ExamsLand provides 100% free Cisco 300-210 practice questions and answers in pdf. Instant access.

Cisco

300-210 Exam

Cisco Threat Control Solutions Exam

Questions & Answers
Demo

Version: 17.0

Question: 1

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

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

Answer: A, C, E

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

Question: 2

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

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

Answer: B

Question: 3

Which feature requires the network discovery policy for it to work on the Cisco Next Generate fusion Prevent-on System,

A. impact flags
B. URL filtering
C. security intelligence
D. health monitoring

Answer: A

Question: 4

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

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

Answer: D

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

Question: 5

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

Question: 6

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

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

Answer: ABE

Question: 7

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

A. data
B. session
C. buffer
D. statistics
E. verbose

Answer: BD

Question: 8

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: B

Question: 9

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

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

D. The physical appliance is configured with a DHCP-enabled management port to receive an IP Address automatically, but you must assign the virtual appliance an IP address manually in your management subnet.

Answer: B

Question: 10

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

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

Answer: D

Question: 11

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

Question: 12

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

Question: 13

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

Question: 14

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: A

Explanation:
http://www.cisco.com/c/en/us/td/docs/security/firesight/54HYPERLINK "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"1/firepower-module-user-guHYPERLINK "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"ide/asa-firepoHYPERLINK "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"wer-module-user-guide-v541/AC-Rules-Tuning-Overview.html

Question: 15

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/datasheHYPERLINK "http://www.cisco.com/c/en/us/products/collateral/security/fireamp-private-cloud-virtual-appliance/datasheet-c78-733180.html"et-c78-73318HYPERLINK "http://www.cisco.com/c/en/us/products/collateral/security/fireamp-private-cloud-virtual-appliance/datasheet-c78-733180.html"0.html

Question: 16

Refer to the exhibit.

```
S*       0.0.0.0.0.0.0.0 [1/0] via 1.1.1.1, outside
C            1.1.1.0 225.255.255.0 is directly connect, outside
S            172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C            192.168.100.0 255.255.255.0 is directly connected, inside
C            172.16.10.0 255.255.255.0 is directly connected, dmz
S             10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz


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

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

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

service-policy inside-policy inside
```

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 if redirected.
C. All TCP traffic that arrives on the inside interface is redirected.
D. All ingress traffic that arrives on the inside interface is redirected.
E. All ingress and egress traffic is redirected to the Cisco FirePOWER module.

Answer: E

Question: 17

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/HYPERLINK "http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Hybrid_Interfaces.html"60/configuration/guide/fpmcHYPERLINK "http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Hybrid_Interfaces.html"-conHYPERLINK "http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Hybrid_Interfaces.html"fig-guide-v60/Hybrid_Interfaces.html

Question: 18

Which type of policy is used to define the scope for applications that are running on hosts?

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

Answer: D

Question: 19

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

Question: 20

Which protocols can be specified in a Snort rule header for analysis?

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

Answer: A

Question: 21

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

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

Answer: B

Question: 22

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: D

Question: 23

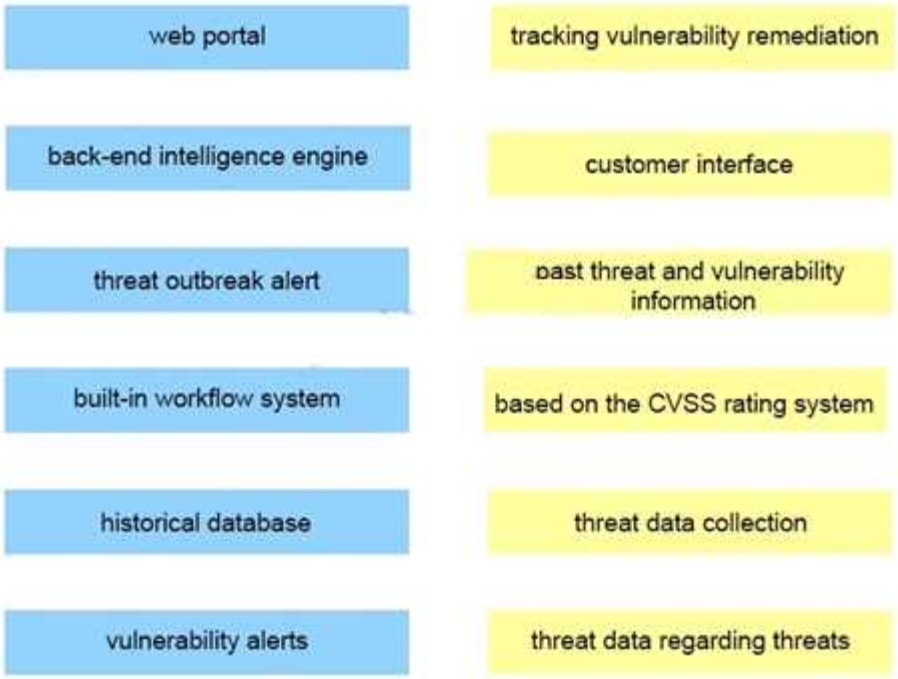
DRAG DROP
Drag and drop the steps on the left into the correct order of initial Cisco IOS IPS configuration on the right.

Answer:

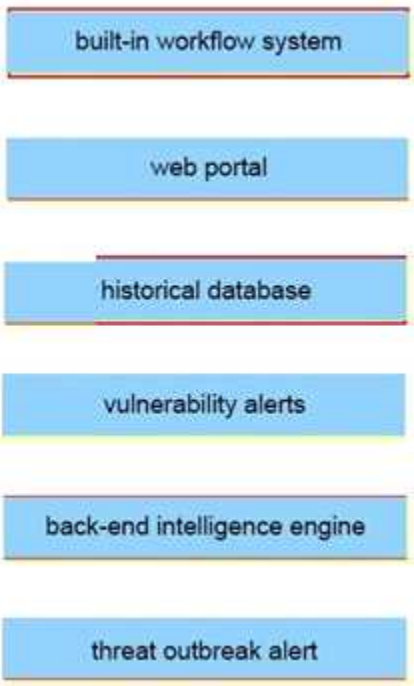
Question: 24

DRAG DROP

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



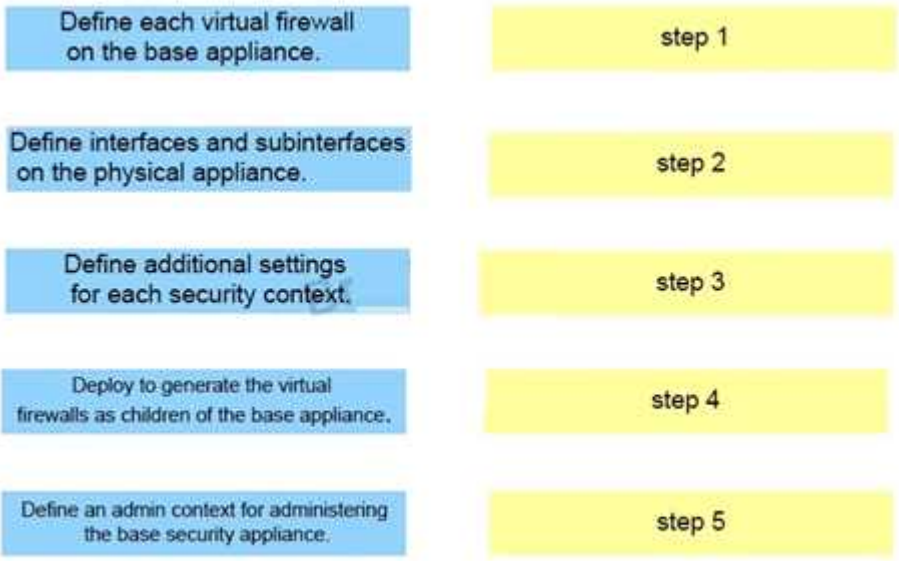
Answer:



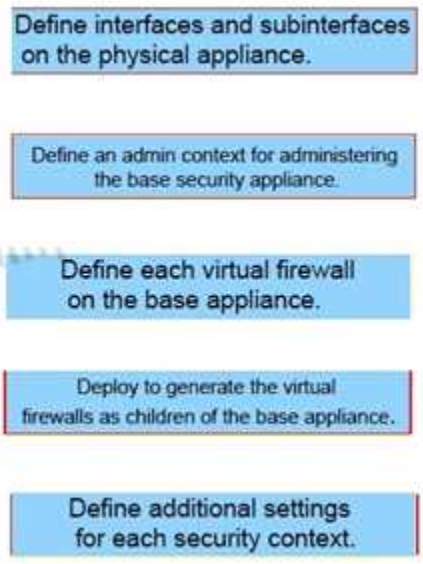
Question: 25

DRAG DROP

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



Answer:



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

Question: 26

When using Cisco FirePOWFR Services for ASA, how is traffic directed form based Cisco ASA to the CiscoPOWER Services?

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

Answer: D

Question: 27

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

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

Answer: B, E

Question: 28

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

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

Answer: C

Question: 29

Which two appliances support logical routed interfaces? (Choose two.)

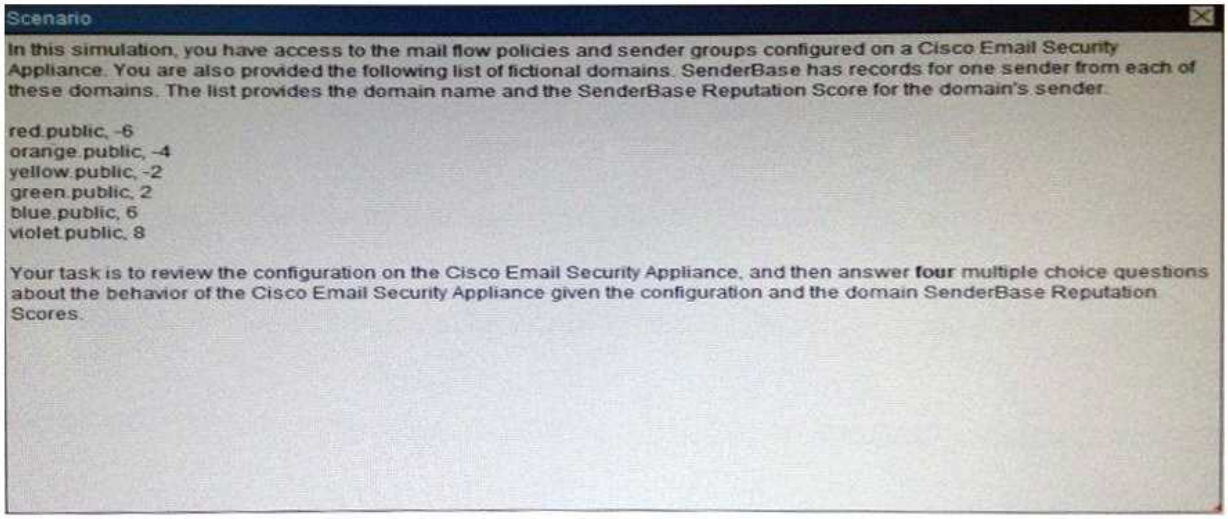
A. FirePOWER services for ASA-5500-X
B. FP-4100-series
C. FP-8000-series

