

### **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:

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

#### 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-configguide-v60/fpmc-config-guide-v60\_appendix\_01011110.html#ID-2201-

00000005"docs/security/firepower/60/configuration/guideHYPERLINK

<u>"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-confi</u>

"http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configguide-v60/fpmc-config-guide-v60\_appendix\_01011110.html#ID-2201-00000005"nfig-guidev60\_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 serverB. a PKI certificate serverC. an HTTP serverD. 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/asafirepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html"1/firepower-module-userguHYPERLINK "http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-moduleuser-guide/asa-firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html"ide/asafirepoHYPERLINK "http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-moduleuser-guide/asa-firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html"ide/asafirepoHYPERLINK "http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-moduleuser-guide/asa-firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html"wer-moduleuser-guide/asa-firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html"wer-moduleuser-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-virtualappliance/datasheHYPERLINK "http://www.cisco.com/c/en/us/products/collateral/security/fireampprivate-cloud-virtual-appliance/datasheet-c78-733180.html"et-c78-73318HYPERLINK "http://www.cisco.com/c/en/us/products/collateral/security/fireamp-private-cloud-virtualappliance/datasheet-c78-733180.html"0.html

#### **Question: 16**

Refer to the exhibit.

s*	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
с с	192.168.100.0 255.255.255.0 is directly connected, inside
	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
<u></u>	
	s-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
acces	s-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any
class	-map redirect-class
n	atch access-list redirect-acl
polic	y-map inside-policy
c	lass redirect-class
	sfr fail-open
servi	ce-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-configguide-v60/Hybrid\_Interfaces.html"60/configuration/guide/fpmcHYPERLINK "http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configguide-v60/Hybrid\_Interfaces.html"-conHYPERLINK "http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configguide-v60/Hybrid\_Interfaces.html"-conHYPERLINK "http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configguide-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 detectionB. spam scanningC. APT detectionD. antivirus scanningE. 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

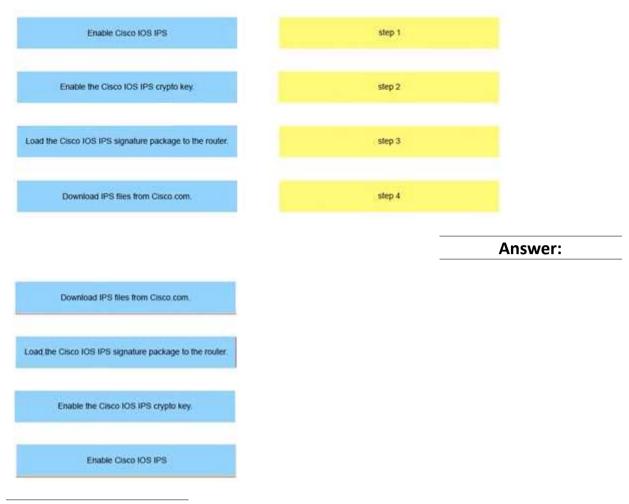
- B. passive
- C. inline tap
- D. routed
- E. transparent

Answer: D

#### Question: 23

DRAG DROP

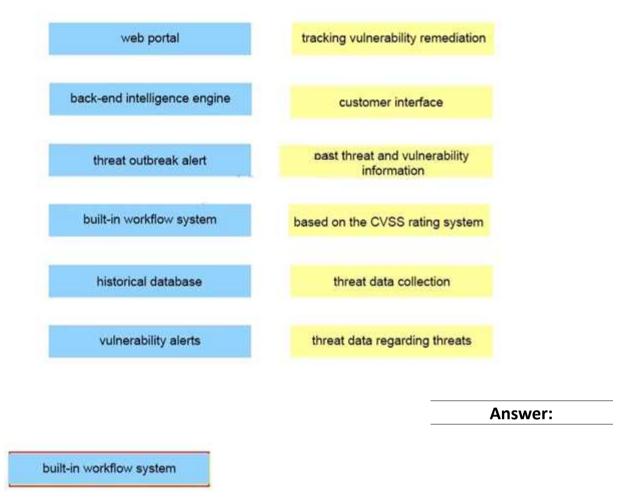
Drag and drop the steps on the left into the correct order of initial Cisco IOS IPS configuration on the right.



#### **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.



web portal

historical database

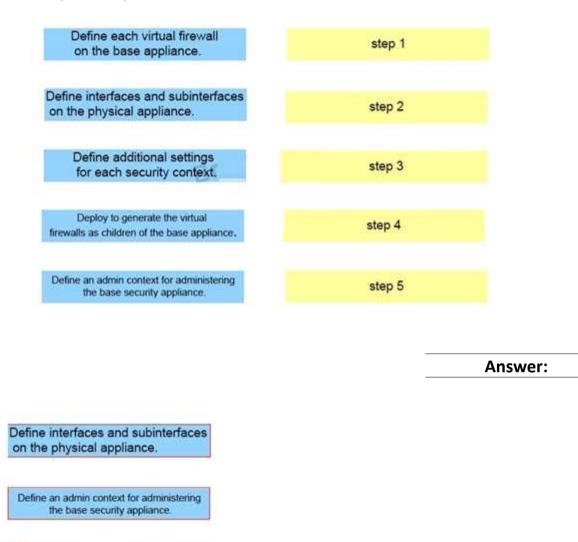
vulnerability alerts

back-end intelligence engine

threat outbreak alert

Question: 25

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.



Reference:

http://www.cisco.com/c/en/us/td/docs/security/security\_management/cisco\_security\_manager/sec urity\_manager/4-4/user/guide/CSMUserGuide\_wrapper/pxcontexts.pdf (page 2 to 4)

Question: 26

Define each virtual firewall on the base appliance.

