

## Exam Questions 300-210

Implementing Cisco Threat Control Solutions (SITCS)

<https://www.2passeasy.com/dumps/300-210/>



#### NEW QUESTION 1

What is the function of the Web Proxy Auto Discovery protocol?

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

**Answer:** D

#### NEW QUESTION 2

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 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

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. Explicitly 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 6

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 7

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

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

**Answer:** D

#### 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 HTTP

**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 university policy has to allow open access to resources on the Internet for research, but internal workstations have been exposed to malware. Which AMP feature allows the engineering team to determine whether a file is installed on a selected few workstations?

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

**Answer:** A

#### NEW QUESTION 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 18

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 23

When creating an SSL policy on Cisco FirePOWER, which three options do you have

- A. do not decrypt
- B. trust
- C. allow
- D. block with reset
- E. block
- F. encrypt

**Answer:** ADE

**Explanation:** <http://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/200202-Configuration-of-an-S-Inspection-Polic.html>

### NEW QUESTION 28

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 31

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 33

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

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

Answer: D

### NEW QUESTION 36

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

The simulator will provide access to the graphical user interfaces of one Cisco ASA and one Cisco WSA that are participating in a WCCP service. Not all aspects of the GUIs are implemented in the simulator. The options that have been implemented are sufficient to determine the best answer to each of the questions that are presented.

Your task is to examine the details available in the simulated graphical user interfaces and select the best answer.



Adaptive  
Security Appliance



Web  
Security Appliance

ASA-C: DeviceSetup-interfaces

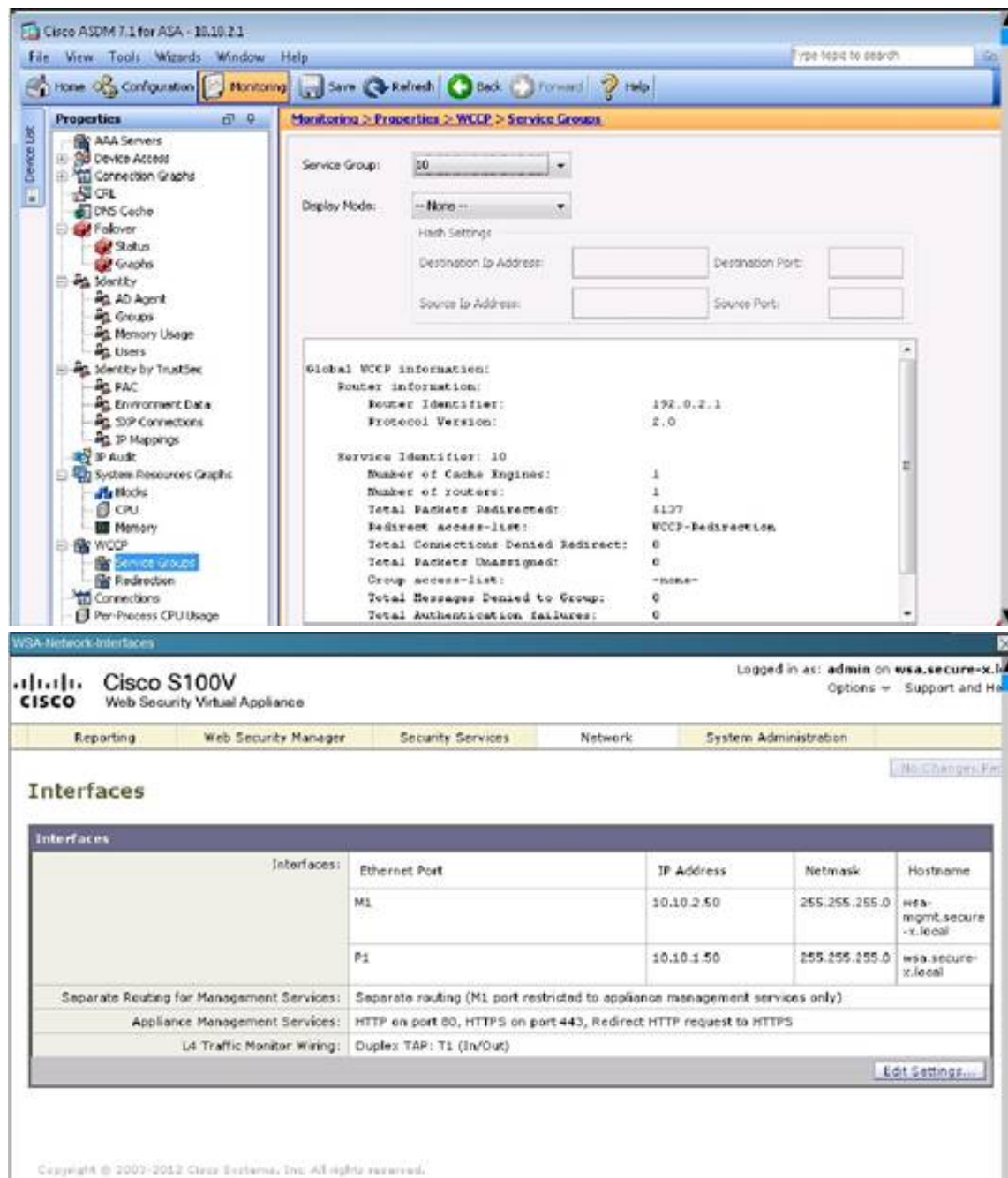
Cisco ASDM 7.1 for ASA - 18.10.3.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN	Gr
GigabitEthernet0/0	outside	Enabled		0/192.0.2.1	255.255.255.0	native	
GigabitEthernet0/1		Enabled				native	
GigabitEthernet0/1.4	inside	Enabled		100.10.10.1.1	255.255.255.0	vlan4	
GigabitEthernet0/1.250	Guest	Enabled		30.10.10.250.1	255.255.255.0	vlan250	
GigabitEthernet0/2	DMZ	Enabled		50.172.16.1.1	255.255.255.0	native	
GigabitEthernet0/3	Site-Ter...	Enabled		60.172.16.2.1	255.255.255.0	native	
GigabitEthernet0/4		Disabled				native	
GigabitEthernet0/5		Disabled				native	
Management0/0	manage...	Enabled		90.10.10.2.1	255.255.255.0	native	



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 41

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 45

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 47

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

Which two TCP ports can allow the Cisco Firepower Management Center to communication with FireAMP cloud for file disposition information? (Choose two.)

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

Answer: DE

Explanation: <http://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-private-cloud-virtual-appliance/118336-configure-fireamp-page=http://www.cisco.com/c/en/us/support/docs/security/sourcefire-amp-appliances/118121-technote-sourcefire-00.html>

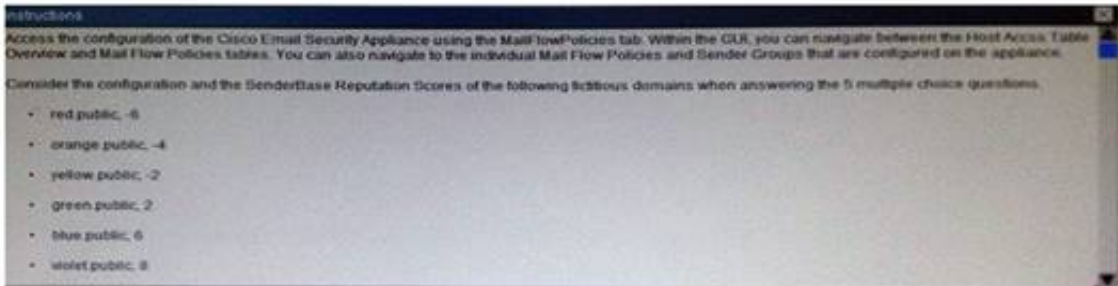
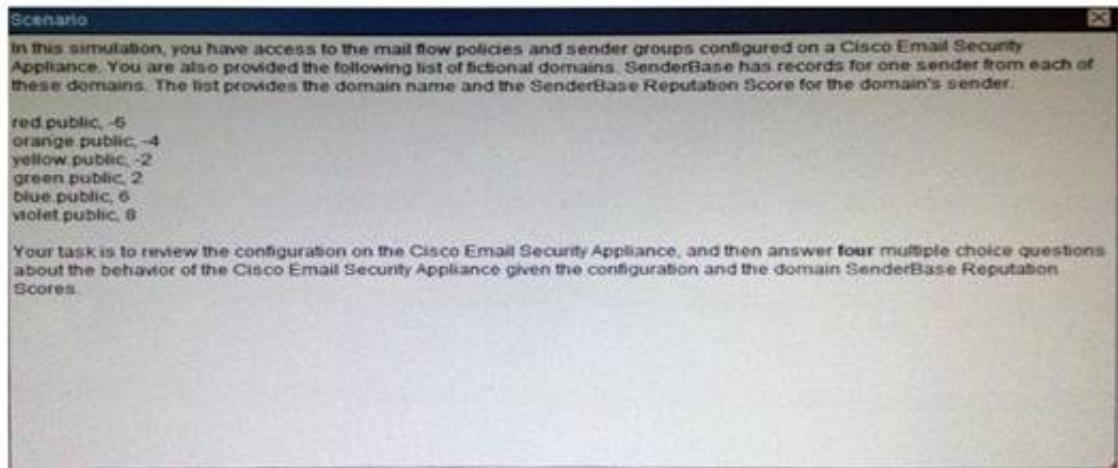
NEW QUESTION 52

Which Cisco Advanced Matware Protection event is generated when a file disposition changes because more information is gathered and evaluated about the file?

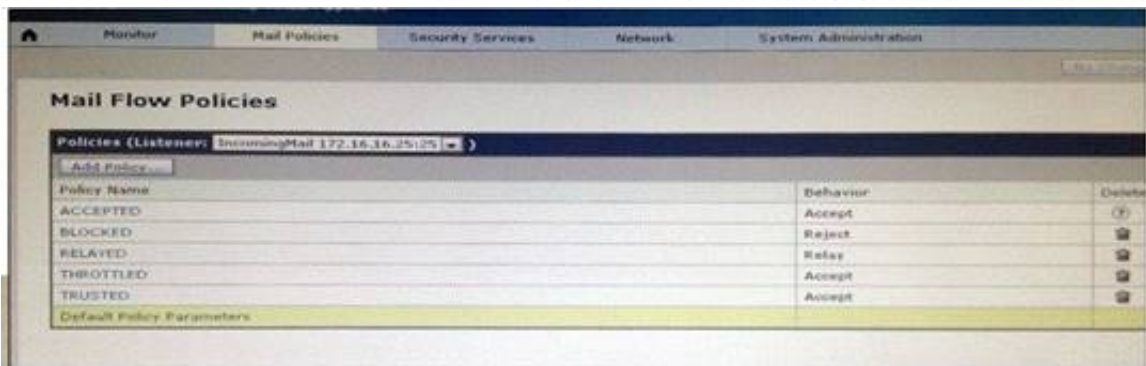
- A. quarantine event
- B. threat detected event
- C. policy update event
- D. retrospective event

Answer: D

NEW QUESTION 56



THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.  
Click on the Mail Flow Policies 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.



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 58

An engineering team has implemented Transparent User Identification on their Cisco Web Security Appliance. How is the User success authenticated?

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

**Answer:** A

#### NEW QUESTION 60

An engineer must architect an AMP private cloud deployment. What is the benefit of running in air-gaped mode?

- A. Internet connection is not required for disposition.
- B. Database sync time is reduced.
- C. Disposition queries are done on AMP appliances.
- D. A dedicated server is needed to run amp-sync.

**Answer:** D

#### NEW QUESTION 65

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 67

Which policy is used to capture host information on the Cisco Next Generation Intrusion Prevention System?

- A. network discovery
- B. correlation
- C. intrusion
- D. access control

**Answer:** C

#### NEW QUESTION 69

Which type of interface do you configure to receive traffic from a switch or tap, promiscuously, on a cisco firePOWER device?

- A. inline set
- B. transparent
- C. Routed
- D. Passive

**Answer:** D

#### NEW QUESTION 73

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 75

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 76

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.

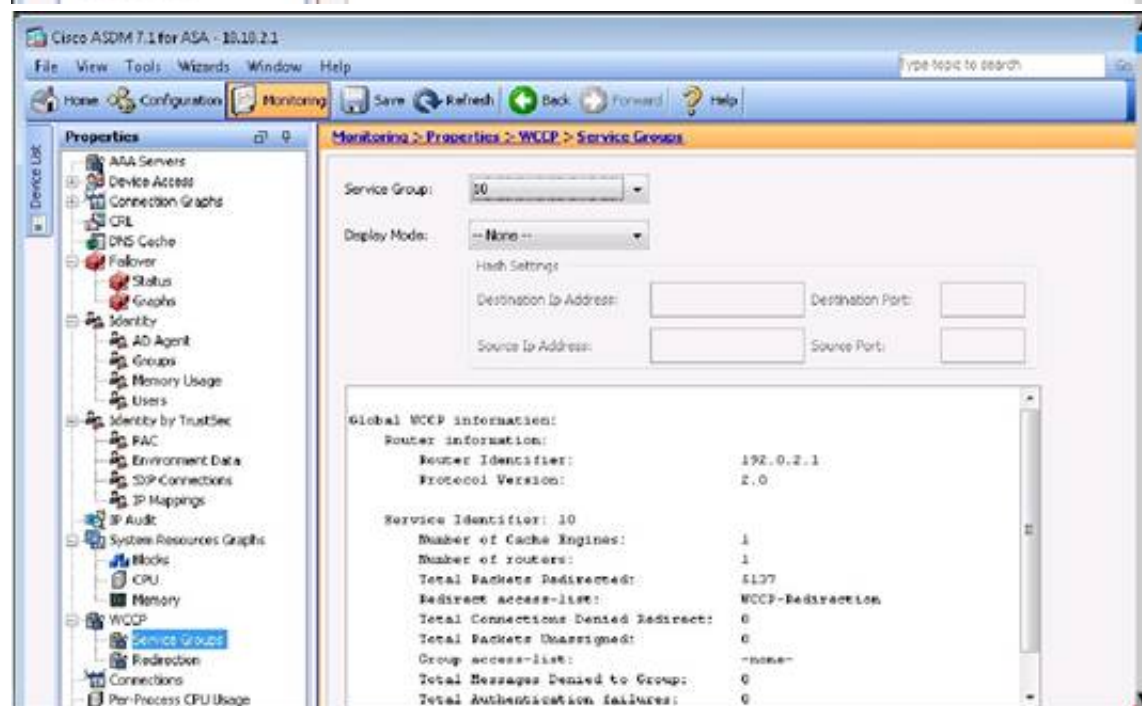
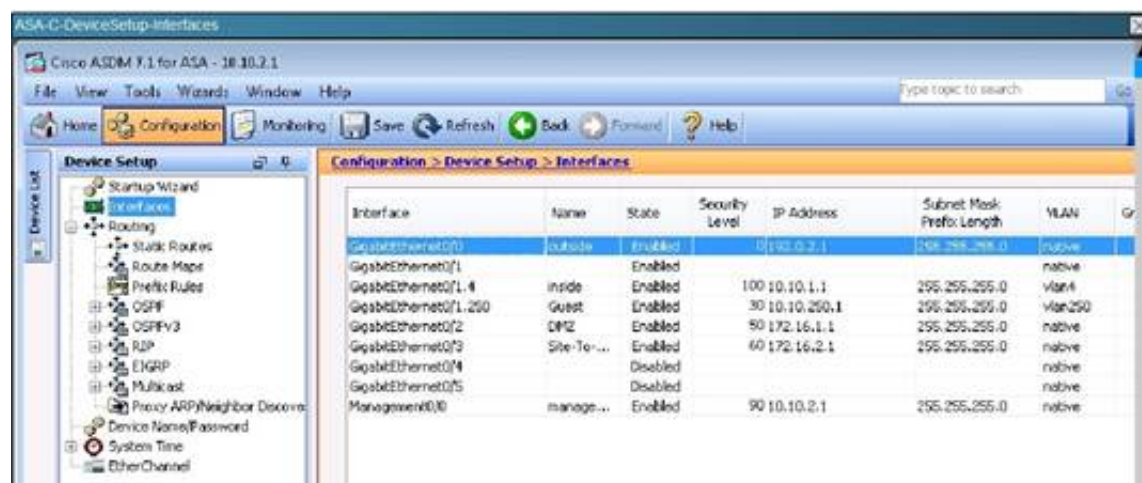
Your task is to examine the details available in the simulated graphical user interfaces and select the best answer.



Adaptive  
Security Appliance



Web  
Security Appliance





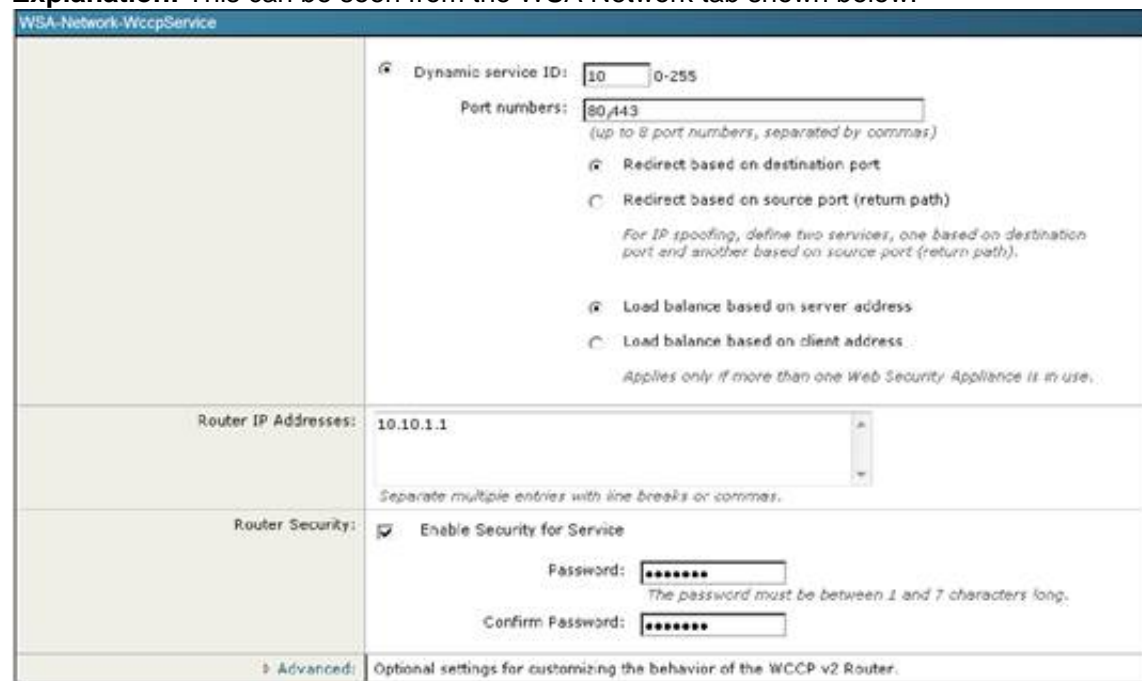


Between the Cisco ASA configuration and the Cisco WSA configuration, what is true with respect to redirected ports?

- 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 77

which two tasks can the network discovery feature perform? (choose two)

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

Answer: AC

## NEW QUESTION 82

An engineer is using the policy trace tool to troubleshoot a WSA. Which behavior is seen?

