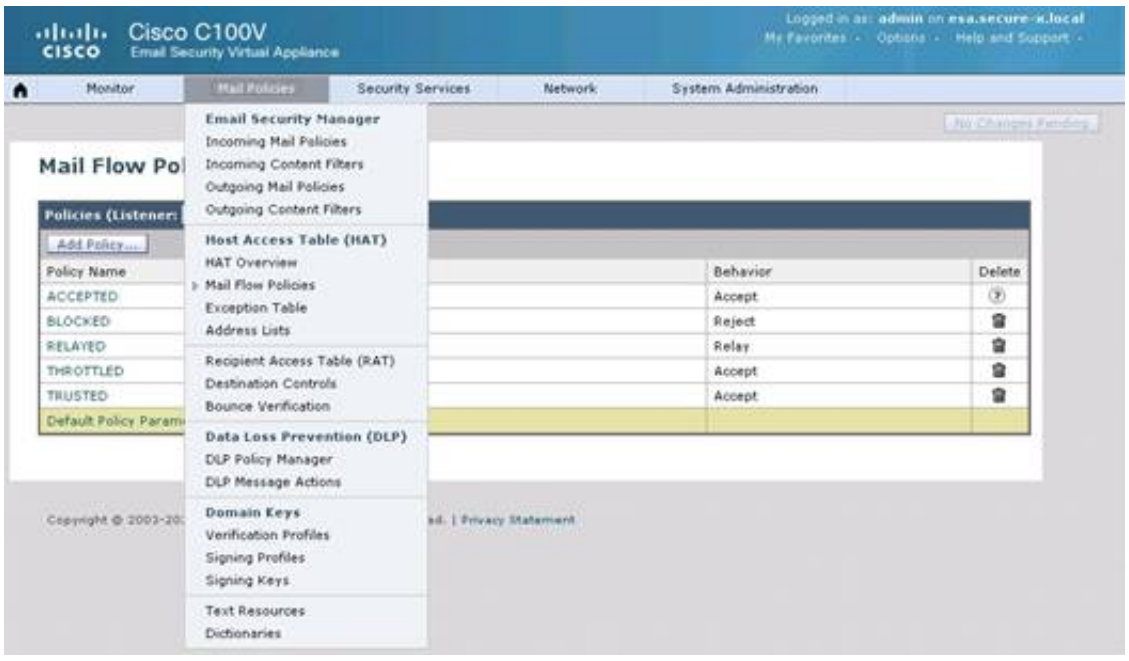
NEW QUESTION 647

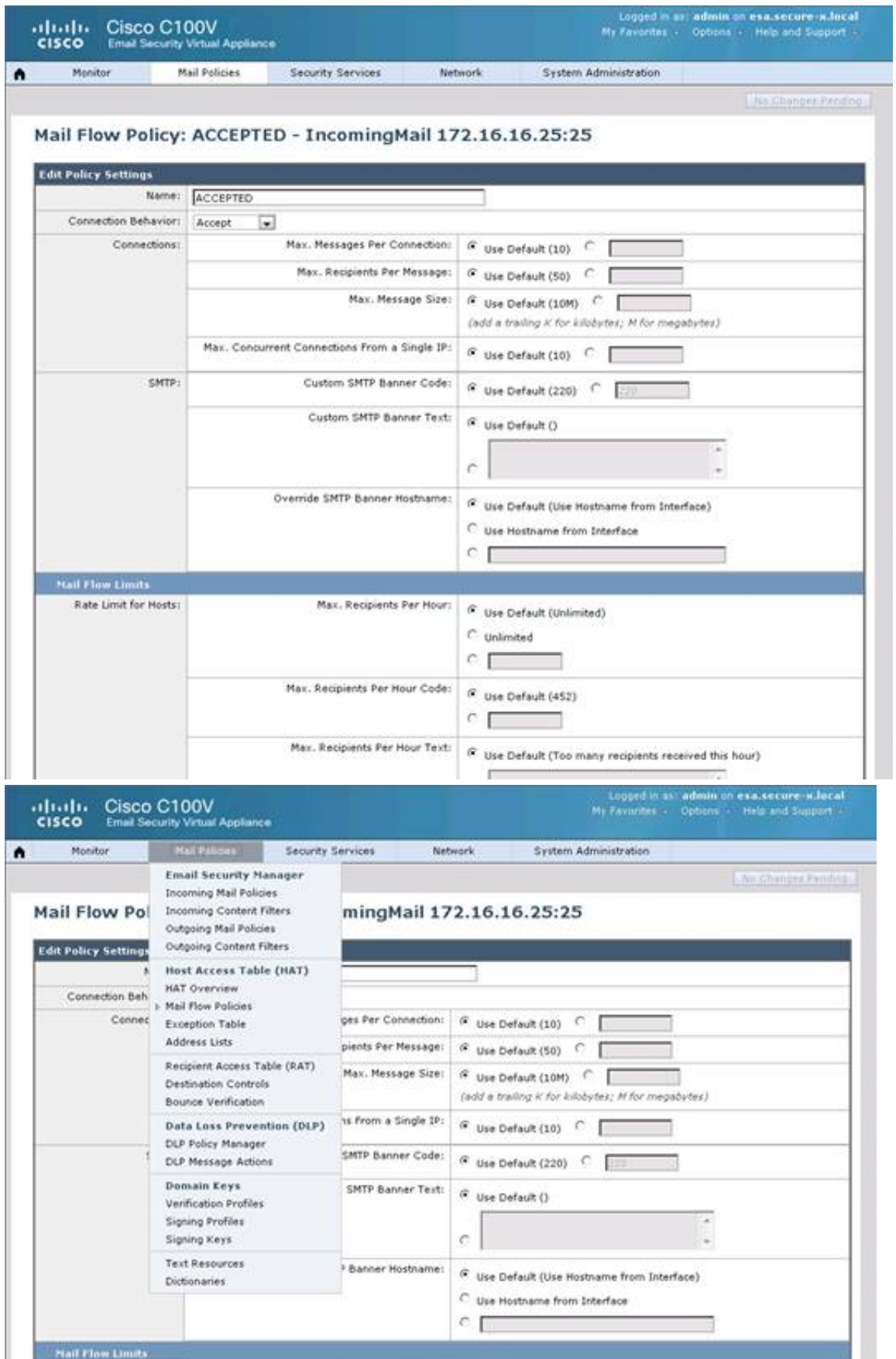





Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing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

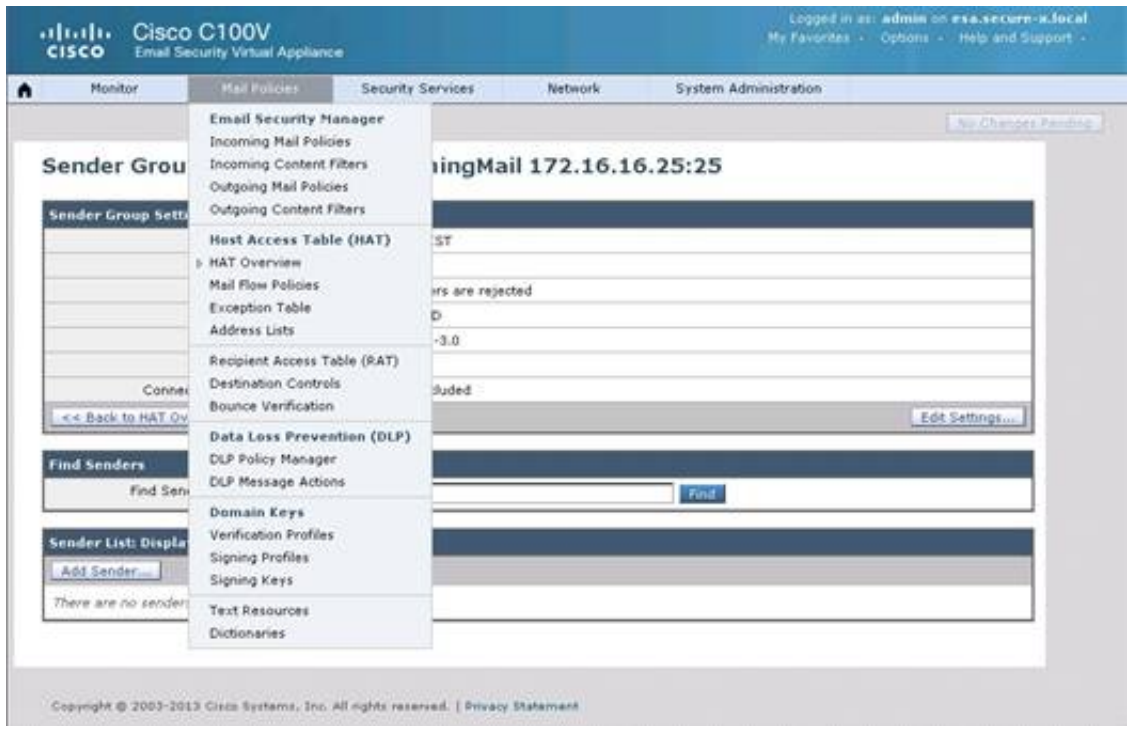

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
HAT Overview
Find Senders
Find Senders that Contain this Text:
Find
Sender Groups (Listener: IncomingMail 172.16.16.25:25)
Add Sender Group...
Import HAT...
Export HAT...
Edit Order...
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
Key: Custom Default
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

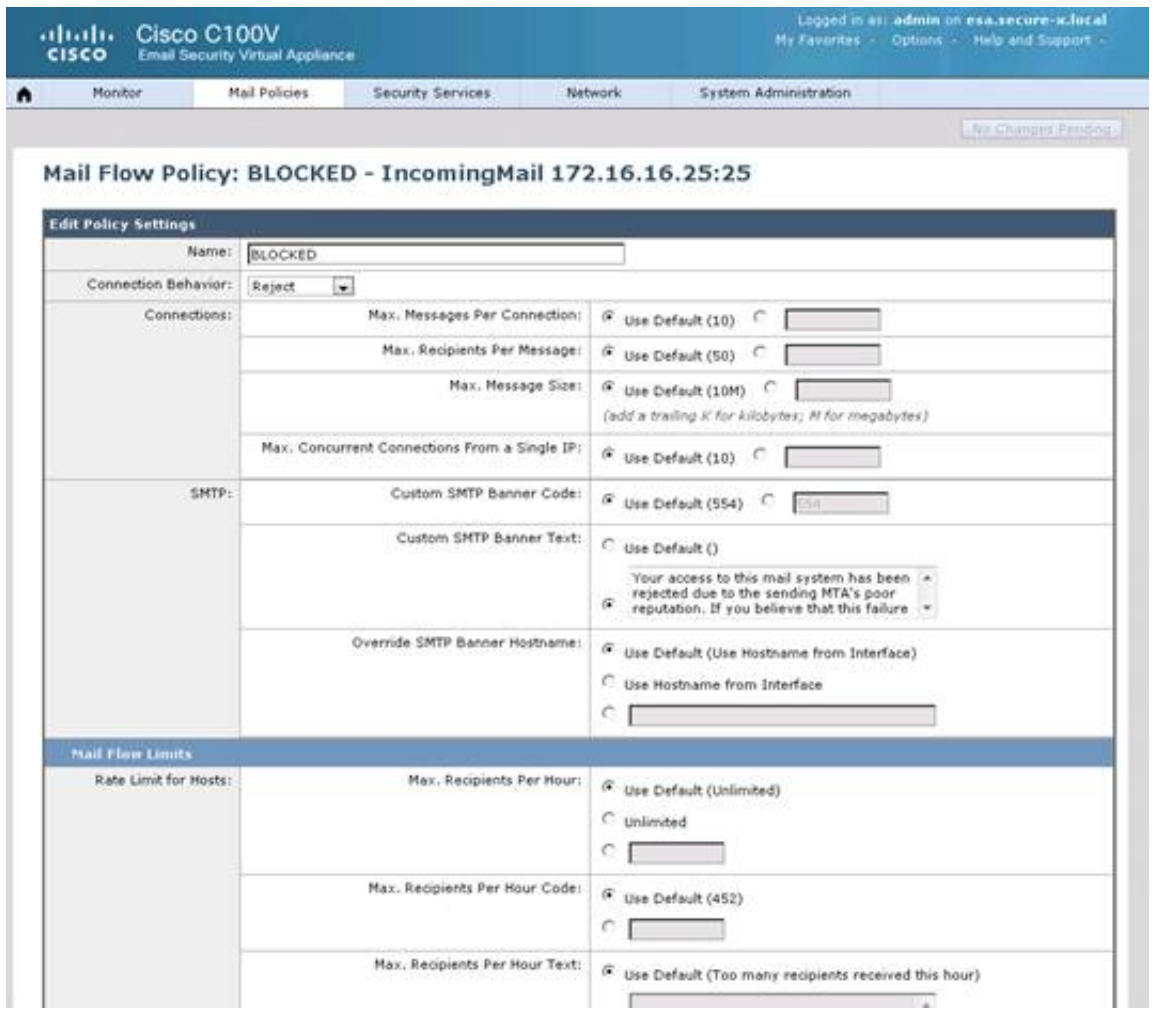

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing 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
Policies (Listener:
Add Policy...
Policy Name
Behavior
Delete
ACCEPTED Accept
BLOCKED Reject
RELAYED Relay
THROTTLED Accept
TRUSTED Accept
Default Policy Param

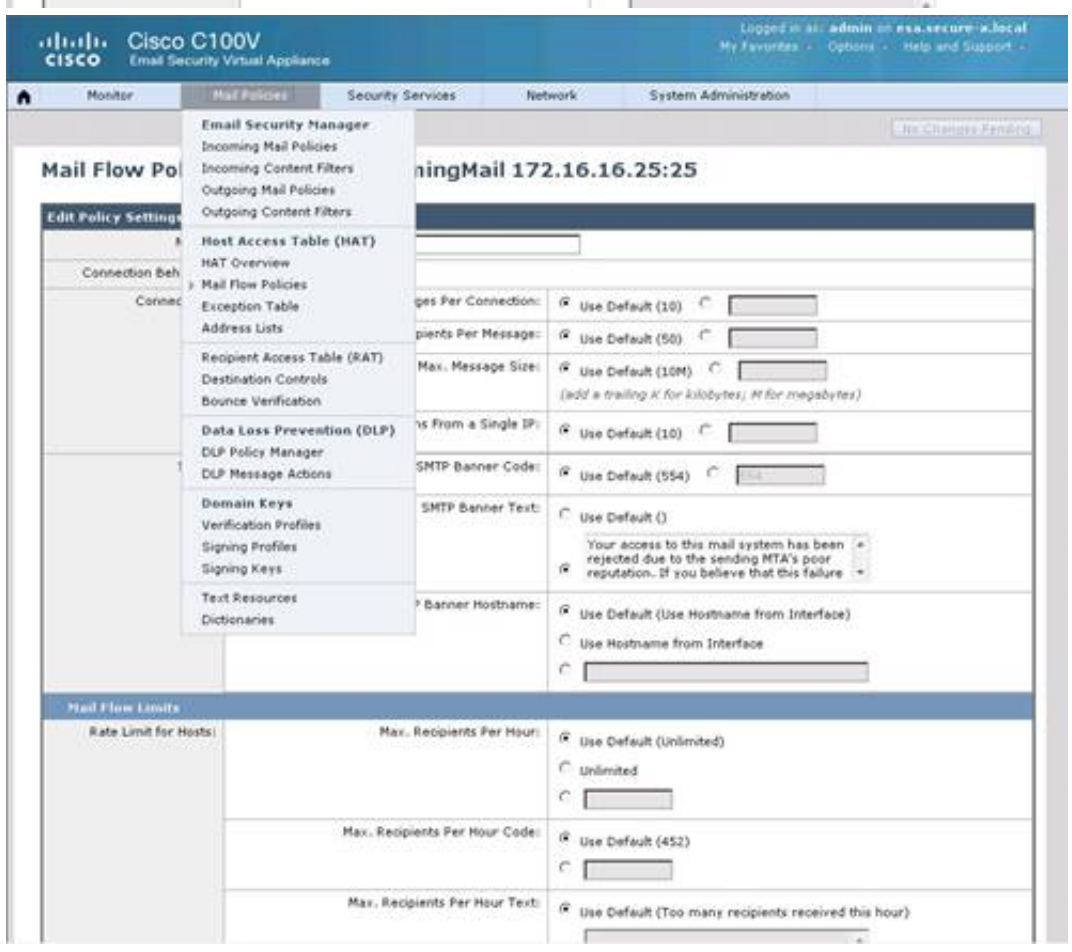

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Mail Flow Policy: ACCEPTED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: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