Deploy to generate the virtual firewalls as children of the base appliance.

> Define additional settings for each security context.

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

Scenario	×
In this simulation, you have access to the mail flow policies and sender groups configure Appliance. You are also provided the following list of fictional domains. SenderBase has a these domains. The list provides the domain name and the SenderBase Reputation Score	records for one sender from each of
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 an about the behavior of the Cisco Email Security Appliance given the configuration and the d Scores.	
nstructions	
Access the configuration of the Cisco Email Security Appliance using the MailFlowPolicies tab. Within the GUI, you	can navigate between the Host Accss Table
Overview and Mail Flow Policies tables. You can also navigate to the individual Mail Flow Policies and Sender Grou	
Consider the configuration and the SenderBase Reputation Scores of the following fictitious domains when answe	ering the 5 multiple choice questions.
red public, -6	
orange public, -4	
yellow public, -2	
green public, 2	
blue.public, 6	
blue public, 6     violet public, 8	

Crick on the Mail low 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.

			Contraction of the second		Na.5h
Ma	ail Flow Po	licies			
Po	licies (Listener:	IncomingMail 172.16	16.25:25 .		
4	Add Policy				1. Contract (1997)
Po	licy Name			Behavior	De
AC	CCEPTED			Accept	0
BL	OCKED			Reject	1
RE	LAYED			Relay	-
TH	ROTTLED			Accept	
	RUSTED			Accept	1
TR		neters			

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

Scenario	$\times$
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 o these domains. The list provides the domain name and the SenderBase Reputation Score for the domain's sender.	ot
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 four multiple choice question about the behavior of the Cisco Email Security Appliance given the configuration and the domain SenderBase Reputation Scores.	ons

ructions					1.8
ess the configuration of rview and Mail Flow Poly	the Cisco Email Securit icles tables. You can als	y Appliance using the MailFlow so navigate to the individual Ma	Policies tab. Within I I Flow Policies and	the GUI, you can navigate between the F Sender Groups that are configured on It	tost Accss Table appliance.
sider the configuration	and the SenderBase Re	putation Scores of the followin	g lictitious domains	when answering the 5 multiple choice of	puestions.
red public, -6					
• orange public, -4					
vellow public, -2					
• green public, 2					
and and a second and					
<ul> <li>blue.public, 6</li> </ul>					
<ul> <li>violet public, 8</li> </ul>					
ck on the MailFlowPolic access the multiple-ch					
ck on the MailFlowPolic access the multiple-ch	cies tab to access the d loice questions, click of	levice configuration. In the numbered boxes on the			Nor-cyre
ck on the MailFlowPolic access the multiple-ch ere are four multiple-ch Monitor Mail Flow Po	des tab to access the d noice questions, click or noice questions with thi Mail Policies	levice configuration. In the numbered boxes on the s task. Be sure to answer all t Security Services	our questions befor	e selecting the Next button.	599.527#
ck on the MailFlowPolic access the multiple-ch ere are four multiple-ch Monitor Mail Flow Po	cies tab to access the d noice questions, click or noice questions with thi Mail Policies	levice configuration. In the numbered boxes on the s task. Be sure to answer all t Security Services	our questions befor	e selecting the Next button.	
ck on the MailFlowPolic access the multiple-ch ere are four multiple-ch Monitor Mail Flow Policies (Listener	des tab to access the d noice questions, click or noice questions with thi Mail Policies	levice configuration. In the numbered boxes on the s task. Be sure to answer all t Security Services	our questions befor	e selecting the Next button.	(App S2)ar
ck on the MailFlowPolic access the multiple-ch ere are four multiple-ch Manitor Mail Flow Policies Policies (Listener Add Policy	des tab to access the d noice questions, click or noice questions with thi Mail Policies	levice configuration. In the numbered boxes on the s task. Be sure to answer all t Security Services	our questions befor	e selecting the Next button. System Administration	CEGE COLLEGE
A con the MailFlowPolic access the multiple ch ere are four multiple ch Monitor Mail Flow Policies Add Policy Policy Name	des tab to access the d noice questions, click or noice questions with thi Mail Policies	levice configuration. In the numbered boxes on the s task. Be sure to answer all t Security Services	our questions befor	e selecting the Next button. System Administration Behavior	Defe
Accepted	des tab to access the d noice questions, click or noice questions with thi Mail Policies	levice configuration. In the numbered boxes on the s task. Be sure to answer all t Security Services	our questions befor	e selecting the Next button. System Administration Behavior Accept	Dela
Add Policy Name Add Policy Name Add Policy Name Add Policy Name ACCEPTED BLOCKED	des tab to access the d noice questions, click or noice questions with thi Mail Policies	levice configuration. In the numbered boxes on the s task. Be sure to answer all t Security Services	our questions befor	e selecting the Next button System Administration Behavior Accept Reject	Dela
Add Policy Name Accepted BLOCKED RELAYED	des tab to access the d noice questions, click or noice questions with thi Mail Policies	levice configuration. In the numbered boxes on the s task. Be sure to answer all t Security Services	our questions befor	e selecting the Next button System Administration Behavior Accept Reject Relay	Defe T