- A. A real client request and details of how it will be processed by the web proxy are developed.
- B. SOCKS policies are evaluated by the tool.
- C. External DLP policies are evaluated by the tool.
- D. the web proxy does not record the policy trace test requests in the access log when the tool is in use.

Answer: A

## NEW QUESTION 87

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

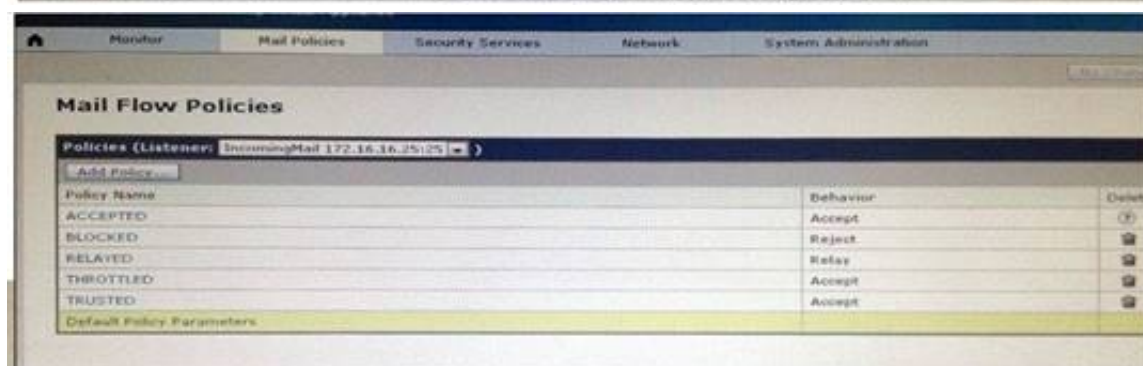
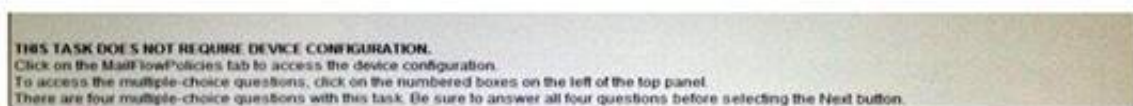
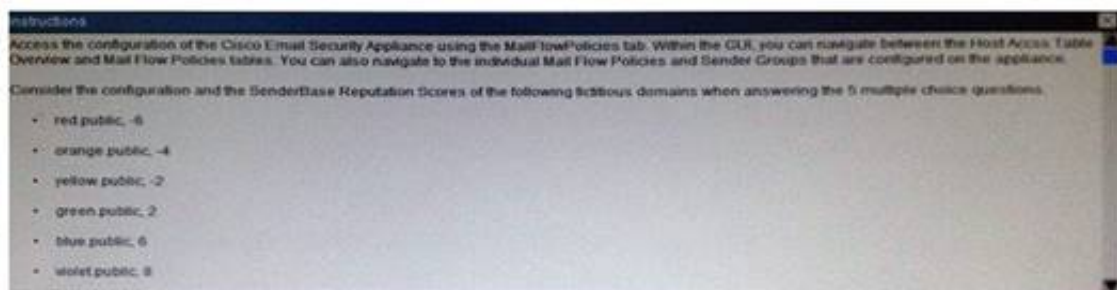
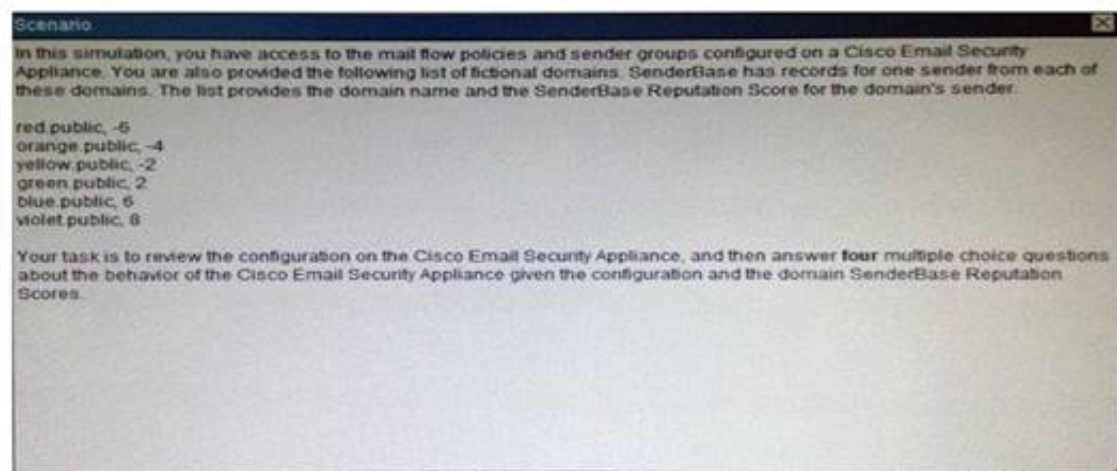
- A. pass
- B. trust
- C. monitor
- D. allow
- E. permit

F. inspect

**Answer:** BCD

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

## NEW QUESTION 90



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 92

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 94

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 98

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 99

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 101

Which two authentication options can be leveraged for directory integration with the Cisco Cloud Security ISR-G2 connector? (Choose Two)

- A. Kerberos
- B. NTLM
- C. LDAP
- D. OpenID
- E. SAML

**Answer:** BC

#### NEW QUESTION 105

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 109



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 114

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 116

An engineer wants to configure a method to verify the authenticity of emails on cisco ESA and noticed the sender policy framework. How can the SPF help in that task?

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

**Answer:** B

#### NEW QUESTION 117

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 119

Which three operating systems are supported with Cisco AMP for Endpoints? (Choose three.)

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

**Answer:** ACE

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

#### NEW QUESTION 121

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 126

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 129

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.

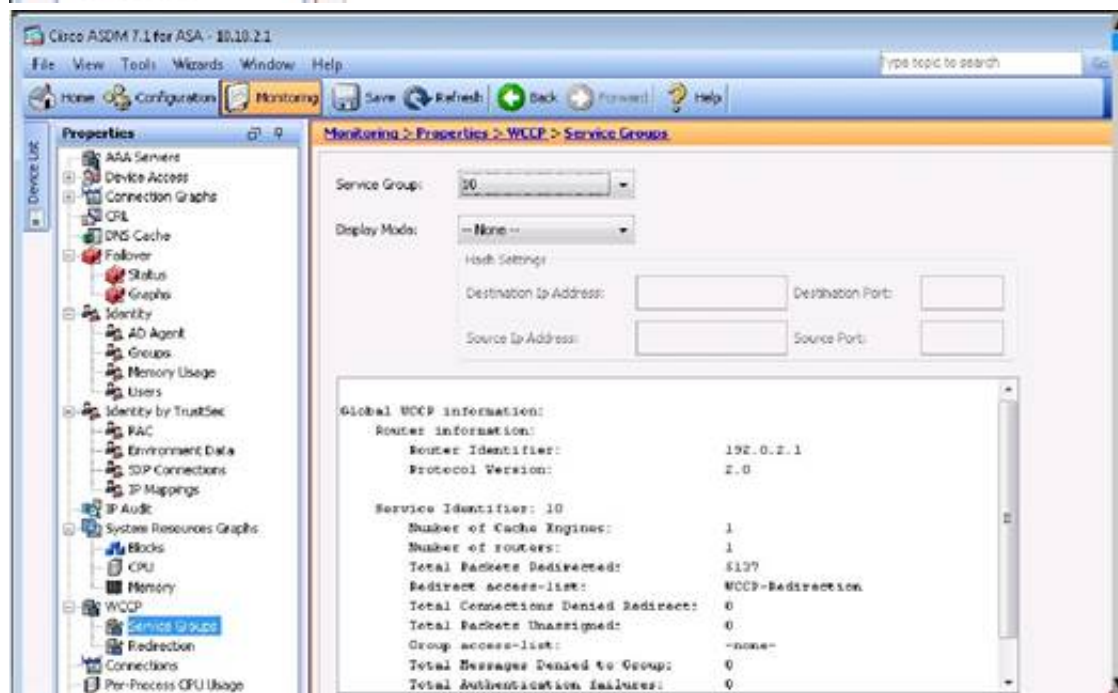
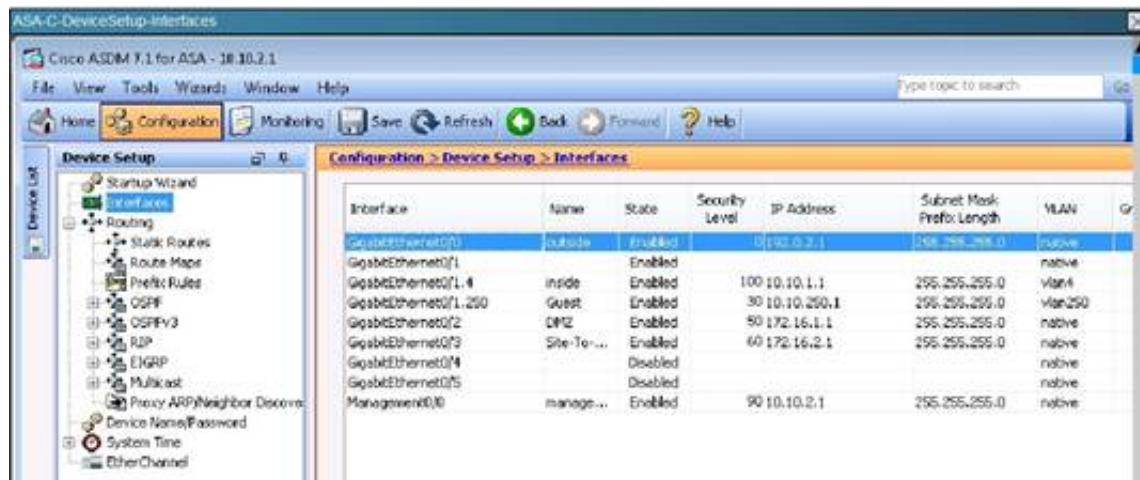




Adaptive  
Security Appliance



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 133

With Cisco FirePOWER Threat Defense software, which interface mode do you configure to passively receive traffic that passes the appliance?

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

**Answer:** C

#### NEW QUESTION 138

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 RIPv1
- 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 143

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 144

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 149

Which CLI command is used to generate firewall debug messages on a Cisco FirePOWER sensor?

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

**Answer:** C

#### NEW QUESTION 151

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 policy must you edit to make changes to the Snort preprocessors?

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

**Answer:** A

#### NEW QUESTION 155

Which feature of the Cisco Hybrid Email Security services enables you to create multiple email senders on a single Cisco ESA?

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

**Answer:** C

#### NEW QUESTION 156

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 158

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

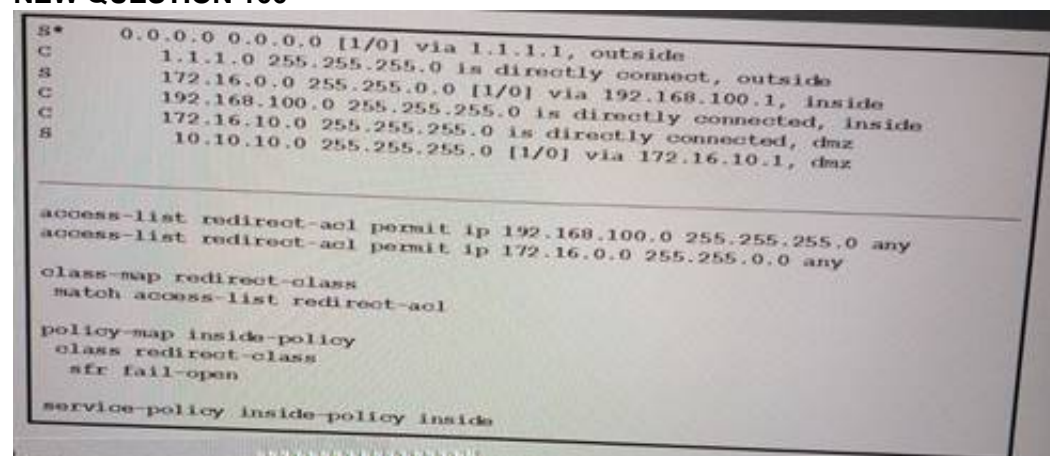
#### NEW QUESTION 162

Which two methods are used to deploy transparent mode traffic redirection? (Choose two)

- A. Microsoft GPO
- B. policy-based routing
- C. DHCP server
- D. PAC files
- E. Web Cache Communication Protocol

**Answer:** BE

#### NEW QUESTION 166



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 170

Which statement describes a traffic profile on a Cisco Next Generation Intrusion Prevention System?

- A. It allows traffic if it does not meet the profile.
- B. It defines a traffic baseline for traffic anomaly deduction.
- C. It inspects hosts that meet the profile with more intrusion rules.
- D. It blocks traffic if it does not meet the profile.

**Answer:** B

#### NEW QUESTION 171

An engineer wants to cluster an existing ESA physical appliance with an ESA virtual appliance. Which statement is true?

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

**Answer:** A

#### NEW QUESTION 176

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

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

**Answer:** C

#### NEW QUESTION 179

With Cisco FirePOWER Threat Defense software, which interface mode do you configure for an IPS deployment, where traffic passes through the appliance but does not require VLAN rewriting?

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

**Answer:** E

#### NEW QUESTION 184

Which type of server is required to communicate with a third-party DLP solution?

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

**Answer:** A

#### NEW QUESTION 185

When deploying Cisco FirePOWER appliances, which option must you configure to enable VLAN rewriting?

- A. hybrid interfaces
- B. virtual switch
- C. virtual router
- D. inline set

**Answer:** B

**Explanation:** [http://www.cisco.com/c/en/us/td/docs/security/firepower/hw/firepower\\_device/firepower\\_7k8k\\_device/deployment.html](http://www.cisco.com/c/en/us/td/docs/security/firepower/hw/firepower_device/firepower_7k8k_device/deployment.html)

#### NEW QUESTION 187



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 189

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 193

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

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

**Answer:** B

#### NEW QUESTION 196

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 201

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 204

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 207

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 212

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 215

In a Cisco FirePOWER intrusion 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 218

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 220

Which three options are valid event actions for a Cisco IPS? (Choose three.)

- A. deny-packet-inline
- B. deny-attack-reset
- C. produce-verbose-alert
- D. log-attacker-packets
- E. deny-packet-internal
- F. request-block-drop-connection

**Answer:** ACD

#### NEW QUESTION 225

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 228

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 229

Joe was asked to secure access to the Cisco Web Security Appliance to prevent unauthorized access. Which four steps should Joe implement to accomplish this goal? (Choose four.)

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

**Answer:** ACDE

#### NEW QUESTION 234

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

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

**Answer:** AC

#### NEW QUESTION 238

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 240

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 244

What are three best practices for a Cisco Intrusion Prevention System? (Choose three.)

- A. Checking for new signatures every 4 hours
- B. Checking for new signatures on a staggered schedule
- C. Automatically updating signature packs
- D. Manually updating signature packs
- E. Group tuning of signatures
- F. Single tuning of signatures

**Answer:** BCE

#### NEW QUESTION 248

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

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

**Answer:** A

#### NEW QUESTION 249

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 250

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 251

##### Instructions

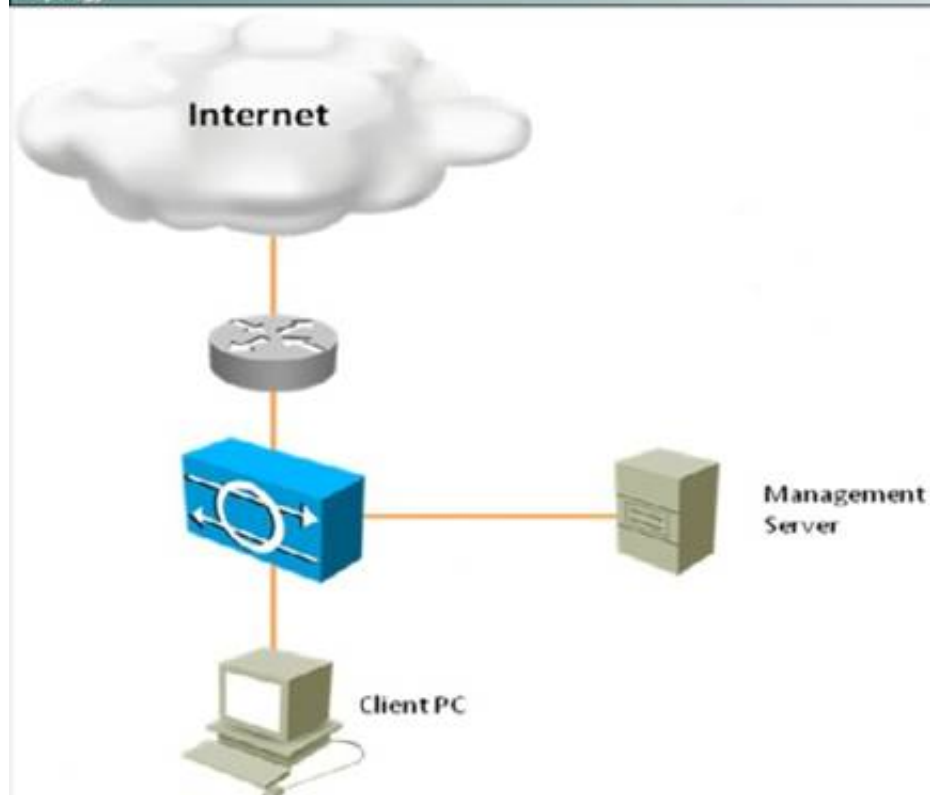
You can click the grey buttons at the bottom of this frame to view the different windows.

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 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 duration 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 252



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 255

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 260

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 265

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 266

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 267

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 268

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 270

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 274

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 278

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

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

**Answer:** D

#### NEW QUESTION 283

Which Cisco ESA command is used to edit the ciphers that are used for GUI access?

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

**Answer:** D

#### NEW QUESTION 285

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

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

**Answer:** D

#### NEW QUESTION 290

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 295

What are two benefits of using SPAN with promiscuous mode deployment? (Choose two.)

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

**Answer:** AD

#### NEW QUESTION 296

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 301

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 305

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 307

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 311

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 316

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 319

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

- A. sslconfig
- B. sslciphers
- C. tlsconfig
- D. certconfig

**Answer:** A

#### NEW QUESTION 324

Which antispam technology assumes that email from server A, which has a history of distributing spam, is more likely to be spam than email from server B, which does not have a history of distributing spam?

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

Answer: A

#### NEW QUESTION 328

**Instructions**

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

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

**Scenario**

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

**Topology**

The diagram shows a network topology. On the left, there is a 'High Value Segment' represented by two red circles connected to a vertical line. This segment is connected to the 'GigabitEthernet 0/0' interface of an 'IPS' device (represented by a blue box with a circular arrow). The 'IPS' device is also connected to the 'GigabitEthernet 0/1' interface, which is connected to the 'Internet' (represented by a cloud).