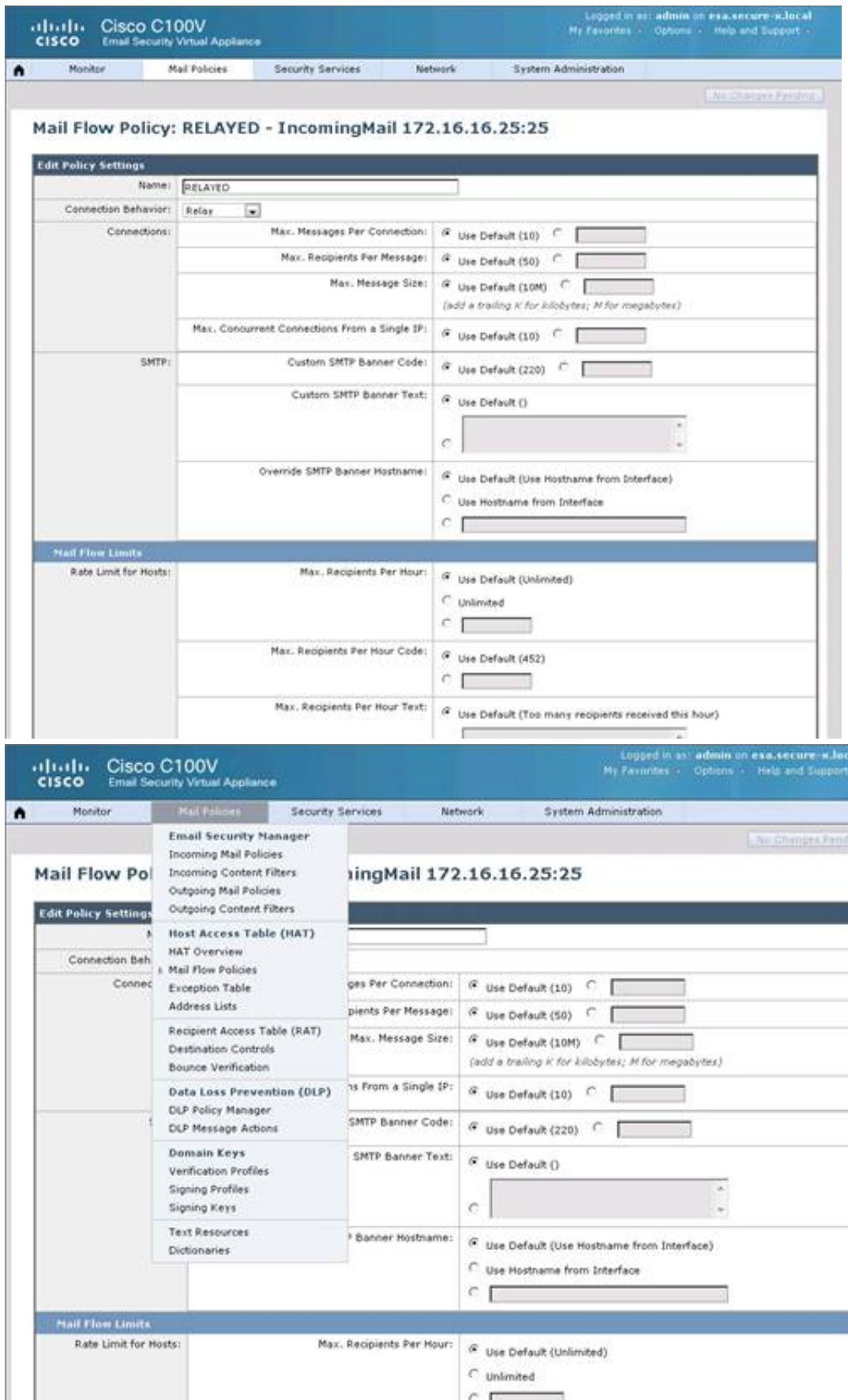
Cisco C100V
Email Security Virtual Appliance
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing Content Filters
Host Access Table (HAT)
HAT Overview
Mail Flow Policies
Exception Table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

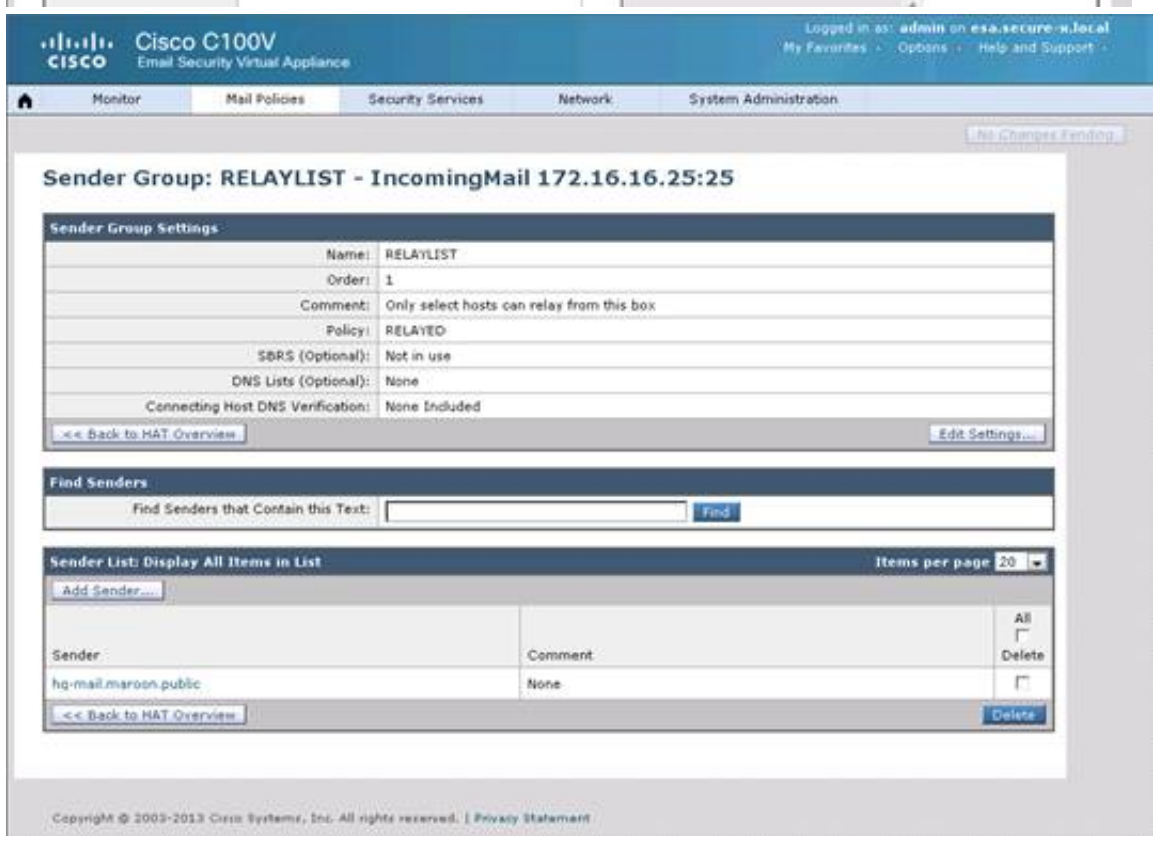

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Sender Group: BLACKLIST - IncomingMail 172.16.16.25:25
Sender Group Settings
Name: BLACKLIST
Order: 3
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

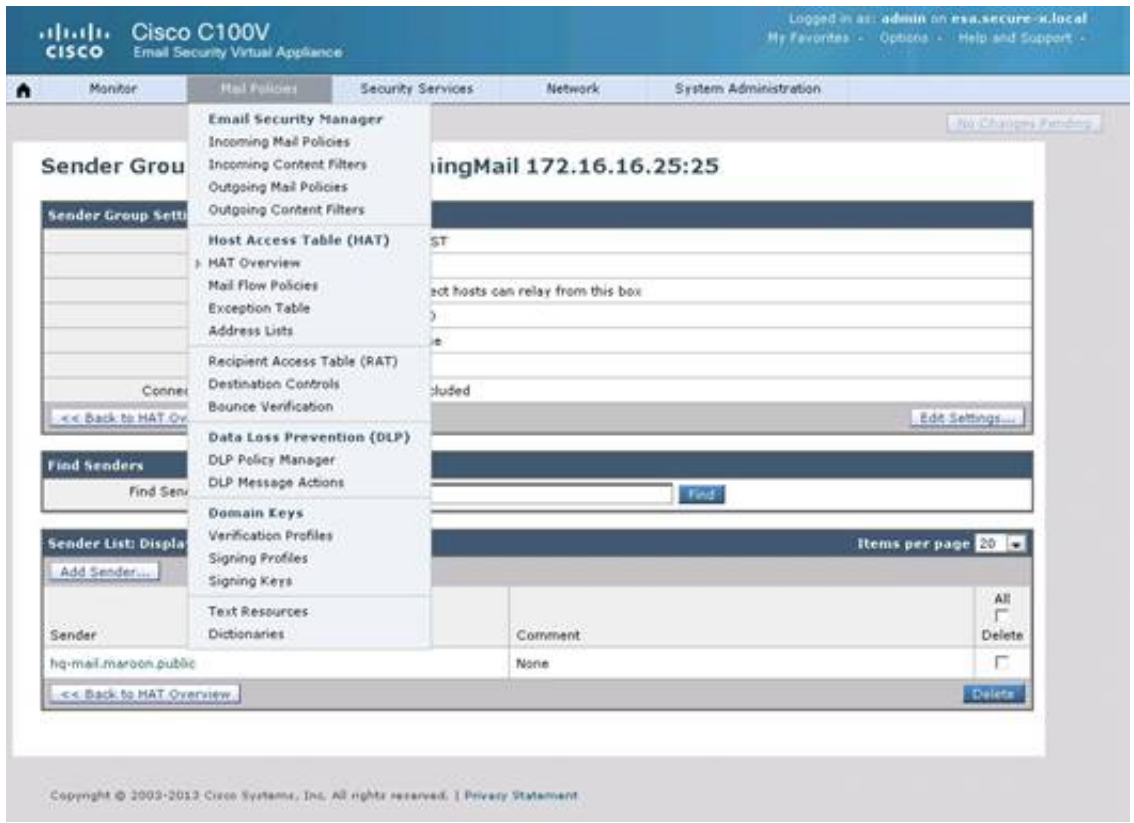

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.securex.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing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

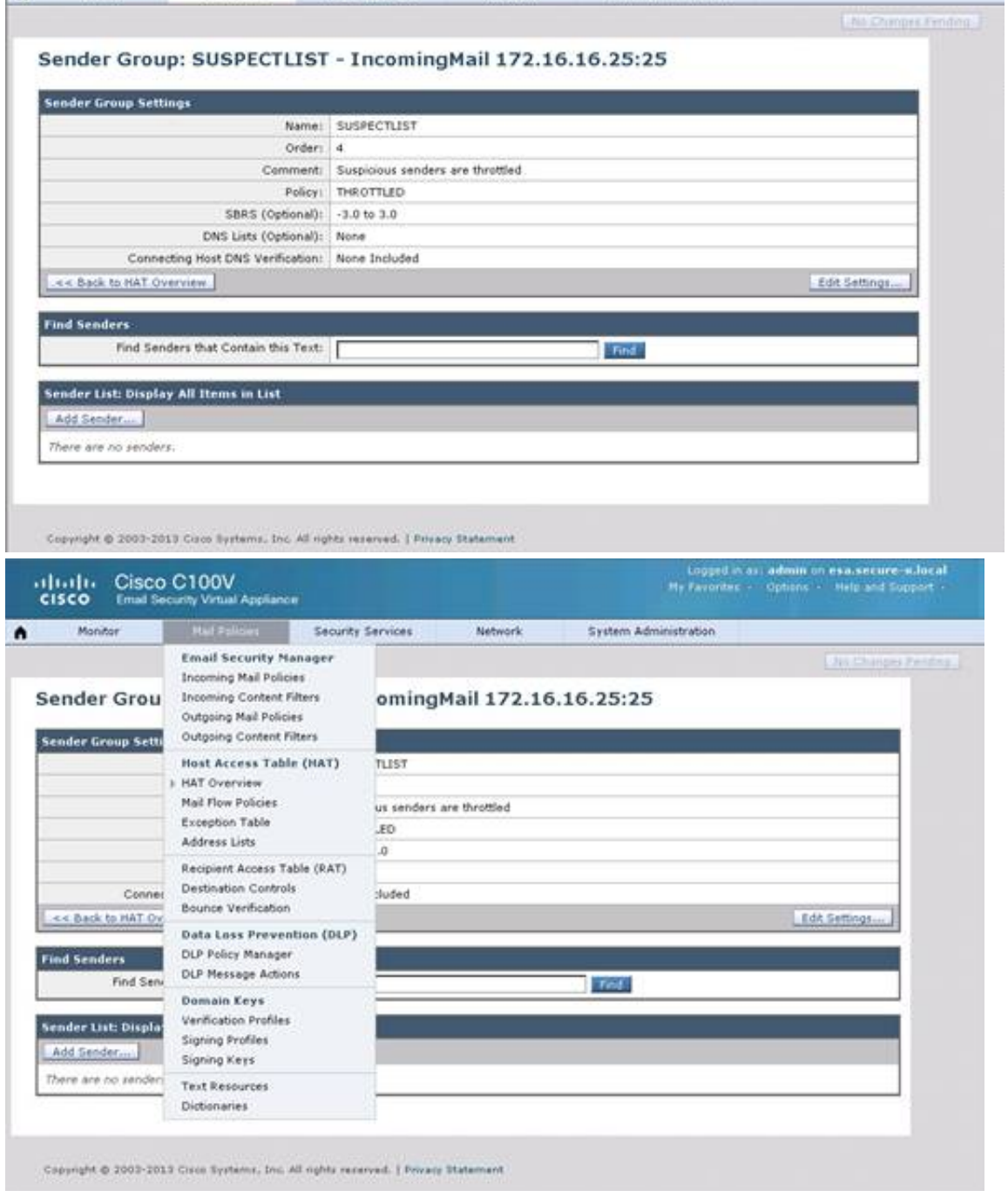

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: BLOCKED
Connection 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)

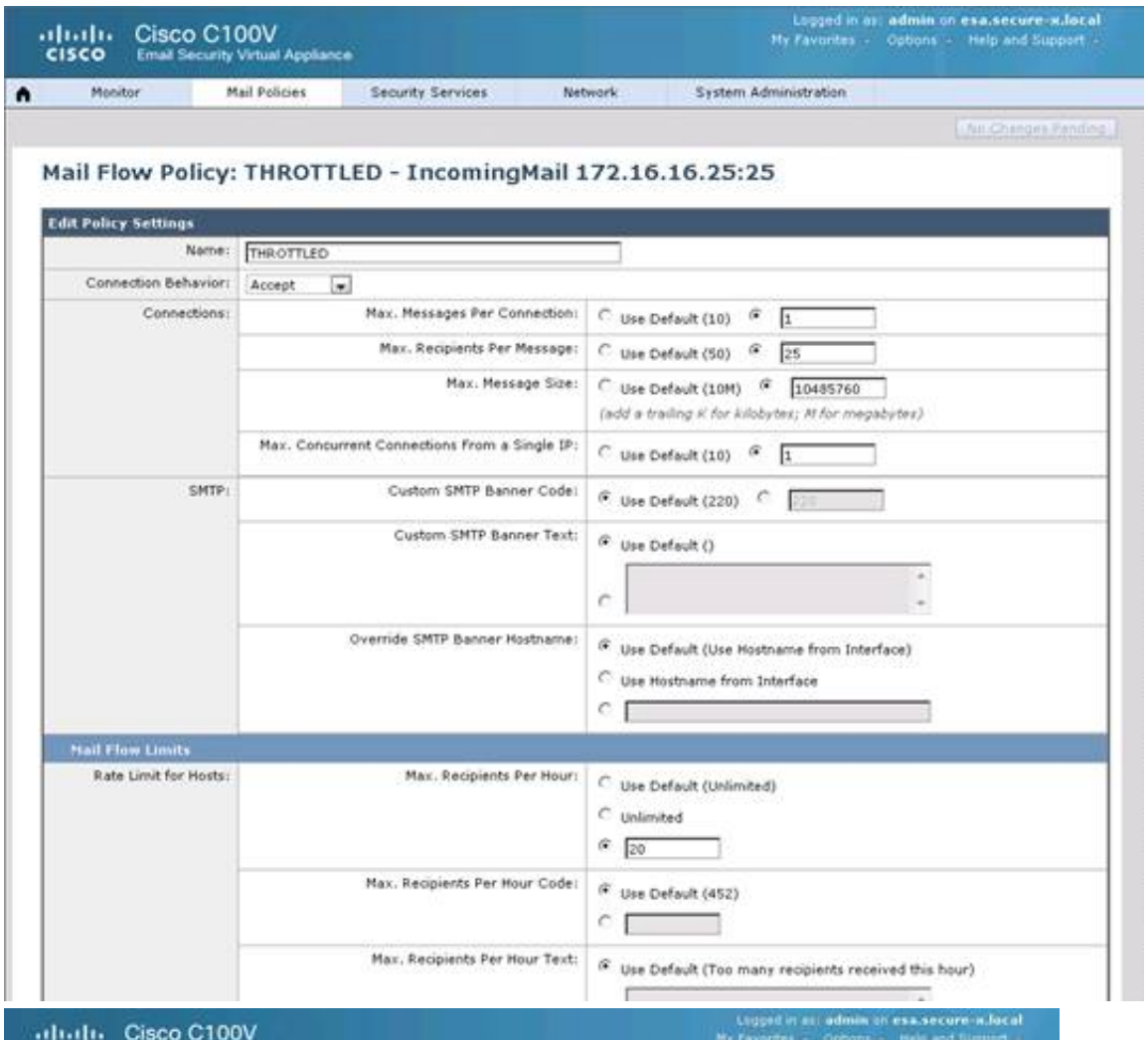

Cisco C100V
Email Security Virtual Appliance
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing Content Filters
Host Access Table (HAT)
HAT Overview
Mail Flow Policies
Exception Table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