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

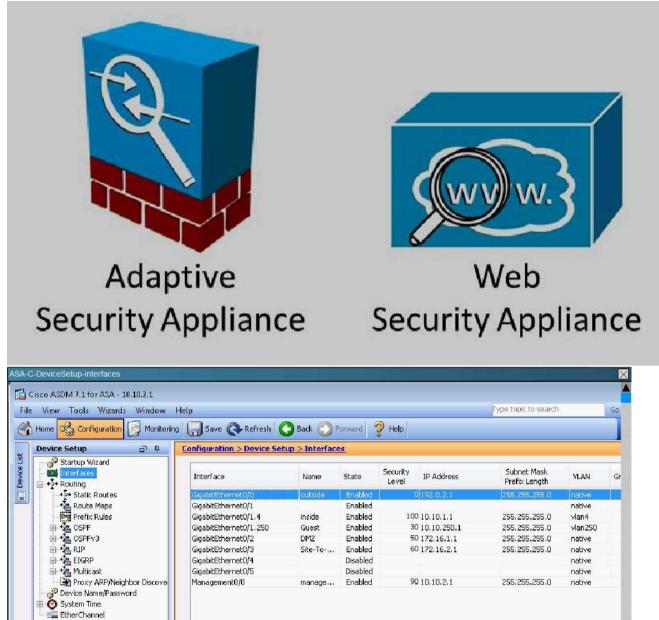
#### Question: 32

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.



Gisco ASDM 7.1 for ASA - 10.10.2.1 File View Tools Wizards Window Help			Type topic to searc	h
home 🖧 Configuration 🔯 Monitoring	Save 🔇 Refresh 🔇 Back 🕥 Forward 🦻 He	elp		
Properties a P Monito	pring > Properties > WCCP > Service Groups			
AAA Servers Device Access Connection Graphs Connection Graphs DNS Cache DNS Cache Status Graphs Caphs Connection Graphs Connection Graph	bal WCCP information: Router Information:	Destination Po Source Port:	rt:	
SXP Connections IP Mappings IP Audit System Resources Graphs IP Blocks CP Service Groups Redirection Connections Per-Process CPU Usage CANetwork-Interfaces	Frotocol Version: Protocol Version: Service Identifier: 10 Number of Cache Engines: Number of routers: Total Packets Redirected: Redirect access-list: Total Connections Denied Redirect: Total Packets Unassigned: Group access-list: Total Messages Denied to Group: Total Messages Denied to Group: Total Authentication failures:	1 1 1 5137 WCCD-Redirection 0 		E
SCO Cisco S100V Web Security Virtual Appliance		Logged i	n as: <b>admin</b> on Options <del>v</del>	wsa.secure-x Support and I
Reporting Web Security Manag	er Security Services Network	System Admir	nistration	
Interfaces Interfaces Interface	S: Ethernet Port	IP Address	Netmask 255.255.255.0	No Changes F Hostname wsa-
			2001200120010	mgmt.secure -x.local
1000 N 000 M 100 - 550 - 550 - 550	P1	10.10.1.50	255.255.255.0	wsa.secure- x.local
Separate Routing for Management Service			30.50	
Appliance Management Service		t HTTP request to HTTPS		
L4 Traffic Monitor Wirin	g: Duplex TAP: T1 (In/Out)		E	dit Settings
Copyright © 2003-2012 Cisco Systems, Inc. All.	rights received			

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.





