Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

　　All examinations will be up to date.

* 24/7 Quality Support

　　We will provide service round the clock.

* 100% Pass Rate

　　Our guarantee that you will pass the exam.
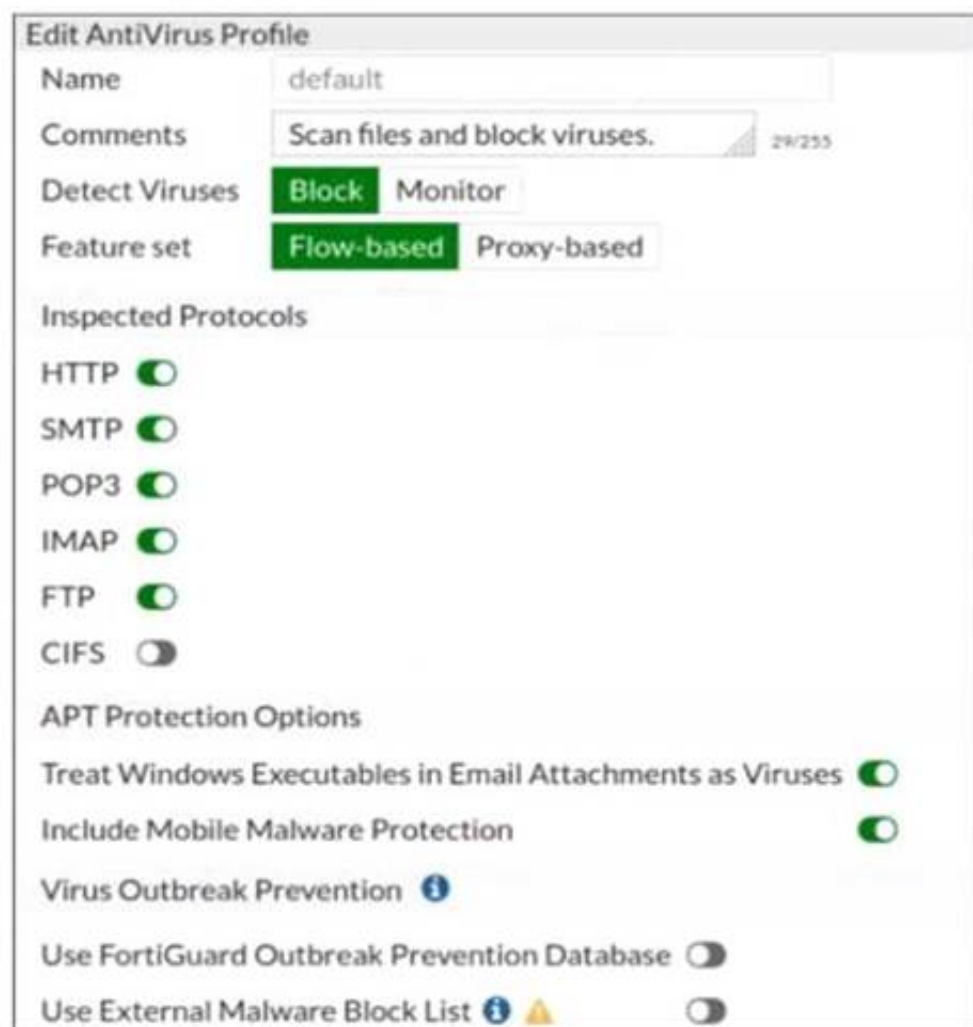
* Unique Gurantee

　　If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 1)
Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

A. The firewall policy performs the full content inspection on the file.
B. The flow-based inspection is used, which resets the last packet to the user.
C. The volume of traffic being inspected is too high for this model of FortiGate.
D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Answer: B

Explanation:
• "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately
• When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.
In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