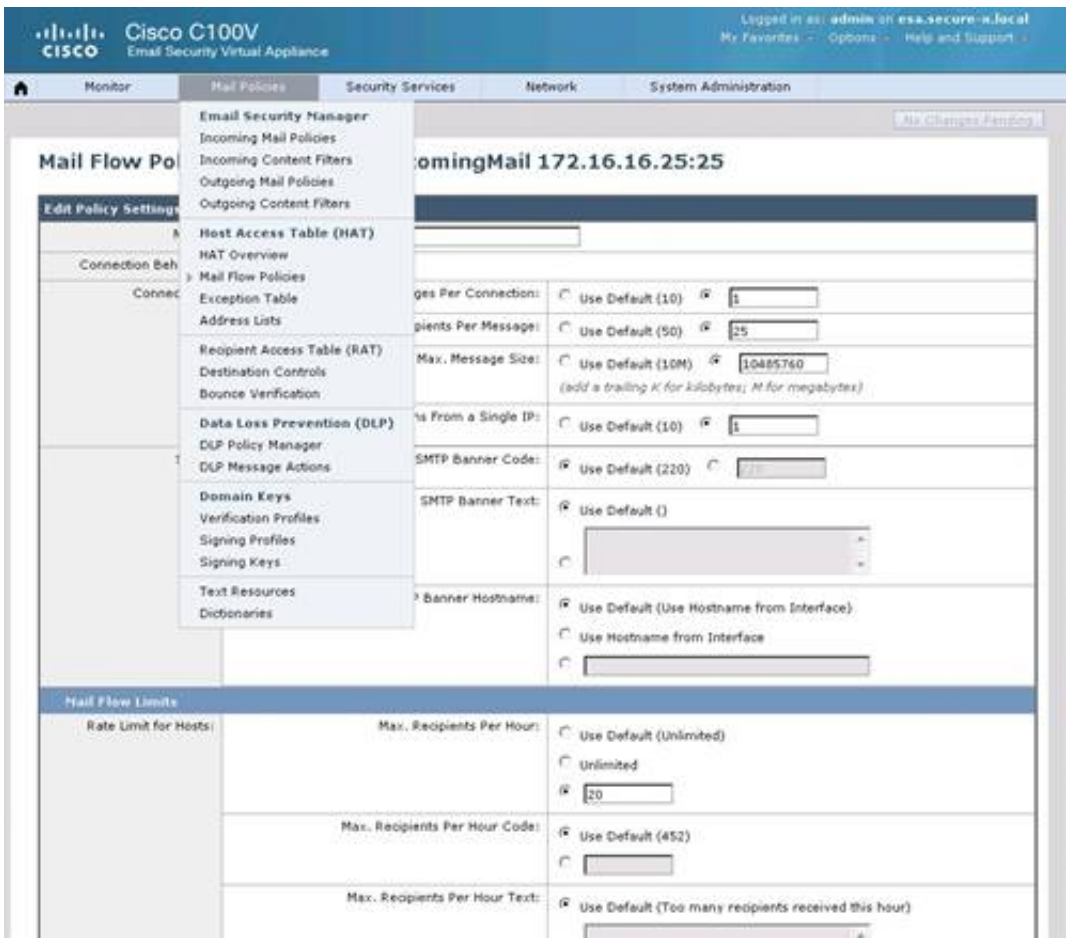

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: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

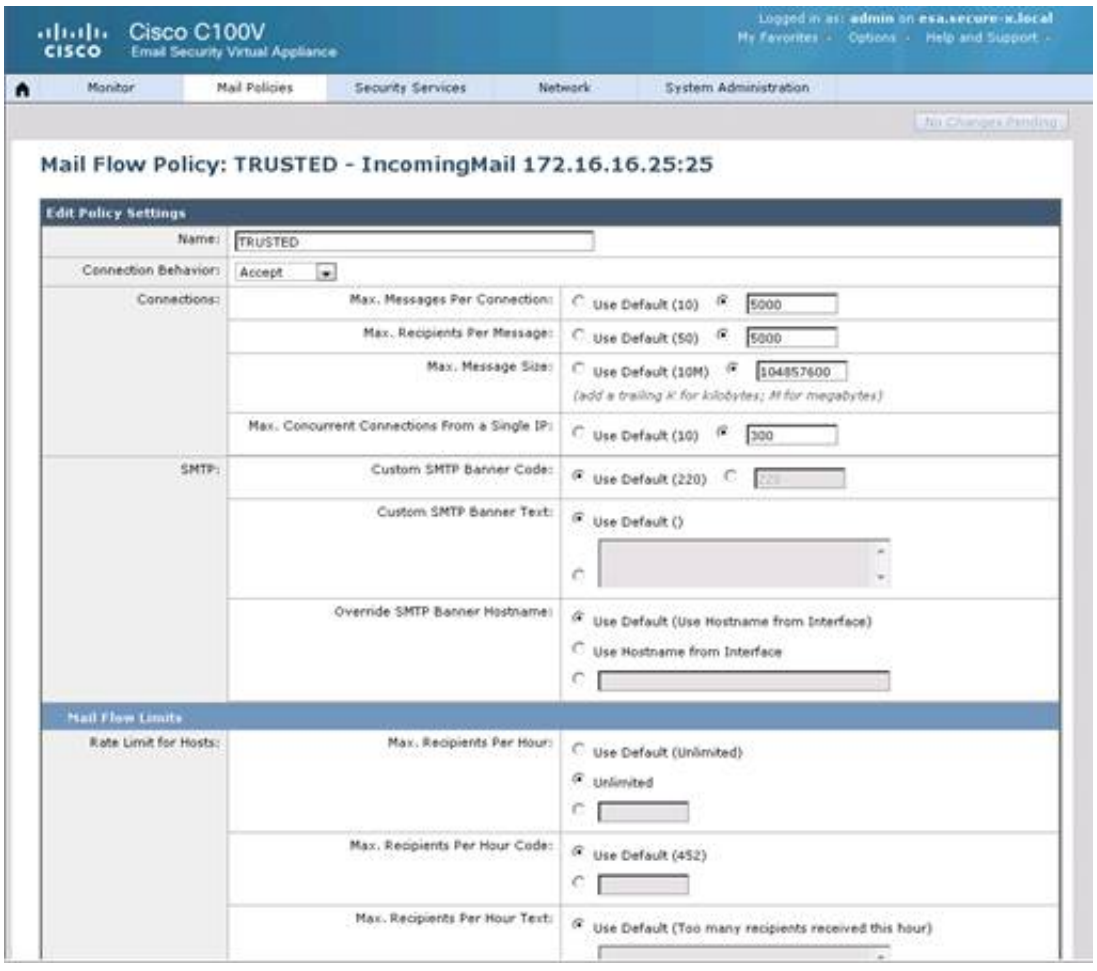

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Sender Group: RELAYLIST - IncomingMail 172.16.16.25:25
Sender Group Settings
Name: 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
<< Back to HAT Overview
Delete
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

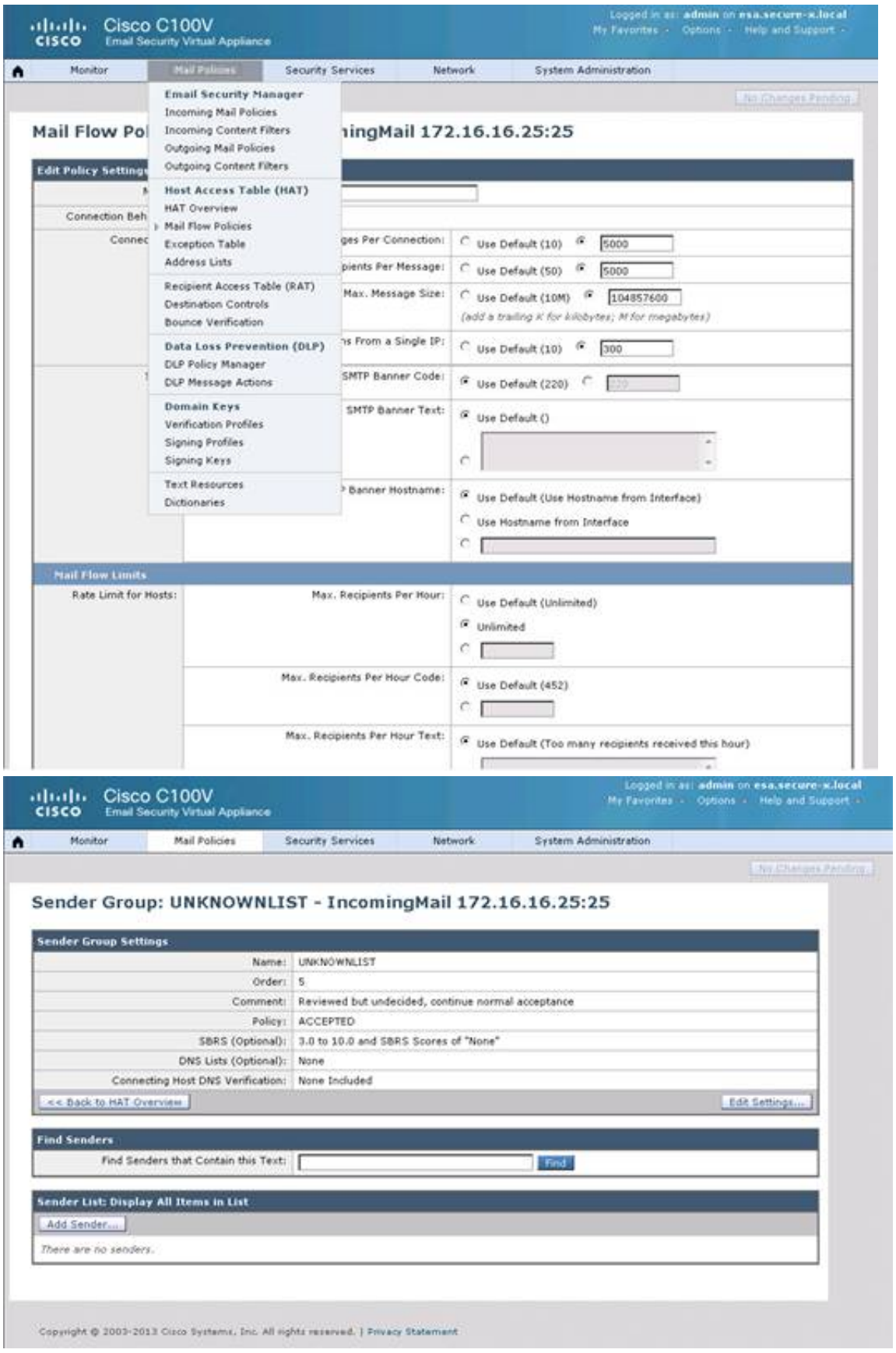

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing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

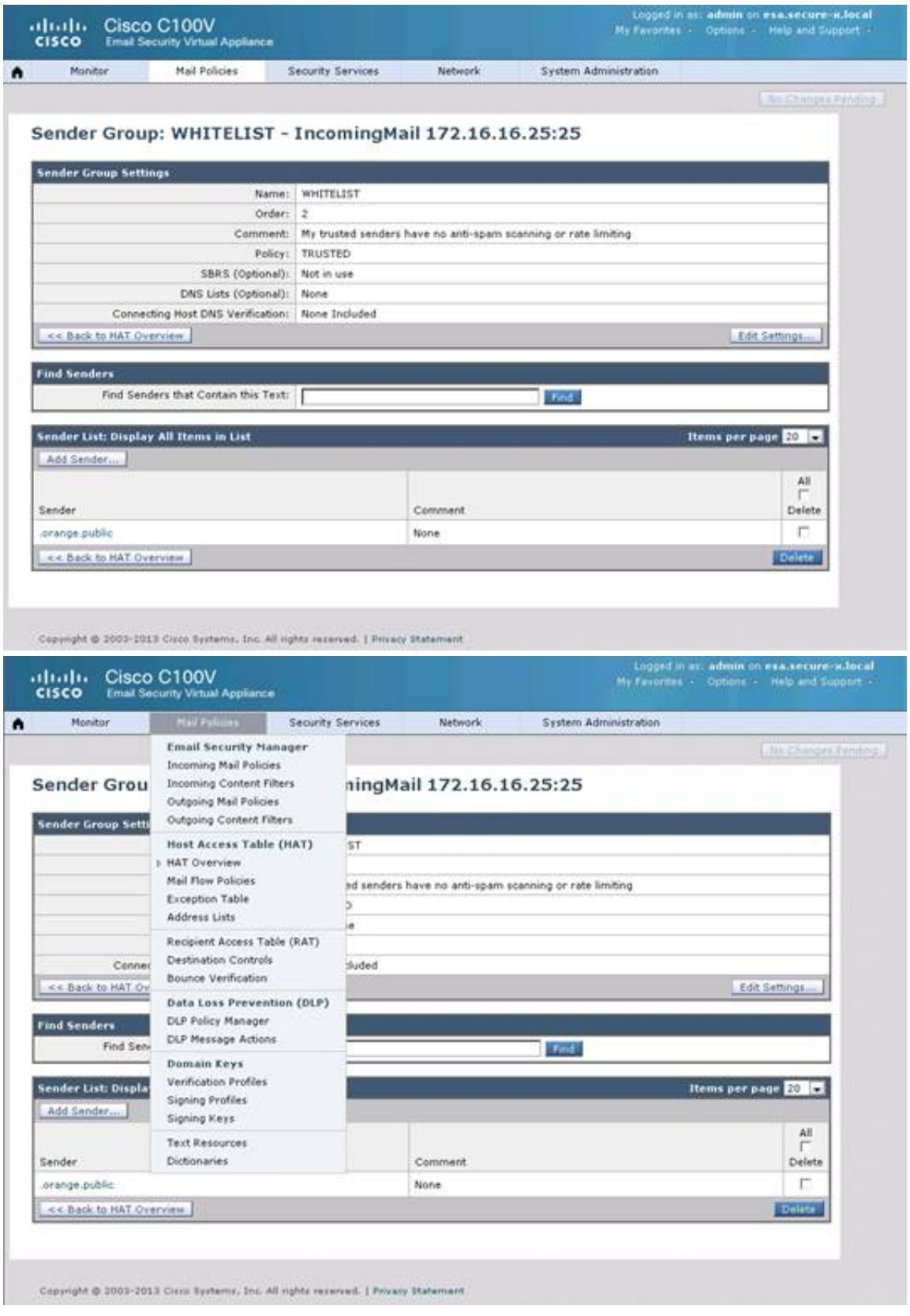

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing 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 Senders
Find
Sender List: Displa
Add Sender...
Edit Settings...
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
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
No Changes Pending
Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: TRUSTED
Connection Behavior: Accept
Connections:
Max. Messages Per Connection: Use Default (10) 5000
Max. Recipients Per Message: Use Default (50) 5000
Max. Message Size: Use Default (10M) 104857600
(add a trailing K for kilobytes; M for megabytes)
Max. Concurrent Connections From a Single IP: Use Default (10) 300
SMTP:
Custom SMTP Banner Code: Use Default (220)
Custom SMTP Banner Text: Use Default ()
Override SMTP Banner Hostname: Use Default (Use Hostname from Interface)
Use Hostname from Interface
Mail Flow Limits
Rate Limit for Hosts:
Max. Recipients Per Hour: Use Default (Unlimited)
Unlimited
Max. Recipients Per Hour Code: Use Default (452)
Max. Recipients Per Hour Text: Use Default (Too many recipients received this hour)


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: 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

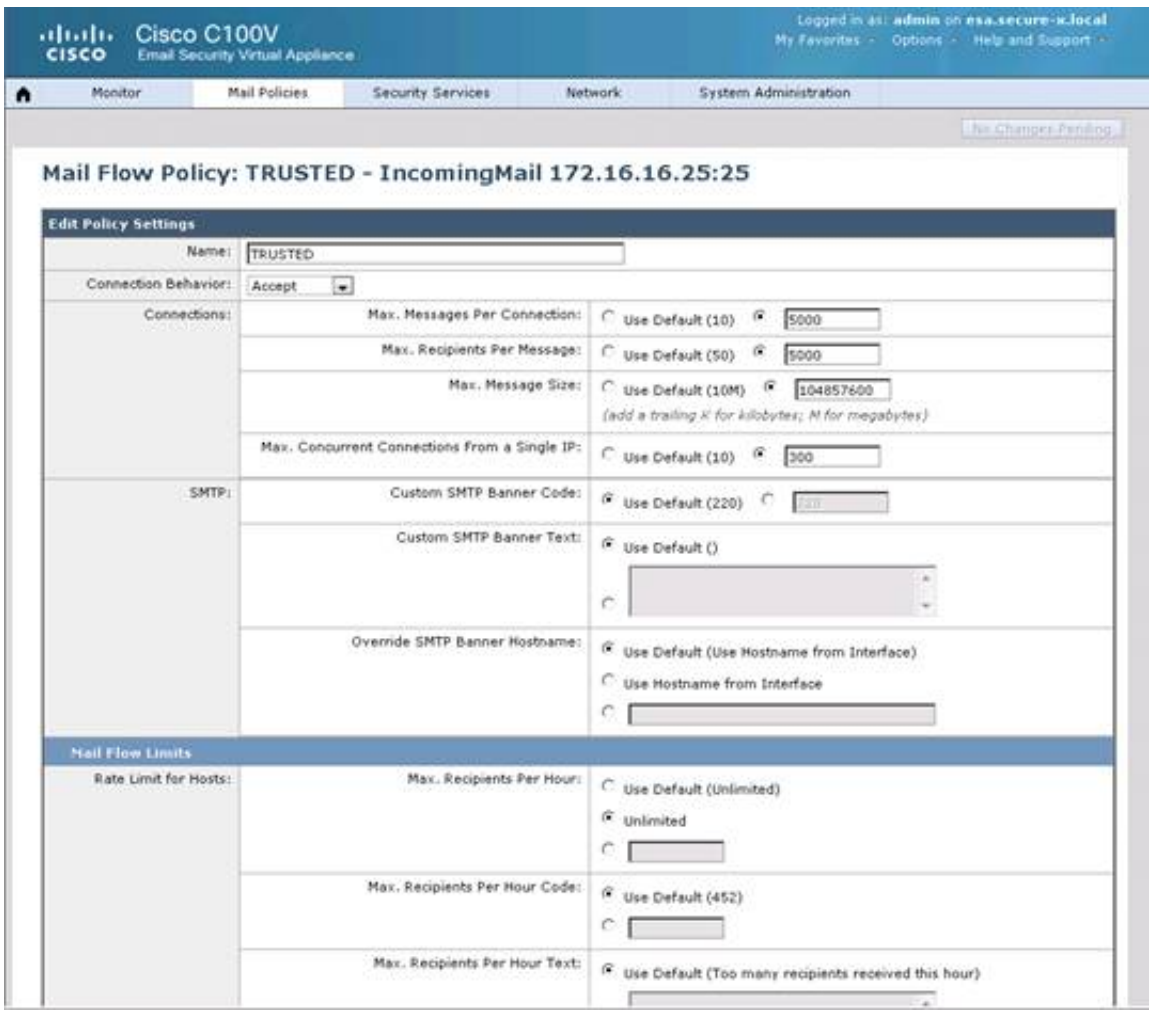


For which domains will the Cisco Email Security Appliance allow up to 5000 recipients per message?