Web Security Appliance

-	isco ASDM 7.1 for ASA - 10.10.2.1 View Tools Wizards Window	Usla					Type topic to search		Go
- 14		1.1704 <b>4</b> .02		10			i ypo copie co sedreri		90
1	Home Configuration Monitorin	g 🔚 Save 🔇 Refresh	n 🚺 Back 🔘 I	Forward	Help				
	Device Setup 🗗 म	Configuration > Device	Setup > Interfac	es					
	🚽 🔗 Startup Wizard				12 00		1 10 10 10 10 10 10 10 10 10 10 10 10 10		
	Interfaces	Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN	Gr
	➡ +♣ Routing	GigabitEthernet0/0	outside	Enabled		0 192.0.2.1	255.255.255.0	native	
	**** Route Maps	GigabitEthernet0/1	COUSIGE	Enabled		0 192/0-2-1	(200,200,200,0	native	-
	Prefix Rules	GigabitEthernet0/1.4	inside	Enabled	100	0 10.10.1.1	255,255,255.0	vlan4	
		GigabitEthernet0/1.250		Enabled		0 10.10.250.1	255,255,255.0	vlan250	
		GigabitEthernet0/2	DMZ	Enabled		0 172.16.1.1	255.255.255.0	native	
	+ + RIP	GigabitEthernet0/3	Site-To			0 172.16.2.1	255.255.255.0	native	
	🖶 🧏 EIGRP	GigabitEthernet0/4		Disabled				native	
	🕀 📲 Multicast	GigabitEthernet0/5		Disabled				native	
	Proxy ARP/Neighbor Discove	Management0/0	manage	Enabled	90	0 10.10.2.1	255.255.255.0	native	
	Bevice Name/Password	844	22						
	🗄 🧑 System Time								
	EtherChannel								
	View Tools Wizards Window Home of Configuration Monitor Properties a P				*	P	Type topic to s	earch	
	Home of Configuration Monitor Properties a P	ing 🕞 Save 🗨 Refn Monitoring > Proper	ties > WCCP > Se		*	p	Type topic to s	earch	
Device List	Home Configuration Monitor Properties	ing 🕞 Save 🗨 Refn Monitoring > Proper			*	p	Type topic to s	earch	
Device List	Home Configuration Monitor Properties	ing Save ( Refr Monitoring > Proper Service Group:	ties > WCCP > Se		*	P	Type topic to s	earch	
newce risc	Home Configuration Monitor Properties P P AAA Servers Device Access Connection Graphs Connection Graphs CRL DNS Cache	Ing Save Refn Monitoring > Proper Service Group: Display Mode:	ties > WCCP > Se 10 None		*	P	Type topic to s	earch	
Device List	Home Configuration Monitor Properties I Monitor Pro	Ing Save Refn Monitoring > Proper Service Group: Display Mode:	ties > WCCP > Se		*	p	Type topic to s	earch	
newce risc	Home Configuration Monitor Properties I Monitor Pro	Ing Save Refr Monitoring > Proper Service Group: Display Mode:	ties > WCCP > Se 10 None Hash Settings	rvice Group	*	, 		earch	
newce risc	Home Configuration Monitor Properties AAA Servers AAA Servers Connection Graphs CRL DNS Cache Falover Status Graphs	Ing Save Refr Monitoring > Proper Service Group: Display Mode:	ties > WCCP > Se 10 None	rvice Group	*	, 	Type topic to s	earch	
	Home Configuration Monitor Properties  AAA Servers Connection Graphs CRL CRL CNL CNL CNL CNL CNL CNL CNL CNL CNL CN	Ing Save ( Refr Monitoring > Proper Service Group: Display Mode:	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr	rvice Group	*	Desti	nation Port:	earch	
	Home Configuration Monitor Properties I Monitor Pro	Ing Save ( Refr Monitoring > Proper Service Group: Display Mode:	ties > WCCP > Se 10 None Hash Settings	rvice Group	*	Desti		earch	
	Home Configuration Monitor Properties I Monitor Properties I Monitor Properties I Monitor Properties I Monitor Partice Access Connection Graphs CRL DNS Cache DNS Cache Failover Status Graphs I dentity AD Agent A D Agent A Groups	Ing Save ( Refr Monitoring > Proper Service Group: Display Mode:	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr	rvice Group	*	Desti	nation Port:	earch	
	Home Configuration Monitor Properties I Monitor Pro	Ing Save ( Refr Monitoring > Proper Service Group: Display Mode:	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr	rvice Group	*	Desti	nation Port:	earch	
	Home Configuration Monitor Properties I Monitor Properties I Monitor Properties I Monitor Properties I Monitor Partice Access Connection Graphs CRL DNS Cache DNS Cache Failover Status Graphs I dentity AD Agent A D Agent A Groups	Ing Save ( Refr Monitoring > Proper Service Group: Display Mode:	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr Source Ip Address:	rvice Group	*	Desti	nation Port:		
	Home Configuration Monitor Properties I Monitor Pro	Ing Save Refr Monitoring > Proper Service Group: Display Mode:	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr Source Ip Address: formation:	rvice Group	*	Desti	nation Port:	earch	
	Home Configuration Monitor Properties I Monitor Pro	Save Refr Monitoring > Proper Service Group: Display Mode: Global WCCP in: Router info	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr Source Ip Address: formation:	rvice Group	*	Desti	nation Port:	earch	
	Home Configuration Monitor Properties I Monitor Properties I Monitor Properties I Monitor Partice Access Connection Graphs CRL DMS Cache CRL DMS Cache CRL Cache C	Global WCCP in: Router info	10 None Hash Settings Destination Ip Addr Source Ip Address: formation: prmation:	rvice Group	*	Desti	nation Port:	earch	
	Home Configuration Monitor Properties AAA Servers AAA Servers Connection Graphs Connection Graphs CRL DNS Cache Connection Graphs CRL Connection Graphs CR	Global WCCP in: Router info	ties > WCCP > Se 10 None Hash Settings Destination Ip Address: formation: prmation: Identifier:	rvice Group	*	Desti Sourc 192.0.2.1	nation Port:	earch	
	Home Configuration Monitor Properties I Monitor Properties MAA Servers Partice Access Partice Ac	Global WCCP in: Router info Router Protoco	ties > WCCP > Se 10 None Hash Settings Destination Ip Address: formation: prmation: Identifier:	rvice Group	*	Desti Sourc 192.0.2.1	nation Port:		
	Home Configuration Monitor Properties I Monitor Properties MAA Servers Properties Device Access Properties Connection Graphs Properties Connection Graphs Properties Connections Proper	Global UCCP in: Router info Router info Router info Router info	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr Source Ip Address: formation: ormation: Identifier: ol Version:	ess:	*	Desti Sourc 192.0.2.1	nation Port:	E	
	Home Configuration Monitor Properties I Monitor Pro	Global WCCP in: Router info Router info Router info Router info Router info Router info Router info Router info Router info Router info	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr Source Ip Address: formation: Identifier: bl Version: entifier: 10	ess:	*	Desti Source 192.0.2.1 2.0	nation Port:		
	Home Configuration Monitor Properties I Monitor Pro	Global WCCP in: Router info Router info Router info Router info Router info Router Protoco	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr Source Ip Address; formation: Identifier: ol Version: antifier: 10 of Cache Ingi	rvice Group	*	Desti Source 192.0.2.1 2.0	nation Port:		
	Home Configuration Monitor Properties AAA Servers AAA Servers Connection Graphs CRL Connection Graphs CRL DNS Cache Cach	Global WCCP in: Router info Service Idd Service Idd Number Number Total J	<pre>ites &gt; WCCP &gt; Se ites &gt; WCCP &gt; Se ites &gt; WCCP &gt; Se ites &gt; None Hash Settings Destination Ip Addr Source Ip Address: formation: Itentifier: pol Version: entifier: 10 of Cache Ingi of routers:</pre>	rvice Group	*	Desti Source 192.0.2.1 2.0	nation Port:		
	Home Configuration Monitor Properties I Monitor Pro	Global WCCP in: Router info Service Ide Number Total J Redired	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr Source Ip Address: formation: Identifier: of Version: entifier: 10 of Cache Engi of routers: Packets Redire	nes: cted:	5	192.0.2.1 2.0	nation Port:		
newce risc	Home Configuration Monitor Properties I Monitor Pro	Global UCCP in: Router info Service Group: Display Mode: Global UCCP in: Router info Router Protoco Service Ide Number Number Total 0 Redirec Total 0	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr Source Ip Address: formation: Identifier: ol Version: entifier: 10 of Cache Engl of routers: Packets Redire et access-list	nes: cted: : nied Redin	5	Desti Source 192.0.2.1 2.0 1 1 5137 WCCP-Redirec	nation Port:		
Device List	Home Configuration Monitor Properties AAA Servers AAA Servers Connection Graphs Connection Graphs Connection Graphs Connection Graphs Connections Connections Connections Context by TrustSec Connections Connecti	Global WCCP in: Router info Router info Ro	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr Source Ip Address: formation: Identifier: DI Version: antifier: 10 of Cache Engi of Cache Engi of routers: Packets Redirect ta cacess-list Connections De	nes: cted: : nied Redin	5	Desti 5ourc 192.0.2.1 2.0 1 1 5137 WCCP-Redirec 0	nation Port:		
	Home Configuration Monitor Properties AAA Servers AAA Servers Connection Graphs CRL DMS Cache CRL DMS Cache CRL DMS Cache CRL CACASS CRL CACAS CRL CACASS CRL CACAS CRL CACASS C	Global WCCP in: Router info Bervice Group: Display Mode: Global WCCP in: Router info Router Protoco Service Idd Number Total D Redirec Total D Croup a Total D	ties > WCCP > Se 10 None Hash Settings Destination Ip Addr Source Ip Address: formation: Identifier: D1 Version: actifier: 10 of Cache Engi of Couters: Packets Redire taccess-list Connections De Packets Unassi	nes: cted: ; nied Redi; gned: d to Group	s	Desti 500rd 192.0.2.1 2.0 1 1 5137 WCCP-Redirec 0 0	nation Port:		