**ASDM**

File View Help

Home Configuration Monitoring Back Forward Refresh Help

**Configuration > Interfaces > Summary**

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

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

Answer:

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

**ASDM**

Monitoring Back Forward Refresh Help

**Configuration > Interfaces > Interfaces**

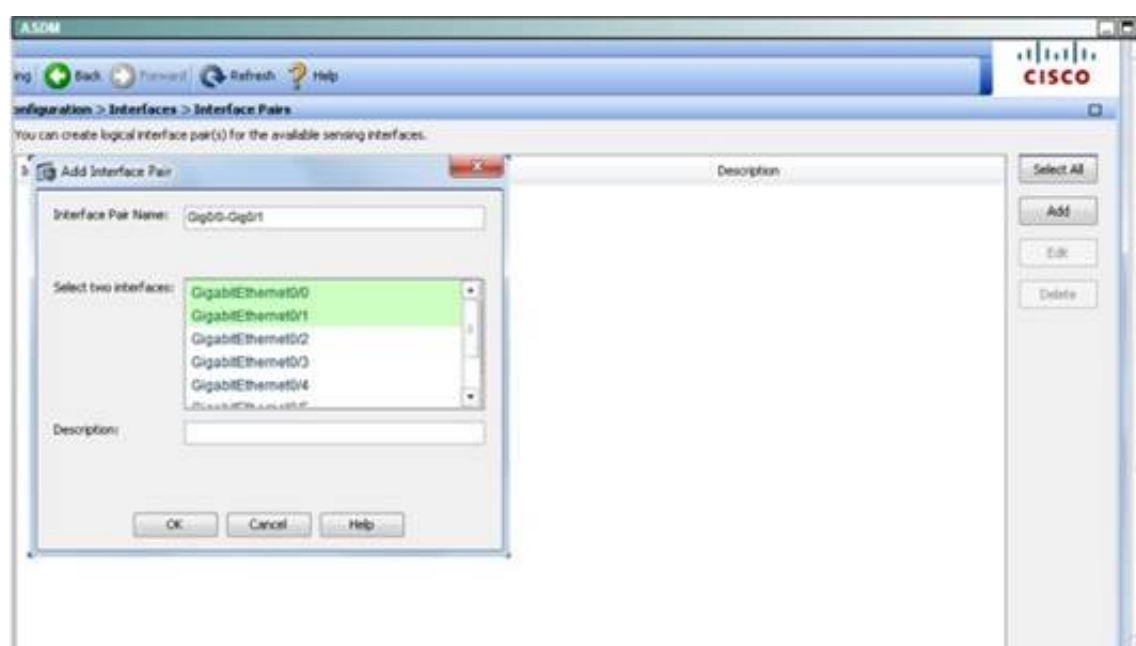
A sensing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enable/disable the available sensing interfaces by selecting the row(s) and clicking Enable or Disable.

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

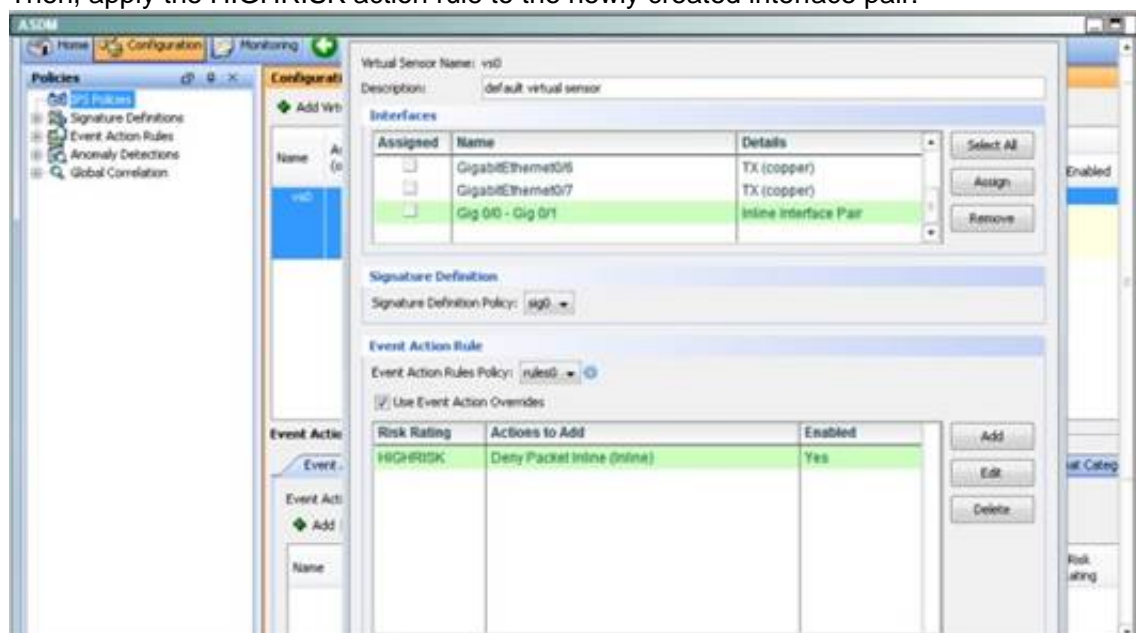
Select All Edit Enable Disable

Second, create the pair under the "interface pairs" tab.

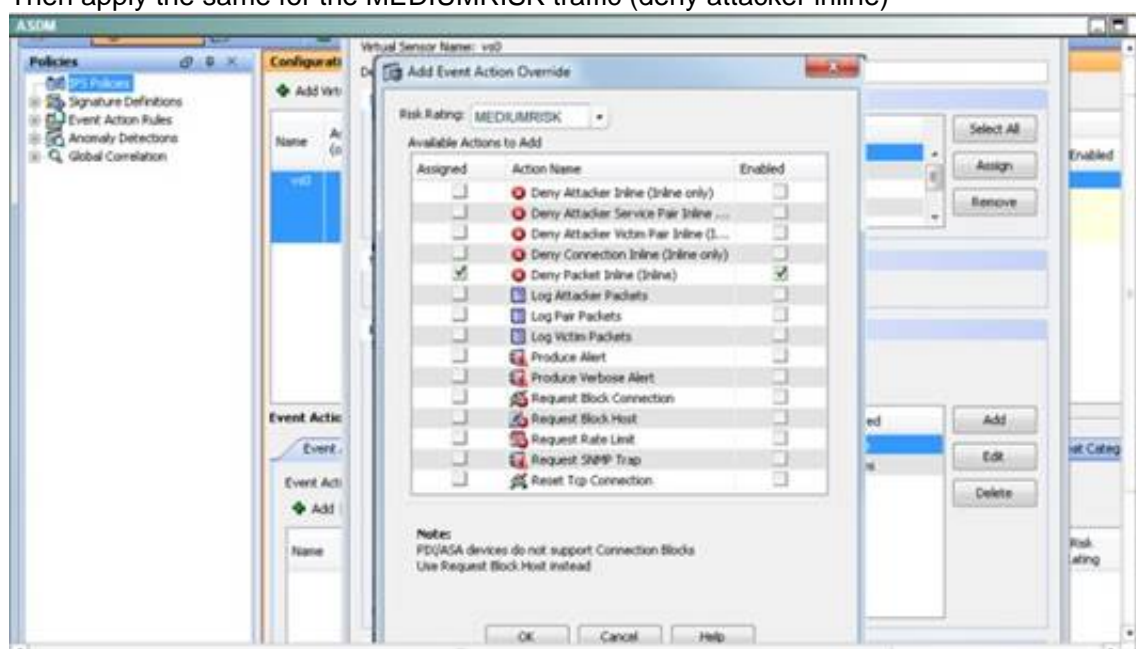




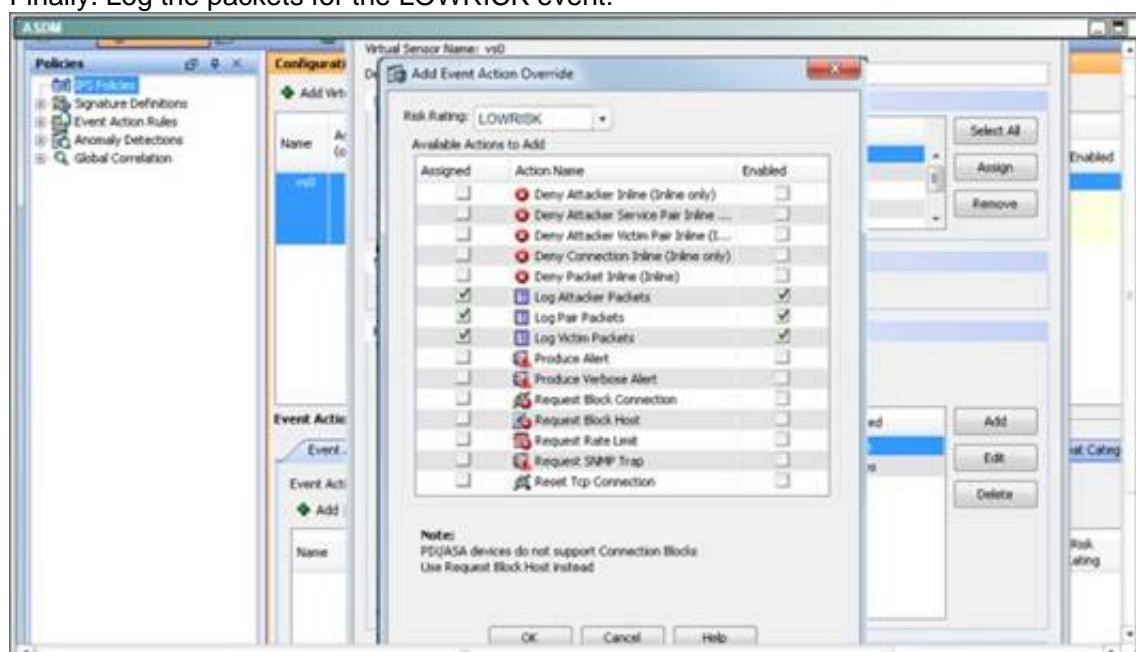
Then, apply the HIGHRISK action rule to the newly created interface pair:



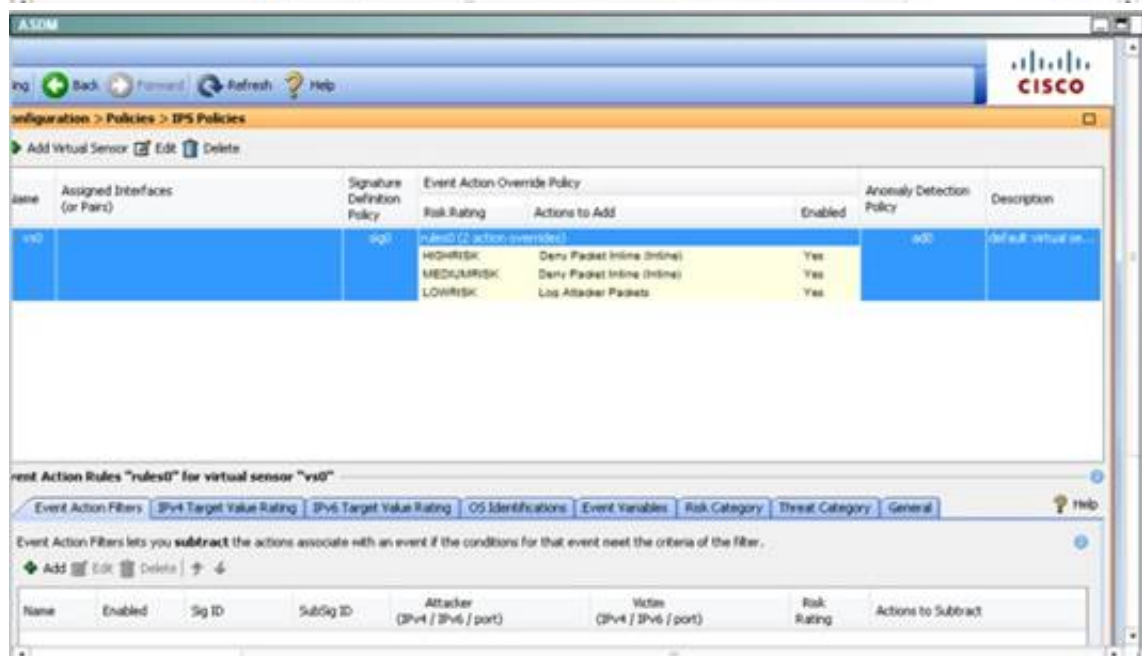
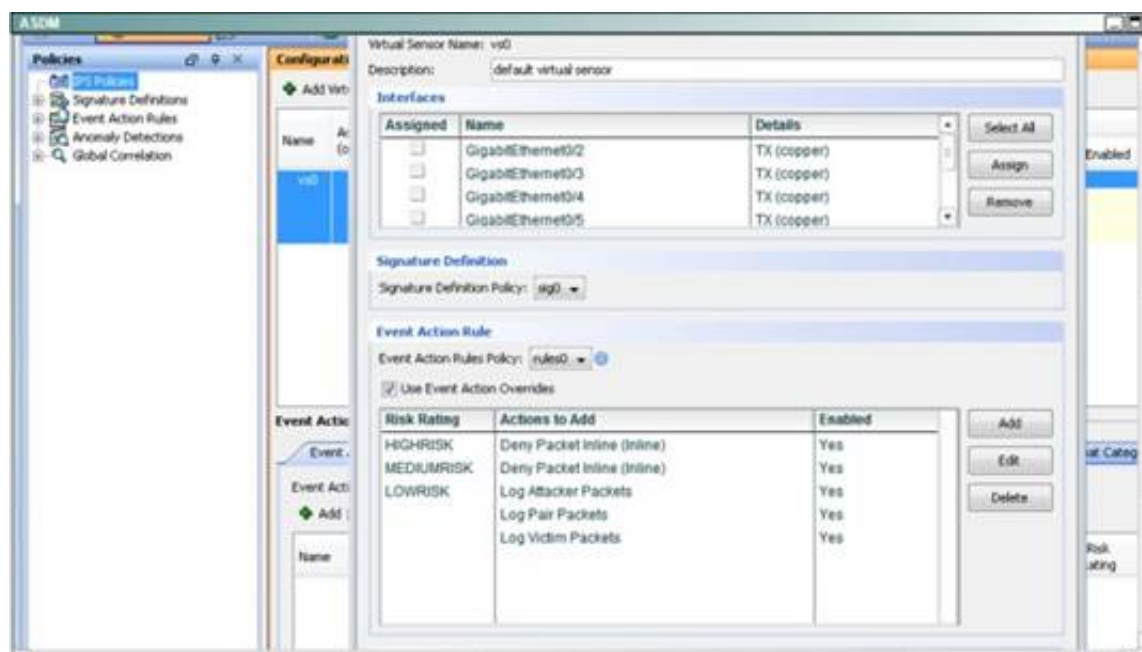
Then apply the same for the MEDIUMRISK traffic (deny attacker inline)



Finally. Log the packets for the LOWRISK event:



When done it should look like this:



## NEW QUESTION 329

### Instructions

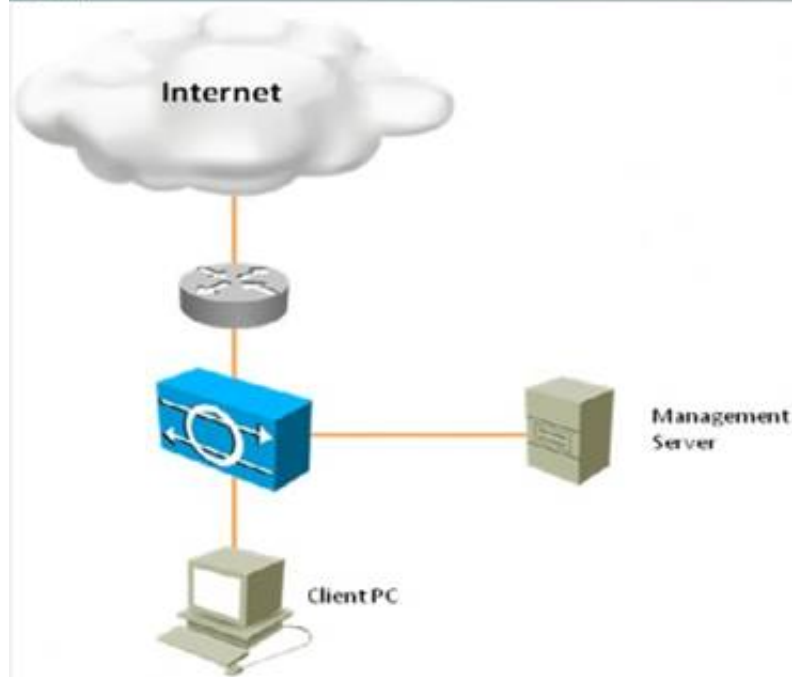
You can click the grey buttons at the bottom of this frame to view the different windows.

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 signature definition is virtual sensor 0 assigned to use?

- A. rules0
- B. vs0
- C. sig0
- D. ad0
- E. ad1
- F. sig1

**Answer: C**

**Explanation:** This is the default signature.

You can create multiple security policies and apply them to individual virtual sensors. A security policy is made up of a signature definition policy, an event action rules policy, and an anomaly detection policy. Cisco

IPS contains a default signature definition policy called sig0, a default event action rules policy called rules0, and a default anomaly detection policy called ad0.

You can assign the default policies to a virtual sensor or you can create new policies.

### NEW QUESTION 334

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.
```

#	Recipient Host	Active Recip.	Conn. Out	Deliv. Recip.	Soft Bounced	Hard 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
6	*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 Cisco ESACLI command generated the output?

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

**Answer: B**

### NEW QUESTION 335

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 339

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 341

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.

```

#	Recipient Host	Active Recip.	Conn. Out	Deliv. Recip.	Soft Bounced	Hard 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 342

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 347

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 348

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

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

**Answer:** BDF

#### NEW QUESTION 350

Within Cisco IPS anomaly detection, 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 355

### Instructions

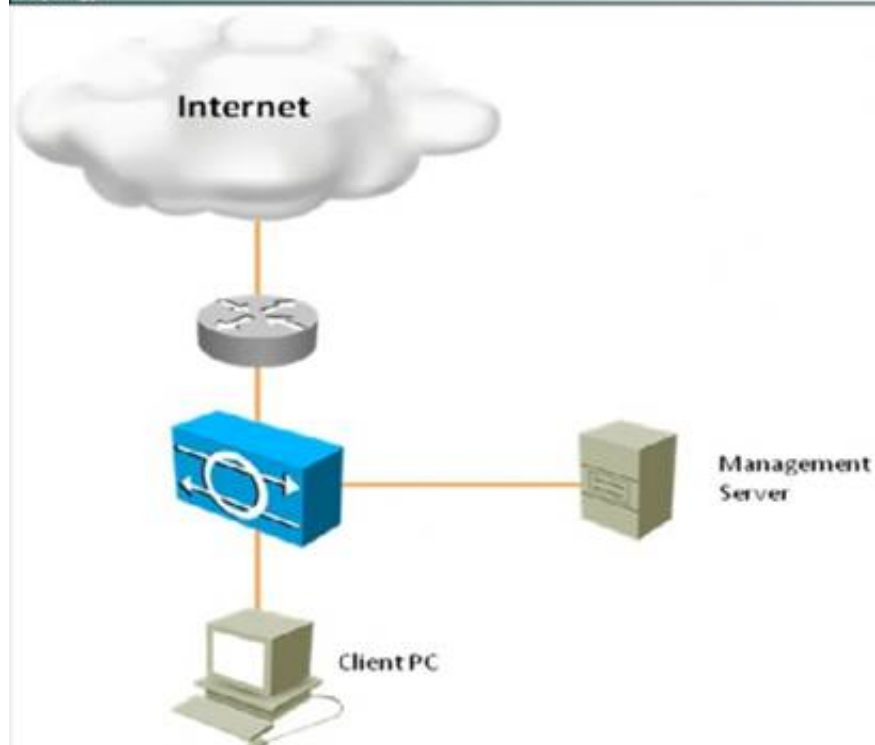
You can click the grey buttons at the bottom of this frame to view the different windows.