NEW QUESTION 2
- (Exam Topic 1)
Refer to the exhibit.
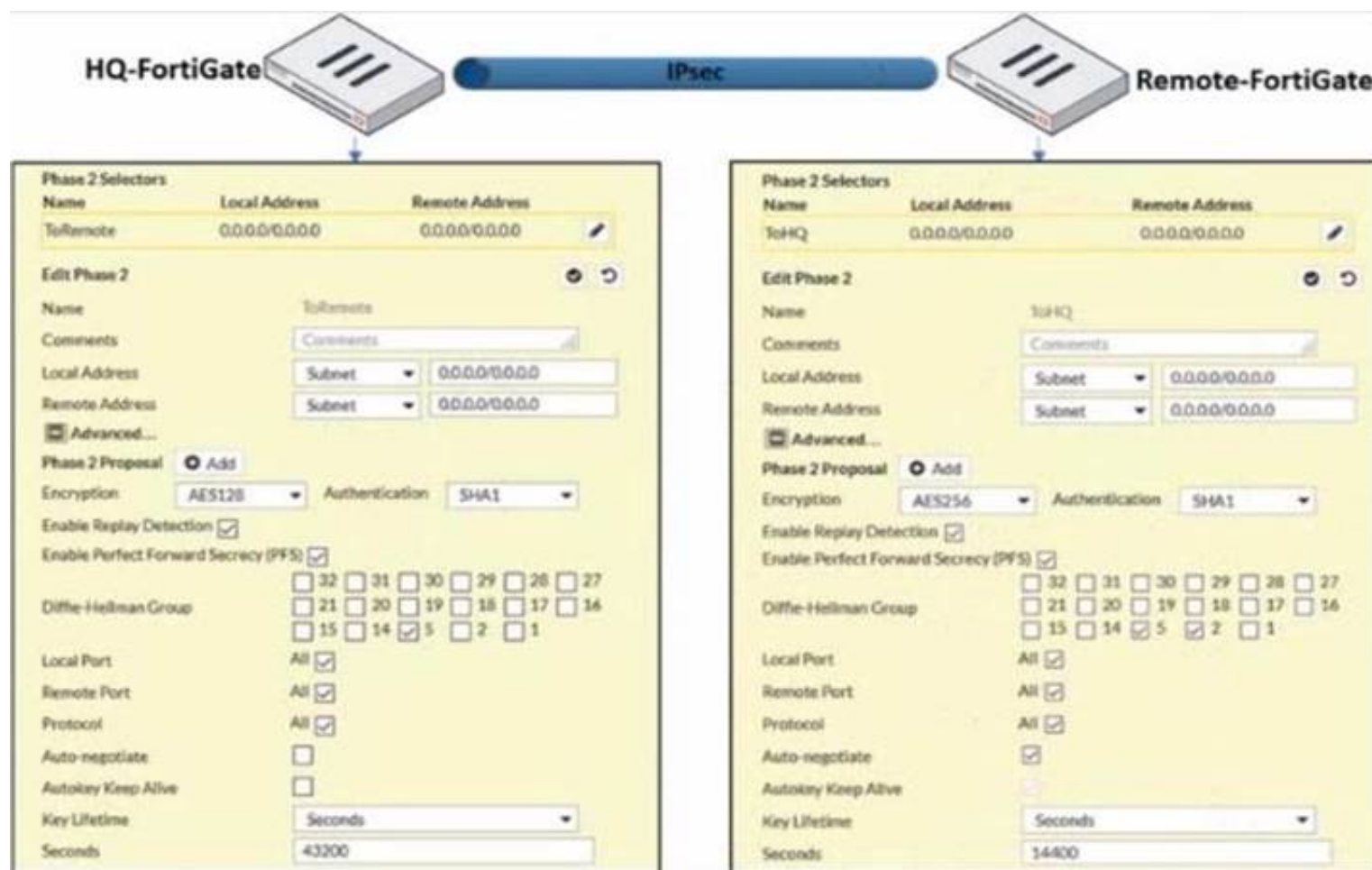
A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up. but phase 2 fails to come up.
Based on the phase 2 configuration shown in the exhibit, what configuration change will bring phase 2 up?

A. On HQ-FortiGate, enable Auto-negotiate.
B. On Remote-FortiGate, set Seconds to 43200.
C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
D. On HQ-FortiGate, set Encryption to AES256.

Answer: D

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/168495
Encryption and authentication algorithm needs to match in order for IPSEC be successfully established.

NEW QUESTION 3
- (Exam Topic 1)
Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

A. System time
B. FortiGuaid update servers
C. Operating mode
D. NGFW mode

Answer: CD

Explanation:
C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.
D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate_Infrastructure_6.4_Study_Guide

NEW QUESTION 4
- (Exam Topic 1)
Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

A. FortiGate uses the AD server as the collector agent.
B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
C. FortiGate does not support workstation check.
D. FortiGate directs the collector agent to use a remote LDAP server.

Answer: BD

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732

NEW QUESTION 5
- (Exam Topic 1)
Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

A. Proxy-based inspection
B. Certificate inspection
C. Flow-based inspection

D. Full Content inspection

Answer: AC

**NEW QUESTION 6**
- (Exam Topic 1)
Refer to the exhibit.

The exhibit shows the IPS sensor configuration.
If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will allow attackers matching the NTP.Spoofed.KoD.DoS signature.
B. The sensor will block all attacks aimed at Windows servers.
C. The sensor will reset all connections that match these signatures.
D. The sensor will gather a packet log for all matched traffic.