Reporting	Web Security Manager	Security Services	Network	System A	administration	No Changes
nterfaces					L	па снанде»
nterfaces						
	Interfaces:	Ethernet Port	I	P Address	Netmask	Hostname
	-	Ml	1	0.10.2.50	255.255.255.0	wsa- mgmt.secur -x.local
		Pi	11	0.10.1.50	255.255.255.0	wsa.secure- x.local
Separate Routing for	Management Services:	Separate routing (M1 port res	tricted to appliance	management s	ervices only)	
Appliance	Management Services:	HTTP on port 80, HTTPS on po	rt 443, Redirect HT	TP request to H	TTPS	
لد	4 Traffic Monitor Wiring:	Duplex TAP: T1 (In/Out)				
					Ed	dit Settings

- 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.

	111 *	💙 αιγτ	COD 1 Program #	and such
Pro Randard ACL	7 🕑	iany4	📑 HQ-srv	icmp.
Conderd ALL	8 2	any4	🛎 ESA	sn/p
ASA CLAuth Proxy	9 17	any4	ESA ESA	🔐 kmo
Per Season rates	E 525_access_in			
	B WCCP-Redirection	in .		
	1 1	i any	<u></u> 10.0.0.0/8	IP ID
	2 19	any	172.16.0.0/12	are lo
	3 12	any	通 192.168.0.0/16	ar ip
	4 📝	any	any	NO http
A Device Setup	5 🕅	ary ary	intervention of the second sec	1 https
Fronal .				
Remote Access VPN				

#### **Question: 34**

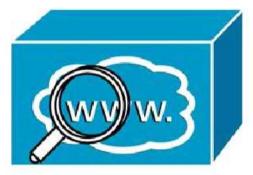
The Web Cache Communication Protocol (WCCP) is a content-routing protocol that can facilitate the redirection of traffic flows in real time. Your organization has deployed WCCP to redirect web traffic that traverses their Cisco Adaptive Security Appliances (ASAs) to their Cisco Web Security Appliances

(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

ile View Tools Wizards Window	Help					Type topic to search		G
h Home 😪 Configuration 👩 Monitori	ng 🔚 Save 🔇 Refresh 🄇	🔵 Back 🔘 F	forward 4	P Help				
Device Setup 🗗 म	Configuration > Device Set	up > Interface	25					
Startup Wizard	Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN	0
••• Static Routes	GigabitEthernet0/0	outside	Enabled	(	192.0.2.1	255.255.255.0	native	
*2 Route Maps	GigabitEthernet0/1		Enabled				native	
Prefix Rules	GigabitEthernet0/1.4	inside	Enabled	100	0 10.10.1.1	255.255.255.0	vlan4	
🕀 📲 OSPF	GigabitEthernet0/1.250	Guest	Enabled	30	0 10.10.250.1	255,255,255.0	vlan250	
🗄 🏟 OSPFv3	GigabitEthernet0/2	DMZ	Enabled	50	172.16.1.1	255.255.255.0	native	
🗇 📲 RIP	GigabitEthernet0/3	Site-To	Enabled	60	172.16.2.1	255.255.255.0	native	
🕀 📲 🚾 EIGRP	GigabitEthernet0/4		Disabled				native	
🕀 🤹 Multicast	GigabitEthernet0/5		Disabled				native	
Proxy ARP/Neighbor Discove	Management0/0	manage	Enabled	90	0 10, 10, 2, 1	255,255,255,0	native	