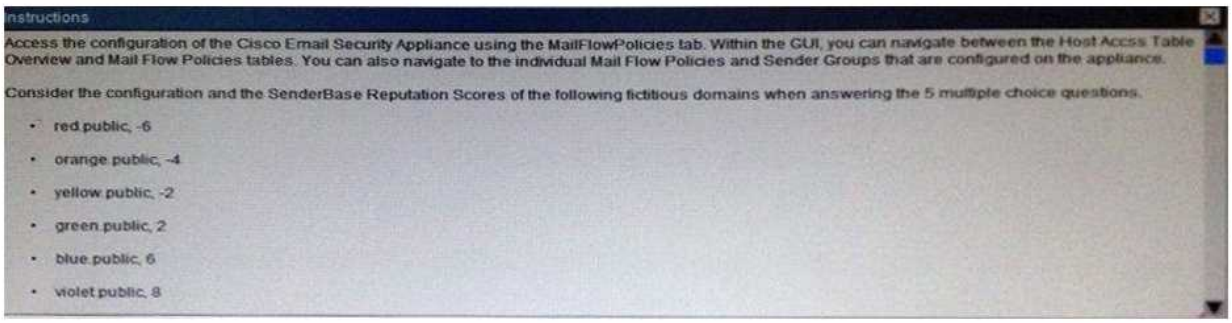
D. FP-7000-series
E. FP-9300-series

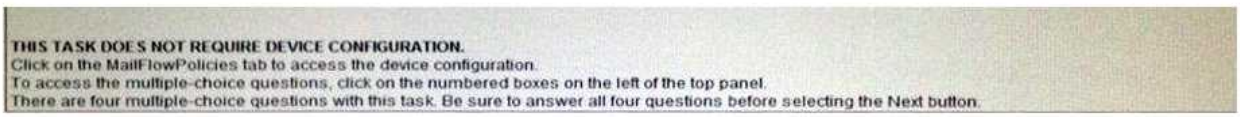
Answer: D

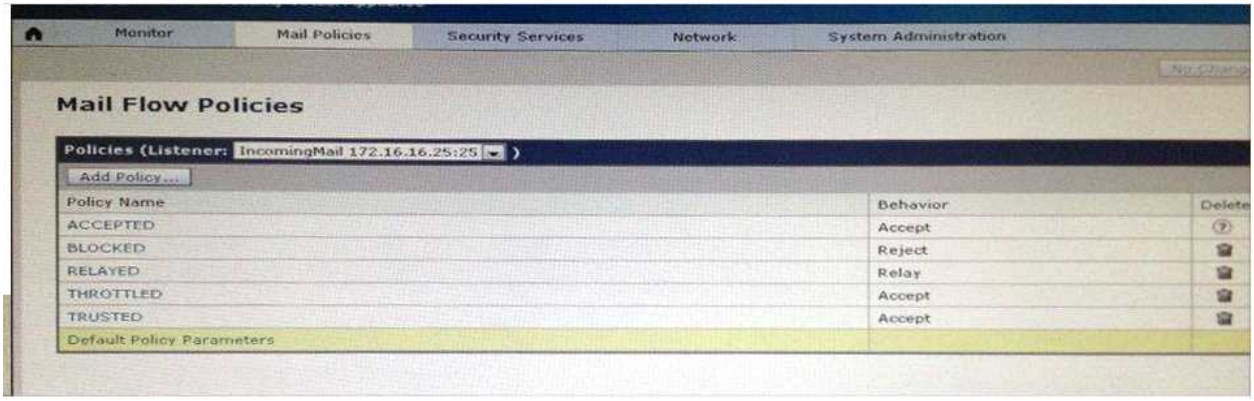
Question: 30

Scenario









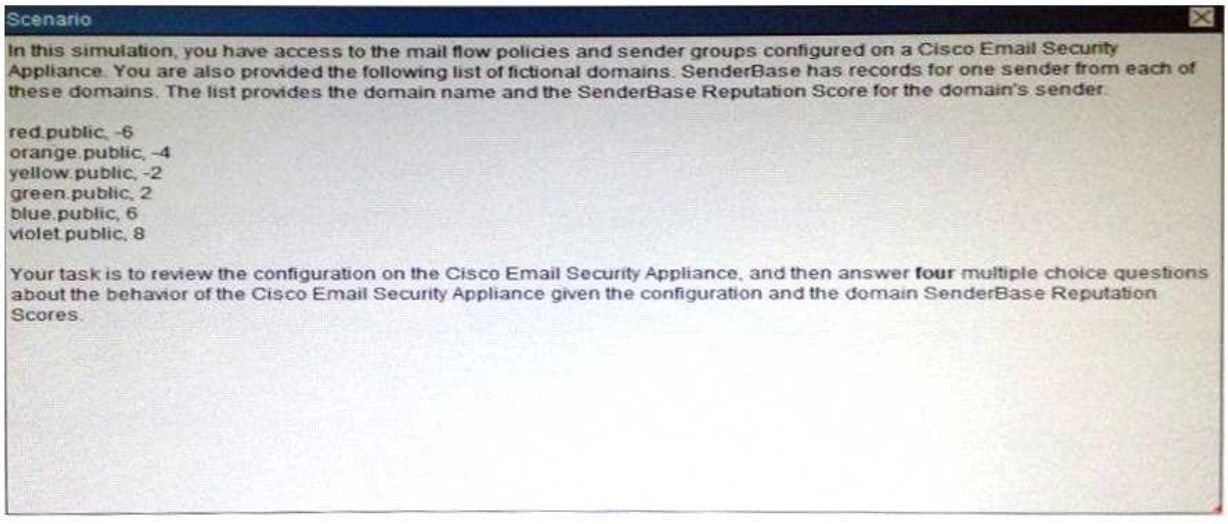
For which domains will the Cisco Email Security Appliance allow up to 5000 recipients per message?

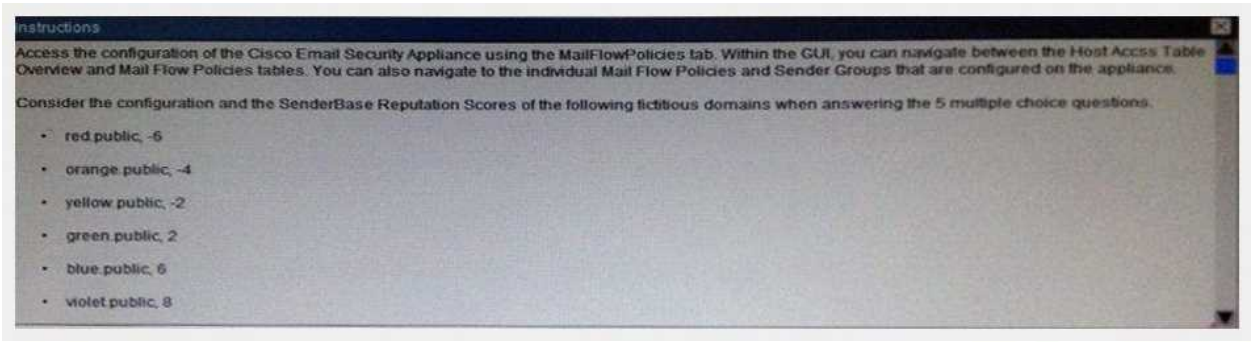
A. violet.public
B. violet.public and blue.public
C. violet.public, blue.public and green.public
D. red.public
E. orange.public
F. red.public and orange.public