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

### Scenario

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

### Topology



What is the status of OS Identification?

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

**Answer: D**

### Explanation: Understanding Passive OS Fingerprinting

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

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

Passive OS fingerprinting consists of three components:

#### •Passive OS learning

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

#### •User-configurable OS identification

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

#### •Computation of attack relevance rating and risk rating.

## NEW QUESTION 357

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 359

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 362

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 366

##### Instructions

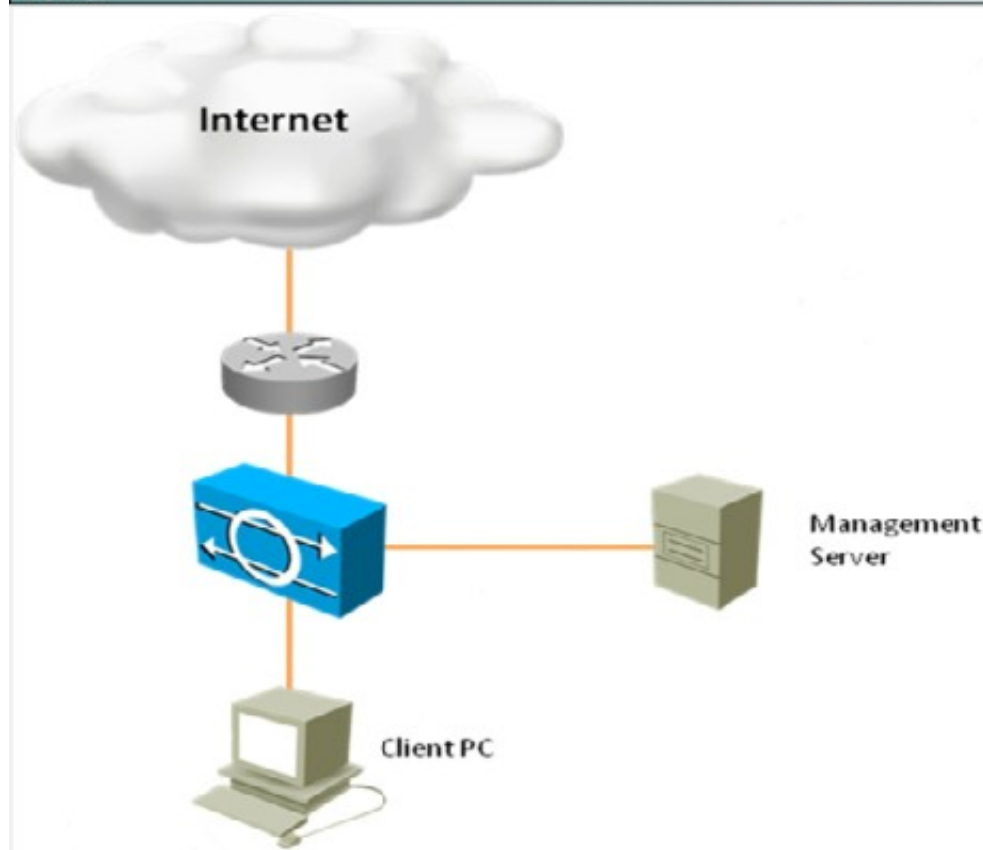
You can click the grey buttons at the bottom of this frame to view the different windows.

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

##### Scenario

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

##### Topology



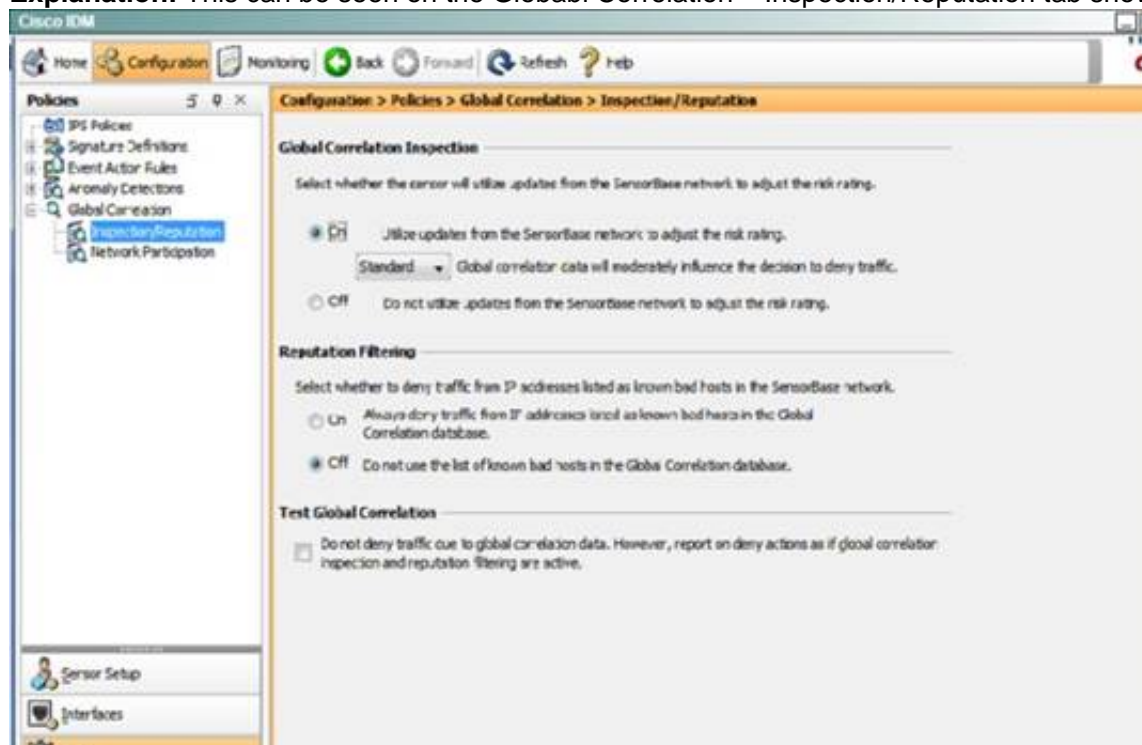


What action will the sensor take regarding IP addresses listed as known bad hosts in the Cisco SensorBase network?

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

**Answer: D**

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



#### NEW QUESTION 367

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 370

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 373

At which value do custom signatures begin?

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

**Answer:** D

#### NEW QUESTION 374

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

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

**Answer:** A

#### NEW QUESTION 376

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 377

What is the correct deployment for an IPS appliance in a network where traffic identified as threat traffic should be blocked and all traffic is blocked if the IPS fails?

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

**Answer:** B

#### NEW QUESTION 382

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 383

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 385

Which Cisco technology is a modular security service that combines a stateful inspection firewall with next-generation application awareness, providing near real-time threat protection?

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

**Answer:**



B

#### NEW QUESTION 386

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 388

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 393

Which option describes a customer benefit of the Cisco Security IntelliShield Alert Manager?

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

**Answer:** C

#### NEW QUESTION 398

What is a primary difference between the web security features of the Cisco WSA and the Cisco ASA NGFW?

- A. Cisco WSA provides URL filtering, while Cisco ASA NGFW does not.
- B. Cisco ASA NGFW provides caching services, while Cisco WSA does not.
- C. Cisco WSA provides web reputation filtering, while Cisco ASA NGFW does not.
- D. Cisco ASA NGFW provides application visibility and control on all ports, while Cisco WSA does not.

**Answer:** D

#### NEW QUESTION 399

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 403

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 406

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

- A. The firewall allows 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 408

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 409

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 413

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 416

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

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

**Answer:** B

#### NEW QUESTION 418

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 419

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 423

What does the anomaly detection Cisco IOS IPS component detect?

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

Answer: B

#### NEW QUESTION 425

Which statement about Cisco IPS Manager Express is true?

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

Answer: B

#### NEW QUESTION 430

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

web portal	tracking vulnerability remediation
back-end intelligence engine	customer interface
threat outbreak alert	past threat and vulnerability information
built-in workflow system	based on the CVSS rating system
historical database	threat data collection
vulnerability alerts	threat data regarding threats

Answer:

Explanation:

web portal	built-in workflow system
back-end intelligence engine	web portal
threat outbreak alert	historical database
built-in workflow system	vulnerability alerts
historical database	back-end intelligence engine
vulnerability alerts	threat outbreak alert

#### NEW QUESTION 433

Refer to the exhibit.

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

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

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

Answer: AB

#### NEW QUESTION 434

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 436

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 440

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

#### NEW QUESTION 445

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 does not contain the DNS host.
- C. An explicit 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 450

Which Cisco Web Security Appliance feature enables the appliance to block suspicious traffic on all of its ports and IP addresses?

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

**Answer:** A

#### NEW QUESTION 453

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 454



**Scenario**

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

V120 red.public, -6  
orange.public, -4  
yellow.public, -2  
green.public, 2  
blue.public, 6  
violet.public, 8

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

**Instructions**

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

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

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

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

**Cisco C100V Email Security Virtual Appliance**

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

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policies

Policies (Listener: IncomingMail 172.16.16.25:25 )

Add Policy...

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

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

**Cisco C100V Email Security Virtual Appliance**

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

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### HAT Overview

Find Senders

Find Senders that Contain this Text: Find

Sender Groups (Listener: IncomingMail 172.16.16.25:25 )

Add Sender Group...

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

Import HAT... Export HAT...

Key: Custom Default

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

**Cisco C100V Email Security Virtual Appliance**

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

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### HAT Overview

Find Senders

Find Senders that Contain this Text: Find

Sender Groups (Listener: IncomingMail 172.16.16.25:25 )

Add Sender Group...

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

Import HAT... Export HAT...

Key: Custom Default

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policy**

Policies (Listeners):

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

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

Behavior	Delete
Accept	
Reject	
Relay	
Accept	

Copyright © 2003-2010 Cisco Systems, Inc. All rights reserved. Cisco Confidential

**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:

Connection Behavior:

Connections:

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

SMTP:

- Custom SMTP Banner Code: ☒ Use Default (220)
- Custom SMTP Banner Text: ☒ Use Default ()
- Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts:

- Max. Recipients Per Hour: ☒ Use Default (Unlimited) ☐ Unlimited
- Max. Recipients Per Hour Code: ☒ Use Default (452)
- Max. Recipients Per Hour Text: ☒ Use Default (Too many recipients received this hour)

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policy: IncomingMail 172.16.16.25:25**

**Edit Policy Settings**

Name:

Connection Behavior:

Connections:

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

SMTP:

- Custom SMTP Banner Code: ☒ Use Default (220)
- Custom SMTP Banner Text: ☒ Use Default ()
- Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts:

- Max. Recipients Per Hour: ☒ Use Default (Unlimited) ☐ Unlimited
- Max. Recipients Per Hour Code: ☒ Use Default (452)
- Max. Recipients Per Hour Text: ☒ Use Default (Too many recipients received this hour)



**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Sender Group: BLACKLIST - IncomingMail 172.16.16.25:25

Sender Group Settings	
Name:	BLACKLIST
Order:	3
Comment:	Spammers are rejected
Policy:	BLOCKED
SBR/S (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

No Changes Pending

### Sender Group: BLACKLIST - IncomingMail 172.16.16.25:25

Sender Group Settings	
Name:	BLACKLIST
Order:	3
Comment:	Spammers are rejected
Policy:	BLOCKED
SBR/S (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

No Changes Pending

### Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policy: IncomingMail 172.16.16.25:25**

**Edit Policy Settings**

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

Connections

Max. Messages Per Connection: ☒ Use Default (10)

Max. Recipients Per Message: ☒ Use Default (50)

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

Max. Concurrent Connections From a Single IP: ☒ Use Default (10)

SMTP Banner Code: ☒ Use Default (554)

SMTP Banner Text: ☐ Use Default ()  
☒ Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure

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-a.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-a.local  
 My Favorites - Options - Help and Support

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policy: IncomingMail 172.16.16.25:25**

**Edit Policy Settings**

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

Connections

Max. Messages Per Connection: ☒ Use Default (10)

Max. Recipients Per Message: ☒ Use Default (50)

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

Max. Concurrent Connections From a Single IP: ☒ Use Default (10)

SMTP Banner Code: ☒ Use Default (220)

SMTP Banner Text: ☒ Use Default ()

Banner Hostname: ☒ Use Default (Use Hostname from Interface)  
☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts: Max. Recipients Per Hour: ☒ Use Default (Unlimited)  
☐ Unlimited

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

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



**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

[No Changes Pending](#)

### Sender Group: 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
<a href="#">&lt;&lt; Back to HAT Overview</a> <a href="#">Edit Settings...</a>	

**Find Senders**

Find Senders that Contain this Text:  [Find](#)

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

[Add Sender...](#)

Sender	Comment	All	Delete
hq-mail.maroon.public	None	<input type="checkbox"/>	<input type="checkbox"/>

[<< Back to HAT Overview](#) [Delete](#)

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

[No Changes Pending](#)

### Sender Group: RELAYLIST - IncomingMail 172.16.16.25:25

Sender Group Settings	
Name:	RELAYLIST
Order:	1
Comment:	Only select hosts can relay from this box
Policy:	RELAYED
SBRs (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included
<a href="#">&lt;&lt; Back to HAT Overview</a> <a href="#">Edit Settings...</a>	

**Find Senders**

Find Senders that Contain this Text:  [Find](#)

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

[Add Sender...](#)

Sender	Comment	All	Delete
hq-mail.maroon.public	None	<input type="checkbox"/>	<input type="checkbox"/>

[<< Back to HAT Overview](#) [Delete](#)

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

[No Changes Pending](#)

### Sender Group: 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
<a href="#">&lt;&lt; Back to HAT Overview</a> <a href="#">Edit Settings...</a>	

**Find Senders**

Find Senders that Contain this Text:  [Find](#)

**Sender List: Display All Items in List**

[Add Sender...](#)

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Sender Group**

Sender Group Settings

Find Senders

Sender List: Display

Add Sender...

There are no senders

**Email Security Manager**

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

**IncomingMail 172.16.16.25:25**

TLIST

us senders are throttled

ED

ED

cluded

Edit Settings...

Find

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

**Cisco C100V**  
Email Security Virtual Appliance

Logged in as: admin on esa.secure-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) 220
- Custom SMTP Banner Text: Use Default ()
- Override SMTP Banner Hostname: Use Default (Use Hostname from Interface)

Mail Flow Limits

Rate Limit for Hosts:

- Max. Recipients Per Hour: Use Default (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: THROTTLED - IncomingMail 172.16.16.25:25**

Edit Policy Settings

Name: THROTTLED

Connection Behavior: Accept

Connections:

- Max. Messages Per Connection: Use Default (10) 1
- Max. Recipients Per Message: Use Default (50) 25
- Max. Message Size: Use Default (10M) 10485760 (add a trailing K for kilobytes; M for megabytes)
- Max. Concurrent Connections From a Single IP: Use Default (10) 1

SMTP:

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

Mail Flow Limits

Rate Limit for Hosts:

- Max. Recipients Per Hour: Use Default (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) ☐ 220

Custom SMTP Banner Text: ☒ Use Default () ☐

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Use Hostname from Interface ☐

**Mail Flow Limits**

Rate Limit for Hosts: Max. Recipients Per Hour: ☐ Use Default (Unlimited) ☒ Unlimited ☐

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

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name: TRUSTED

Connection Behavior: Accept

Connections:

Max. Messages Per Connection: ☐ Use Default (10) ☒ 5000

Max. Recipients Per Message: ☐ Use Default (50) ☒ 5000

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

Max. Concurrent Connections From a Single IP: ☐ Use Default (10) ☒ 300

SMTP:

Custom SMTP Banner Code: ☒ Use Default (220) ☐ 220

Custom SMTP Banner Text: ☒ Use Default () ☐

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Use Hostname from Interface ☐

**Mail Flow Limits**

Rate Limit for Hosts: Max. Recipients Per Hour: ☐ Use Default (Unlimited) ☒ Unlimited ☐

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

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

**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.

[illegible]

**Cisco C100V**  
Email Security Virtual Appliance

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

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

No Changes Pending

## 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
<a href="#">&lt;&lt; Back to M&amp;T Overview</a> <a href="#">Edit Settings...</a>	

### Find Senders

Find Senders that Contain this Text:  [Find](#)

Sender List: Display All Items in List		Items per page: 20 ▾
<a href="#">Add Sender...</a>		
Sender	Comment	All <input type="checkbox"/>
orange public	None	Delete <input type="checkbox"/>
<a href="#">&lt;&lt; Back to M&amp;T Overview</a>		<a href="#">Delete</a>

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								
<h2>Sender Group Management</h2> <p>No Changes Pending</p> <p><b>Sender Group Settings</b></p> <ul style="list-style-type: none"> <li>Email Security Manager</li> <li>Incoming Mail Policies</li> <li>Incoming Content Filters</li> <li>Outgoing Mail Policies</li> <li>Outgoing Content Filters</li> <li>Host Access Table (HAT)               <ul style="list-style-type: none"> <li>HAT Overview</li> <li>Mail Flow Policies</li> <li>Exception Table</li> <li>Address Lists</li> </ul> </li> <li>Recipient Access Table (RAT)</li> <li>Destination Controls</li> <li>Bounce Verification</li> <li>Data Loss Prevention (DLP)               <ul style="list-style-type: none"> <li>DLP Policy Manager</li> <li>DLP Message Actions</li> </ul> </li> <li>Domain Keys               <ul style="list-style-type: none"> <li>Verification Profiles</li> <li>Signing Profiles</li> <li>Signing Keys</li> </ul> </li> <li>Text Resources</li> <li>Dictionaries</li> </ul> <p>&lt;&lt; Back to HAT Overview</p> <p><b>Find Senders</b></p> <p>Find Sender: [orange.public] Find</p> <p><b>Sender List: Display</b></p> <p>Add Sender...</p> <table border="1"> <thead> <tr> <th>Sender</th> <th>Comment</th> <th>All</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>orange.public</td> <td>None</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p>&lt;&lt; Back to HAT Overview Delete</p>					Sender	Comment	All	Delete	orange.public	None	<input type="checkbox"/>	<input type="checkbox"/>
Sender	Comment	All	Delete									
orange.public	None	<input type="checkbox"/>	<input type="checkbox"/>									