Properties         Markeving 2 Properties 2 WCP 2 Service Groups           Properties         Work Addisons         Description           Back Addison of Sector         Service Group:         Description         Description           Back Addison         Description         Description         Description         Description           Back Addison         Description         Description         Description         Description         Description           Back Addison         Description         Description <thdescription< th=""> <thdescription< th=""></thdescription<></thdescription<>		lp		ype topic to search	
Weth Service Group:       Wether         Depth Access       Depth Access	Home 🏤 Configuration 🔀 Monitoring	🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦃	Help		
Service Group:       Number of comparison         Option Society       Destination Part:         Destination Part:       Destination Part:         Destination:       Rours:         Destination:       Rours:         Destination:       Rours:         Destination:       Rours:         Destination:       Rours:         Service Team: If Crantation:       Rours:         Rours:       Rours:         Service Team: If Crantation:       Rours:         Rours:       Rours:       Image: Rours:         Service Team: If Crantation:       Rours:         Rours:       Rours:       Image: Rours:         Service Team: If Crantation:       Rours:       Image: Rours:         Rours:       Rours:       Number of Crache: Rourse:       Image: Rours:		Ionitoring > Properties > WCCP > Service Groups			
DNS Cache       Dappy Mode:       Data Settings         Description       Description       Description         Description <th>H Gana Servers H Servers H Servers H Connection Graphs</th> <th>Service Group:</th> <th></th> <th></th> <th></th>	H Gana Servers H Servers H Servers H Connection Graphs	Service Group:			
Image: Seconds       Destination is Address:       Destination Port:         Source 10 Address:       Source Port:         Source 10 Address:       10 Constraint:         Source 10 Address:       2.0         Source 10 Address:       2.0         Source 10 Address:       1.0         Source 10 Address       1.0         Source 10 Ad	DNS Cache				
A Groups       Convertions       Convertions         B Users       Delter I dentifier:       192.0.2.1         Protocol Version:       2.0         B Protocol Version:       1         Protocol Version:       2.0         B Protocol Version:       1         D Rubber of Contel Institut:       100         B Protocol Version:       1         D Rubber of Contections       112         D Robert D Roberts Duarest gnedi:       0         D Corup eccess-list:	Graphs			4 4	
Image: Security Virtual Appliance       Security Services       Network       System         Interfaces       Interfaces       Interfaces         Interfaces       Interfaces       Security Services       Network       System         Interfaces       Interfaces       Security Services       Security Services       Network       System         Interfaces       Interfaces       Interfaces       Security Services       Network       System         Interfaces       Interfaces       Interfaces       Interfaces       Network       System Administration         Interfaces       Interfaces       Interfaces       Security Services       Network       System Administration         Interfaces       Interfaces       Interfaces       Interfaces       Network       System Administration         Interfaces       Interfaces       Interfaces       Network       System Administration       Mo Change         Separate Routing for Management Services       Separate routing (M1 port restricted to appliance management services only)       Appliance Management Services       Separate Routing for Management Services	Groups	Source Ip Address:	Source Port:		
Image: Start Consections       Frotocol Version:       2.0         Image: Start Resources Graphs       Service Identifier: 10       Image: Service Identifier: 10         Image: Start Resources Graphs       Mumber of Totache Regimes:       1         Image: Start Resources Graphs       Mumber of Totache Regimes:       1         Image: Start Resources Graphs       Resources:       1         Image: Start Resources Graphs       Resources Graphs       Resources:         Image: Start Resources Graphs       Resources Graphs       Resources:         Image: Start Resources Graphs       Resources Graphs       Resources:         Image: Start Resources Graphs       Network Start Resources:       Network:         Image: Start Resources Graphs       Network Start Resources:       Network:         Image: Start Resources Graphs       Network: Start Resources:       Network:         Image: Start Resources Graphs       Network: Start Resources:       Network: Start Resources:         Image: Start Resources Graphs: Start Resources Graphs       Network: </th <th>E A Identity by TrustSec</th> <th>Router information:</th> <th>197 012 1</th> <th></th> <th></th>	E A Identity by TrustSec	Router information:	197 012 1		
System Resources Graphs       Number of Cache Engines:       1         Mumber of Toutal Packets Redirected:       5137         Redirect access-list:       WCCP-Redirection         Total Packets Redirected:       5137         Redirections Paniel Redirections       0         Croup access-list:       WCCP-Redirection         Total Packets Redirections Paniel Redirect:       0         Croup access-list:       -none-         Total Packets Unassigned:       0         Segond In est: admin on wsassecurr       Options = Support an         Cherritic Cisco S100V       Segond:       System Administration         Interfaces       -       -         Interfaces       -       -         Interfaces       -       -         Pi	SXP Connections	Protocol Version:			