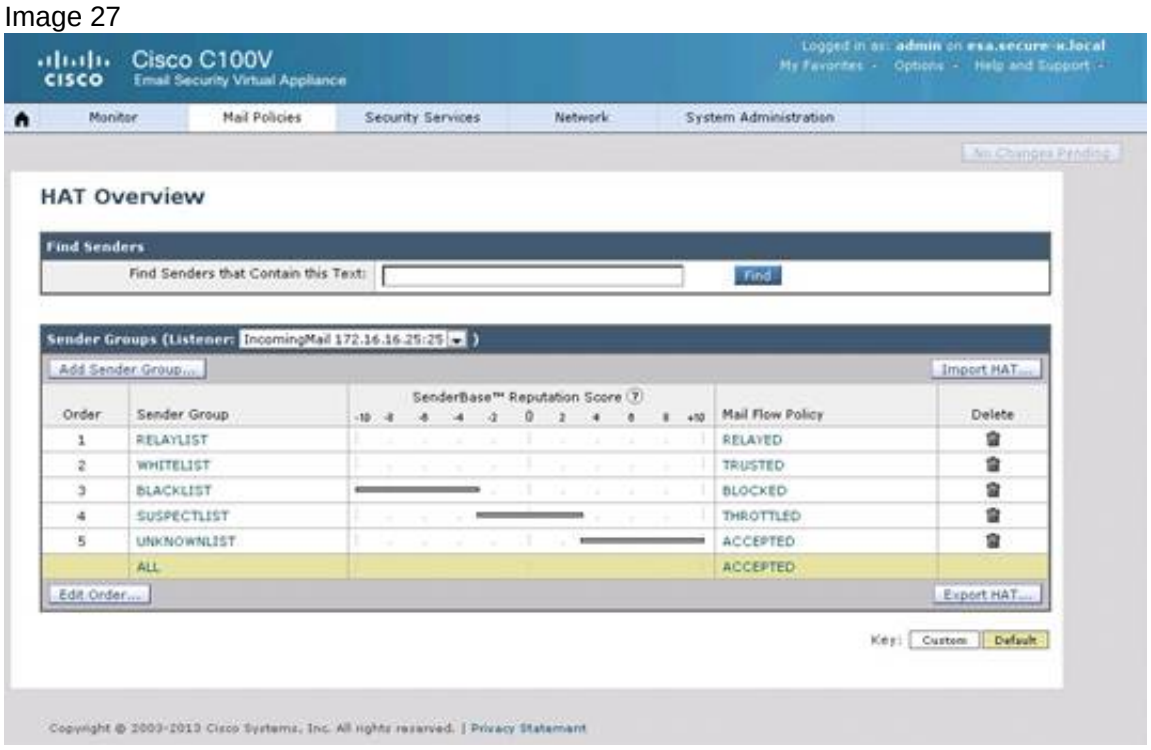
A. violet.public
B. violet.public and blue.public
C. violet.public, blue.public and green.public
D. red.public
E. orange.public
F. red.public and orange.public

Answer: E

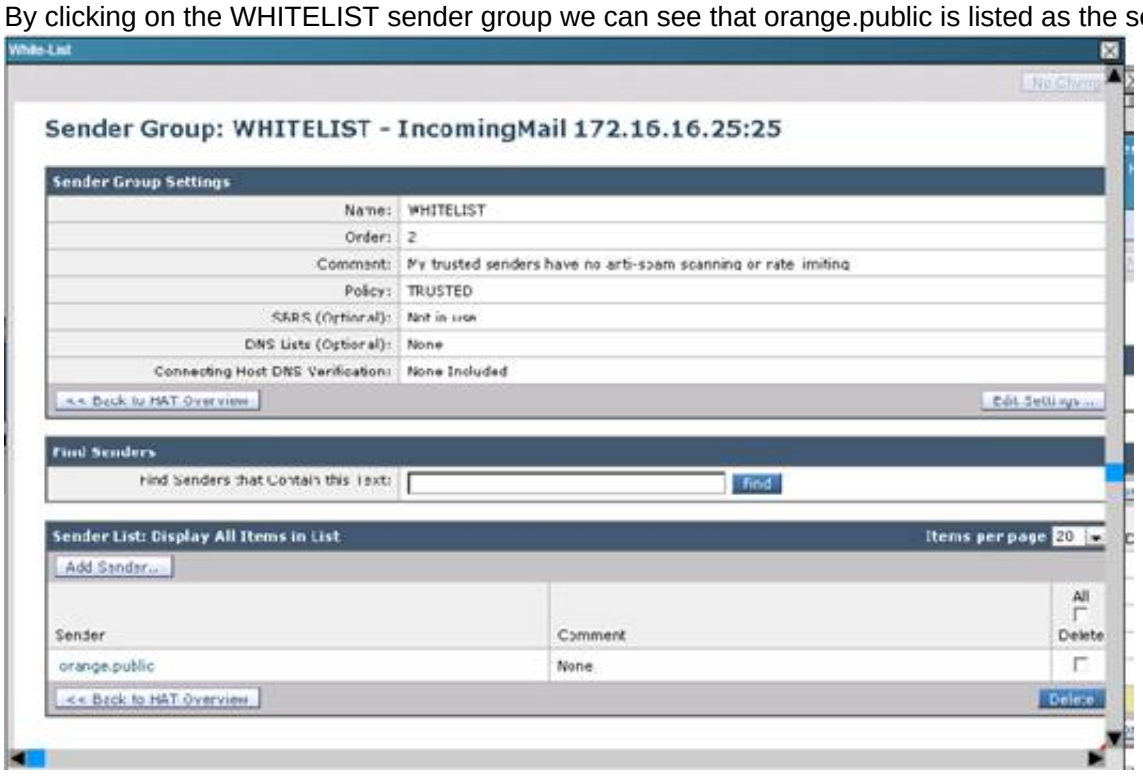
Explanation: Here we see that the TRUSTED policy is being throttled to 5000 recipients per message. Image%2075



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 650
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 655
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 657
Which two statements about Cisco ESA clusters are true? (Choose two.)

A. A cluster must contain exactly one group.
B. A cluster can contain multiple groups.
C. Clusters are implemented in a client/server relationship.
D. The cluster configuration must be managed by the cluster administrator.
E. The cluster configuration can be created and managed through either the GUI or the CLI.

Answer: BE

NEW QUESTION 662
When does the Cisco ASA send traffic to the Cisco ASA IPS module for analysis?

A. before firewall policy are applied
B. after outgoing VPN traffic is encrypted
C. after firewall policies are applied
D. before incoming VPN traffic is decrypted.

Answer: C

NEW QUESTION 666
Which IPS feature allows you to aggregate multiple IPS links over a single port channel?

A. UDLD
B. ECLB
C. LACP
D. PAgP

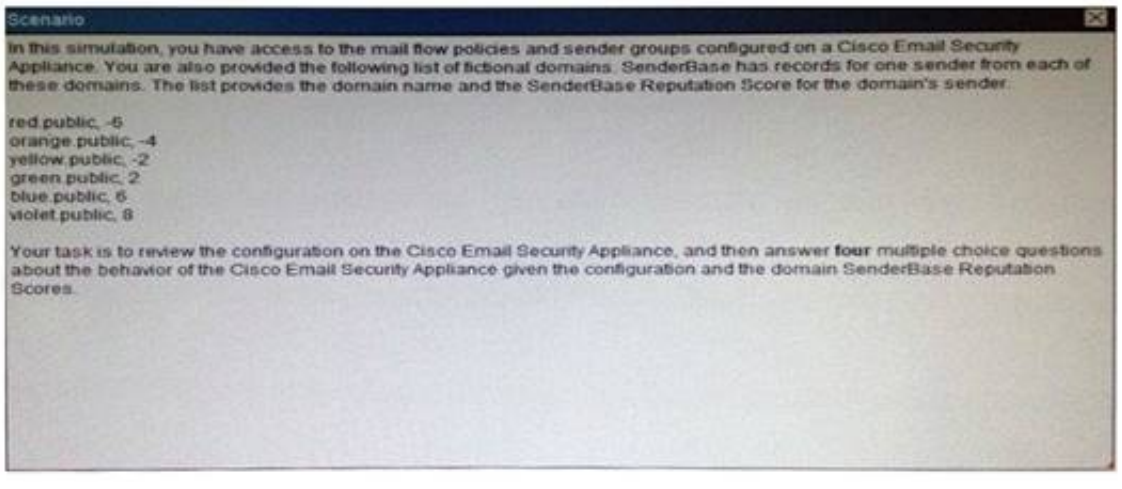
Answer: B

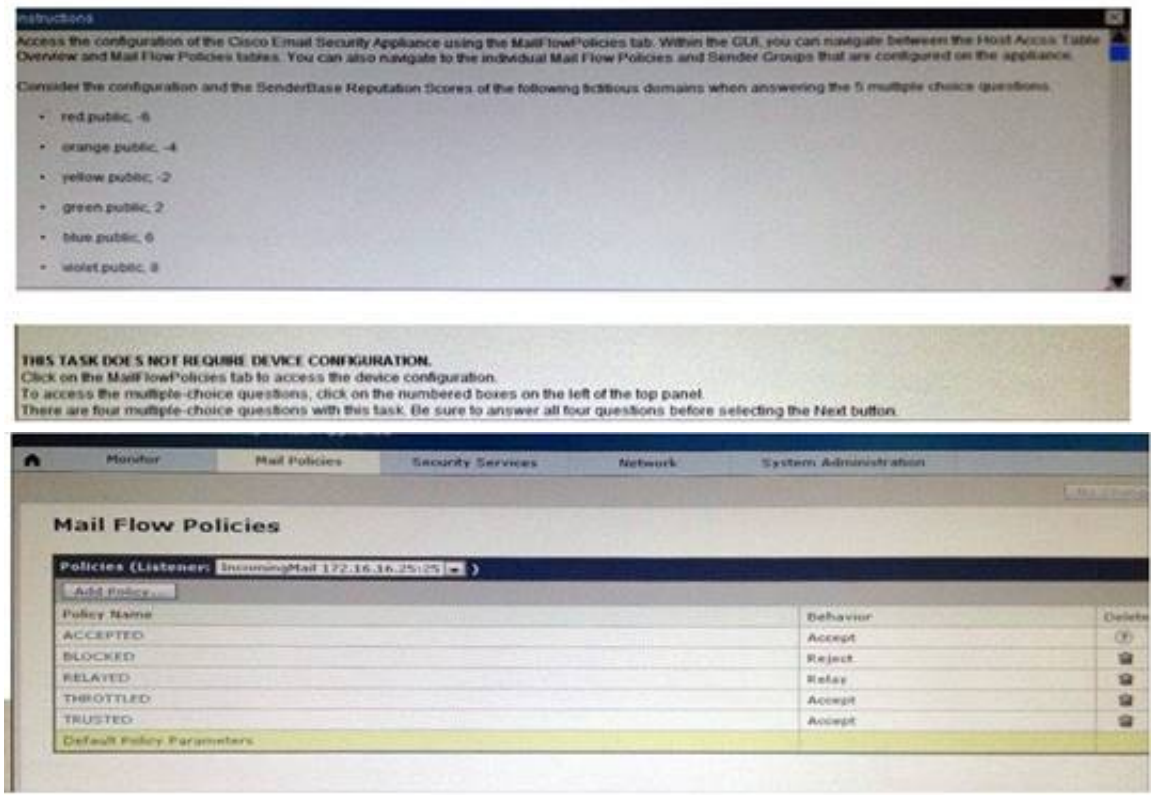
NEW QUESTION 667
Which Cisco ESA component receives connections from external mail servers?

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

Answer: B

NEW QUESTION 671





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 672
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

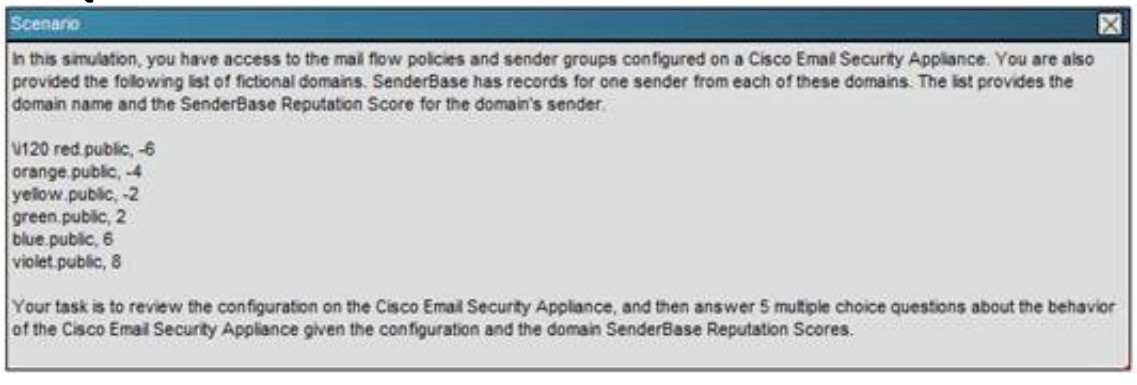
Answer: AEF

NEW QUESTION 675
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 680



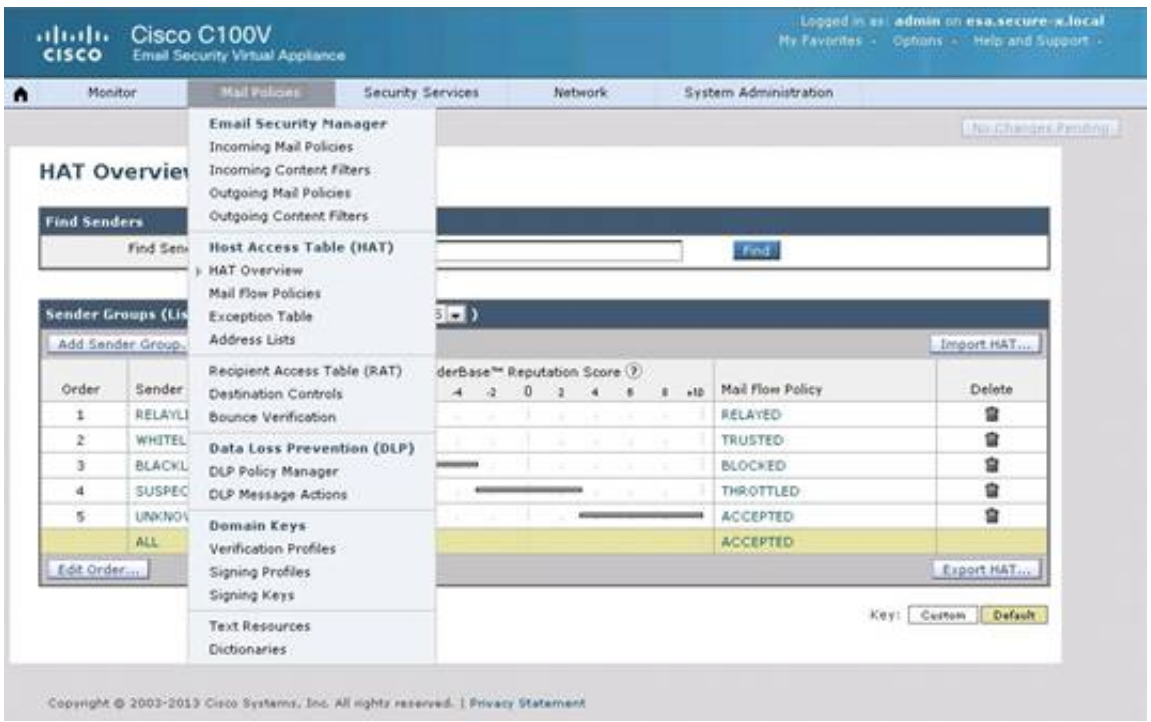
Instructions

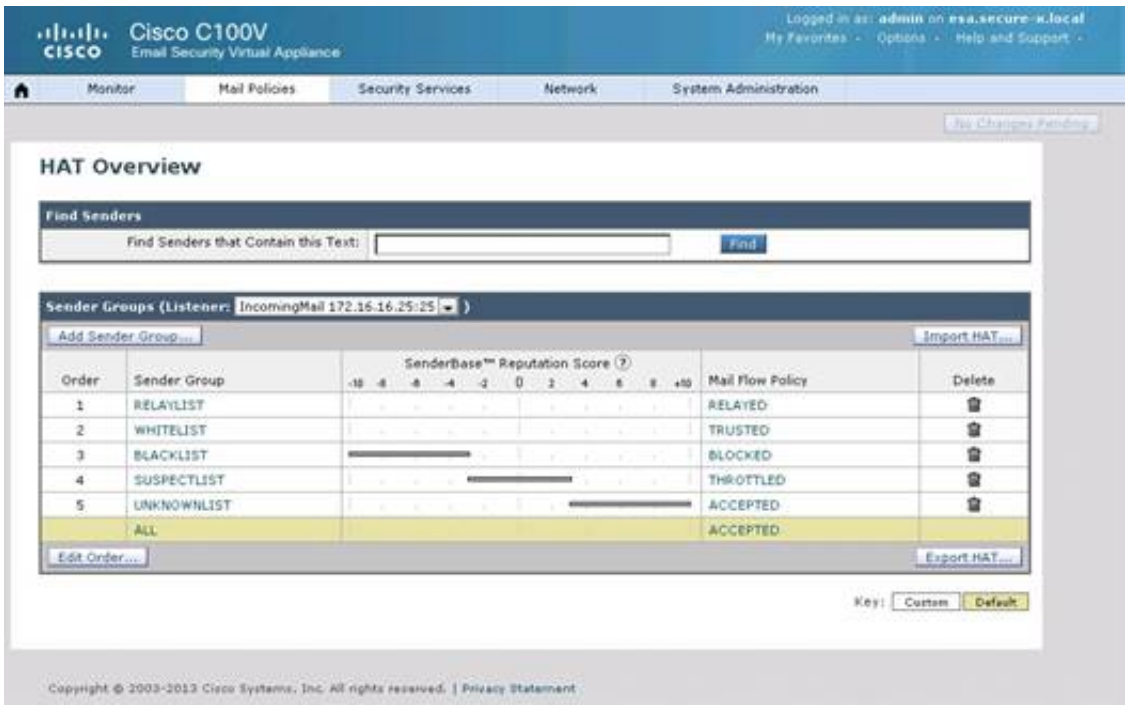
Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you can navigate between the HAT Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Groups that are configured on the appliance.