Answer: AB

NEW QUESTION 7
- (Exam Topic 1)
Refer to the exhibit.
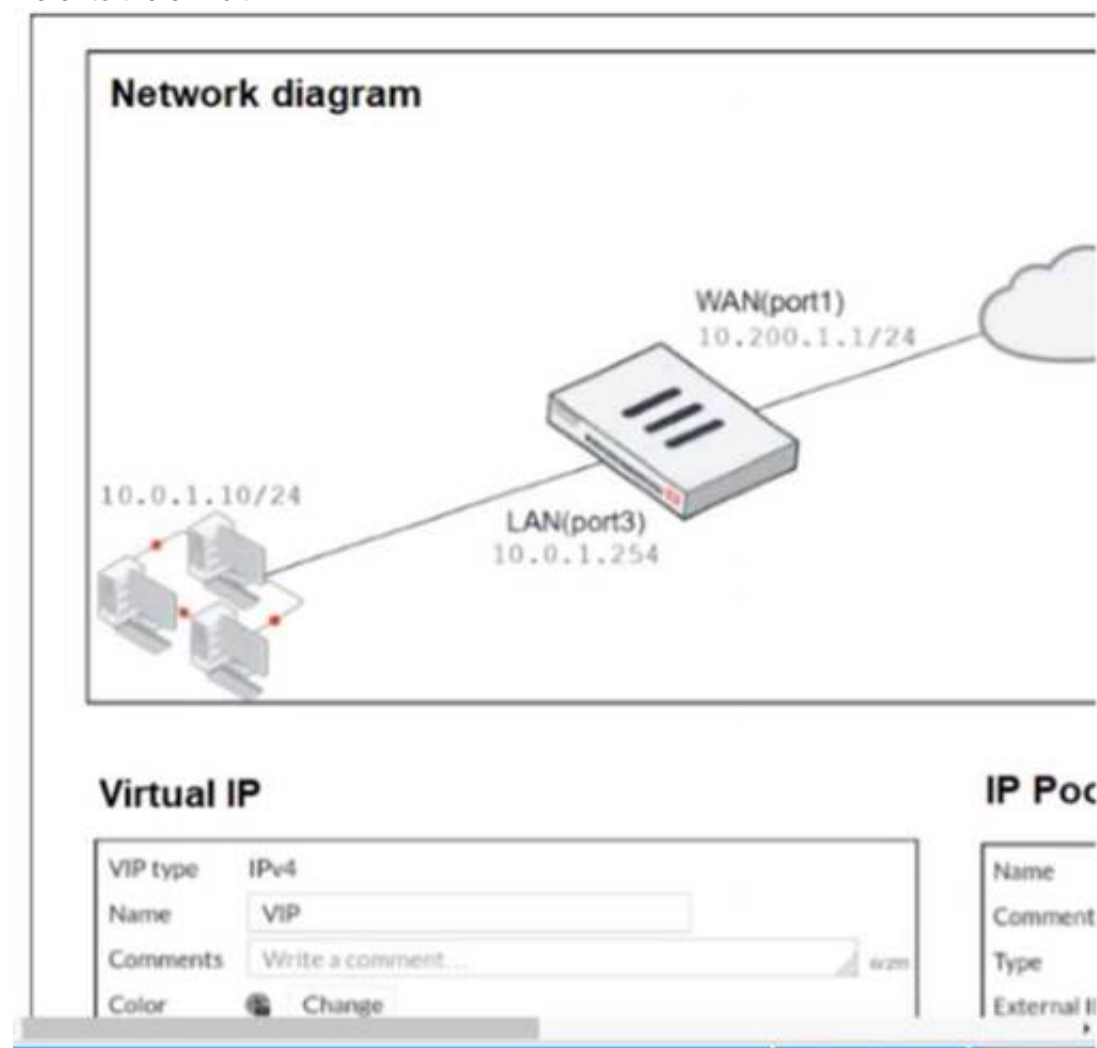
The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies configuration. The WAN (port1) interface has the IP address 10.200.1.1/24.
The LAN (port3) interface has the IP address 10 .0.1.254. /24. The first firewall policy has NAT enabled using IP Pool.
The second firewall policy is configured with a VIP as the destination address.
Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0.1.10?

A. 10.200.1.1
B. 10.200.3.1
C. 10.200.1.100
D. 10.200.1.10

Answer: A

Explanation:
Reference:
https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-firewall/Concepts%20-%20Firewall/Static%20N
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD44529

NEW QUESTION 8
- (Exam Topic 1)
Refer to the web filter raw logs.

```
date=2020-07-09 time=12:51:51 logid= "0316013057" type= "utm"
subtype= "webfilter" eventtype= "ftgd_blk" level- "warning"
vd= "root" eventtime=1594313511250173744 tz= "-0400" policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf= "port2"
srcintfrole= "undefined" dstip=104.244.42.193 dstport=443
dstintf= "port1" dstintfrole= "undefined" proto=6 service= "HTTPS"
hostname= "twitter.com" profile= "all_users_web" action= "blocked"
reqtype= "direct" url= "https://twitter.com/" sentbyte=517
rcvdbyte=0 direction= "outgoing" msg= "URL belongs to a category
with warnings enabled" method= "domain" cat=37 catdesc= "Social"
Networking"

date=2020-07-09 time=12:52:16 logid= "0316013057" type= "utm"
subtype= "webfilter" eventtype= "ftgd_blk" level- "warning"
vd= "root" eventtime=1594313537024536428 tz= "-0400" policyid=1
sessionid=5552 srcip=10.0.1.10 srcport=48698 srcintf= "port2"
srcintfrole= "undefined" dstip=104.244.42.193 dstport=443
dstintf= "port1" dstintfrole= "undefined" proto=6 service= "HTTPS"
hostname= "twitter.com" profile= "all_users_web"
action= "passthrough" reqtype= "direct" url= "https://twitter.com/"
sentbyte=369 rcvdbyte=0 direction= "outgoing" msg= "URL belongs to
a category with warnings enabled" method= "domain" cat=37
catdesc= "Social Networking"
```

Based on the raw logs shown in the exhibit, which statement is correct?

A. Social networking web filter category is configured with the action set to authenticate.
B. The action on firewall policy ID 1 is set to warning.
C. Access to the social networking web filter category was explicitly blocked to all users.
D. The name of the firewall policy is all_users_web.

Answer: A

NEW QUESTION 9
- (Exam Topic 1)
Which statement about video filtering on FortiGate is true?