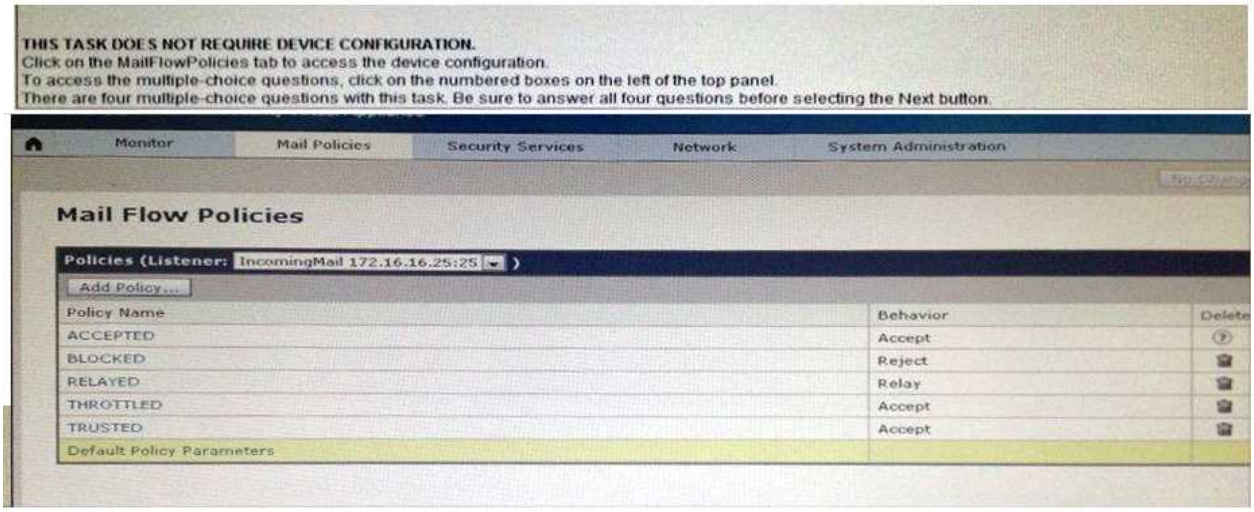
Answer: E

Question: 31

Scenario







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

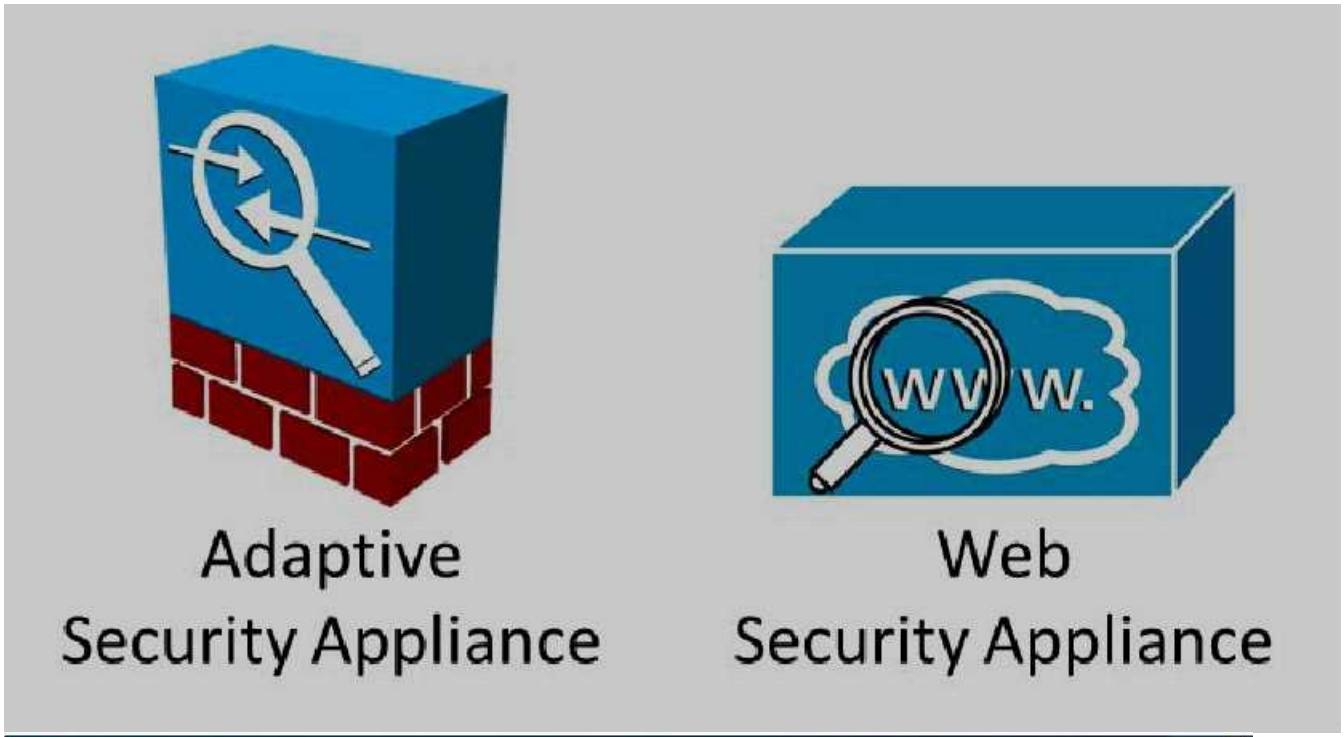
A. 1 KB
B. 100 KB
C. 1 MB
D. 10 MB
E. 100 MB
F. Unlimited