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

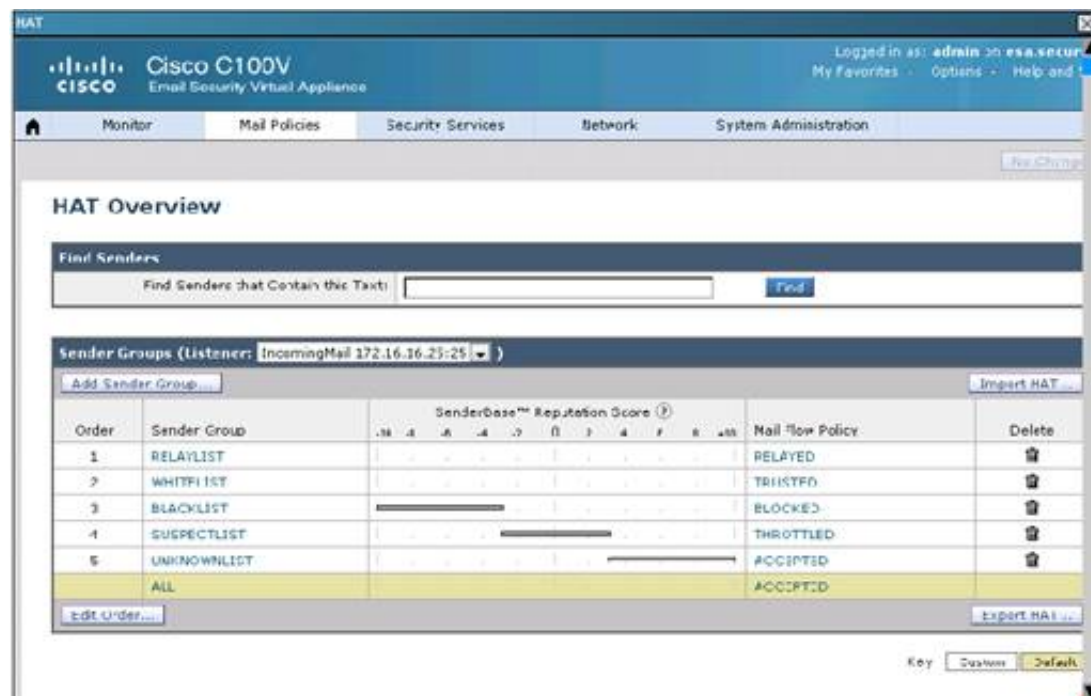
- A. 1 KB  
B. 100 KB  
C. 1 MB  
D. 10 MB  
E. 100 MB  
F. Unlimited

**Answer: D**

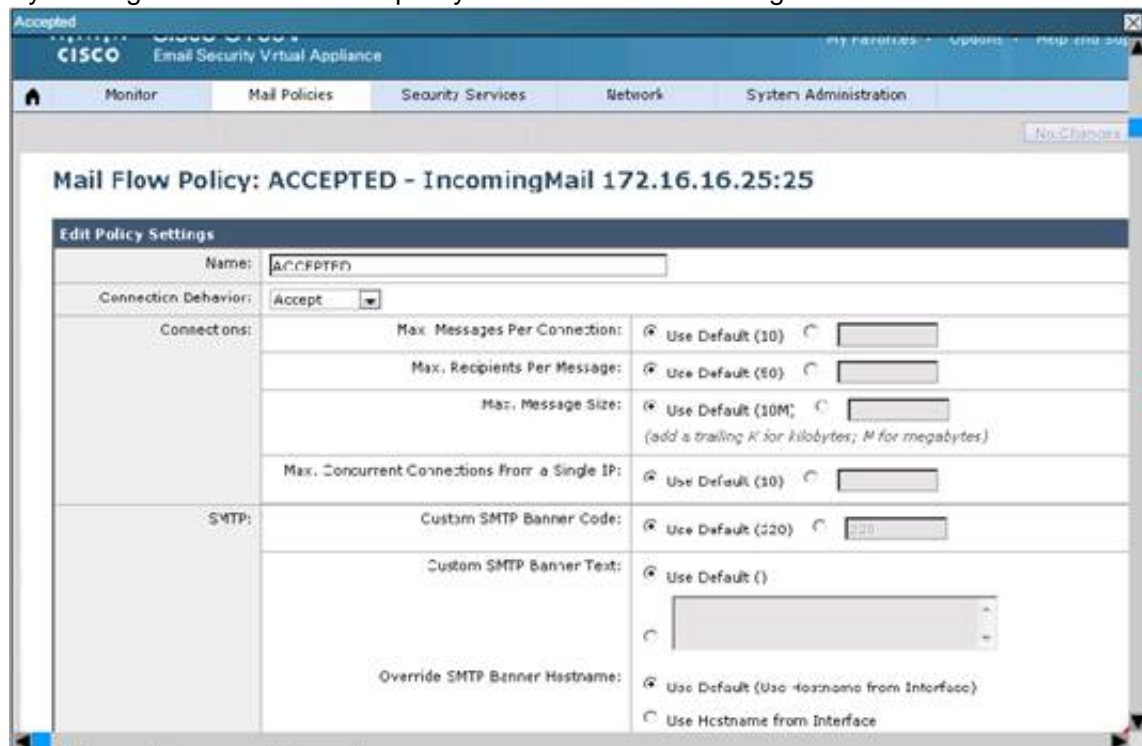
**Explanation:** From the instructions we know that the reputation score for the violet.public domain has been set to 8. From the HAT table shown below we know that a score of 8 belongs to the UNKNOWNLIST group, which is assigned the ACCEPTED policy.

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 458

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 462

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

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

Answer: AD

#### NEW QUESTION 466

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

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

**Answer:** C

**Explanation:** [http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products\\_configuration\\_example09186\\_a0080671a8d.shtml](http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_example09186_a0080671a8d.shtml)

#### NEW QUESTION 468

Which four methods are used to deploy transparent mode traffic redirection? (Choose four.)

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

**Answer:** BCEG

#### NEW QUESTION 470

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 474

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 475

Refer to the exhibit.

Option	WCCP Service	Protocol
1	60	WAAS – reverse
2	61	WAAS – forward
3	62	FTP
4	70	HTTPS
5	88	CIFS-Cache WAAS
6	90-97	User Configurable
7	98	RTSPU
8	99	Reverse Proxy

Which four rows exhibit the correct WCCP service to protocol assignments? (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:** BDFH

#### NEW QUESTION 480

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

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

D. It controls content that passes into and out of the network.

**Answer:** A

#### NEW QUESTION 485

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 489

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 492

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

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

**Answer:** A

#### NEW QUESTION 497

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

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

**Answer:** D

#### NEW QUESTION 502

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 506

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/crlIntro.html>

#### NEW QUESTION 510

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

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

**Answer:** D

#### NEW QUESTION 515

Which technique is deployed to harden network devices?

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

**Answer:** B

#### NEW QUESTION 517

Which feature of the Cisco Hybrid Email Security services enables you to create multiple email senders on a single Cisco ESA?

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

**Answer:** A

#### NEW QUESTION 522

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

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

**Answer:** A

#### NEW QUESTION 526

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

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

**Answer:** AB

#### NEW QUESTION 527

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 529

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

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

**Answer:** BC

#### NEW QUESTION 531

Which two commands are used to verify that CWS redirection is working on a Cisco ASA appliance? (Choose two.)



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

**Answer:** AC

#### NEW QUESTION 533

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 535

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

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

**Answer:** A

#### NEW QUESTION 536

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

signature fidelity rating	amount of potential damage
attack severity rating	accuracy difference from inline sensing
target value rating	vulnerability of attack target
attack relevancy rating	degree of attack certainty
watch list rating	criticality of attack target
promiscuous delta	Cisco Security agent rating

**Answer:**

**Explanation:** Reference:

[http://www.cisco.com/c/en/us/products/collateral/security/ips-4200-seriessensors/prod\\_white\\_paper0900aecd806e7299.html](http://www.cisco.com/c/en/us/products/collateral/security/ips-4200-seriessensors/prod_white_paper0900aecd806e7299.html)

#### NEW QUESTION 540

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 545

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 547

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

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

**Answer:** AC

#### NEW QUESTION 550

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 551

What are the two policy types that can use a web reputation profile to perform reputation-based processing? (Choose two.)

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

**Answer:** CD

#### NEW QUESTION 556

Which centralized reporting function of the Cisco Content Security Management Appliance aggregates data from multiple Cisco ESA devices?

- A. message tracking
- B. web tracking
- C. system tracking
- D. logging

**Answer:** A

#### NEW QUESTION 560

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.

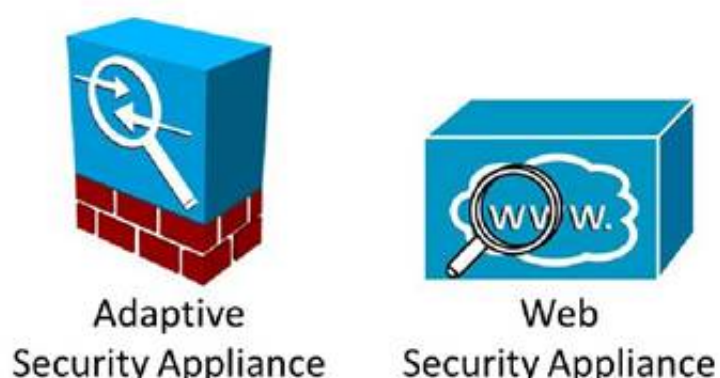
**Answer:** B

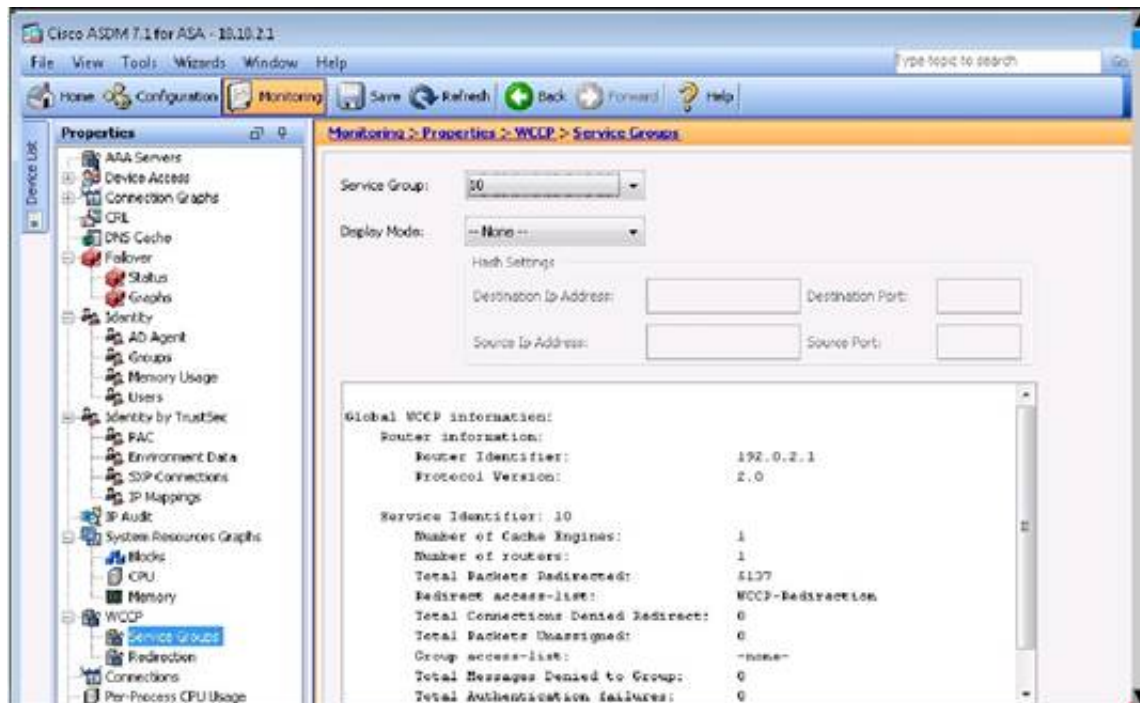
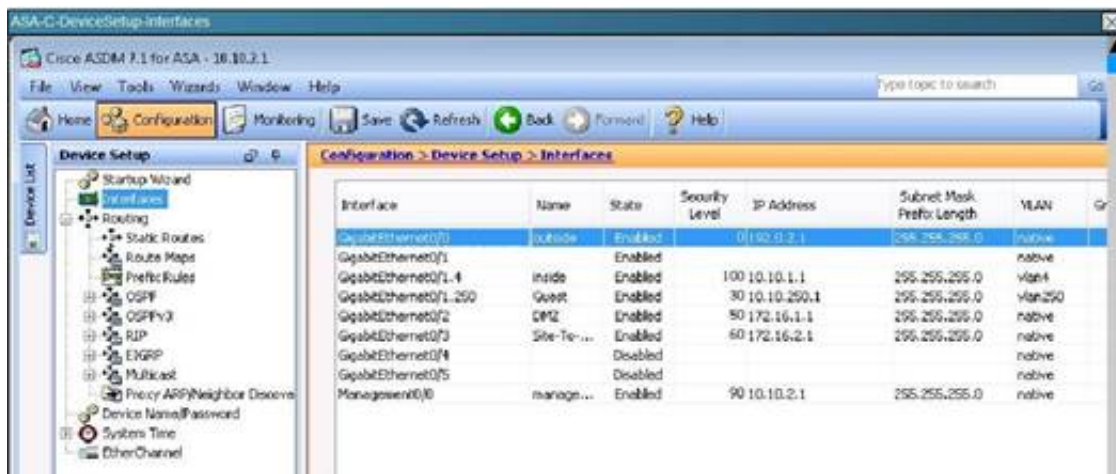
#### NEW QUESTION 564

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.



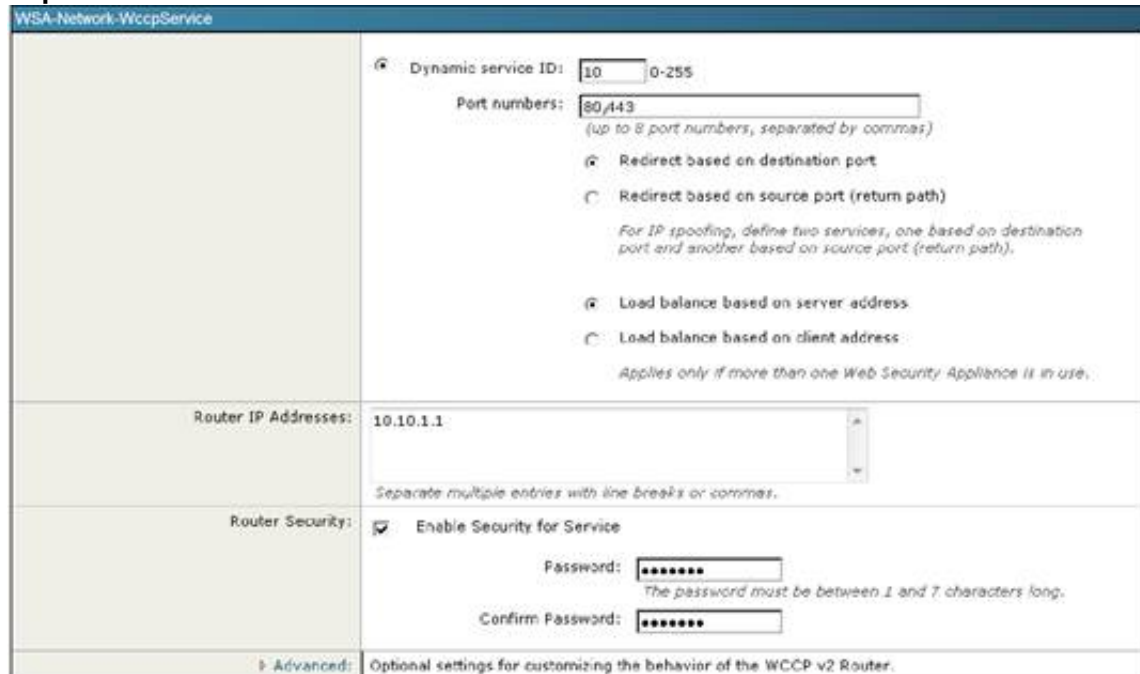


Between the Cisco ASA configuration and the Cisco WSA configuration, what is true with respect to redirected ports?

- 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 567

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 570

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.

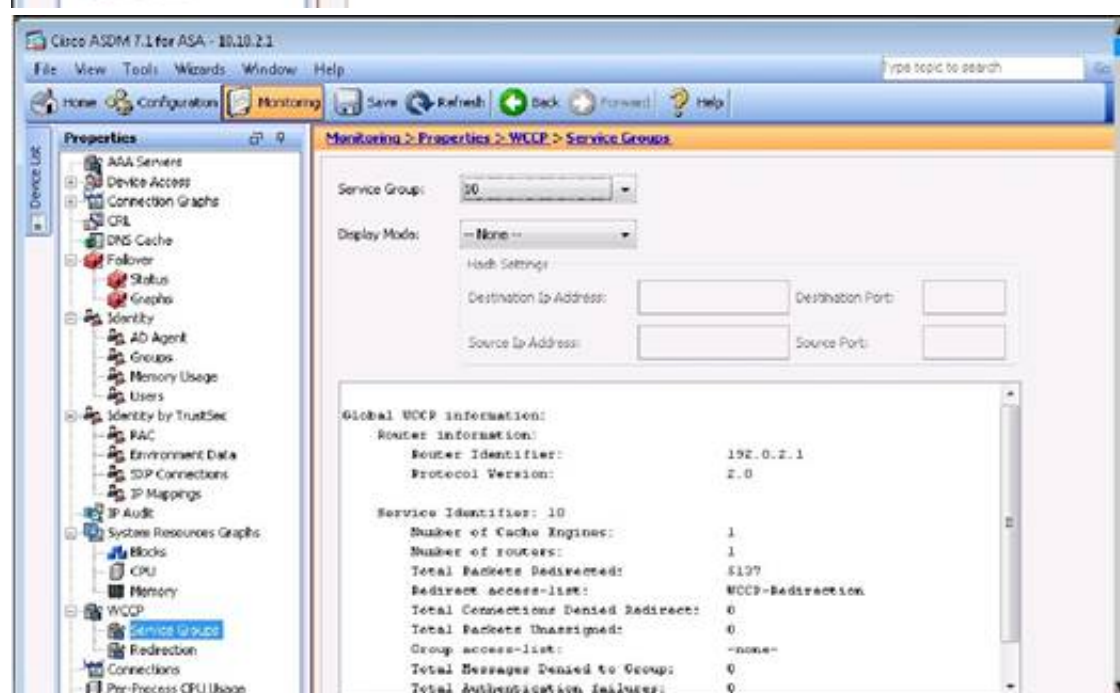
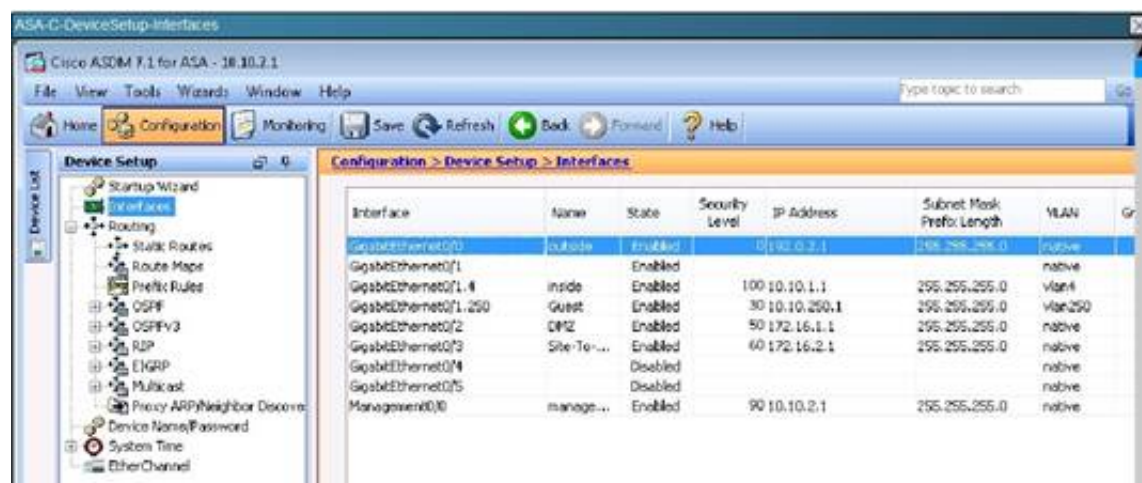
Your task is to examine the details available in the simulated graphical user interfaces and select the best answer.