Image: Process	System Resources Graphs	Number of Cache Ingines: Number of routers:	1		
Group access=list:       -none-         Total Reseages Denied to Group:       0         Previous CPU Usage       Total Reseages Denied to Group:       0         Avetwork Interfaces       Logged in es: admin on wsa.secure         Reporting       Web Security Virtual Appliance       Support an         Reporting       Web Security Virtual Appliance       Network         Sco       Web Security Manager       Security Services       Network         Sco       Interfaces       Interfaces:       Ethernet Port       IP Address       Netmask         M1       10.10.2.50       255.255.05       wsa- mgmt.security.iocal       v.iocal         Separate Routing for Management Services:       Separate routing (M1 port restricted to appliance management services only)       Mappliance Management Services:       HTP on port 403, Redirect HTTP reguest to HTTPS         L4 Traffic Monitor Wiring:       Duplex TAP: T1 (In/Out)       Unies TAP: T1 (In/Out)       Unies TAP: T1 (In/Out)	Memory	Redirect access-list: Total Connections Denied Redirect	WCCP-Redirection t: 0		
Initial Cisco S100V       Logged in as: admin on wsa.secure Options ⇒ Support at Options ⇒ Sup	Redirection	Group access-list: Total Messages Denied to Group:	-none- 0		-
Image: Second State Sta		Total Anomenoi Cación Talinies.			
No Change         Interfaces         Interfaces       IP Address       Netmask       Hostname         M1.       10.10.2.50       255.255.255.0       wsa- mgmt.secu- -x.local         P1       10.10.1.50       255.255.255.0       wsa.secure x.local         Separate Routing for Management Services:       Separate routing (M1 port restricted to appliance management services only)       HTTP on port 60, HTTPS on port 443, Redirect HTTP reguest to HTTPS         L4 Traffic Monitor Wiring:       Duplex TAP: T1 (In/Out)       Upplex TAP: T1 (In/Out)	2. 양 양 전통 2. 이 이 가슴에 가지 않는 것 같은 것 같아. 가슴이 있는 것 같아. 귀에 있는 것 같아. 가슴이 있는 것 같아. 가슴 가슴 것이 것 같아. 가슴 것이 것 같아. 가슴 것이 것 같아. 가슴 것이 것이 있는 것이 것이 것 같아. 가슴 것이 있는 것이 것 같아. 가슴 있는 것이 있는 것이 것이 같아. 가슴 것이 있는 것이 것이 같아. 가슴 것이 것이 않는 것이 같아. 가슴 것이 것이 않아. 가슴 것이 것이 않아. 가슴 것이 같아. 가슴 것이 있는 것이 것이 같아. 가슴 가슴 것이 것이 않아. 것이 것이 같아. 가슴 것이 것이 같아. 가슴 것이 않아. 것이 않아. 가슴 것이 것이 않아. 가슴 것이 것이 않아. 가슴 것이 것이 않아. 귀에 있는 것이 않아. 귀에 있는 것이 않아. 가슴 것이 것이 않아. 귀에 있다. 것이 것이 같아. 것이 않아. 것이 같아. 가슴 것이 것이 않아. 가슴 것이 것이 같아. 가슴 것이 것이 같아. 가슴 것이 것이 않아. 것이 않아. 것이 같아. 가슴 것이 것이 않아. 것이 않아. 가슴 것이 것이 않아. 가슴 것이 것이 않아. 가슴 것이 않아. 것이 같아. 가슴 것이 않아. 가슴 것이 않아.	3	Logged in		
Interfaces Interfaces Interfaces: Interfac				stration	
Ethernet Port       IP Address       Netmask       Hostname         M1.       10.10.2.50       255.255.255.0       wsa- mgmt.sect -x.local         P1       10.10.1.50       255.255.255.0       wsa- mgmt.sect -x.local         Separate Routing for Management Services:       Separate routing (M1 port restricted to appliance management services only)       wsa-secure HTTP on port 80, HTTPS on port 443, Redirect HTTP request to HTTPS         L4 Traffic Monitor Wiring:       Duplex TAP: T1 (In/Out)       Upplex TAP: T1 (In/Out)	Reporting Web Security M	lanager Security Services Netwo	System Admini:		
Marking for Management Services:     Separate Routing for Management Services:     Separate routing (M1 port restricted to appliance management services only)     Viscolar vis	nterfaces	lanager Security Services Netwo	ork System Admini:	I	No Changes I
Appliance Management Services:       Separate routing (M1 port restricted to appliance management services only)         Appliance Management Services:       HTTP on port 80, HTTPS on port 443, Redirect HTTP request to HTTPS         L4 Traffic Monitor Wiring:       Duplex TAP: T1 (In/Out)	Interfaces			Netmask	No Changes I Hostname
Appliance Management Services:         HTTP on port 80, HTTPS on port 443, Redirect HTTP request to HTTPS           L4 Traffic Monitor Wiring:         Duplex TAP: T1 (In/Out)	nterfaces	faces: Ethernet Port	IP Address		Hostname wsa- mgmt.secure
L4 Traffic Monitor Wiring: Duplex TAP: T1 (In/Out)	nterfaces nterfaces Inter	rfaces: Ethernet Port M1 P1	IP Address           10.10.2.50         3           10.10.1.50         3	255.255.255.0 255.255.255.0	Hostname wsa- mgmt.secure -x.local wsa.secure-
and the second	nterfaces Interfaces Inter Separate Routing for Management Ser	rfaces: Ethernet Port M1 P1 rvices: Separate routing (M1 port restricted to ap	IP Address 10.10.2.50 10.10.1.50 iopliance management services	255.255.255.0 255.255.255.0	Hostname wsa- mgmt.secure -x.local wsa.secure-
	nterfaces Interfaces Inter Separate Routing for Management Ser Appliance Management Ser	rfaces: Ethernet Port M1 P1 rvices: Separate routing (M1 port restricted to ap rvices: HTTP on port 80, HTTPS on port 443, Redi	IP Address 10.10.2.50 10.10.1.50 iopliance management services	255.255.255.0 255.255.255.0	Hostname wsa- mgmt.secure -x.local wsa.secure-
	Interfaces Interfaces Inter Separate Routing for Management Ser Appliance Management Ser	rfaces: Ethernet Port M1 P1 rvices: Separate routing (M1 port restricted to ap rvices: HTTP on port 80, HTTPS on port 443, Redi	IP Address 10.10.2.50 10.10.1.50 iopliance management services	255,255,255.0 255,255,255.0 5 only)	Hostname wsa- mgmt.secure -x.local wsa.secure- x.local