A. Full SSL Inspection is not required.
B. It is available only on a proxy-based firewall policy.
C. It inspects video files hosted on file sharing services.
D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Answer: B

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/190873/video-filtering

NEW QUESTION 10
- (Exam Topic 1)
An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

A. Policy lookup will be disabled.
B. By Sequence view will be disabled.
C. Search option will be disabled
D. Interface Pair view will be disabled.

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821

NEW QUESTION 10
- (Exam Topic 1)
Which three statements about a flow-based antivirus profile are correct? (Choose three.)

A. IPS engine handles the process as a standalone.
B. FortiGate buffers the whole file but transmits to the client simultaneously.
C. If the virus is detected, the last packet is delivered to the client.
D. Optimized performance compared to proxy-based inspection.
E. Flow-based inspection uses a hybrid of scanning modes available in proxy-based inspection.

Answer: BDE

Explanation:
Reference: https://forum.fortinet.com/tm.aspx?m=192309

NEW QUESTION 14
- (Exam Topic 1)
When configuring a firewall virtual wire pair policy, which following statement is true?

A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
B. Only a single virtual wire pair can be included in each policy.
C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
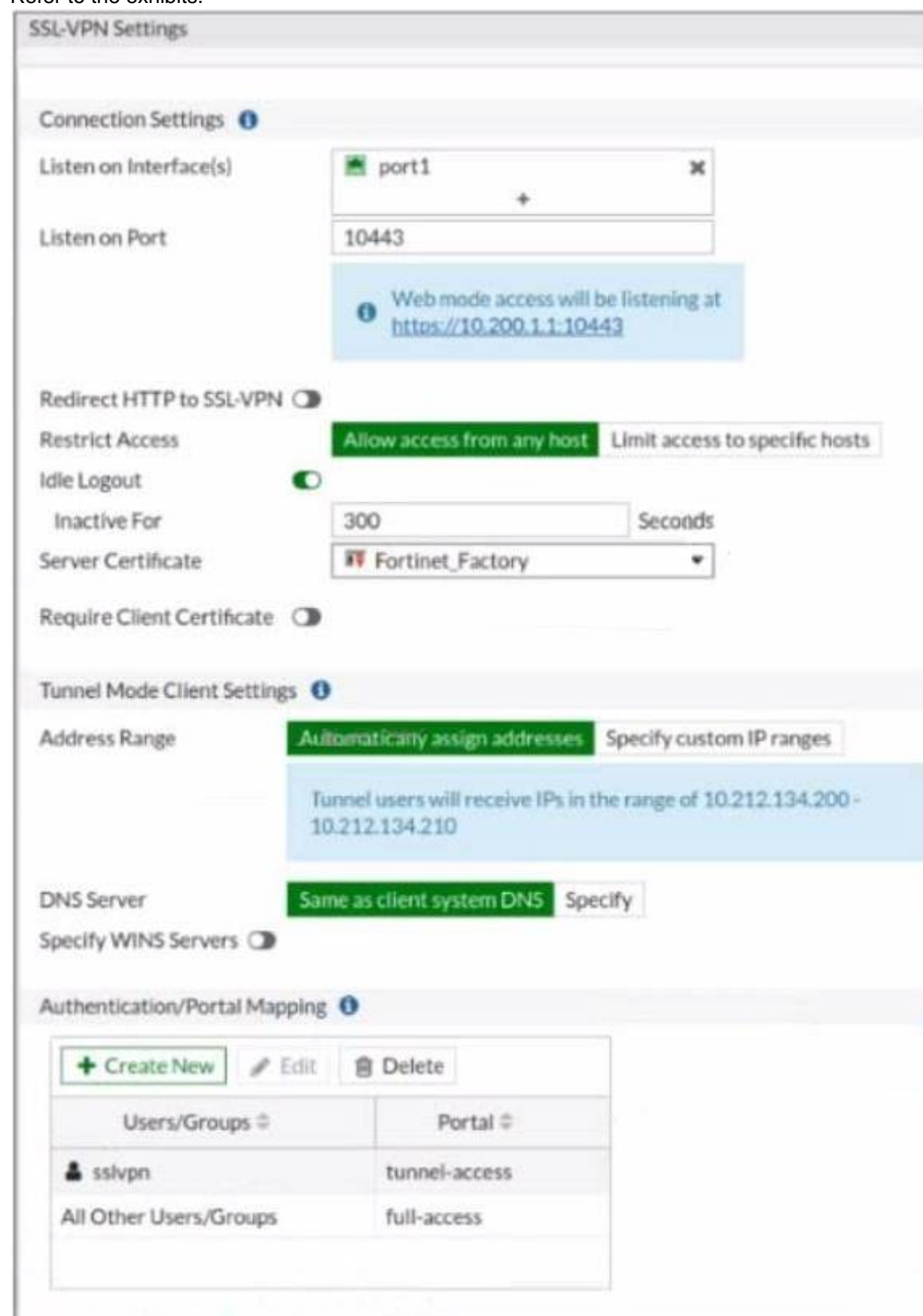D. Exactly two virtual wire pairs need to be included in each policy.

Answer: A

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD48690

NEW QUESTION 19
- (Exam Topic 1)
Refer to the exhibits.

The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

A. Change the SSL VPN port on the client.
B. Change the Server IP address.
C. Change the idle-timeout.
D. Change the SSL VPN portal to the tunnel.