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 573

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 575

Which Option of SNMPv3 ensure authentication but no encryption?

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

**Answer: D**

**Explanation:** SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. The security model combines with the selected security level to determine the security mechanism applied when the SNMP message is processed.

The security level determines the privileges required to view the message associated with an SNMP trap. The privilege level determines whether the message needs to be protected from disclosure or authenticated. The supported security level depends upon which security model is implemented. SNMP security levels support one or more of the following privileges:

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Reference: <http://www.cisco.com/en/US/>

#### NEW QUESTION 580

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

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

D. The IPS is misconfigured.

**Answer:** A

#### NEW QUESTION 582

Refer to the exhibit.

```

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

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

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

**Answer:** C

#### NEW QUESTION 583

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 584

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

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

**Answer:** B

#### NEW QUESTION 585

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 587

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

- A. whoami.scansafe.net

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

**Answer:** B

#### NEW QUESTION 592

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 593

A network security design engineer is considering using a Cisco Intrusion Detection System in the DMZ of the network. Which option is the drawback to using IDS in the DMZ as opposed to using Intrusion Prevention System?

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

**Answer:** B

#### NEW QUESTION 596

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

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

**Answer:** A

#### NEW QUESTION 600

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

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

**Answer:** A

#### NEW QUESTION 602

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 603

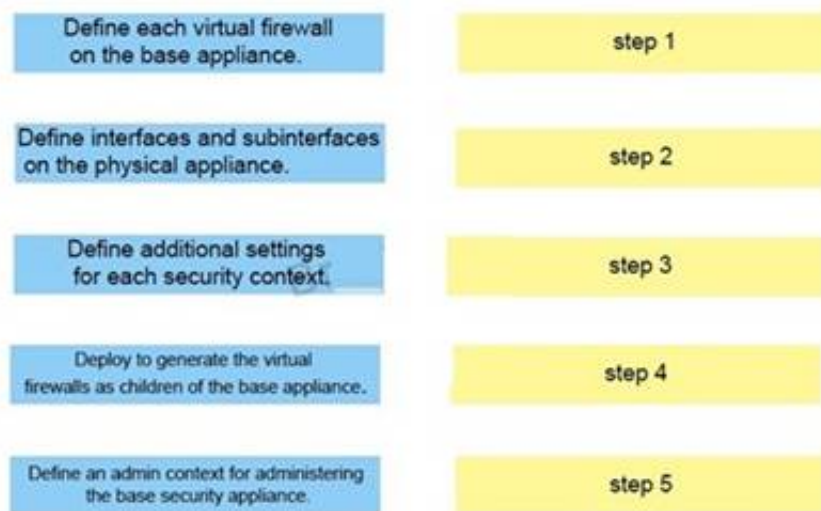
What is a valid search parameter for the Cisco ESA find event tool?

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

**Answer:** C

#### NEW QUESTION 604

Drag and drop the steps on the left into the correct order on the right to configure a Cisco ASA NGFW with multiple security contexts.



**Answer:**

**Explanation:** Reference:

[http://www.cisco.com/c/en/us/td/docs/security/security\\_management/cisco\\_security\\_manager/security\\_manager/4-4/user/guide/CSMUserGuide\\_wrapper/pxcontexts.pdf](http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-4/user/guide/CSMUserGuide_wrapper/pxcontexts.pdf) (page 2 to 4)


#### NEW QUESTION 606

**Scenario**

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

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

You can access the console of the ISR at the branch office using the icon on the topology display. The enable password is Cisco123.



**Branch-ISR**

Press RETURN to get started!

**Answer:**

**Explanation:** We need to define the parameter map, specifying port 8080 for http and https and define the servers and the license:

```
Branch-ISR#config t
```

```
Branch-ISR(config)#parameter-map type content-scan global
```

```
Branch-ISR(config-profile)#server scansafe primary name proxy-a.scansafe.net port http 8080 https 8080 Branch-ISR(config-profile)#server scansafe secondary name proxy-b.scansafe.net port http 8080 https 8080 Branch-ISR(config-profile)#license 0 0123456789abcdef
```

If the CWS proxy servers are not available, we traffic should be denied. This is done by the following configuration:

```
Branch-ISR(config-profile)#server scansafe on-failure block-all Now we need to apply this to the fastethernet 0/1 interface outbound: Branch-ISR(config)#interface Fastethernet 0/1
```