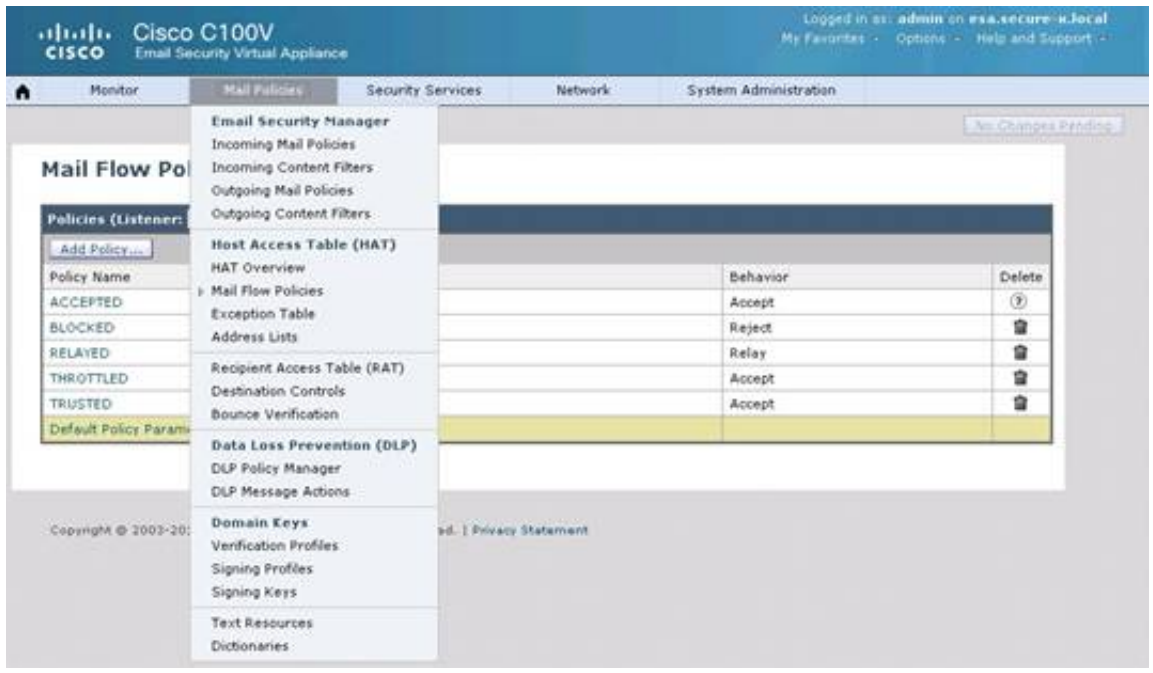
Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answering the 5 multiple choice questions.

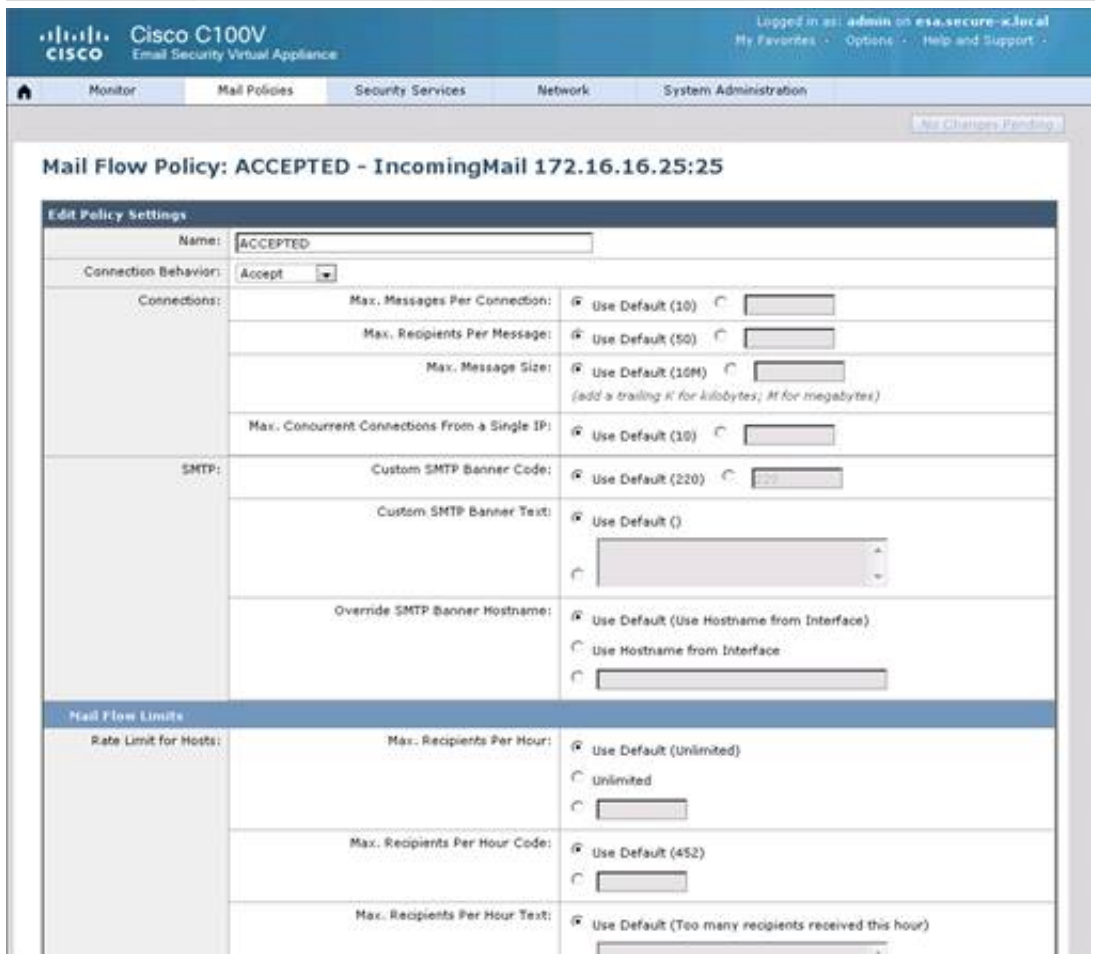
- red.public, -6
- orange.public, -4
- yellow.public, -2
- green.public, 2
- blue.public, 6
- violet.public, 8

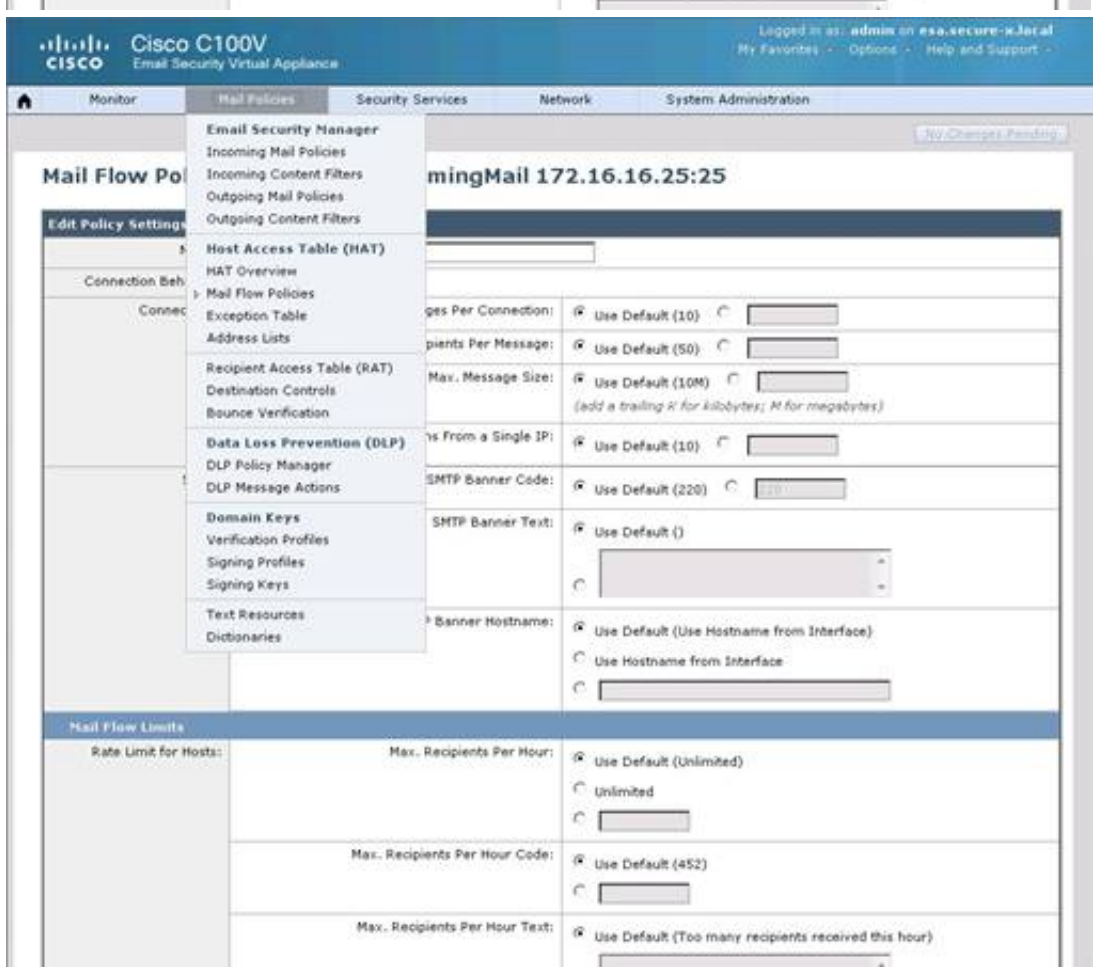
THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
Click on the MailFlowPolicies tab to access the device configuration.
To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
There are four multiple-choice questions with this task. Be sure to answer all four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