Answer: A

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/150494

NEW QUESTION 21
- (Exam Topic 1)
An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

A. Add the support of NTLM authentication.
B. Add user accounts to Active Directory (AD).
C. Add user accounts to the FortiGate group fitter.
D. Add user accounts to the Ignore User List.

Answer: D

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828

NEW QUESTION 25
- (Exam Topic 1)
Refer to the exhibit.
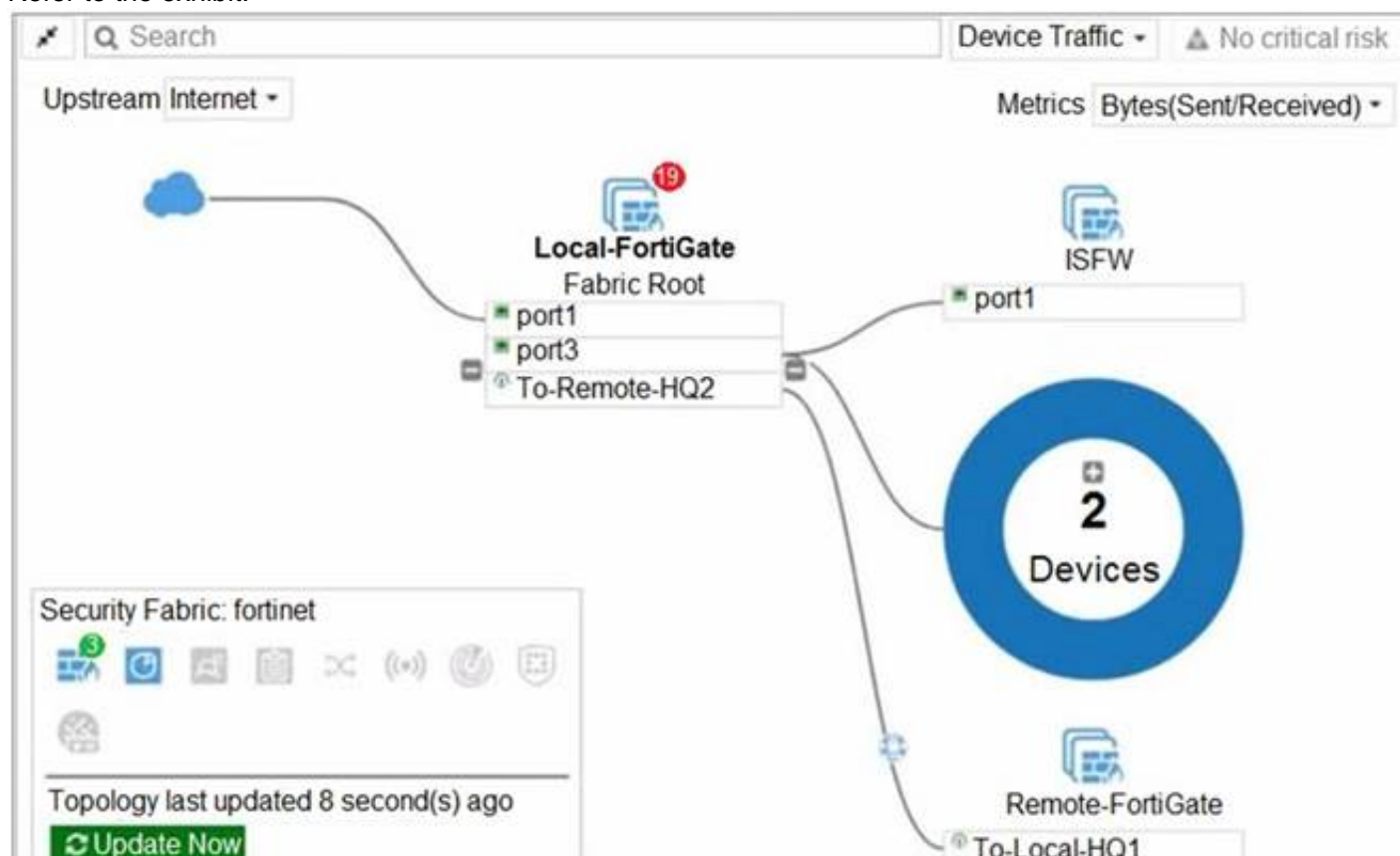
Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

A. There are five devices that are part of the security fabric.
B. Device detection is disabled on all FortiGate devices.
C. This security fabric topology is a logical topology view.
D. There are 19 security recommendations for the security fabric.

Answer: CD

Explanation:
References: https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results
https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology

NEW QUESTION 28
- (Exam Topic 1)
Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites?

A. The security actions applied on the web applications will also be explicitly applied on the third-party websites.
B. The application signature database inspects traffic only from the original web application server.
C. FortiGuard maintains only one signature of each web application that is unique.
D. FortiGate can inspect sub-application traffic regardless where it was originated.