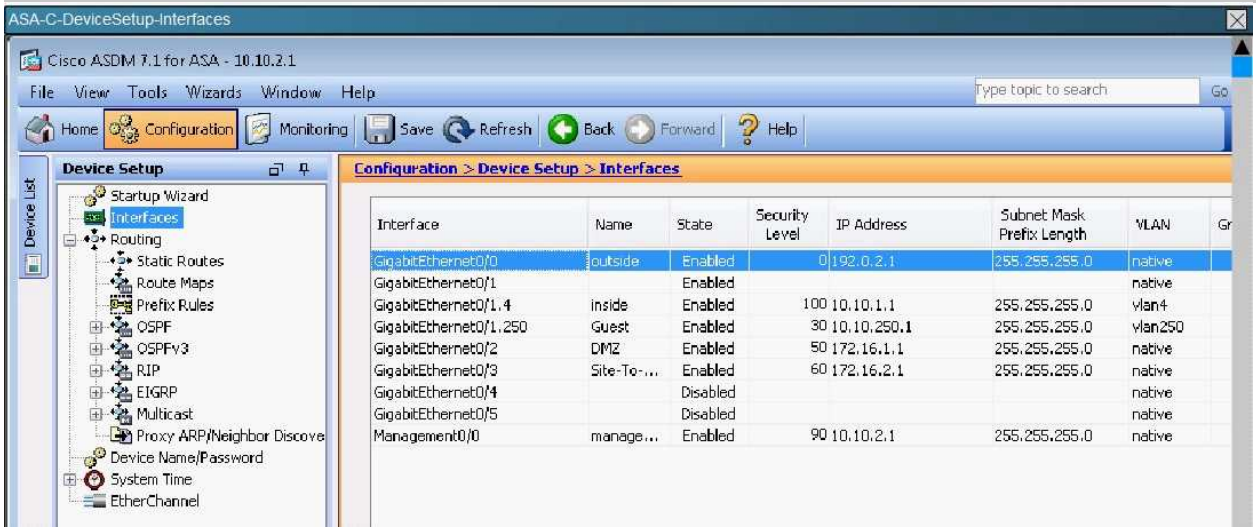
Answer: D

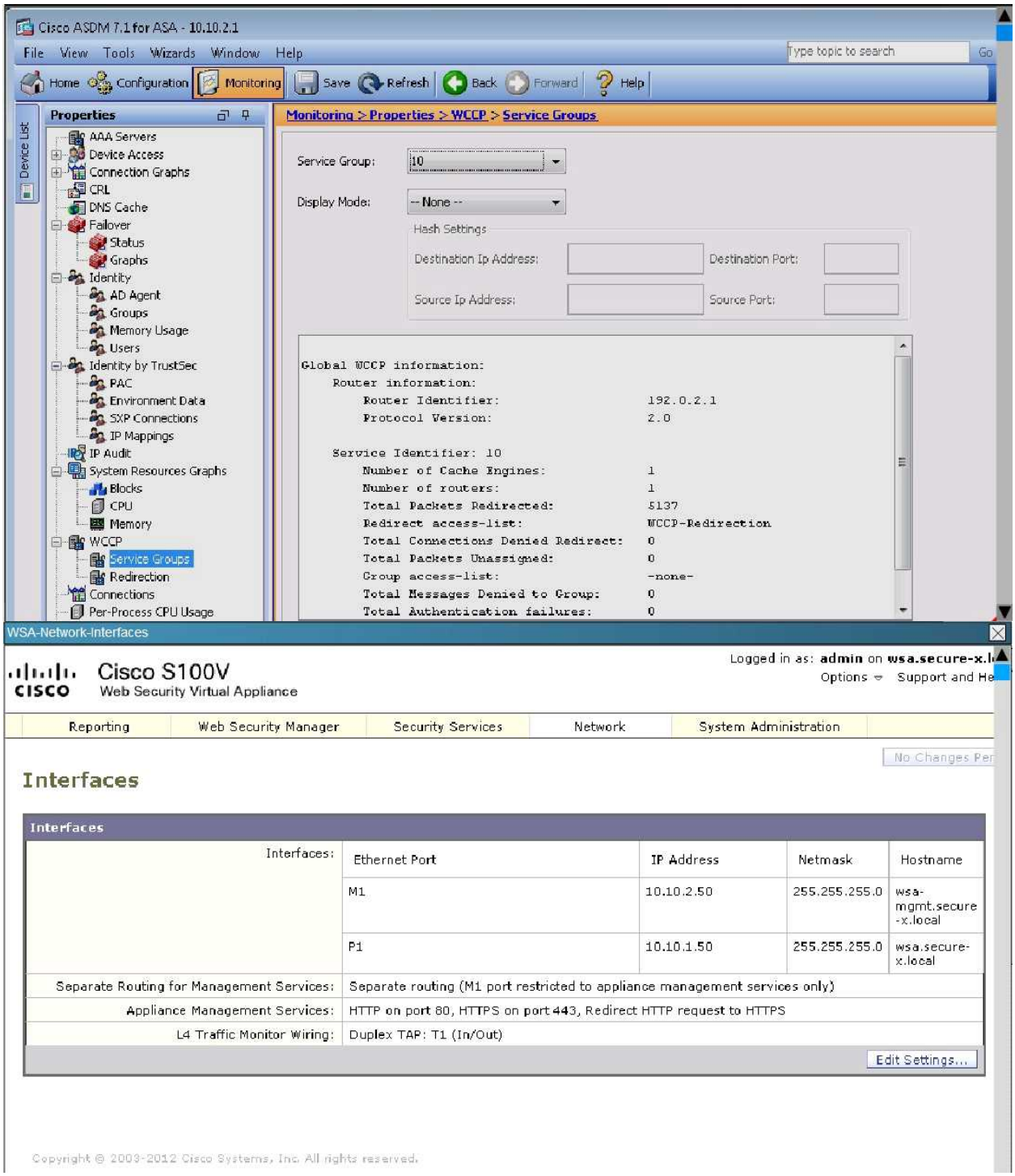
Question: 32

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

best answer.


Adaptive
Security Appliance
Web
Security Appliance


ASA-C-DeviceSetup-Interfaces
Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Device Setup
Startup Wizard
Interfaces
Routing
Static Routes
Route Maps
Prefix Rules
OSPF
OSPFv3
RIP
EIGRP
Multicast
Proxy ARP/Neighbor Discove
Device Name/Password
System Time
EtherChannel
Configuration > Device Setup > Interfaces
Interface Name State Security Level IP Address Subnet Mask Prefix Length VLAN
GigabitEthernet0/0 outside Enabled 0 192.0.2.1 255.255.255.0 native
GigabitEthernet0/1 Enabled native
GigabitEthernet0/1.4 inside Enabled 100 10.10.1.1 255.255.255.0 vlan4
GigabitEthernet0/1.250 Guest Enabled 30 10.10.250.1 255.255.255.0 vlan250
GigabitEthernet0/2 DMZ Enabled 50 172.16.1.1 255.255.255.0 native
GigabitEthernet0/3 Site-To-... Enabled 60 172.16.2.1 255.255.255.0 native
GigabitEthernet0/4 Disabled native
GigabitEthernet0/5 Disabled native
Management0/0 manage... Enabled 90 10.10.2.1 255.255.255.0 native



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.

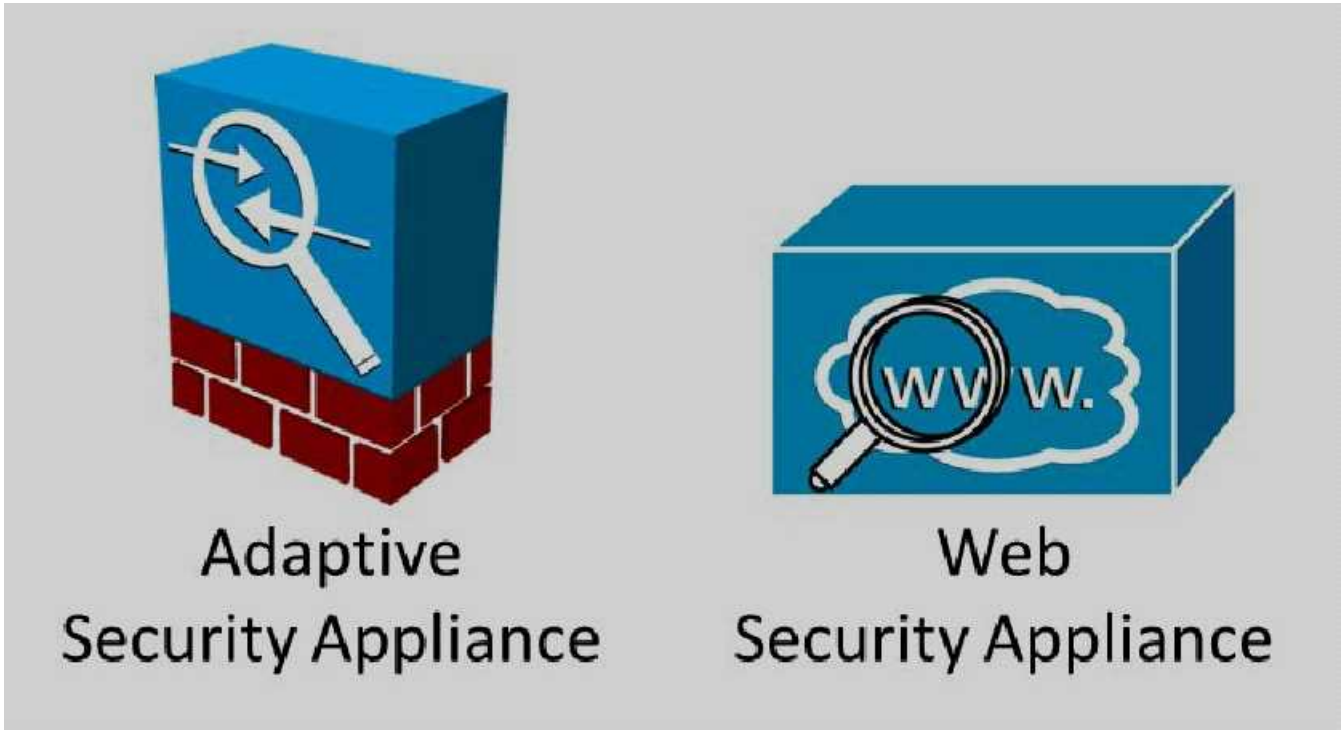
E. Two Cisco ASAs and one Cisco WSA.
F. Two Cisco ASAs and two Cisco WSAs.