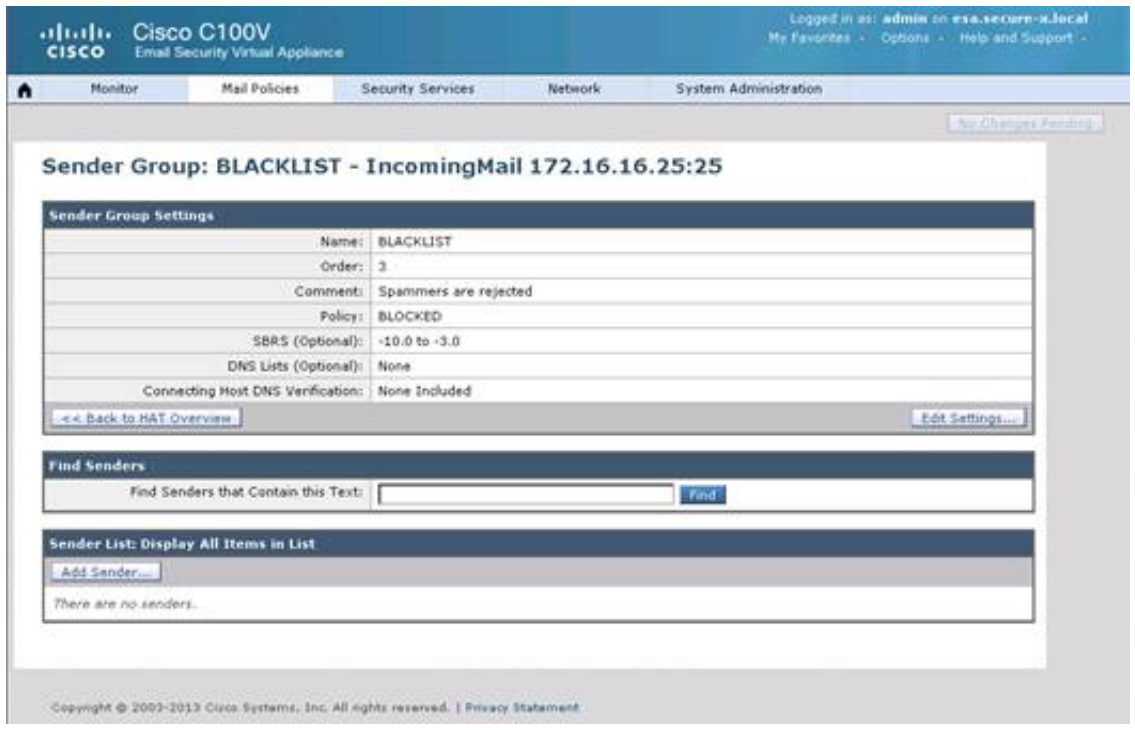


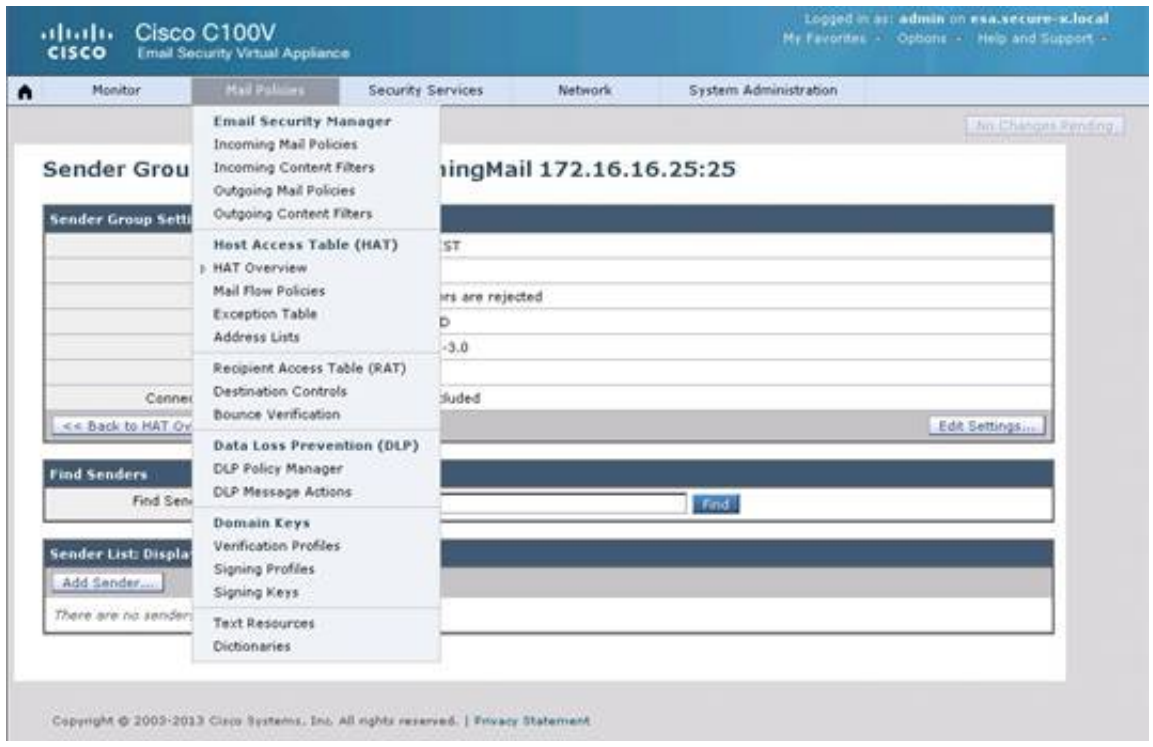


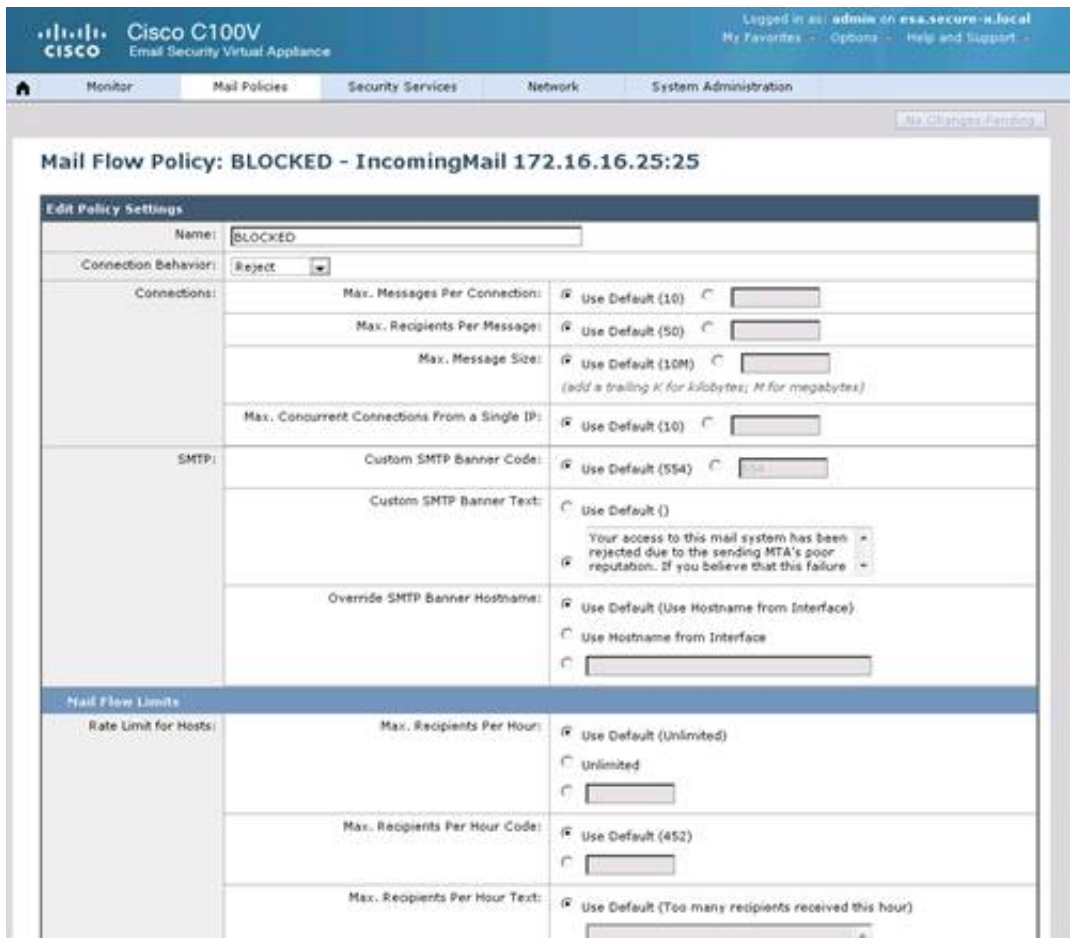

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing 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 Pol
Policies (Listener:
Add Policy...
Policy Name
ACCEPTED
BLOCKED
RELAYED
THROTTLED
TRUSTED
Default Policy Param
Behavior
Delete
Accept
Reject
Relay
Accept
Accept
Privacy Statement

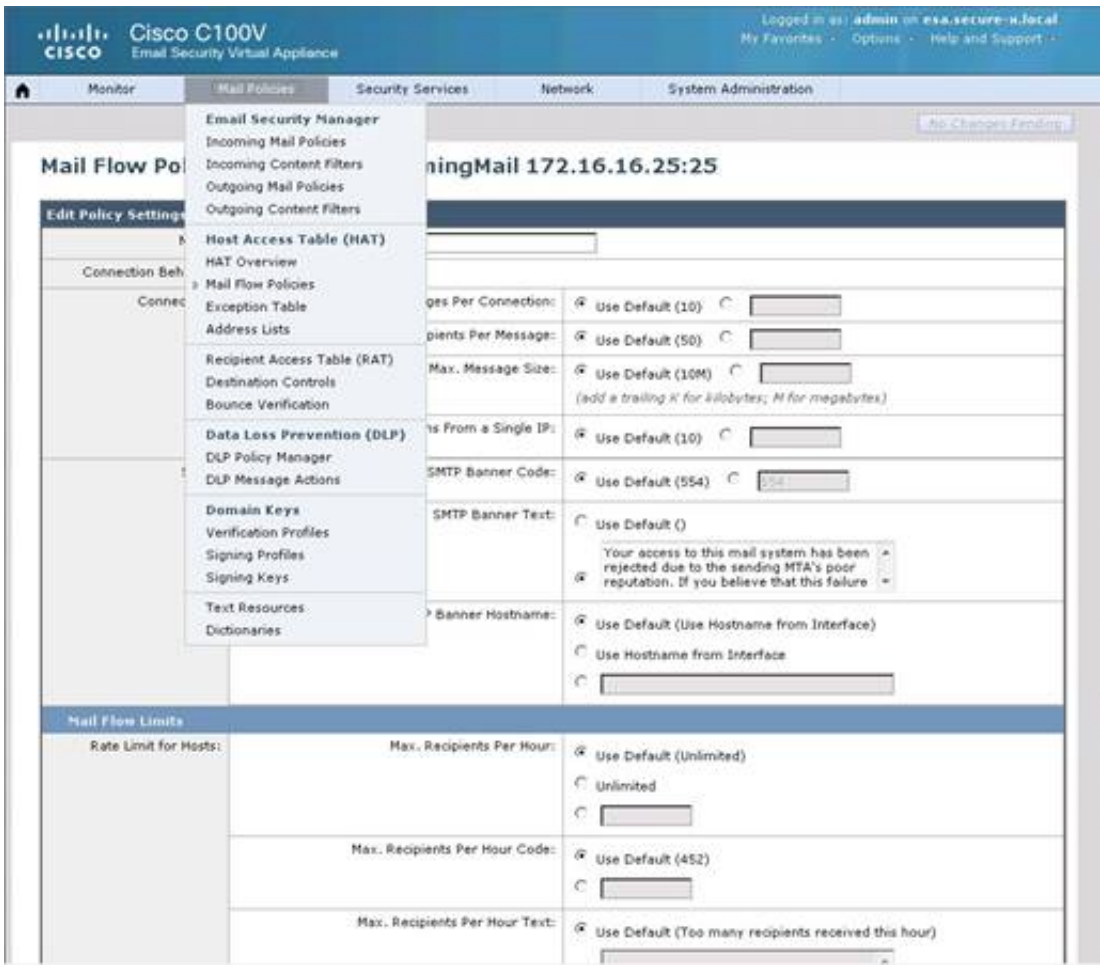

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
Mail Flow Policy: ACCEPTED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: ACCEPTED
Connection 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)

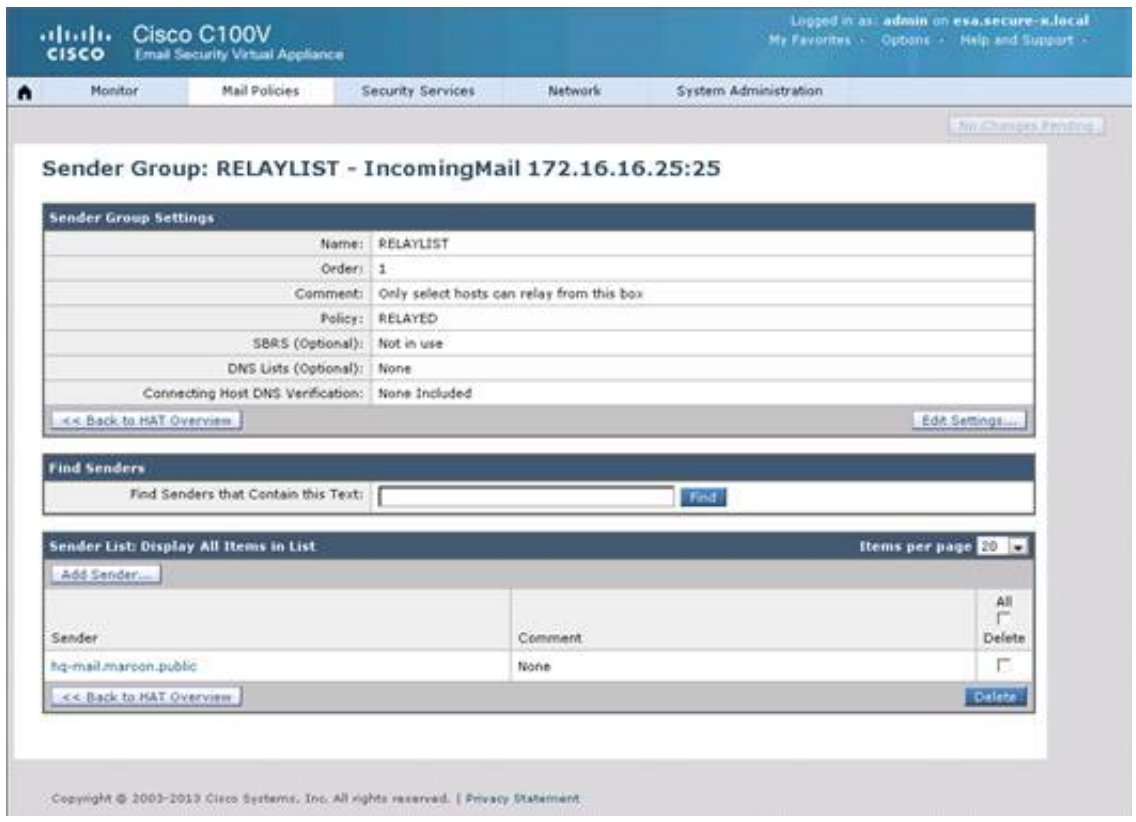

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing 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 Pol
mingMail 172.16.16.25:25
Edit Policy Settings
Connection Beh
Connec
ges Per Connection: Use Default (10)
pients Per Message: Use Default (50)
Max. Message Size: Use Default (10M)
(add a trailing K for kilobytes; M for megabytes)
ns From a Single IP: Use Default (10)
SMTP Banner Code: Use Default (220)
SMTP Banner Text: Use Default ()
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)

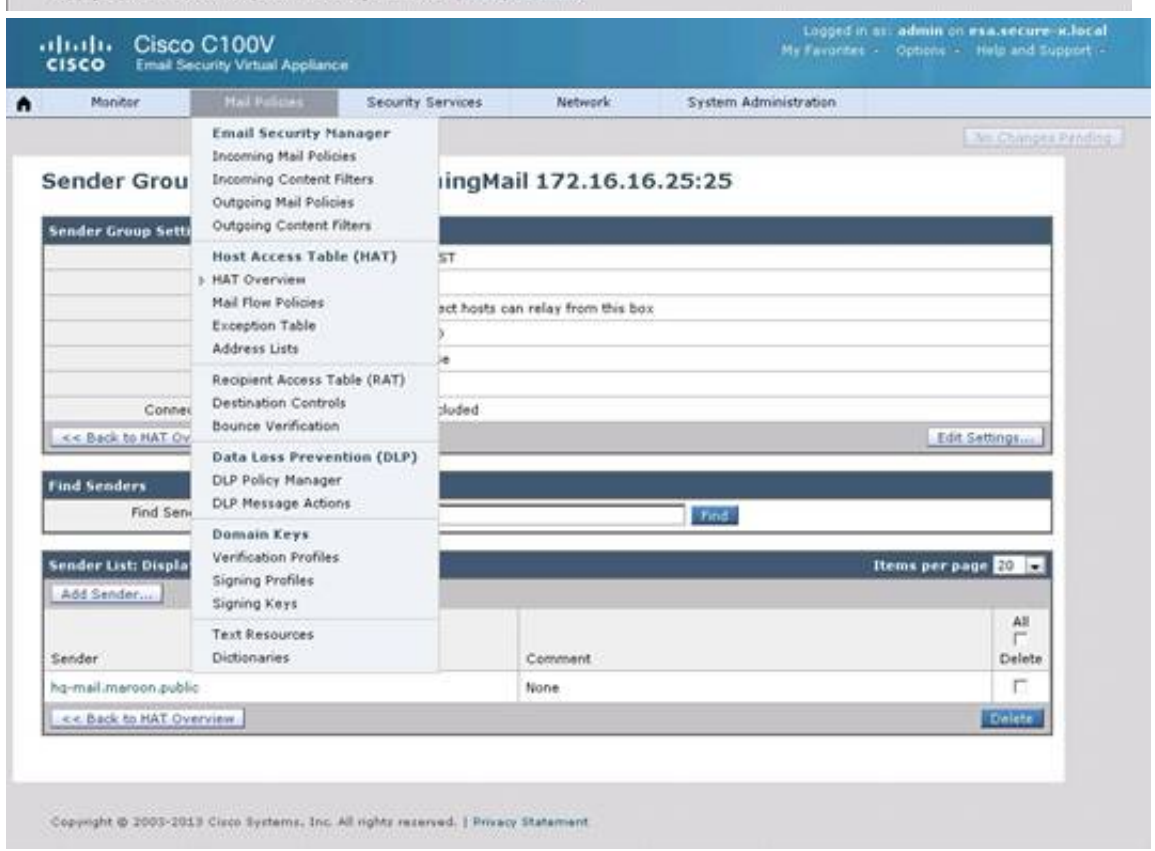

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Sender Group: BLACKLIST - IncomingMail 172.16.16.25:25
Sender Group Settings
Name: BLACKLIST
Order: 3
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-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

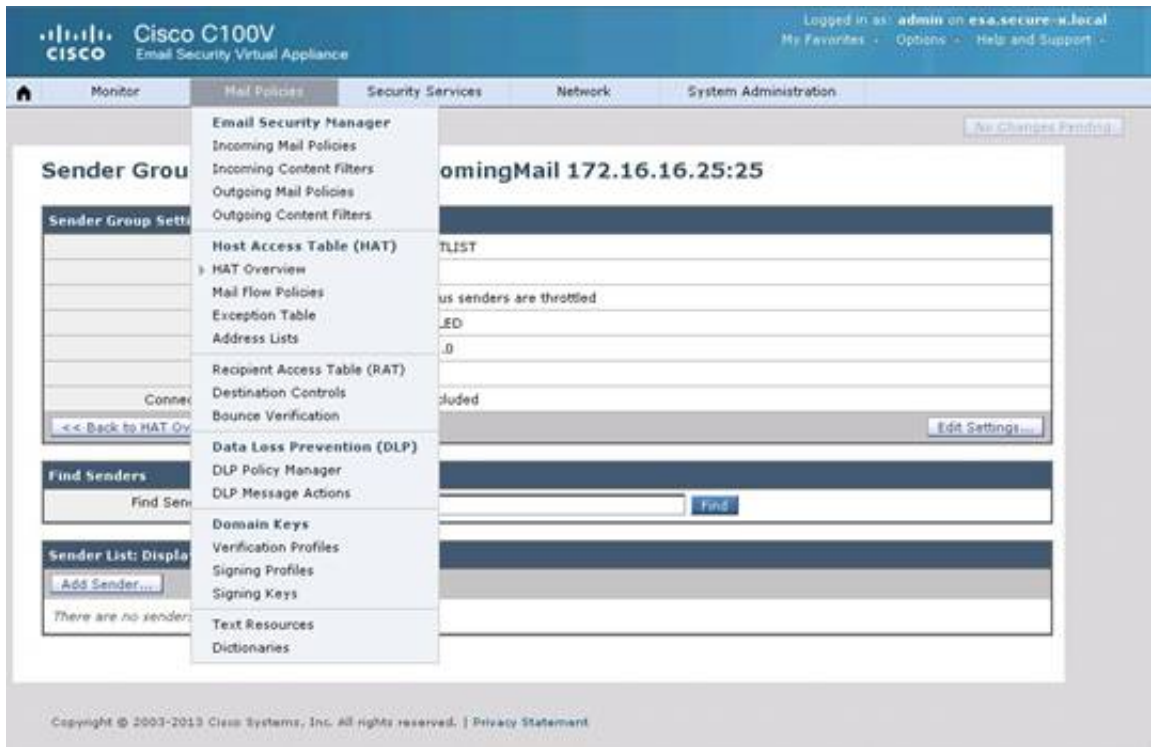

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: BLOCKED
Connection 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)