Answer: D

Explanation:
Reference:
https://help.fortinet.com/fortiproxy/11/Content/Admin%20Guides/FPX-AdminGuide/300_System/303d_FortiG

NEW QUESTION 29
- (Exam Topic 1)
Refer to the exhibit.


```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000    4500 003c 2f8f 0000 8001 f020 0a00 0102        E..</...........
0x0010    0808 0808 0800 4d5a 0001 0001 6162 6364        ......MZ....abcd
0x0020    6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030    7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000    4500 003c 2f8f 0000 7f01 0106 0a38 f0e4        E..</........8..
0x0010    0808 0808 0800 6159 ec01 0001 6162 6364        ......aY....abcd
0x0020    6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030    7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000    4500 003c 0000 0000 7501 3a95 0808 0808        E..<....u.:.....
0x0010    0a38 f0e4 0000 6965 ec01 0001 6162 6364        .8....iY....abcd
0x0020    6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030    7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000    4500 003c 0000 0000 7401 2bb0 0808 0808        E..<....t.+.....
0x0010    0a00 0102 0000 555a 0001 0001 6162 6364        ......UZ....abcd
0x0020    6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030    7576 7761 6263 6465 6667 6869                  uvwabcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.
Which three pieces of information are included in the sniffer output? (Choose three.)

A. Interface name
B. Ethernet header
C. IP header
D. Application header
E. Packet payload

Answer: ACE

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=11186

NEW QUESTION 30
- (Exam Topic 2)
View the exhibit:

▼ Status	▼ Name	▼ VLAN ID	▼ Type	▼ IP/Netmask
Physical(12)				
▣ ○	port1		Physical Interface	10.200.1.1 255.255.255.0
	port1-VLAN1	1	VLAN	10.200.5.1 255.255.255.0
	port1-VLAN10	10	VLAN	10.0.10.1 255.255.255.0
▣ ○	port2		Physical Interface	10.200.2.1 255.255.255.0
	port2-VLAN1	1	VLAN	10.0.5.1 255.255.255.0
	port2-VLAN10	10	VLAN	10.0.20.254 255.255.255.0
○	port3		Physical Interface	10.0.1.254 255.255.255.0

Which the FortiGate handle web proxy traffic rue? (Choose two.)

A. Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.
B. port-VLAN1 is the native VLAN for the port1 physical interface.
C. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.
D. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.

Answer: AC

NEW QUESTION 33
- (Exam Topic 2)
Refer to the exhibit.


```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port 80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
```
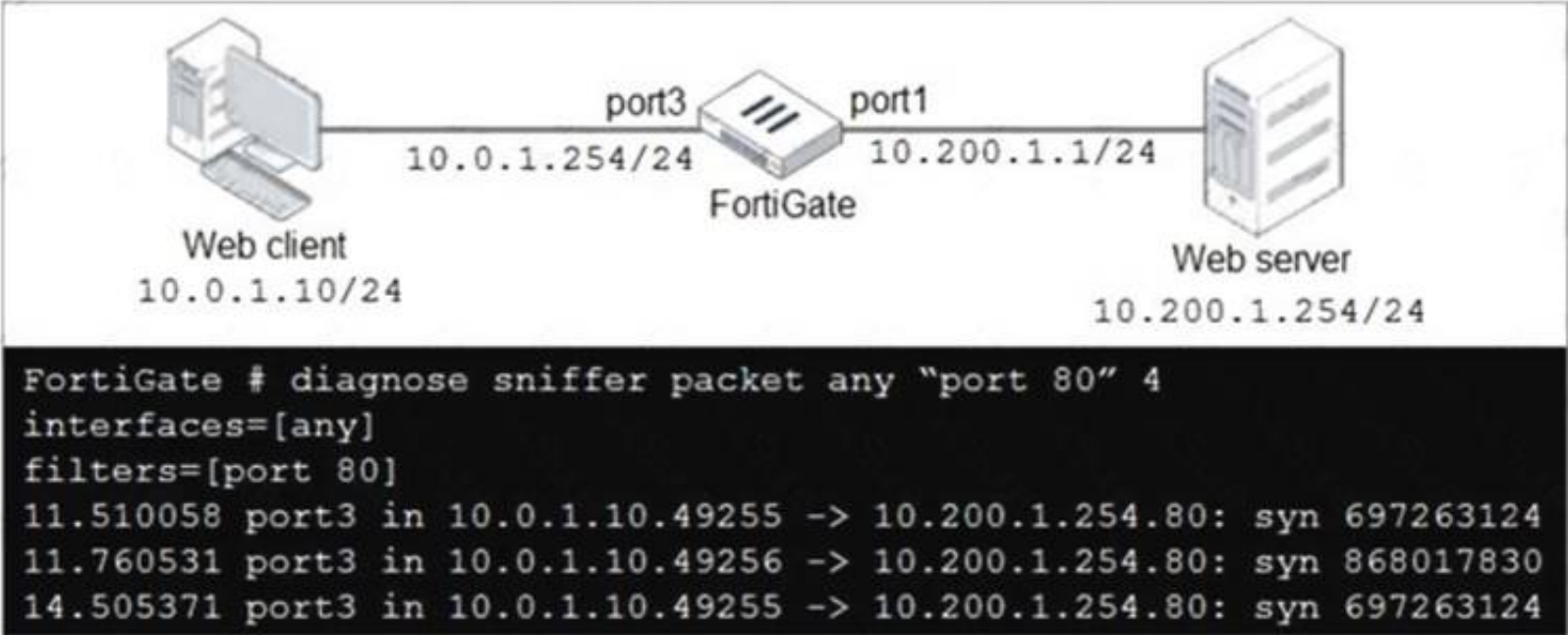
In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.
What should the administrator do next to troubleshoot the problem?

A. Run a sniffer on the web server.
B. Capture the traffic using an external sniffer connected to port1.
C. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10"
D. Execute a debug flow.

Answer: D

NEW QUESTION 37
- (Exam Topic 2)
An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.16.1.0/24 and the remote quick mode selector is 192.16.2.0/24. How must the administrator configure the local quick mode selector for site B?

A. 192.168.3.0/24
B. 192.168.2.0/24
C. 192.168.1.0/24
D. 192.168.0.0/8

Answer: B

NEW QUESTION 40
- (Exam Topic 2)
Examine this PAC file configuration.