Answer: A

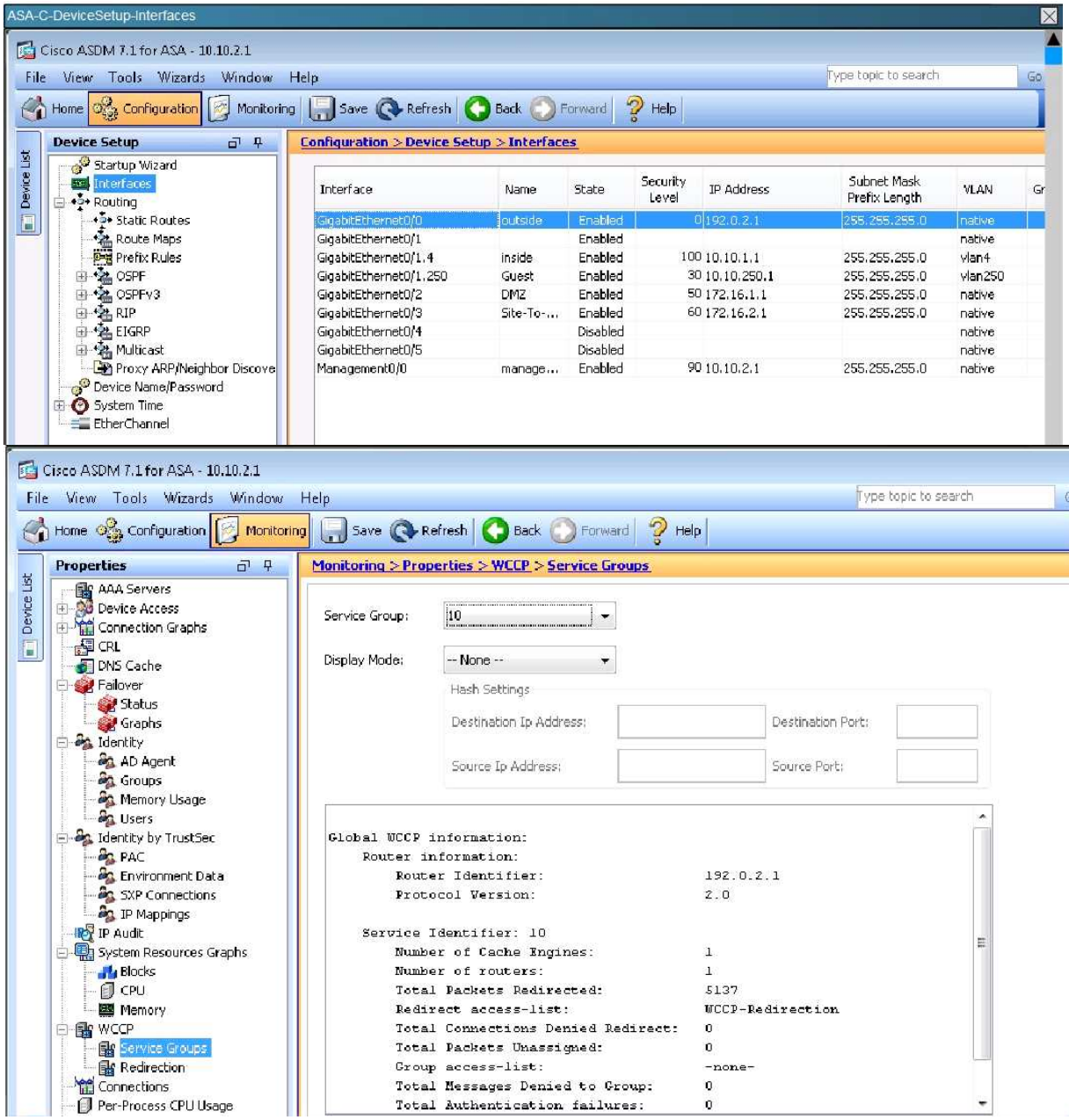
Explanation:
We can see from the output that the number of routers (ASA's) is 1, so there is a single ASA or an active/ standby pair being used, and 1 Cache Engine. If the ASA's were in a active/active role it would show up as 2 routers.

Question: 33

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.



ExamsLand provides 100% free Cisco 300-210 practice questions and answers in pdf. Instant access.



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.