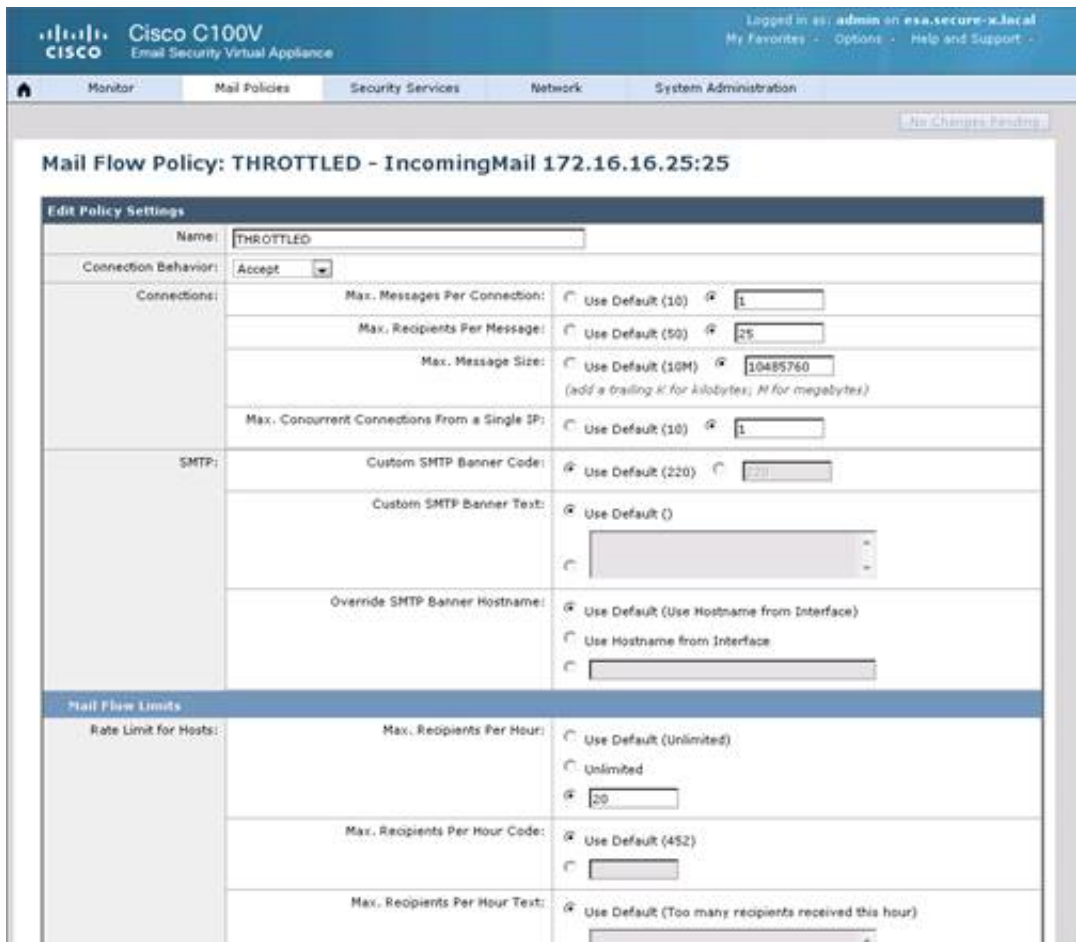

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing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

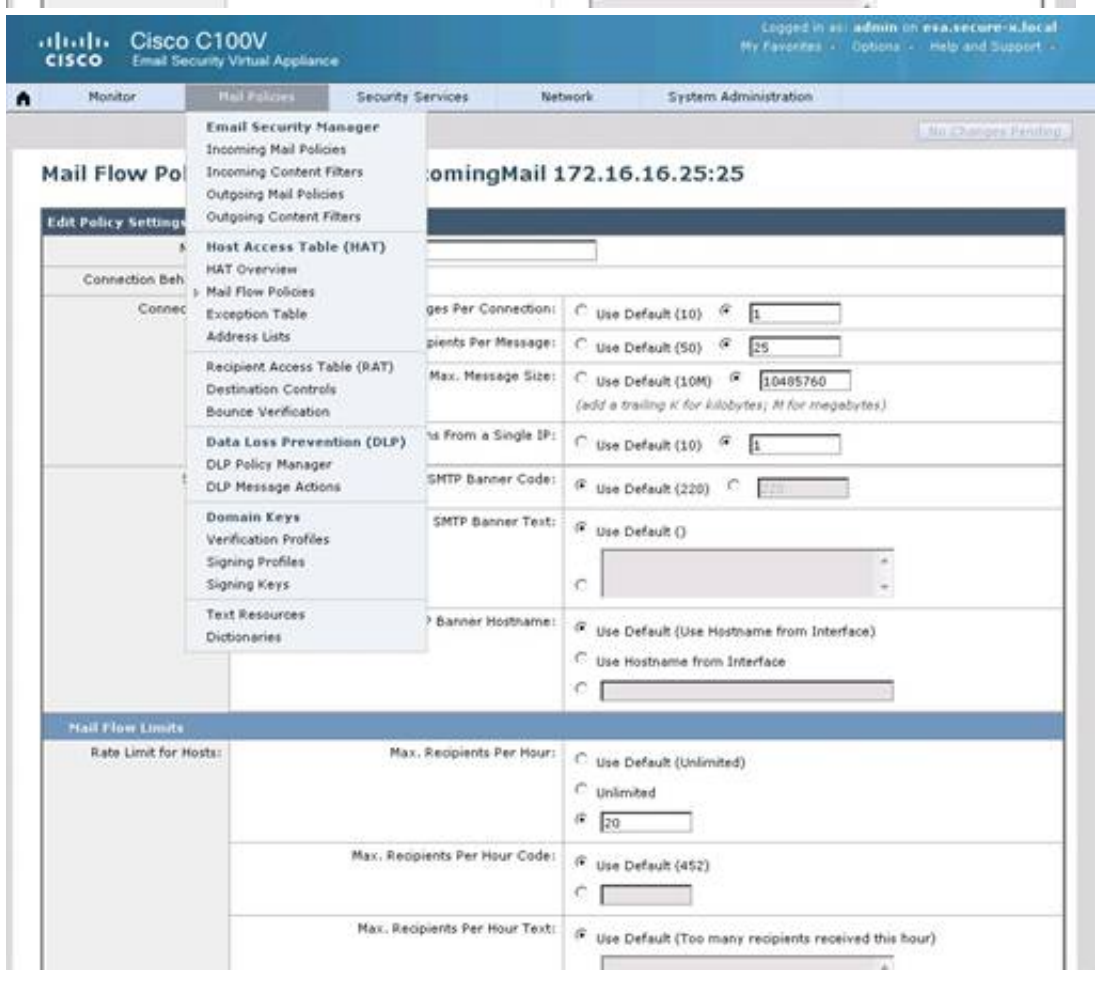

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Sender Group: RELAYLIST - IncomingMail 172.16.16.25:25
Sender Group Settings
Name: RELAYLIST
Order: 1
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

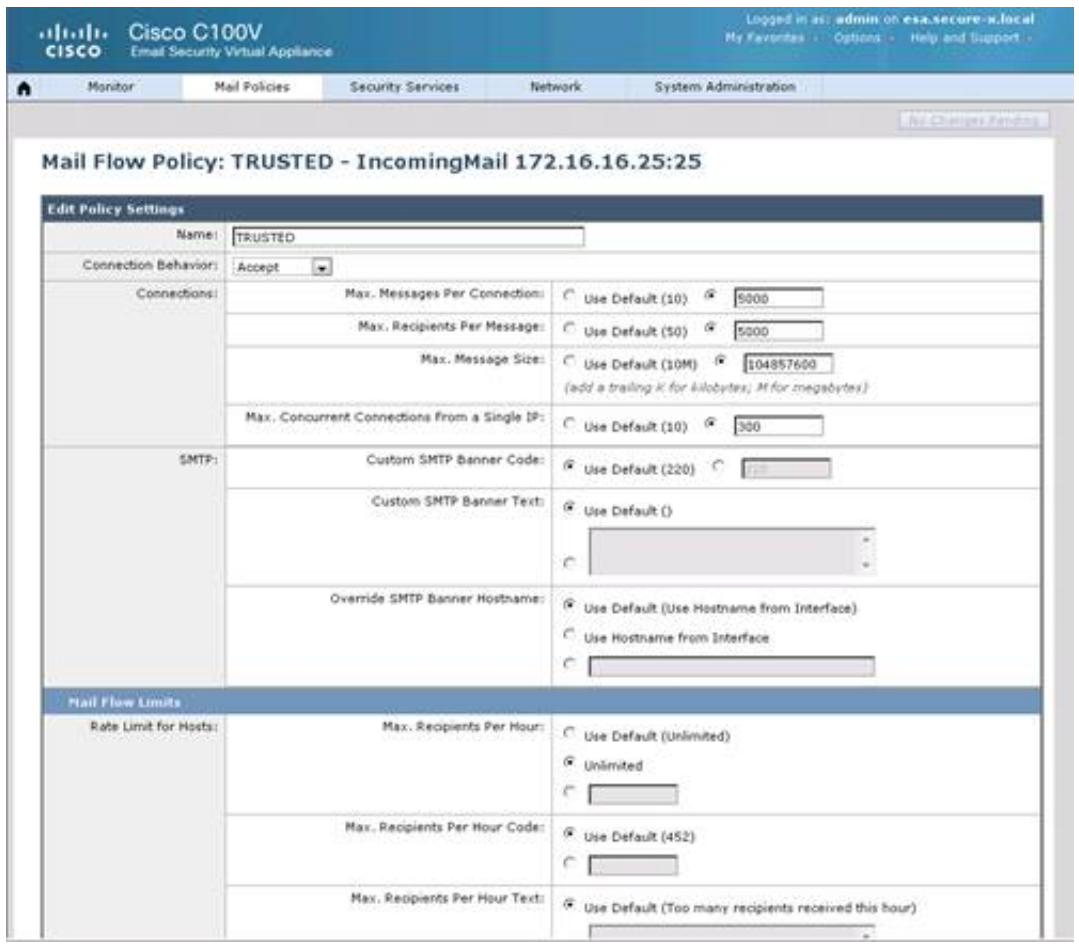

Cisco C100V
Email Security Virtual Appliance
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing Content Filters
Host Access Table (HAT)
HAT Overview
Mail Flow Policies
Exception Table
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
Items per page 20
Add Sender...
Comment
Delete
None
Delete
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

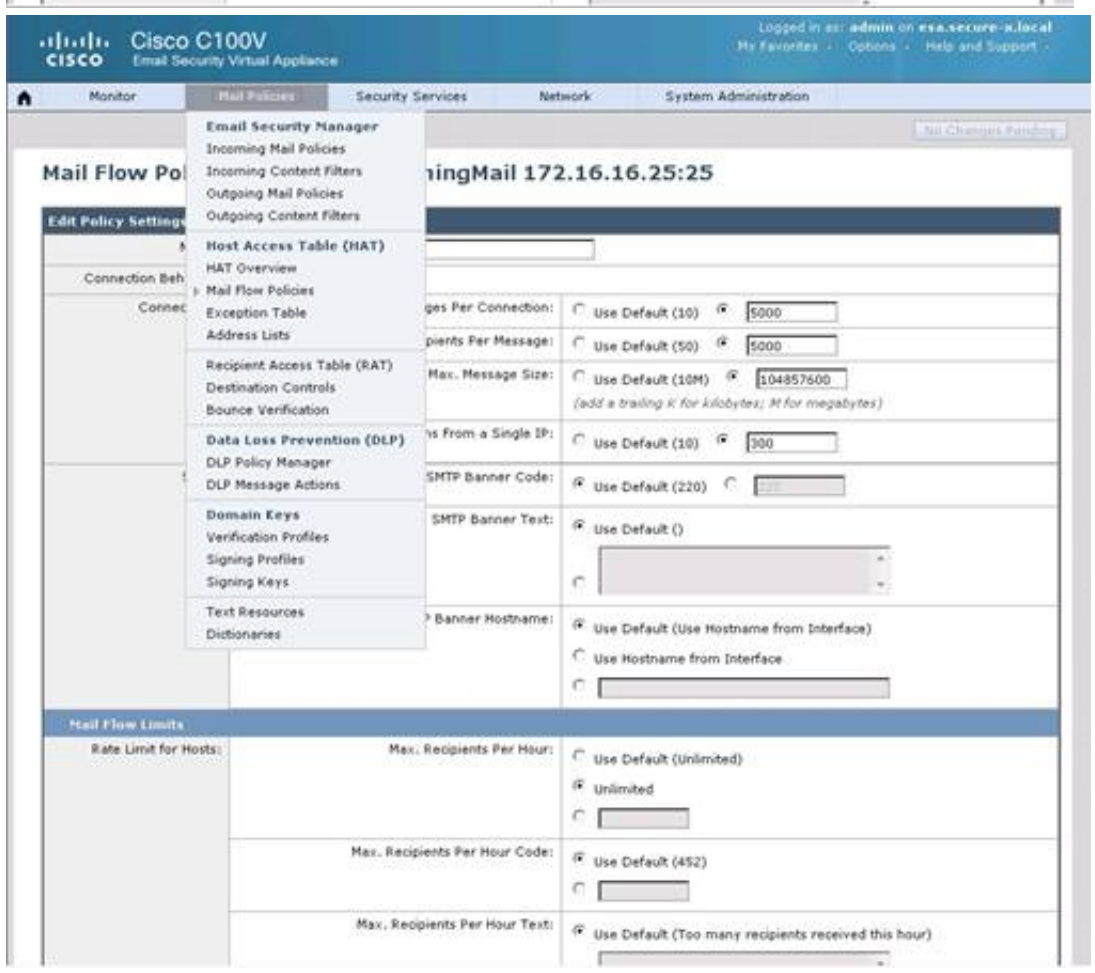

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
Sender Group: SUSPECTLIST - IncomingMail 172.16.16.25:25
Sender Group Settings
Name: SUSPECTLIST
Order: 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

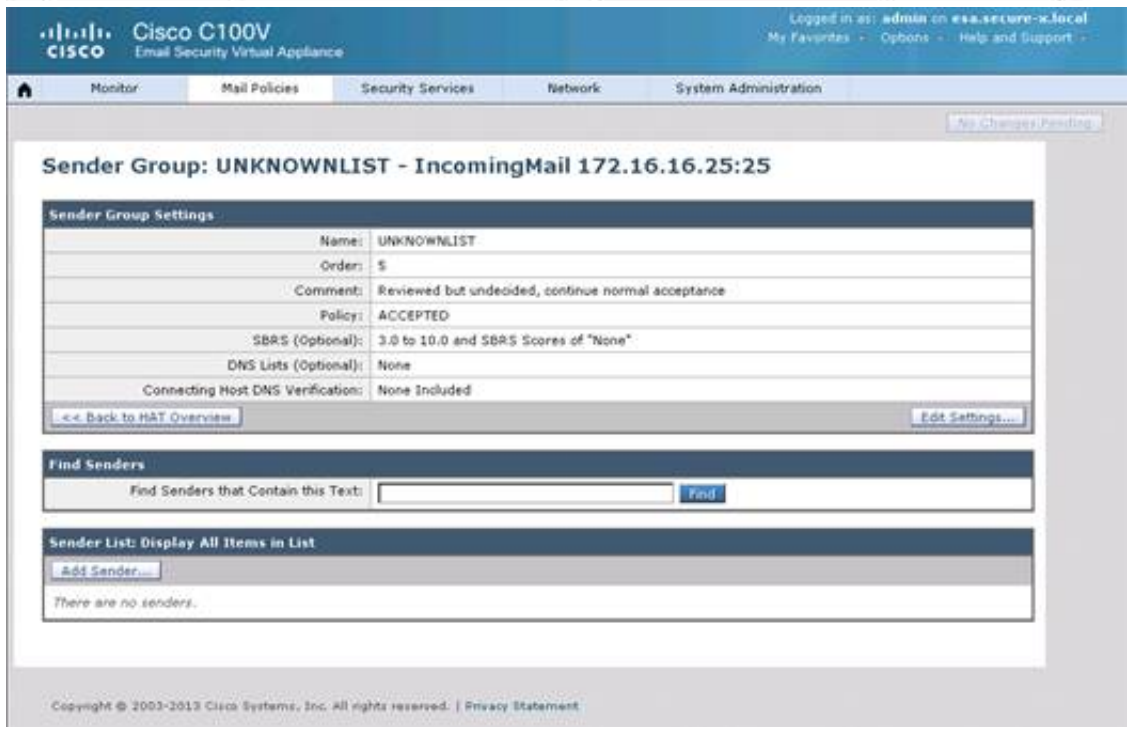

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail Policies
Outgoing 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
Sender Grou
omingMail 172.16.16.25:25
Edit Settings...
Find Senders
Find
Add Sender...
Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | Privacy Statement

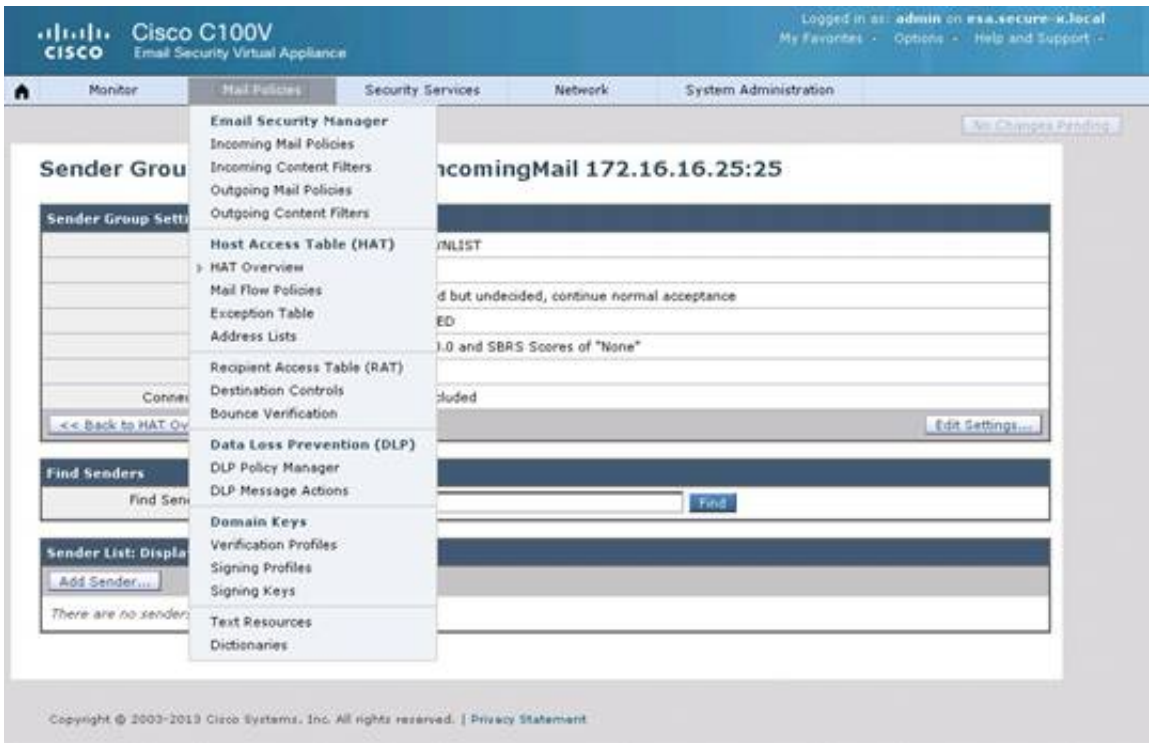

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Mail Flow Policy: THROTTLED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: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