```
function FindProxyForURL (url, host) {
  if (shExpMatch (url, "*.fortinet.com/*")) {
    return "DIRECT";}
  if (isInNet (host, "172.25.120.0", "255.255.255.0")) {
    return "PROXY" altproxy.corp.com: 8060";}
  return "PROXY proxy.corp.com: 8090";
}
```

Which of the following statements are true? (Choose two.)

A. Browsers can be configured to retrieve this PAC file from the FortiGate.
B. Any web request to the 172.25.120.0/24 subnet is allowed to bypass the proxy.
C. All requests not made to Fortinet.com or the 172.25.120.0/24 subnet, have to go through altproxy.corp.com: 8060.
D. Any web request fortinet.com is allowed to bypass the proxy.

Answer: AD

NEW QUESTION 45

- (Exam Topic 2)
Refer to the exhibit.

Which contains a network diagram and routing table output. The Student is unable to access Webserver.
What is the cause of the problem and what is the solution for the problem?

A. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
B. The first reply packet for Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
C. The first reply packet for Student failed the RPF check.This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.
D. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

Answer: D

NEW QUESTION 49

- (Exam Topic 2)
FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.
Which two other security profiles can you apply to the security policy? (Choose two.)

A. Antivirus scanning
B. File filter
C. DNS filter
D. Intrusion prevention

Answer: AD

NEW QUESTION 53

- (Exam Topic 2)
Which two statements are true about the RPF check? (Choose two.)

A. The RPF check is run on the first sent packet of any new session.
B. The RPF check is run on the first reply packet of any new session.
C. The RPF check is run on the first sent and reply packet of any new session.
D. RPF is a mechanism that protects FortiGate and your network from IP spoofing attacks.

Answer: AD

Explanation:
Reference: https://www.programmersought.com/article/16383871634/

NEW QUESTION 57

- (Exam Topic 2)
When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

A. Log ID
B. Universally Unique Identifier
C. Policy ID
D. Sequence ID

Answer: B

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies

NEW QUESTION 59
- (Exam Topic 2)
To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

A. FortiManager
B. Root FortiGate
C. FortiAnalyzer
D. Downstream FortiGate

Answer: B

NEW QUESTION 62
- (Exam Topic 2)
Which two statements are correct about a software switch on FortiGate? (Choose two.)

A. It can be configured only when FortiGate is operating in NAT mode
B. Can act as a Layer 2 switch as well as a Layer 3 router
C. All interfaces in the software switch share the same IP address
D. It can group only physical interfaces

Answer: AC

NEW QUESTION 63
- (Exam Topic 2)
Which of statement is true about SSL VPN web mode?

A. The tunnel is up while the client is connected.
B. It supports a limited number of protocols.
C. The external network application sends data through the VPN.
D. It assigns a virtual IP address to the client.

Answer: B

Explanation:
FortiGate_Security_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

NEW QUESTION 65
- (Exam Topic 2)
The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile.
What order must FortiGate use when the web filter profile has features enabled, such as safe search?

A. DNS-based web filter and proxy-based web filter
B. Static URL filter, FortiGuard category filter, and advanced filters