```
Branch-ISR(config-if)#content-scan outbound
```

```
Branch-ISR(config-if)#exit Branch-ISR(config)#exit
```

Finally, we can verify our configuration by using the “show content-scan summary command: Branch-ISR#show content-scan summary



Primary: 72.37.244.203(Up)\* Secondary: 70.39.231.99 (Up) Interfaces: Fastethernet0/1

#### NEW QUESTION 610

Which Cisco technology provides spam filtering and email protection?

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

**Answer: B**

#### NEW QUESTION 611

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 intrusion rules.
- D. Configure URL filtering criteria in the Cisco ASA FirePOWER access rules.

**Answer: A**

#### NEW QUESTION 613

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 614

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 615

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**

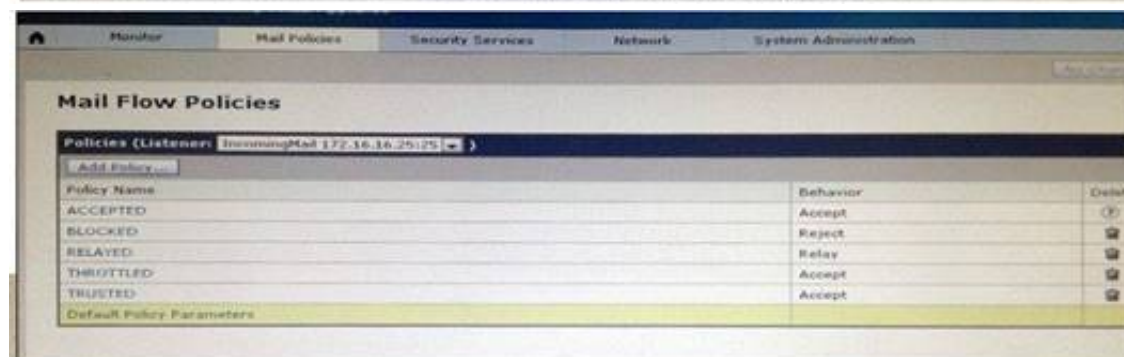
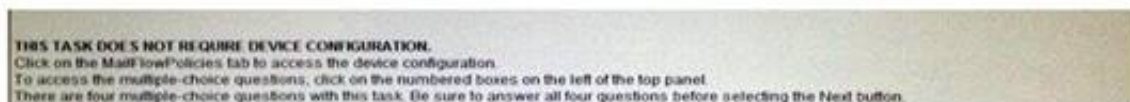
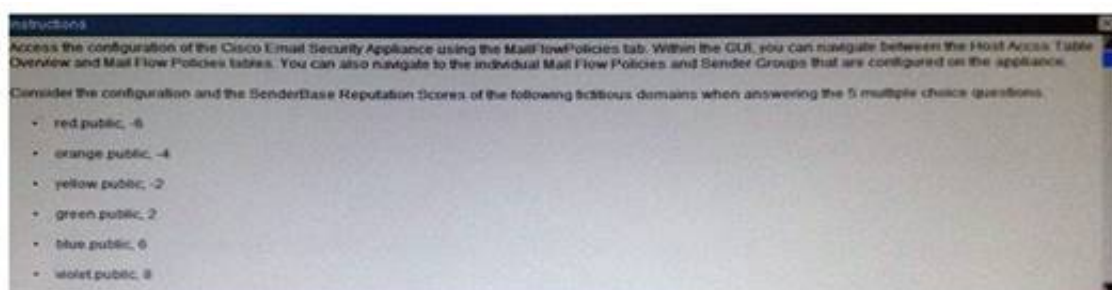
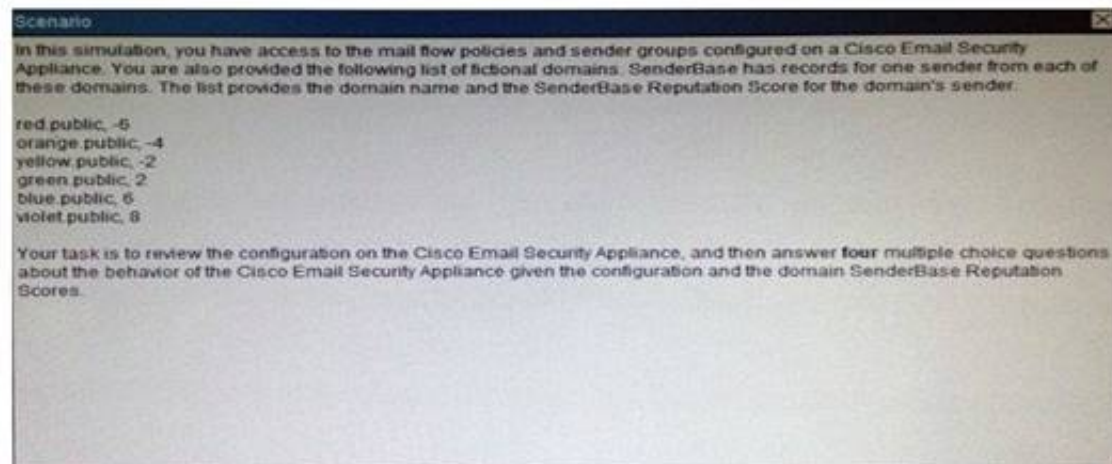
#### NEW QUESTION 616

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 619



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 624

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 628

**Scenario**

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

V120 red.public, -6  
orange.public, -4  
yellow.public, -2  
green.public, 2  
blue.public, 6  
violet.public, 8

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

**Instructions**

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

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

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

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policies

Policies (Listeners: IncomingMail 172.16.16.25:25 )

Add Policy...

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

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### HAT Overview

Find Senders

Find Sender

Sender Groups (List)

Add Sender Group...

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

Import HAT...

Export HAT...

Key: Custom Default

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



**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**HAT Overview**

Find Senders

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

Sender Groups (Listeners: IncomingMail 172.16.16.25:25)

Add Sender Group... Import HAT...

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

Edit Order... Export HAT...

Key: Custom Default

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policy**

Policies (Listeners: Add Policy...)

Policy Name: ACCEPTED, BLOCKED, RELAYED, THROTTLED, TRUSTED, Default Policy Parameters

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

	Behavior	Delete
	Accept	
	Reject	
	Relay	
	Accept	
	Accept	

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: ACCEPTED - IncomingMail 172.16.16.25:25**

Edit Policy Settings

Name: ACCEPTED

Connection Behavior: Accept

Connections:

Max. Messages Per Connection: ☒ Use Default (10)

Max. Recipients Per Message: ☒ Use Default (50)

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

Max. Concurrent Connections From a Single IP: ☒ Use Default (10)

SMTP:

Custom SMTP Banner Code: ☒ Use Default (220)

Custom SMTP Banner Text: ☒ Use Default ()

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Use Hostname from Interface

Mail Flow Limits

Rate Limit for Hosts:

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

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

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



**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policies**

**Host Access Table (HAT)**

**IncomingMail 172.16.16.25:25**

**Mail Flow Limits**

Rate Limit for Hosts: Max. Recipients Per Hour: Max. Recipients Per Hour Code: Max. Recipients Per Hour Text:

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Sender Group: BLACKLIST - IncomingMail 172.16.16.25:25**

**Sender Group Settings**

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

**Find Senders**

Find Senders that Contain this Text: Find

**Sender List: Display All Items in List**

Add Sender...

There are no senders.

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Sender Group: BLACKLIST - IncomingMail 172.16.16.25:25**

**Sender Group Settings**

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

**Find Senders**

Find Senders that Contain this Text: Find

**Sender List: Display All Items in List**

Add Sender...

There are no senders.

Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local

My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name:

Connection Behavior:

Connections:

Max. Messages Per Connection: ☒ Use Default (10)

Max. Recipients Per Message: ☒ Use Default (50)

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

Max. Concurrent Connections From a Single IP: ☒ Use Default (10)

SMTP:

Custom SMTP Banner Code: ☒ Use Default (554)

Custom SMTP Banner Text: ☐ Use Default ()  
☒ Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface)  
☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts:

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

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

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

Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local

My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name:

Connection Behavior:

Connections:

Max. Messages Per Connection: ☒ Use Default (10)

Max. Recipients Per Message: ☒ Use Default (50)

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

Max. Concurrent Connections From a Single IP: ☒ Use Default (10)

SMTP:

Custom SMTP Banner Code: ☒ Use Default (554)

Custom SMTP Banner Text: ☐ Use Default ()  
☒ Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface)  
☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts:

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

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

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

Cisco C100V Email Security Virtual Appliance

Logged in as: admin on esa.secure-x.local

My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name:

Connection Behavior:

Connections:

Max. Messages Per Connection: ☒ Use Default (10)

Max. Recipients Per Message: ☒ Use Default (50)

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

Max. Concurrent Connections From a Single IP: ☒ Use Default (10)

SMTP:

Custom SMTP Banner Code: ☒ Use Default (220)

Custom SMTP Banner Text: ☒ Use Default ()

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface)  
☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts:

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

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

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



Cisco C100V Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

Mail Flow Policies

Host Access Table (HAT)

Host Access Table (HAT) Overview

Mail Flow Policies

Exception Table

Address Lists

Recipient Access Table (RAT)

Destination Controls

Bounce Verification

Data Loss Prevention (DLP)

DLP Policy Manager

DLP Message Actions

Domain Keys

Verification Profiles

Signing Profiles

Signing Keys

Text Resources

Dictionaries

IncomingMail 172.16.16.25:25

Max. Recipients Per Connection: ☒ Use Default (10) ☐ Unlimited

Max. Recipients Per Message: ☒ Use Default (50) ☐ Unlimited

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

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

SMTP Banner Code: ☒ Use Default (220) ☐ Custom

SMTP Banner Text: ☒ Use Default ( ) ☐ Custom

SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Custom

Mail Flow Limits

Rate Limit for Hosts: ☒ Use Default (Unlimited) ☐ Unlimited

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

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

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

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Items per page: 20

Add Sender...

Sender	Comment	All	Delete
hq-mail.maroon.public	None	<input type="checkbox"/>	<input type="checkbox"/>

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: RELAYLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name: RELAYLIST

Order: 1

Comment: Only select hosts can relay from this box

Policy: RELAYED

SBRs (Optional): Not in use

DNS Lists (Optional): None

Connecting Host DNS Verification: None Included

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Items per page: 20

Add Sender...

Sender	Comment	All	Delete
hq-mail.maroon.public	None	<input type="checkbox"/>	<input type="checkbox"/>

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

Sender Group: SUSPECTLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

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

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Add Sender...

There are no senders.

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

Sender Group: IncomingMail 172.16.16.25:25

Sender Group Settings

Name:	TLIST
Order:	
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

Mail Flow Policy: THROTTLED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name:	THROTTLED	
Connection Behavior:	Accept	
Connections:	Max. Messages Per Connection:	<input type="radio"/> Use Default (10) <input checked="" type="radio"/> 1
	Max. Recipients Per Message:	<input type="radio"/> Use Default (50) <input checked="" type="radio"/> 25
	Max. Message Size:	<input type="radio"/> Use Default (10M) <input checked="" type="radio"/> 10485760 (add a trailing K for kilobytes; M for megabytes)
	Max. Concurrent Connections From a Single IP:	<input type="radio"/> Use Default (10) <input checked="" type="radio"/> 1
SMTP:	Custom SMTP Banner Code:	<input checked="" type="radio"/> Use Default (220) <input type="radio"/> 220
	Custom SMTP Banner Text:	<input checked="" type="radio"/> Use Default () <input type="text"/>
	Override SMTP Banner Hostname:	<input checked="" type="radio"/> Use Default (Use Hostname from Interface) <input type="radio"/> Use Hostname from Interface <input type="text"/>

Mail Flow Limits

Rate Limit for Hosts:	Max. Recipients Per Hour:	<input type="radio"/> Use Default (Unlimited) <input type="radio"/> Unlimited <input checked="" type="radio"/> 20
	Max. Recipients Per Hour Code:	<input checked="" type="radio"/> Use Default (452) <input type="text"/>
	Max. Recipients Per Hour Text:	<input checked="" type="radio"/> Use Default (Too many recipients received this hour) <input type="text"/>



**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policy: IncomingMail 172.16.16.25:25**

**Edit Policy Settings**

Host Access Table (HAT)  
 HAT Overview  
 Mail Flow Policies  
 Exception Table  
 Address Lists

Recipient Access Table (RAT)  
 Destination Controls  
 Bounce Verification

Data Loss Prevention (DLP)  
 DLP Policy Manager  
 DLP Message Actions

Domain Keys  
 Verification Profiles  
 Signing Profiles  
 Signing Keys

Text Resources  
 Dictionaries

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 Banner Code: ☒ Use Default (220) ☐ 220

SMTP Banner Text: ☒ Use Default () ☐

SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts: Max. Recipients Per Hour: ☐ Use Default (Unlimited) ☒ Unlimited

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

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25**

**Edit Policy Settings**

Name:

Connection Behavior:

Connections: Max. Messages Per Connection: ☐ Use Default (10) ☒ 5000

Max. Recipients Per Message: ☐ Use Default (50) ☒ 5000

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

Max. Concurrent Connections From a Single IP: ☐ Use Default (10) ☒ 300

SMTP: Custom SMTP Banner Code: ☒ Use Default (220) ☐ 220

Custom SMTP Banner Text: ☒ Use Default () ☐

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts: Max. Recipients Per Hour: ☐ Use Default (Unlimited) ☒ Unlimited

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

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policy: IncomingMail 172.16.16.25:25**

**Edit Policy Settings**

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

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 Banner Code: ☒ Use Default (220) ☐ 220

SMTP Banner Text: ☒ Use Default () ☐

SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts: Max. Recipients Per Hour: ☐ Use Default (Unlimited) ☒ Unlimited

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

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

[No Changes Pending](#)

### Sender Group: UNKNOWNLIST - IncomingMail 172.16.16.25:25

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

[Back to HAT Overview](#) [Edit Settings...](#)

### Find Senders

Find Senders that Contain this Text:  [Find](#)

### Sender List: Display All Items in List

[Add Sender...](#)

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

[No Changes Pending](#)

### Sender Group: UNKNOWNLIST - IncomingMail 172.16.16.25:25

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

[Back to HAT Overview](#) [Edit Settings...](#)

### Find Senders

Find Senders that Contain this Text:  [Find](#)

### Sender List: Display All Items in List

[Add Sender...](#)

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

[No Changes Pending](#)

### Sender Group: WHITELIST - IncomingMail 172.16.16.25:25

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

[Back to HAT Overview](#) [Edit Settings...](#)

### Find Senders

Find Senders that Contain this Text:  [Find](#)

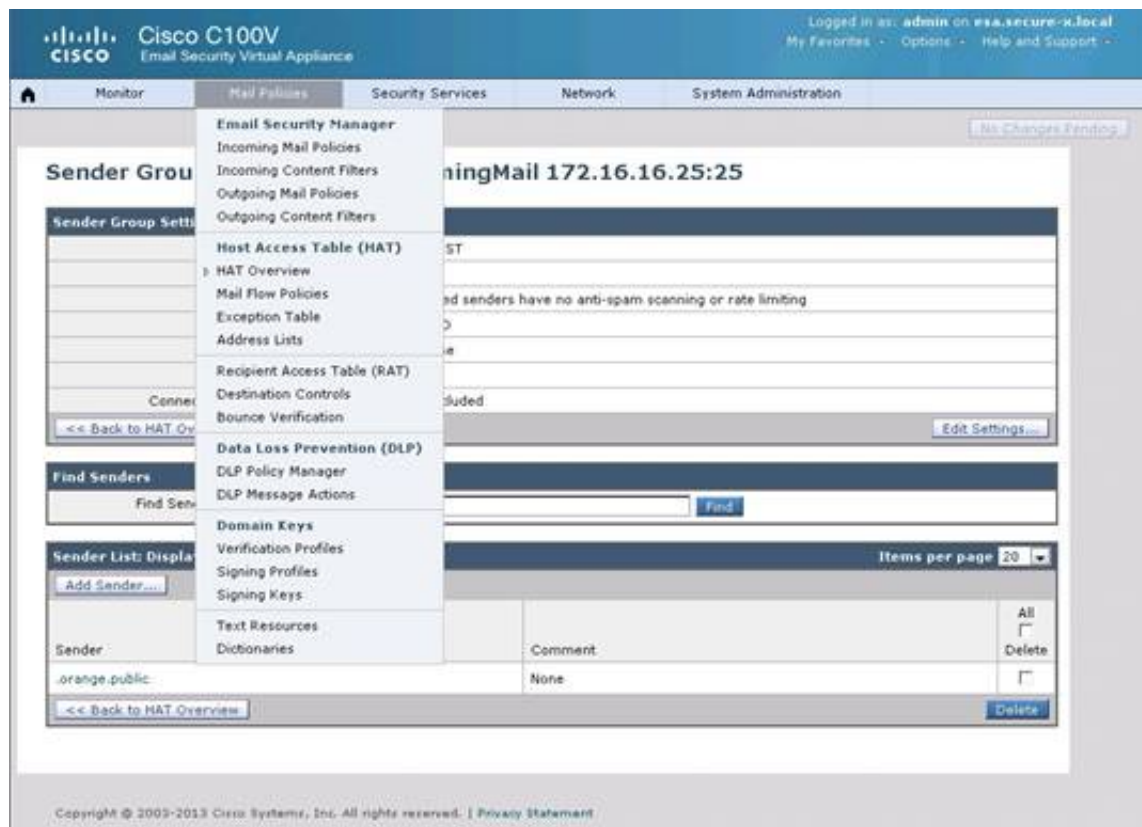
### Sender List: Display All Items in List

[Add Sender...](#) Items per page: 20

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

[Back to HAT Overview](#) [Delete](#)

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

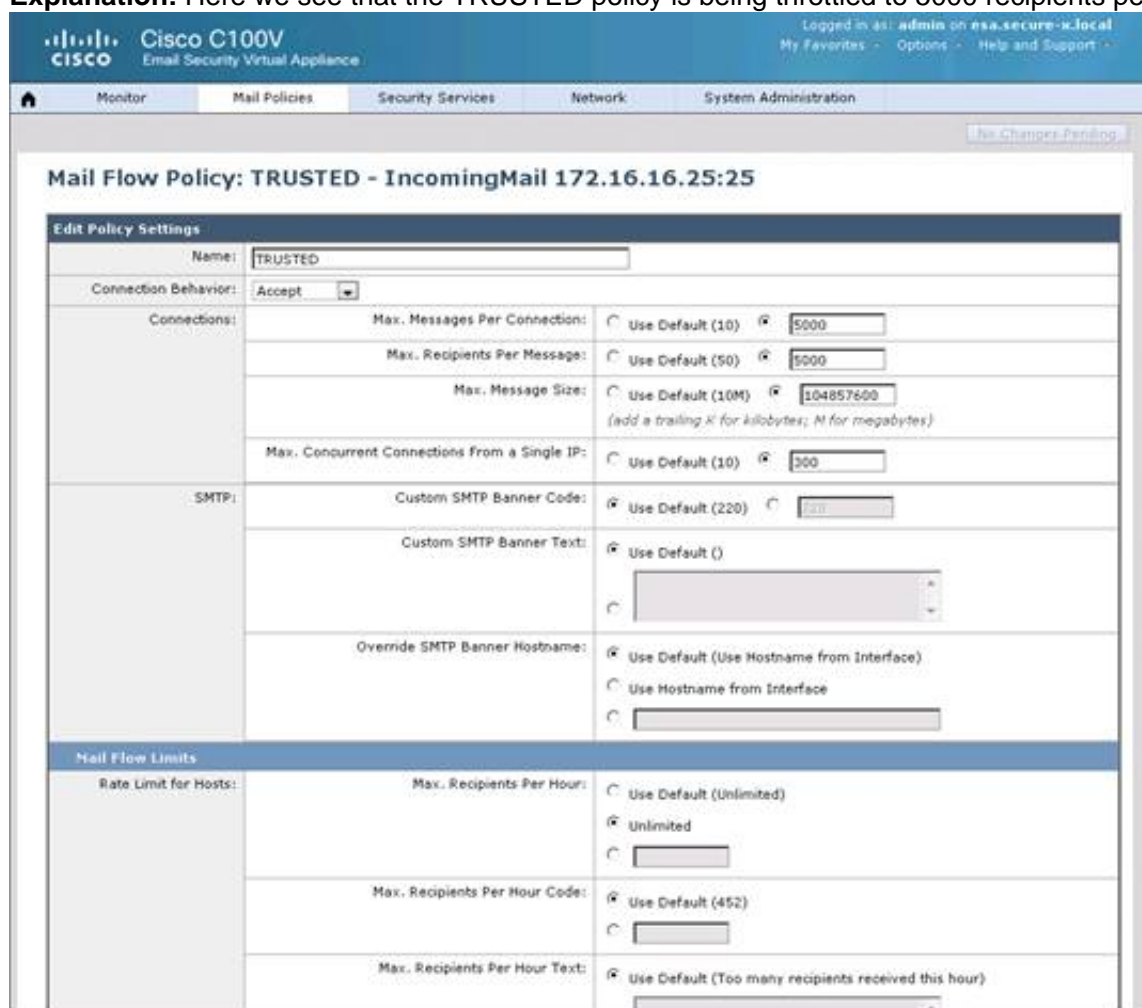


For which domains will the Cisco Email Security Appliance allow up to 5000 recipients per message?

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

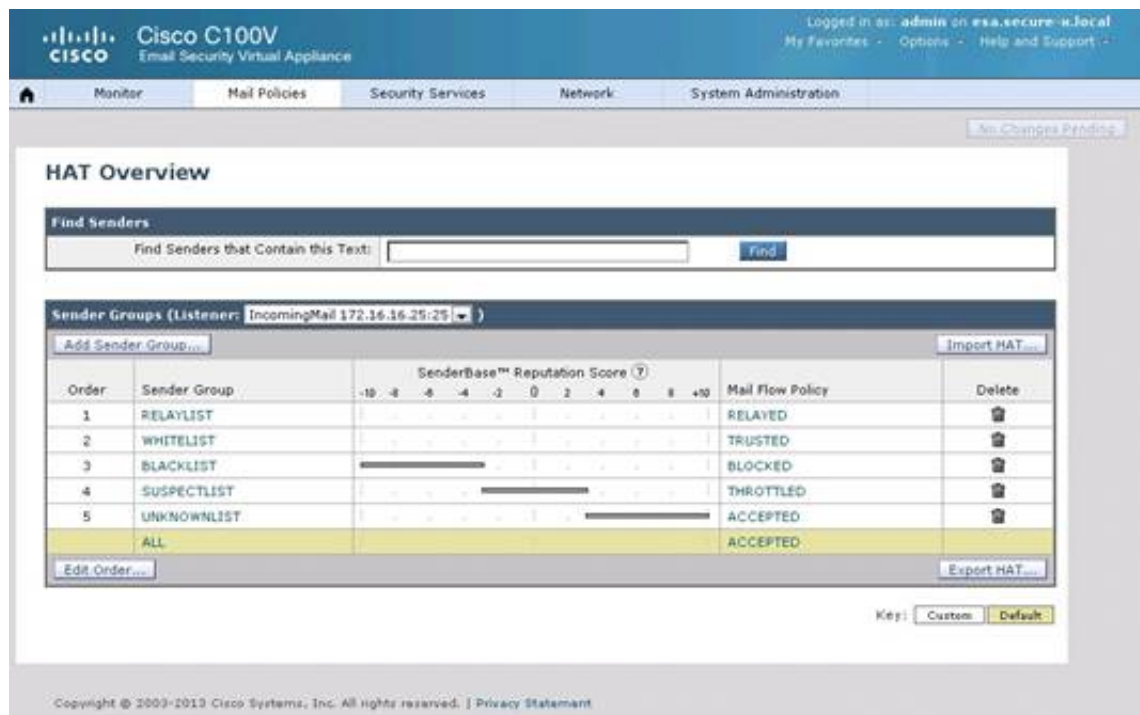
**Answer: E**

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

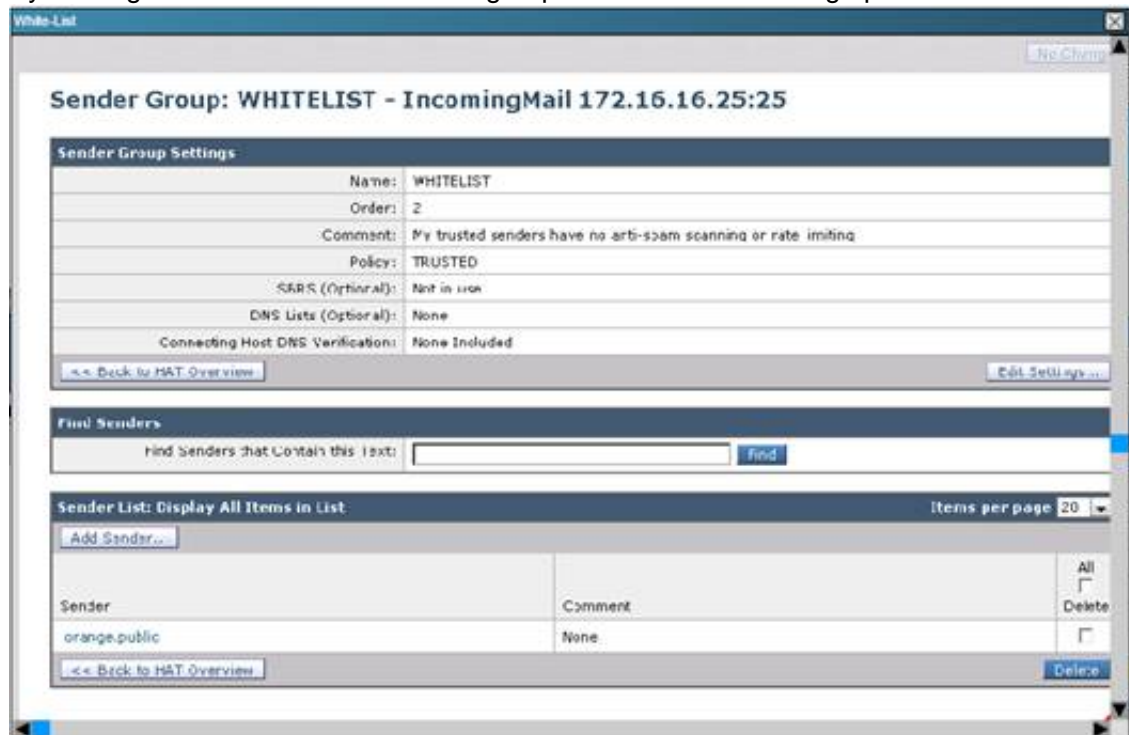


By looking at the HAT policy we see that the TRUSTED policy applies to the WHITELIST sender group.  
Image 27





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



### NEW QUESTION 633

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 634

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 636

Which type of signature is generated by copying a default signature and modifying its behavior?

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

Answer: B

### NEW QUESTION 637

Refer to the exhibit.



Processing Details		
29 Apr 2014 12:37:42 (GMT +00:00)	Protocol SMTP Interface Management (IP 172.16.254.17) on incoming connection (ICID 380) from sender IP 10.150.54.161. Reverse DNS host dhcp-10-150-54-161.cisco.com verified yes.	
29 Apr 2014 12:37:42 (GMT +00:00)	(ICID 380) ACCEPT sender group SUSPECTLIST match 10.150.54.161 SBRS rfc1918	
29 Apr 2014 12:37:50 (GMT +00:00)	Start message 1139 on incoming connection (ICID 380).	
29 Apr 2014 12:37:50 (GMT +00:00)	Message 1139 enqueued on incoming connection (ICID 380) from user@mydomain.com.	
29 Apr 2014 12:37:54 (GMT +00:00)	Message 1139 on incoming connection (ICID 380) added recipient (user@mydomain.com).	
29 Apr 2014 12:37:58 (GMT +00:00)	Message 1139 on incoming connection (ICID 380) added recipient (bob@mydomain.com).	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1139 original subject on injection: Win the lottery today	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1139 (458 bytes) from user@mydomain.com ready.	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1139 was split creating new message 1140 due to recipient match on policy Special_treatment_NO_AS in the inbound	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1139 was split creating new message 1141 due to recipient match on policy DEFAULT in the inbound	
MAIL POLICY "Special_treatment_NO_AS" MATCHED THESE RECIPIENTS: user@mydomain.com		
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1140 enqueued on incoming connection (ICID 0) from user@mydomain.com.	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1140 on incoming connection (ICID 0) added recipient (user@mydomain.com).	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1140 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1140 scanned by Anti-Virus engine. Final verdict: Negative	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1140 queued for delivery.	
MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: bob@mydomain.com		
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1141 enqueued on incoming connection (ICID 0) from user@mydomain.com.	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1141 on incoming connection (ICID 0) added recipient (bob@mydomain.com).	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1141 scanned by Anti-Spam engine: CASE. Interim verdict: Positive	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1141 scanned by Anti-Spam engine: CASE. Final verdict: Positive	
29 Apr 2014 12:38:24 (GMT +00:00)	Message 1141 aborted: Dropped by CASE	

The system administrator of mydomain.com was informed that one of the users in his environment received spam from an Internet sender. Message tracking shows that the emails for this user were not scanned by antispam. Why did the Cisco Email Security gateway fail to do a spam scan on emails for user@mydomain.com?

- A. The remote MTA activated the SUSPECTLIST sender group.
- B. The Cisco Email Security gateway created duplicates of the message.
- C. The user user@mydomain.com matched an inbound rule with antispam disabled.
- D. The user bob@mydomain.com matched an inbound rule with antispam disabled.

**Answer: C**

### NEW QUESTION 638

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 639

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 643

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 644

Refer to the following. Which description of the result of this configuration is true?