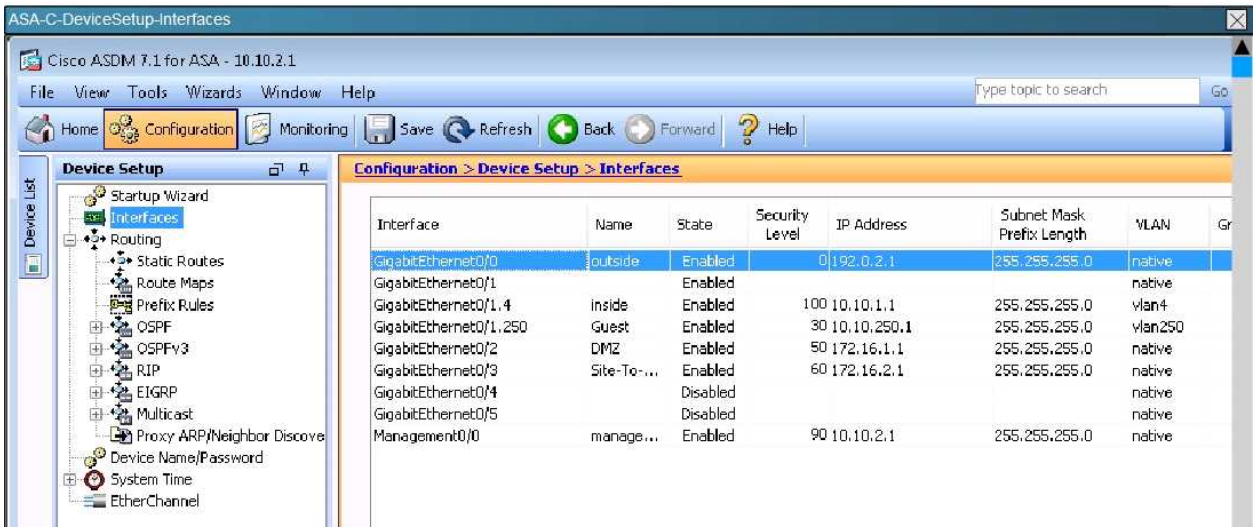
Question: 34

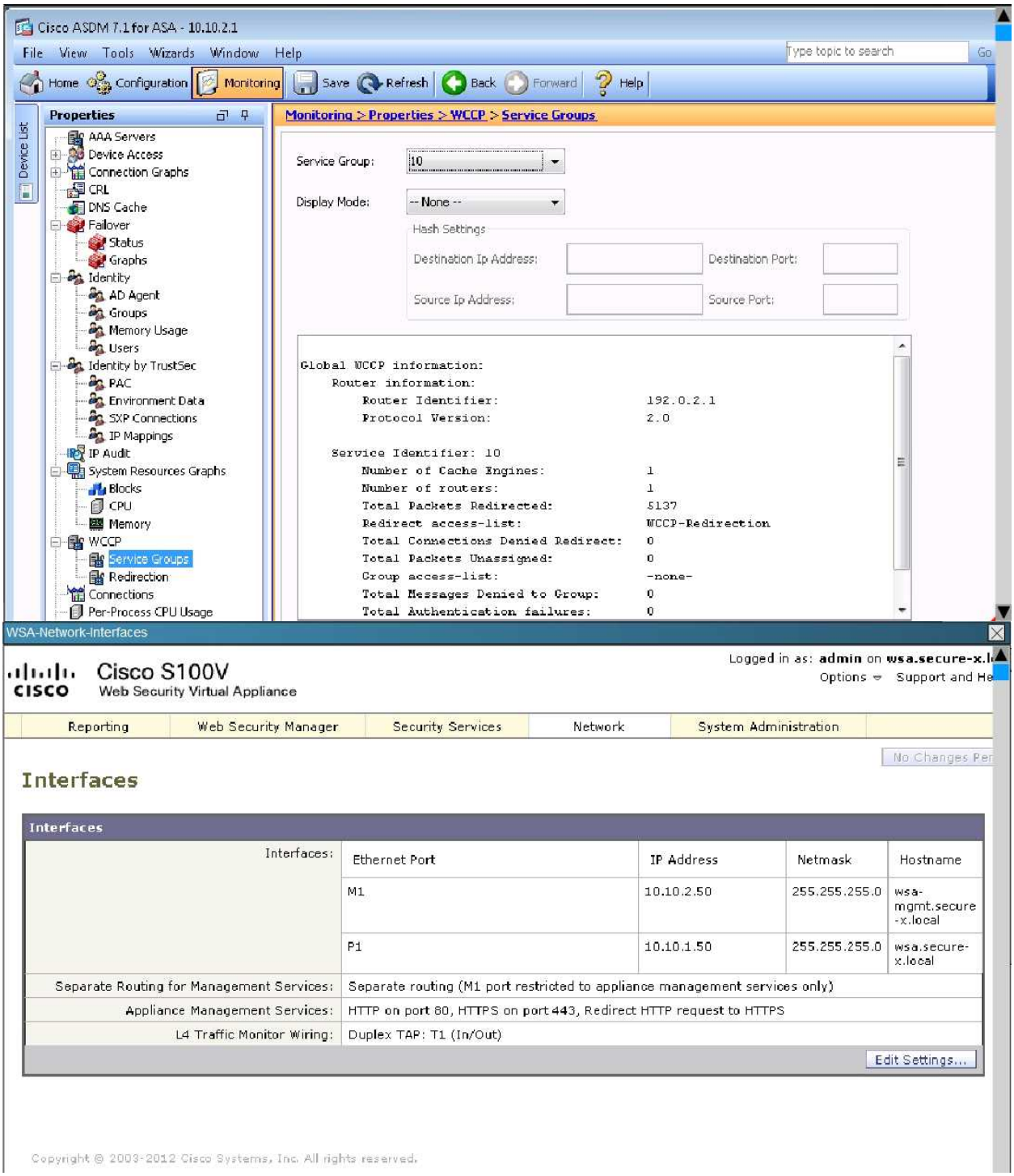
The Web Cache Communication Protocol (WCCP) is a content-routing protocol that can facilitate the redirection of traffic flows in real time. Your organization has deployed WCCP to redirect web traffic that traverses their Cisco Adaptive Security Appliances (ASAs) to their Cisco Web Security Appliances

(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



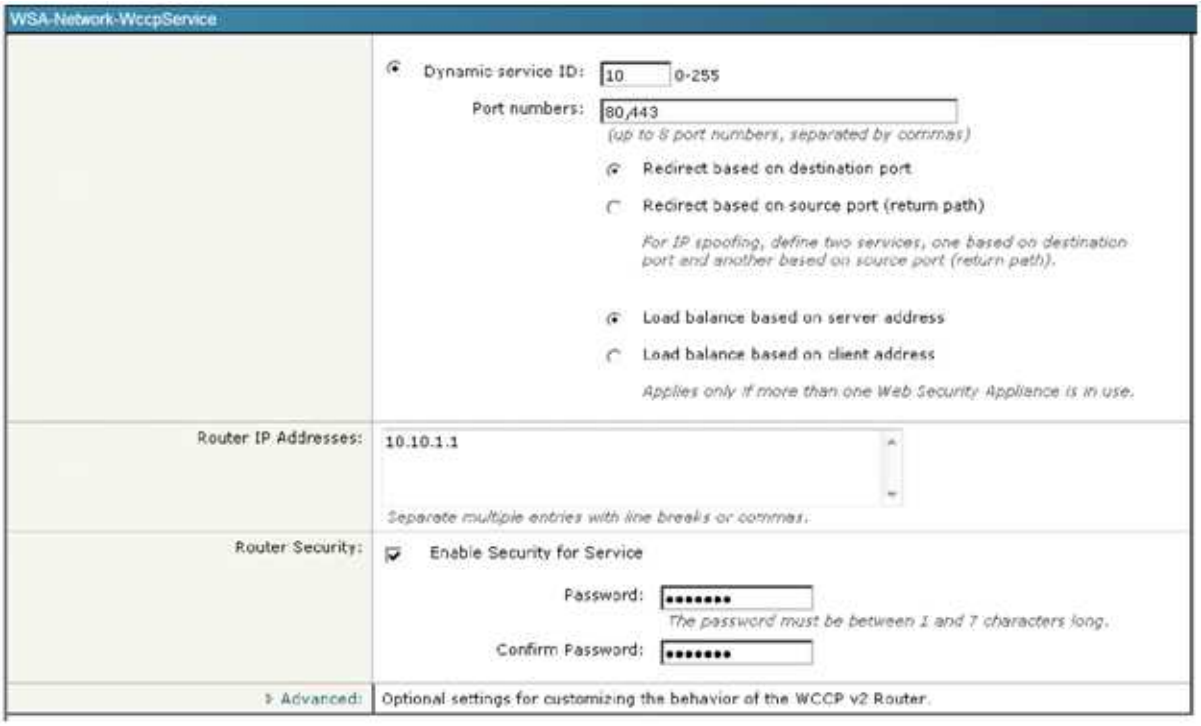


Between the Cisco ASA configuration and the Cisco WSA configuration, what is true with respect to redirected ports?

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:

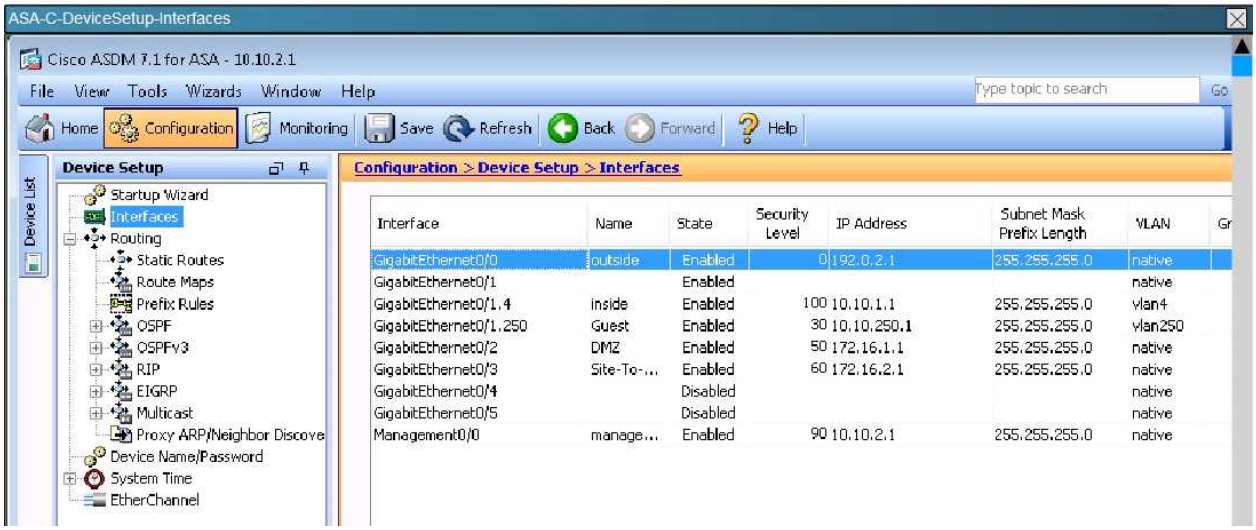


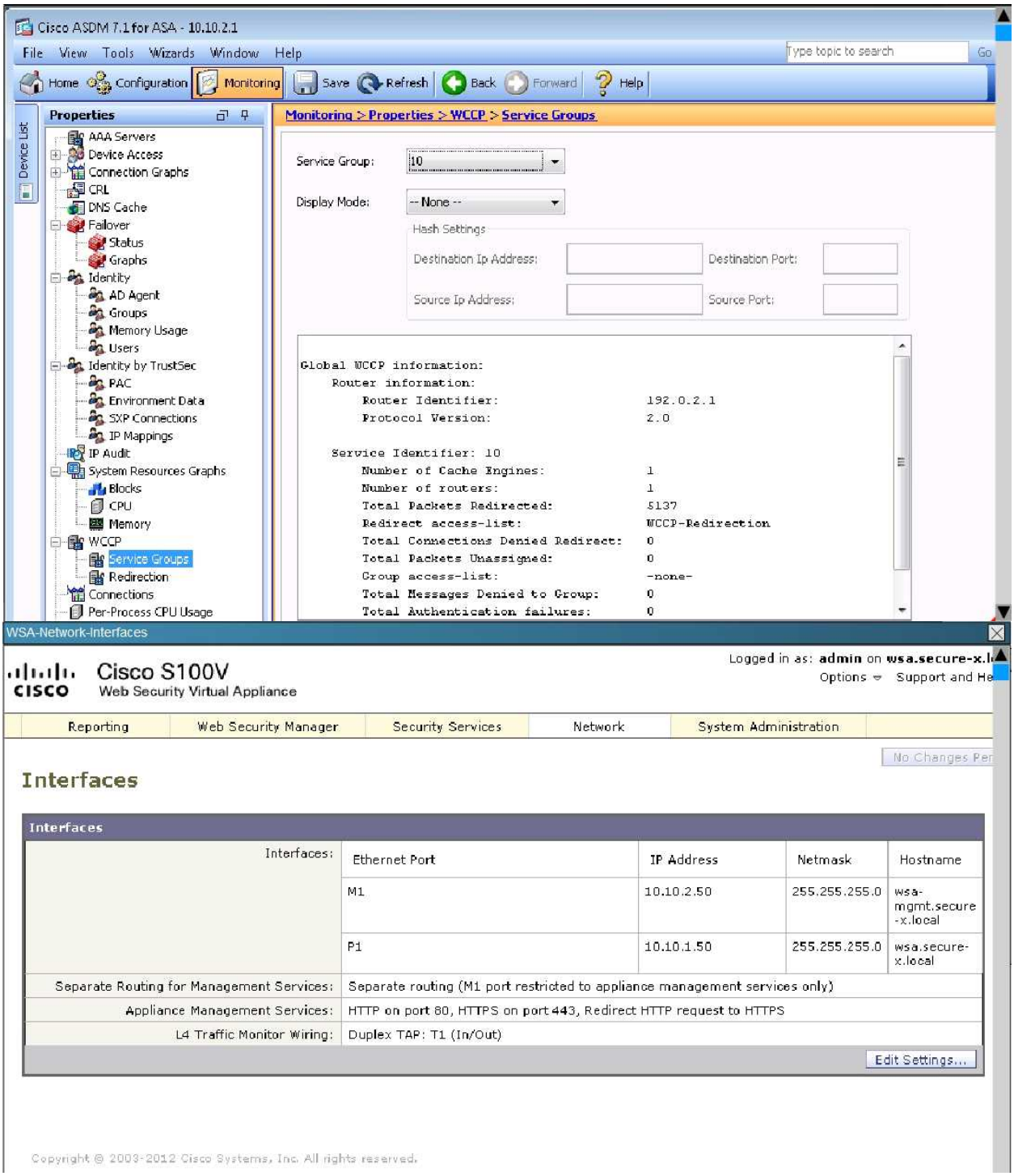
Question: 35

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



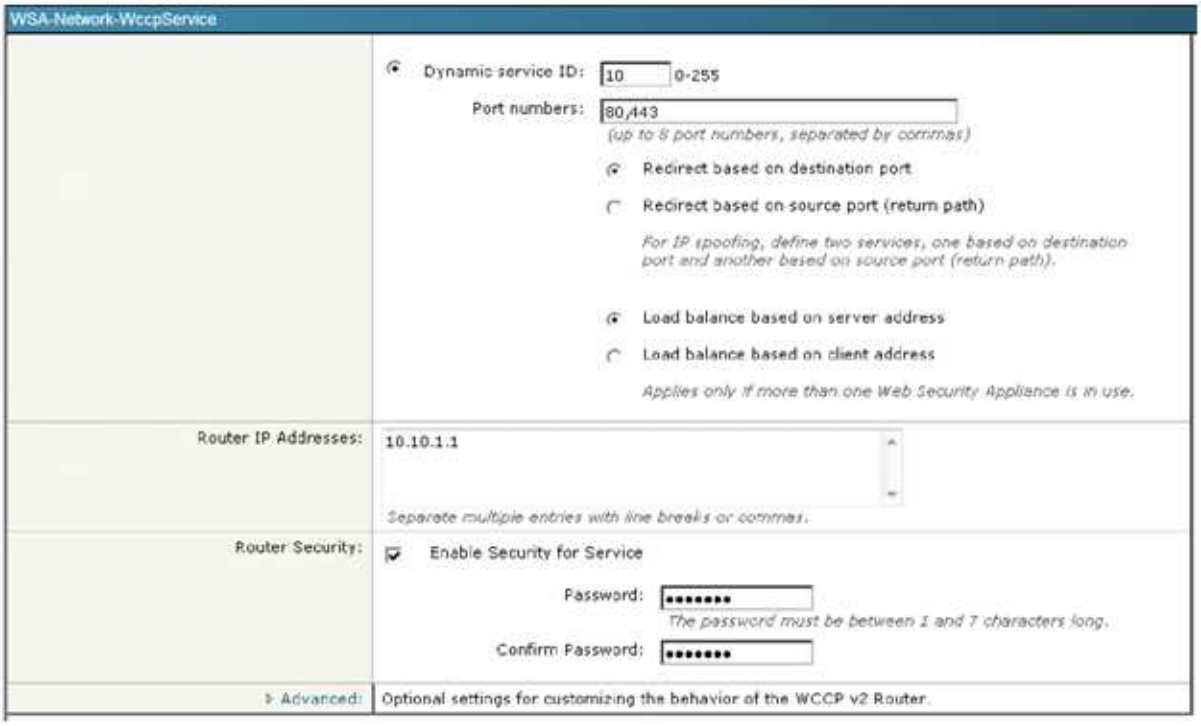


Between the Cisco ASA configuration and the Cisco WSA configuration, what is true with respect to redirected ports?

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:



Thank You For Trying 300-210 PDF Demo

To try our 300-210 Premium Files visit link below:

https://examsland.com/latest-exam-questions/300-210/

Start Your 300-210 Preparation

Use Coupon EL25 for extra 25% discount on the purchase of Practice Test Software.