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:

	Oynamic service ID:	10 0-255		
	Port numbers:	(up to 8 port numbers, separated by commas)		
		Redirect based on destination port.		
		<ul> <li>Recirect based on source port (return path)</li> </ul>		
		For IP spoofing, define two services, one based on destination port and another based on source port (return path).		
		Coad balance based on server address		
		C Load balance based on client address Applies only if more than one Web Security Appliance is in use		
Router IP Addresses:	10.10.1.1 Separate multiple entries	with line breaks or commes.		
Router Security:	Enable Security for S	sword:		

#### 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.





# Web Security Appliance

ile View Tools Wizards Window	Help					Type topic to search		G
home 😪 Configuration 👩 Monitori	ng 🔚 Save 🔇 Refresh 🌔	🔁 Back 🔘 F	forward 4	🥐 Help				
Device Setup 🗗 🖗	Configuration > Device Set	tup > Interface	25					
o <sup>®</sup> Startup Wizard and Interfaces □ • 2 Routing	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	
Route Maps	GigabitEthernet0/1	2010 0010	Enabled				native	
Prefix Rules	GigabitEthernet0/1.4	inside	Enabled		010.10.1.1	255.255.255.0	vlan4	
🕀 🏤 OSPF	GigabitEthernet0/1.250	Guest	Enabled		010.10.250.1	255.255.255.0	vlan250	
🕀 🏂 OSPEV3	GigabitEthernet0/2	DMZ	Enabled		0172.16.1.1	255.255.255.0	native	
🕀 🍓 RIP	GigabitEthernet0/3	Site-To	Enabled	6	0172.16.2.1	255.255.255.0	native	
🕀 🦓 EIGRP	GigabitEthernet0/4		Disabled				native	
🕀 🏰 Multicast	GigabitEthernet0/5		Disabled				native	
Proxy ARP/Neighbor Discove	Management0/0	manage	Enabled	9	0 10,10,2,1	255.255.255.0	native	

	Save 💽 Refresh	Back O TOTWA	rd 🤶 Help			
	Monitoring > Properties	<u>&gt; WCCP &gt; Service Gr</u>	oups			
AAA Servers	Service Group:	- [				
DNS Cache		ne 🔹 👻				
Graphs	Des	ination Ip Address:		Destination Po	ort:	
AD Agent	Sou	rce Ip Address:		Source Port;		
Memory Usage     Users     Jeers     Jeantity by TrustSec     A RAC     Environment Data	Global WCCP inform Router informs Router Ide	tion:		192.0.2.1		
SXP Connections	Protocol 5	Version:		2.0		
	Number of Number of	Service Identifier: 10 Number of Cache Ingines: Number of routers: Total Packets Redirected:				B
Memory	Redirect a Total Conr	access-list: Mections Denied Re	direct:	5137 WCCP-Redirection 0		
Cervice Groups     Groups	Group acce Total Mess	ets Unassigned: ess-list: sages Denied to Gr mentication failur	oup:	0 -none- 0 0		-
A-Network-Interfaces						and the second second
IIII Cisco S100V	e			Logged i	n as: <b>admin</b> on Options ⇔	wsa.secure- Support and
Indu Cisco S100V		y Services	Network	Logged i System Admi	Options 🗢	
Reporting Web Security I		y Services	Network	Market and the set of	Options 🗢	
Interfaces			Network	Market and the set of	Options 🗢	Support and
Interfaces	Manager Securit			System Admi	Options +	Support and
Cisco S100V         SCO       Web Security Virtual Appliance         Reporting       Web Security I         nterfaces       Interfaces	Manager Securit			System Admi IP Address	Options +	Support and No Changes Hostname wsa- mgmt.secure
Cisco S100V           Sco         Web Security Virtual Appliance           Reporting         Web Security I           Interfaces         Interfaces           Separate Routing for Management Set         Interfaces	Manager Securit			System Admi IP Address 10.10.2.50	Options =	Support and No Changes Hostname wsa- mgmt.secure -x.local wsa.secure
Reporting         Web Security Virtual Appliance           Reporting         Web Security I           Interfaces         Interfaces	Manager Securit erfaces: Ethernet Port M1 P1 ervices: Separate rout ervices: HTTP on port	ing (M1 port restricte 30, HTTPS on port 44	d to applianc	System Admi IP Address 10.10.2.50 10.10.1.50	Options +	Support and No Changes Hostname wsa- mgmt.secure -x.local wsa.secure
Cisco S100V           Sco         Web Security Virtual Appliance           Reporting         Web Security I           Interfaces         Interfaces           Separate Routing for Management Set         Interfaces	Manager Securit  arfaces: Ethernet Port M1 P1 ervices: Separate rout ervices: HTTP on port	ing (M1 port restricte 30, HTTPS on port 44	d to applianc	System Admi IP Address 10.10.2.50 10.10.1.50 e management servic	Options +	Support and No Changes Hostname wsa- mgmt.secure -x.local wsa.secure

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:

	Dynamic service ID:     10     0-255     Port numbers:     80,443     (up to 8 port numbers, separated by commas)     (* Redirect based on destination port     (* Redirect based on source port (return path)     For IP spoofing, define two services, one based on destination     port and another based on source port (return path).
	<ul> <li>Load balance based on server address</li> <li>Load balance based on client address</li> <li>Applies only if more than one Web Security Appliance is in use.</li> </ul>
Router IP Addresses:	10.10.1.1  Separate multiple entries with line breaks or commas.
Router Security:	Enable Security for Service     Password:     The password must be between I and 7 characters long.     Confirm Password:     ••••••
> Advanced:	Optional settings for customizing the behavior of the WCCP v2 Router.

## 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.