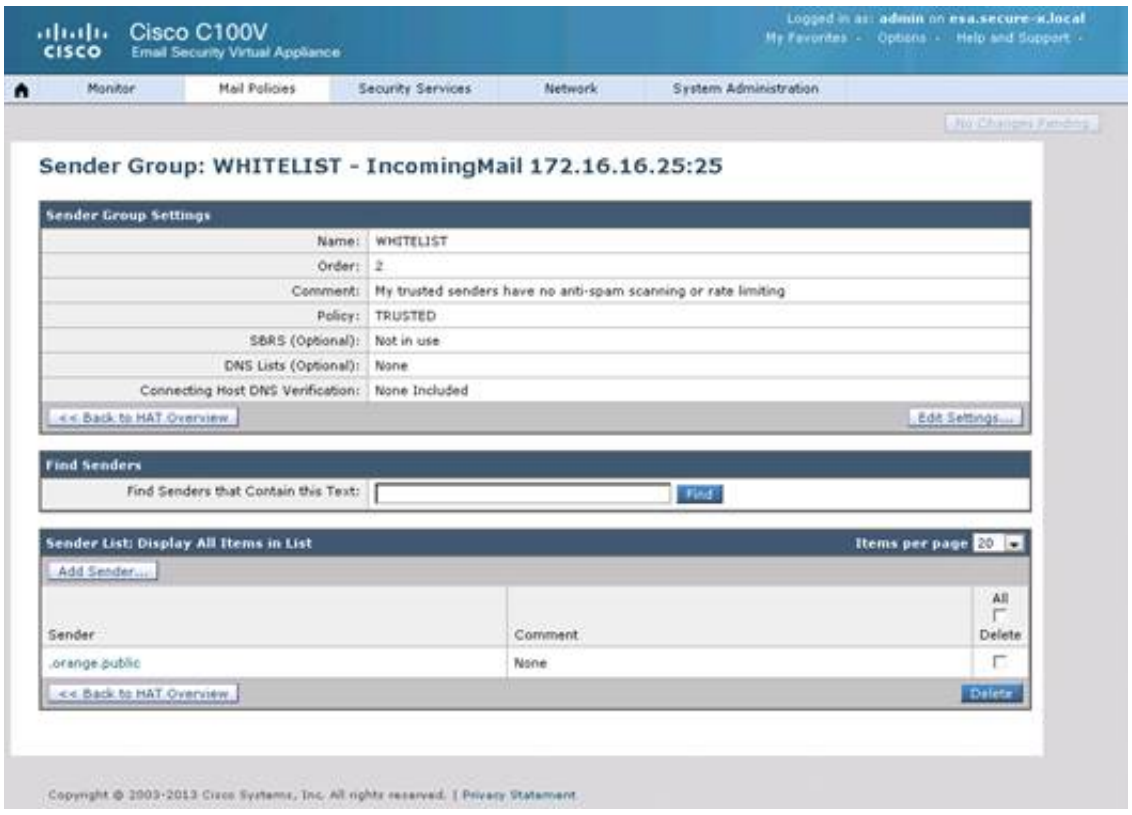

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites - Options - Help and Support -
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending
Email Security Manager
Incoming Mail Policies
Incoming Content Filters
Outgoing Mail 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 Po
omingMail 172.16.16.25:25
Edit Policy Settings
Connection Beh
Connec
ges Per Connection: Use Default (10) 1
pients Per Message: Use Default (50) 25
Max. Message Size: Use Default (10M) 10485760
(add a trailing k for kilobytes; M for megabytes)
s From a Single IP: Use Default (10) 1
SMTP Banner Code: Use Default (220)
SMTP Banner Text: Use Default ()
Banner Hostname: Use Default (Use Hostname from Interface)
Use Hostname from Interface
Mail Flow Limits
Rate Limit for Hosts:
Max. Recipients Per Hour: Use Default (Unlimited)
Unlimited
20
Max. Recipients Per Hour Code: Use Default (452)
Max. Recipients Per Hour Text: Use Default (Too many recipients received this hour)

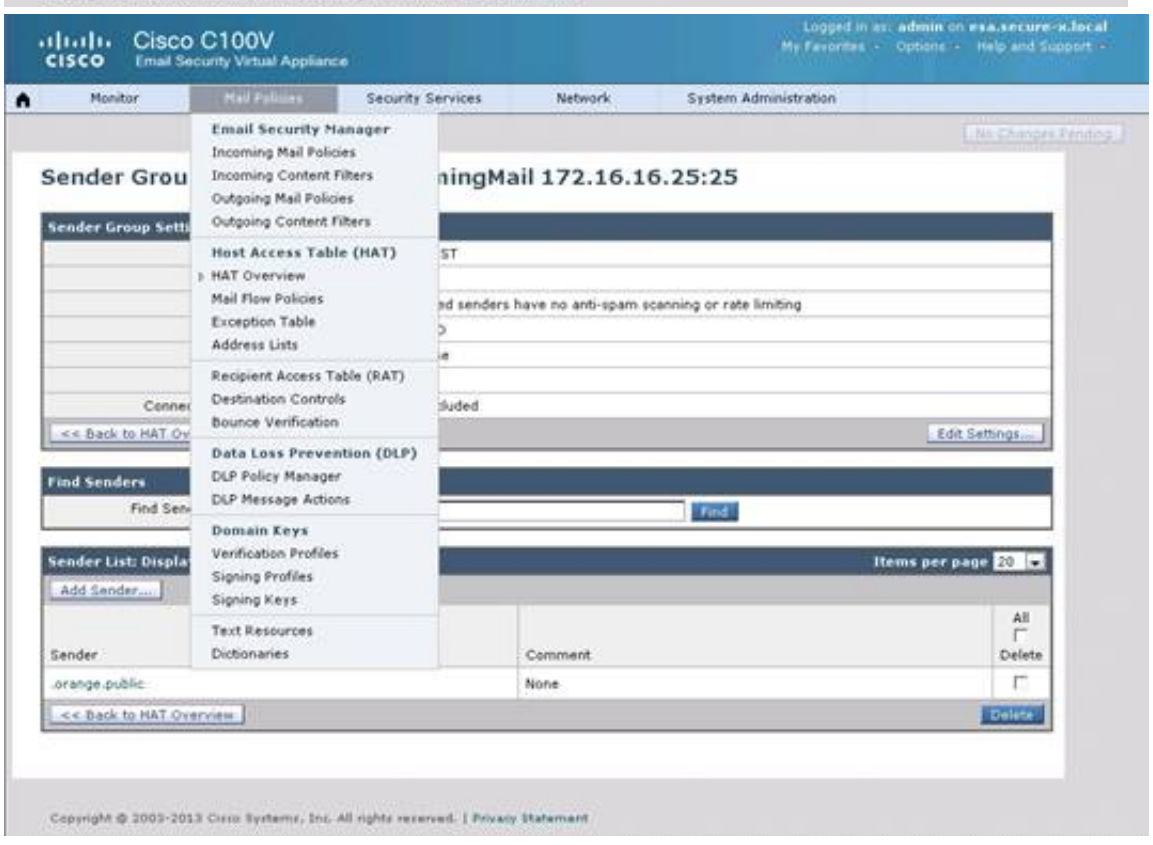

Cisco C100V
Email Security Virtual Appliance
Logged in as: admin on esa.secure-x.local
My Favorites · Options · Help and Support ·
Monitor
Mail Policies
Security Services
Network
System Administration
Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25
Edit Policy Settings
Name: TRUSTED
Connection 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
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 Policies
Edit Policy Settings
Mail Flow Limits
Use Default (Unlimited)
Unlimited
Use Default (452)
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: 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





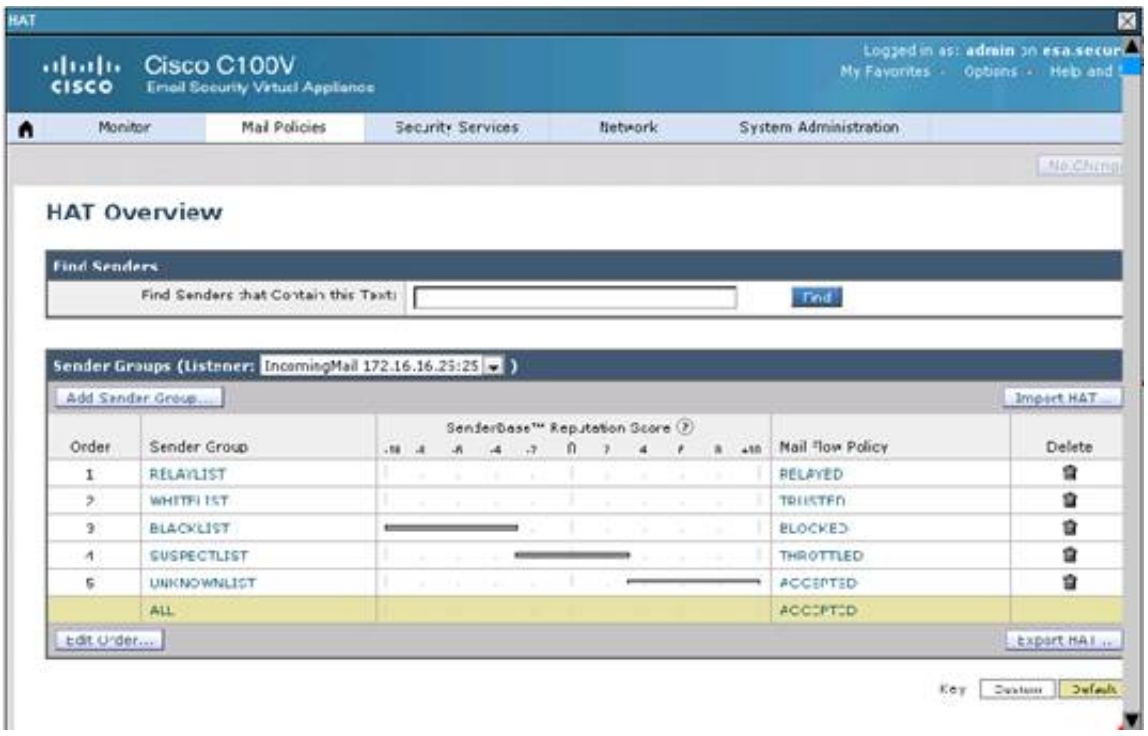


What is the maximum number of recipients per hour that the Cisco Email Security Appliance will accept from the green.public domain?

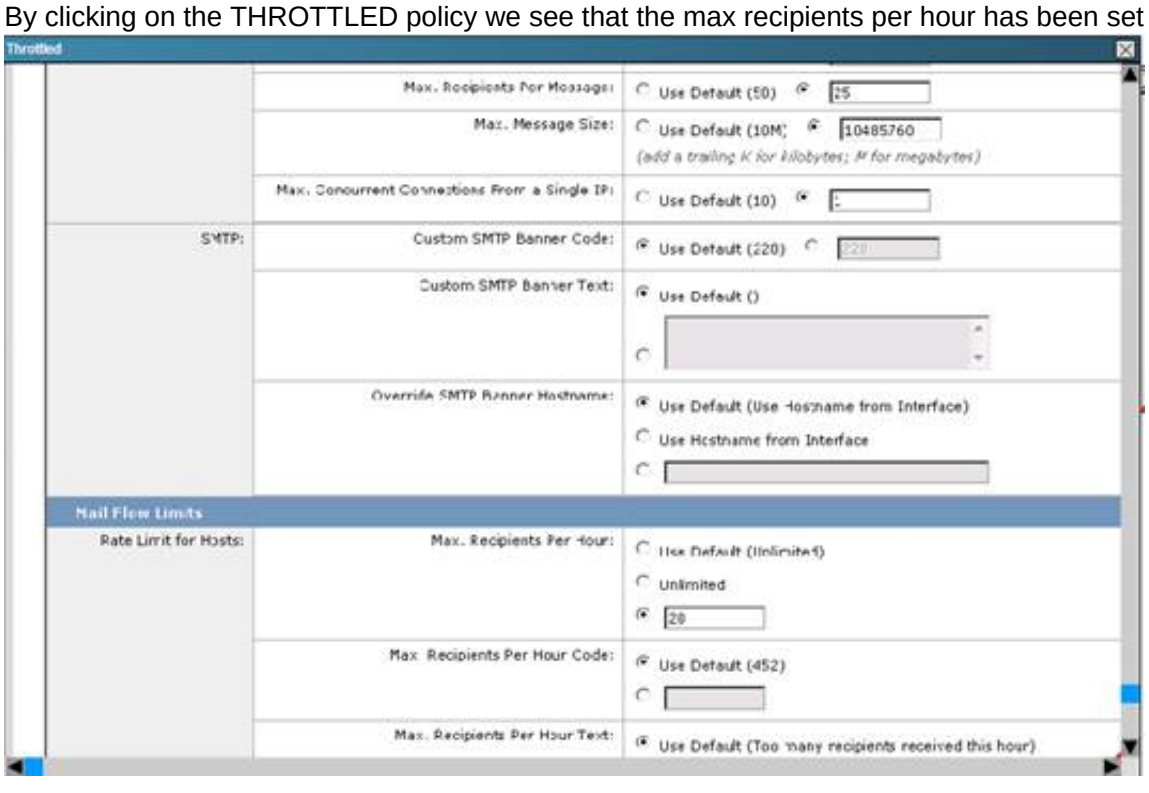
A. 1
B. 20
C. 25
D. 50
E. 5000
F. Unlimited

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: Capture



NEW QUESTION 684
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 688
Which option describes what occurs with asymmetric routing when an IPS normalization engine is enable?

A. It allows the return packets back to the source path.
B. It must see a valued SYN/ACK before it lets a flow pass, otherwise the IPS normalization engine assumes that is is encountering a fragmentation attack, and it drops the return packets
C. It must see a valid ACK/ACK before it lets a flow pass.
D. It must see a valid SYN/ACK before it lets a flow pass, otherwise the IPS normalization engine assumes that it is in encountering an evasion attack and drops the return packets.

Answer: D

NEW QUESTION 690
Which are two requirements for configuration a routed interface in a firepower SD840 sensor?

A. Virtual router
B. An interface
C. IP address
D. 10 G
E. 1 G

Answer: BC

NEW QUESTION 693
When attempting to tunnel FTP traffic through a stateful firewall that may be performing NAT or PAT, which type of VPN tunneling should be used to allow the VPN traffic through the stateful firewall?

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

Answer: B

NEW QUESTION 698
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 699
Which two Snort actions are available by default creating Snort rules, regardless of deployment mode? (Choose two)

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

Answer: AD

NEW QUESTION 704
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 707
Which two types of software can be installed on a FP-9300 appliance? (Choose two.)

A. Cisco Firepower Appliance
B. Cisco ASA
C. Cisco Firepower Management Center
D. Cisco Firepower Service
E. Cisco Firepower Threat Defense

Answer: CE

NEW QUESTION 708
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 710
Which action inspects packets in IPS?

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

Answer: AE

NEW QUESTION 715
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 720
Which characteristic is unique to a Cisco Web Security Virtual Appliance as compared to a physical appliance?

A. requires an additional
B. performance transparent redirection
C. supports VMware vMotion on VMware ESXi
D. supports SSL decryption

Answer: C

NEW QUESTION 722
Which standby protocol which works on NGIPS but not on CWS?

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

Answer: C

NEW QUESTION 724
By default, which access rule is applied inbound to the inside interface?

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

Answer: C

NEW QUESTION 725
Which Cisco Advanced Malware 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 727
An engineer is using policy trace tool to debug how a message is processed by the ESA. Which option is the expected behavior from the tool?

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

Answer: D

NEW QUESTION 728
Which option is a benefit of a Cisco Email Security Virtual Appliance as compared to a physical Cisco ESA?

A. simplifies the distribution of software updates
B. enables the allocation of additional resources
C. provides faster performance
D. provides an automated setup process

Answer: B

NEW QUESTION 730
An engineer is trying to configuring email encryption on Cisco ESA. Which technology could be used as a key server?

A. Cisco Registered Envelop Service
B. Local CA
C. Cisco Talos Services
D. Cisco ISE

Answer: B

NEW QUESTION 732
Which two variable types can be defined within Snort rules? (Choose two.)

A. srcvar
B. portvar
C. dstvar
D. ipvar
E. netvar

Answer: BD

NEW QUESTION 734
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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