```
Router(config)#line vty 5 15
Router(config-line)#access-class 23 in
```

- A. Only clients denied in access list 23 can manage the router.
- B. Only telnet access (TCP) is allowed on the VTY lines of this router
- C. Only clients permitted in access list 23 can manage the router
- D. Only SSH access (TCP 23) is allowed on the VTY lines of this router.

**Answer: C**

### NEW QUESTION 646

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

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

**Answer: B**

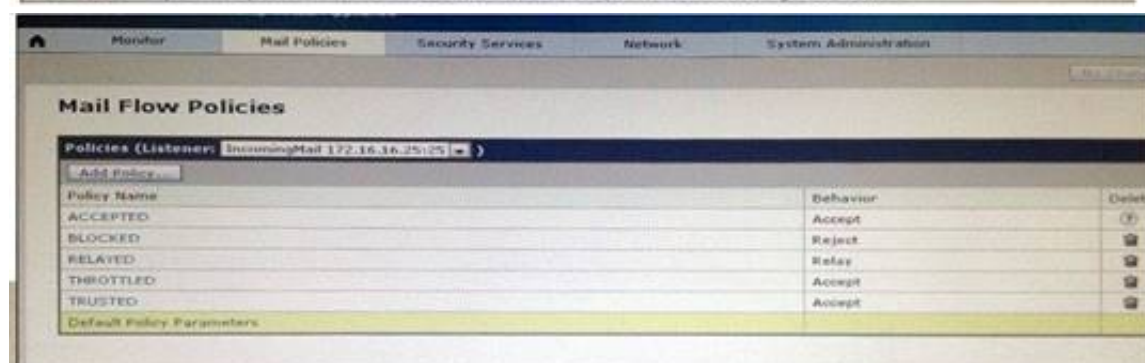
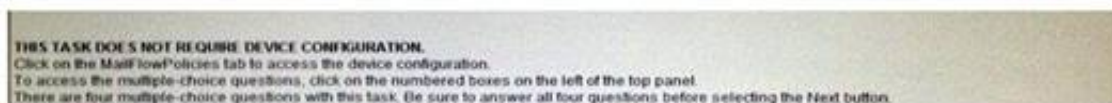
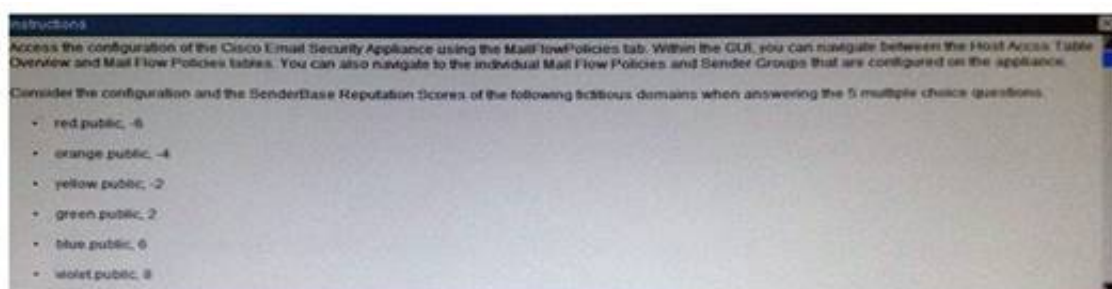
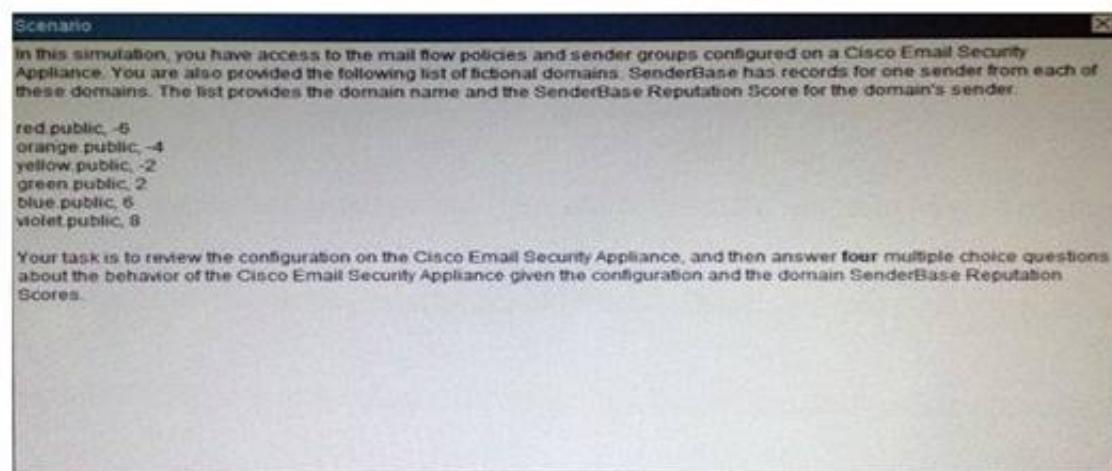
#### NEW QUESTION 647

Which two statements about devices within a Cisco ESA cluster are true? (Choose two.)

- A. Clustered systems must consist of devices in the same hardware series.
- B. Clustered devices can communicate via either SSH or Cluster Communication Service.
- C. Clustered devices can communicate only with Cluster Communication Service.
- D. In-the-cloud devices must be in a separate cluster from on-premise devices.
- E. Clustered devices can run different versions of AsyncOS.

Answer: AB

#### NEW QUESTION 652



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 657

Which type of server is required to communicate with a third-party DLP solution?

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

Answer: C

#### NEW QUESTION 661

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 664

Scenario

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

V120 red.public, -6  
orange.public, -4  
yellow.public, -2  
green.public, 2  
blue.public, 6  
violet.public, 8

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

Instructions

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

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

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

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

Cisco C100V  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

All Changes Pending

### Mail Flow Policies

Policies (Listeners: IncomingMail 172.16.16.25:25 )

Add Policy...

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

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

Cisco C100V  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

All Changes Pending

### HAT Overview

Find Senders

Find Senders

Sender Groups (List)

Add Sender Group...

Order	Sender
1	RELAYED
2	WHITEL
3	BLACKL
4	SUSPEC
5	UNKNOW
	ALL

Edit Order...

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

derBase™ Reputation Score (?)

derBase™ Reputation Score (?)	Mail Flow Policy	Delete
-4 -3 0 2 4 6 8 10	RELAYED	
	TRUSTED	
	BLOCKED	
	THROTTLED	
	ACCEPTED	
	ACCEPTED	

Import HAT...

Export HAT...

Key: Custom Default

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



**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### HAT Overview

Find Senders

Find Senders that Contain this Text:  Find

Sender Groups (Listener: IncomingMail 172.16.16.25:25)

Add Sender Group... Import HAT...

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

Edit Order... Export HAT...

Key: Custom Default

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policy

Policies (Listener: IncomingMail 172.16.16.25:25)

Add Policy...

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

Default Policy Parameters

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

No Changes Pending

### Mail Flow Policy: ACCEPTED - IncomingMail 172.16.16.25:25

Edit Policy Settings

Name: ACCEPTED

Connection Behavior: Accept

Connections:

Max. Messages Per Connection: ☒ Use Default (10)

Max. Recipients Per Message: ☒ Use Default (50)

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

Max. Concurrent Connections From a Single IP: ☒ Use Default (10)

SMTP:

Custom SMTP Banner Code: ☒ Use Default (220)

Custom SMTP Banner Text: ☒ Use Default ()

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Use Hostname from Interface

Mail Flow Limits

Rate Limit for Hosts:

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

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

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



**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policies**

**Host Access Table (HAT)**

**Host Access Table (HAT) Overview**

Connection Behavior

Mail Flow Policies

Exception Table

Address Lists

Recipient Access Table (RAT)

Destination Controls

Bounce Verification

Data Loss Prevention (DLP)

DLP Policy Manager

DLP Message Actions

Domain Keys

Verification Profiles

Signing Profiles

Signing Keys

Text Resources

Dictionaries

**IncomingMail 172.16.16.25:25**

Messages Per Connection: ☒ Use Default (10) ☐ [ ]

Recipients Per Message: ☒ Use Default (50) ☐ [ ]

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

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

SMTP Banner Code: ☒ Use Default (220) ☐ [ ]

SMTP Banner Text: ☒ Use Default ( ) ☐ [ ]

Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Use Hostname from Interface ☐ [ ]

**Mail Flow Limits**

Rate Limit for Hosts: 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
SBRIS (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.

**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
SBRIS (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.

**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:

Connection Behavior:

Connections:

Max. Messages Per Connection: ☒ Use Default (10)

Max. Recipients Per Message: ☒ Use Default (50)

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

Max. Concurrent Connections From a Single IP: ☒ Use Default (10)

SMTP:

Custom SMTP Banner Code: ☒ Use Default (554)

Custom SMTP Banner Text: ☐ Use Default ()  
☒ Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface)  
☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts:

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

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

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

[No Changes Pending](#)

### Mail Flow Policy: BLOCKED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name:

Connection Behavior:

Connections:

Max. Messages Per Connection: ☒ Use Default (10)

Max. Recipients Per Message: ☒ Use Default (50)

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

Max. Concurrent Connections From a Single IP: ☒ Use Default (10)

SMTP:

Custom SMTP Banner Code: ☒ Use Default (554)

Custom SMTP Banner Text: ☐ Use Default ()  
☒ Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you believe that this failure

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface)  
☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts:

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

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

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

[No Changes Pending](#)

### Mail Flow Policy: RELAYED - IncomingMail 172.16.16.25:25

**Edit Policy Settings**

Name:

Connection Behavior:

Connections:

Max. Messages Per Connection: ☒ Use Default (10)

Max. Recipients Per Message: ☒ Use Default (50)

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

Max. Concurrent Connections From a Single IP: ☒ Use Default (10)

SMTP:

Custom SMTP Banner Code: ☒ Use Default (220)

Custom SMTP Banner Text: ☒ Use Default ()

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface)  
☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts:

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

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

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



Cisco C100V Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

Mail Flow Policies

Host Access Table (HAT)

Host Access Table (HAT) Overview

Mail Flow Policies

Exception Table

Address Lists

Recipient Access Table (RAT)

Destination Controls

Bounce Verification

Data Loss Prevention (DLP)

DLP Policy Manager

DLP Message Actions

Domain Keys

Verification Profiles

Signing Profiles

Signing Keys

Text Resources

Dictionaries

IncomingMail 172.16.16.25:25

Max. Recipients Per Connection: ☒ Use Default (10) ☐ Unlimited

Max. Recipients Per Message: ☒ Use Default (50) ☐ Unlimited

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

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

SMTP Banner Code: ☒ Use Default (220) ☐ Custom

SMTP Banner Text: ☒ Use Default () ☐ Custom

SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface) ☐ Use Hostname from Interface

Mail Flow Limits

Rate Limit for Hosts: ☒ Use Default (Unlimited) ☐ Unlimited

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

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

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

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Items per page: 20

Add Sender...

Sender	Comment	All	Delete
hq-mail.maroon.public	None	<input type="checkbox"/>	<input type="checkbox"/>

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: RELAYLIST - IncomingMail 172.16.16.25:25

Sender Group Settings

Name: RELAYLIST

Order: 1

Comment: Only select hosts can relay from this box

Policy: RELAYED

SBRs (Optional): Not in use

DNS Lists (Optional): None

Connecting Host DNS Verification: None Included

Find Senders

Find Senders that Contain this Text:  Find

Sender List: Display All Items in List

Items per page: 20

Add Sender...

Sender	Comment	All	Delete
hq-mail.maroon.public	None	<input type="checkbox"/>	<input type="checkbox"/>

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

All Changes Pending

### Sender Group: SUSPECTLIST - IncomingMail 172.16.16.25:25

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

<< Back to HAT Overview Edit Settings...

#### Find Senders

Find Senders that Contain this Text:  Find

#### Sender List: Display All Items in List

Add Sender...

There are no senders.

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

All Changes Pending

### Sender Group: IncomingMail 172.16.16.25:25

Sender Group Settings	
Name:	TLIST
Order:	
Comment:	Suspicious senders are throttled
Policy:	THROTTLED
SBRs (Optional):	
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

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

Monitor Mail Policies Security Services Network System Administration

All Changes Pending

### Mail Flow Policy: THROTTLED - IncomingMail 172.16.16.25:25

Edit Policy Settings	
Name:	THROTTLED
Connection Behavior:	Accept
Connections:	<div>Max. Messages Per Connection: <input type="radio"/> Use Default (10) <input checked="" type="radio"/> 1</div> <div>Max. Recipients Per Message: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> 25</div> <div>Max. Message Size: <input type="radio"/> Use Default (10M) <input checked="" type="radio"/> 10485760 <small>(add a trailing K for kilobytes; M for megabytes)</small></div> <div>Max. Concurrent Connections From a Single IP: <input type="radio"/> Use Default (10) <input checked="" type="radio"/> 1</div>
SMTP:	<div>Custom SMTP Banner Code: <input type="radio"/> Use Default (220) <input checked="" type="radio"/> 220</div> <div>Custom SMTP Banner Text: <input type="radio"/> Use Default () <input checked="" type="radio"/> <input type="text"/></div> <div>Override SMTP Banner Hostname: <input type="radio"/> Use Default (Use Hostname from Interface) <input type="radio"/> Use Hostname from Interface <input checked="" type="radio"/> <input type="text"/></div>
Mail Flow Limits	
Rate Limit for Hosts:	<div>Max. Recipients Per Hour: <input type="radio"/> Use Default (Unlimited) <input type="radio"/> Unlimited <input checked="" type="radio"/> 20</div> <div>Max. Recipients Per Hour Code: <input type="radio"/> Use Default (452) <input checked="" type="radio"/> <input type="text"/></div> <div>Max. Recipients Per Hour Text: <input type="radio"/> Use Default (Too many recipients received this hour) <input checked="" type="radio"/> <input type="text"/></div>

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policy: IncomingMail 172.16.16.25:25**

**Edit Policy Settings**

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

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 Banner Code: ☒ Use Default (220) ☐ 220

SMTP Banner Text: ☒ Use Default ()  
☐

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface)  
☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts: Max. Recipients Per Hour: ☐ Use Default (Unlimited)  
☒ Unlimited

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

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policy: TRUSTED - IncomingMail 172.16.16.25:25**

**Edit Policy Settings**

Name:

Connection Behavior:

Connections: Max. Messages Per Connection: ☐ Use Default (10) ☒ 5000

Max. Recipients Per Message: ☐ Use Default (50) ☒ 5000

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

Max. Concurrent Connections From a Single IP: ☐ Use Default (10) ☒ 300

SMTP: Custom SMTP Banner Code: ☒ Use Default (220) ☐ 220

Custom SMTP Banner Text: ☒ Use Default ()  
☐

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface)  
☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts: Max. Recipients Per Hour: ☐ Use Default (Unlimited)  
☒ Unlimited

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

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

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

**Mail Flow Policy: IncomingMail 172.16.16.25:25**

**Edit Policy Settings**

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

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 Banner Code: ☒ Use Default (220) ☐ 220

SMTP Banner Text: ☒ Use Default ()  
☐

Override SMTP Banner Hostname: ☒ Use Default (Use Hostname from Interface)  
☐ Use Hostname from Interface

**Mail Flow Limits**

Rate Limit for Hosts: Max. Recipients Per Hour: ☐ Use Default (Unlimited)  
☒ Unlimited

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

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



**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

[No Changes Pending](#)

### Sender Group: UNKNOWNLIST - IncomingMail 172.16.16.25:25

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

[Back to HAT Overview](#) [Edit Settings...](#)

### Find Senders

Find Senders that Contain this Text:  [Find](#)

### Sender List: Display All Items in List

[Add Sender...](#)

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

[No Changes Pending](#)

### Sender Group: UNKNOWNLIST - IncomingMail 172.16.16.25:25

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

[Back to HAT Overview](#) [Edit Settings...](#)

### Find Senders

Find Senders that Contain this Text:  [Find](#)

### Sender List: Display All Items in List

[Add Sender...](#)

There are no senders.

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

**Cisco C100V**  
Email Security Virtual Appliance

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

Monitor Mail Policies Security Services Network System Administration

[No Changes Pending](#)

### Sender Group: WHITELIST - IncomingMail 172.16.16.25:25

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

[Back to HAT Overview](#) [Edit Settings...](#)

### Find Senders

Find Senders that Contain this Text:  [Find](#)

### Sender List: Display All Items in List

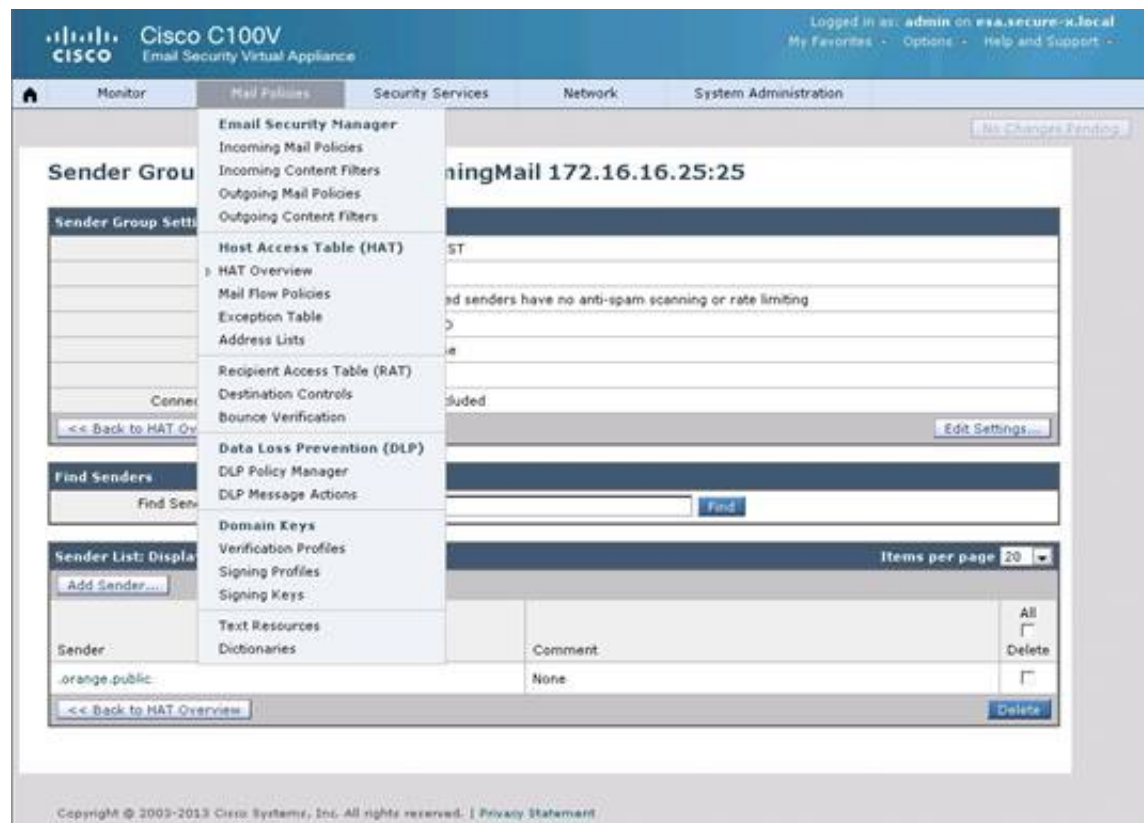
[Add Sender...](#) Items per page: 20

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

[Back to HAT Overview](#) [Delete](#)

Copyright © 2003-2013 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)



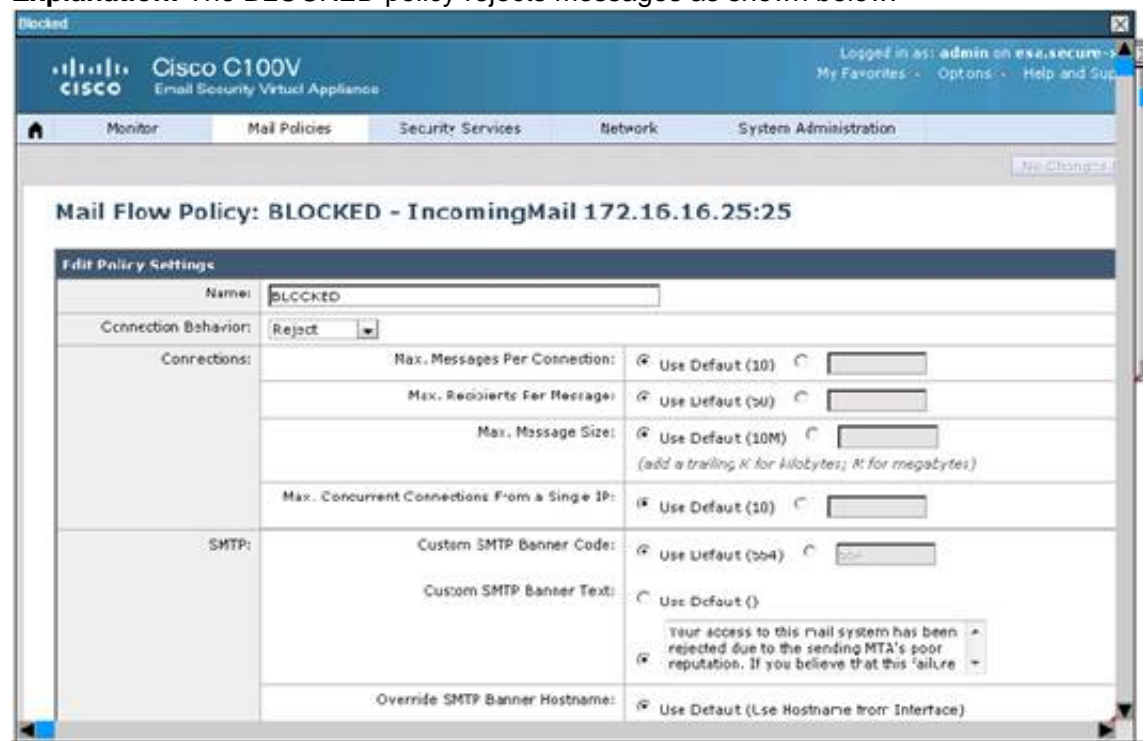


The Cisco Email Security Appliance will reject messages from which domains?

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

**Answer:** G

**Explanation:** The BLOCKED policy rejects messages as shown below:



Capture

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



Capture

**NEW QUESTION 666**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-210 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-210 Product From:

<https://www.2passeasy.com/dumps/300-210/>

## Money Back Guarantee

### 300-210 Practice Exam Features:

- \* 300-210 Questions and Answers Updated Frequently
- \* 300-210 Practice Questions Verified by Expert Senior Certified Staff
- \* 300-210 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 300-210 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year