C. Static domain filter, SSL inspection filter, and external connectors filters
D. FortiGuard category filter and rating filter

Answer: B

Explanation:
Reference: https://fortinet121.rssing.com/chan-67705148/all_p1.html

NEW QUESTION 70
- (Exam Topic 2)
Which two statements are true about collector agent standard access mode? (Choose two.)

A. Standard mode uses Windows convention-NetBios: Domain\Username.
B. Standard mode security profiles apply to organizational units (OU).
C. Standard mode security profiles apply to user groups.
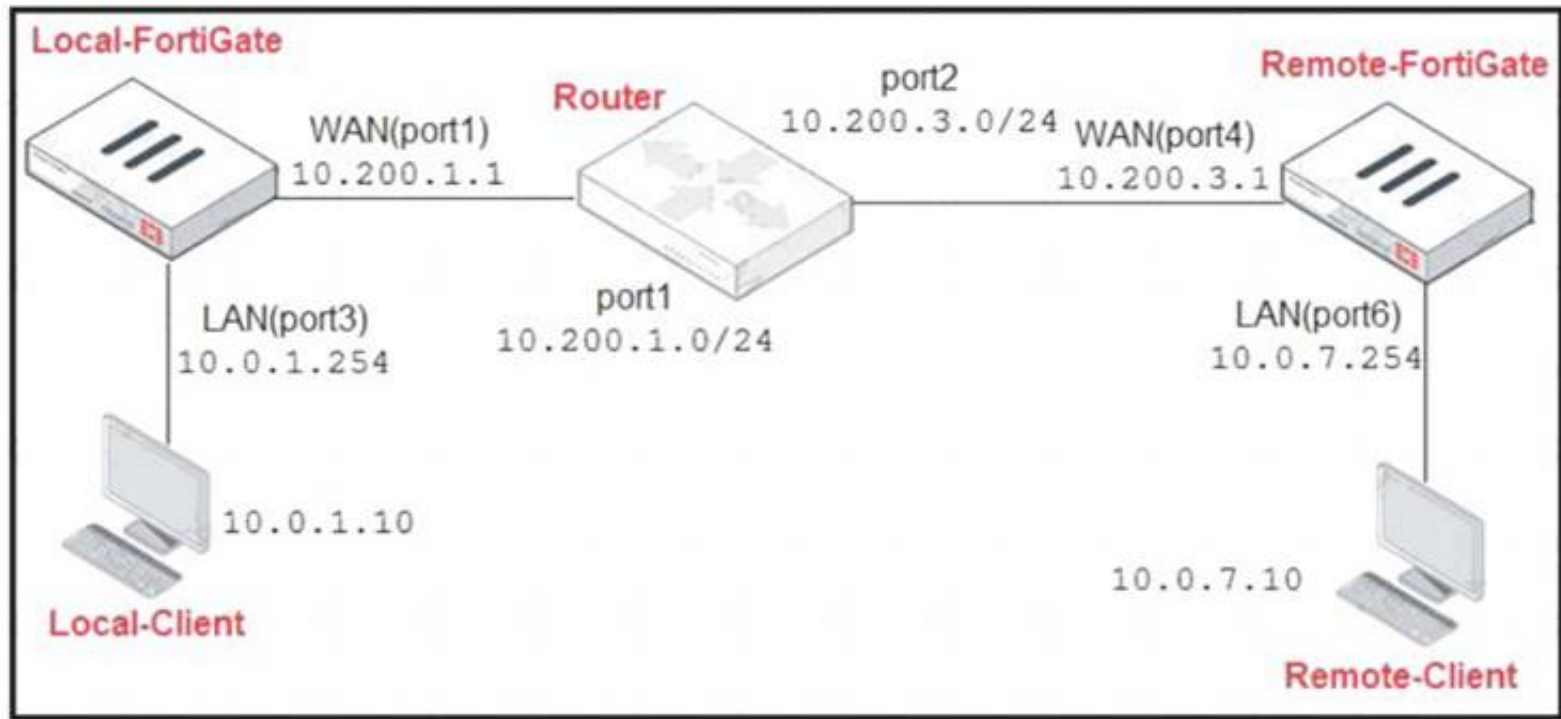D. Standard access mode supports nested groups.

Answer: AC

Explanation:

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso

NEW QUESTION 73
- (Exam Topic 2)
Refer to the exhibit.

Network Diagram

Central SNAT Policies Local-FortiGate

ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
	○					
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

IP Pool Local-FortiGate

Name ⇕	External IP Range ⇕	Type ⇕	ARP Reply ⇕
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	✓ Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	✓ Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	✓ Enabled

Protocol Number Table

Protocol Number Table	
Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration. The WAN (port1) interface has the IP address 10.200.1.1/24.
The LAN (port3) interface has the IP address 10.0.1.254/24.
A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied.
Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

A. 10.200.1.149
B. 10.200.1.1
C. 10.200.1.49
D. 10.200.1.99

Answer: D

NEW QUESTION 77
- (Exam Topic 2)
View the exhibit.

Destination ⓘ	Subnet	Named Address	Internet Service
	172.13.24.0/255.255.255.0 ▾		
Interface	🔼 TunnelB ▾		
Administrative Distance ⓘ	5		
Comments			0/255
Status	⬆ Enabled ⬇ Disabled		
⊟ Advanced Options			
Priority ⓘ	30		

Destination ⓘ	Subnet	Named Address	Internet Service
	172.13.24.0/255.255.255.0 ▾		
Interface	🔼 Tunnel A ▾		
Administrative Distance ⓘ	10		
Comments			0/255
Status	⬆ Enabled ⬇ Disabled		
⊟ Advanced Options			
Priority ⓘ	0		

Which of the following statements are correct? (Choose two.)

A. This setup requires at least two firewall policies with the action set to IPsec.
B. Dead peer detection must be disabled to support this type of IPsec setup.
C. The TunnelB route is the primary route for reaching the remote sit
D. The TunnelA route is used only if the TunnelB VPN is down.
E. This is a redundant IPsec setup.

Answer: CD

NEW QUESTION 80
- (Exam Topic 2)
Which two types of traffic are managed only by the management VDOM? (Choose two.)

A. FortiGuard web filter queries
B. PKI
C. Traffic shaping
D. DNS

Answer: AD

NEW QUESTION 85
- (Exam Topic 2)
Which of the following SD-WAN load –balancing method use interface weight value to distribute traffic? (Choose two.)

A. Source IP
B. Spillover
C. Volume
D. Session

Answer: CD

Explanation:
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/49719/configuring-sd-wan-load-balancing

NEW QUESTION 89
- (Exam Topic 2)
In which two ways can RPF checking be disabled? (Choose two)

A. Enable anti-replay in firewall policy.
B. Disable the RPF check at the FortiGate interface level for the source check
C. Enable asymmetric routing.
D. Disable strict-arc-check under system settings.

Answer: CD

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955

NEW QUESTION 92
- (Exam Topic 2)
Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)
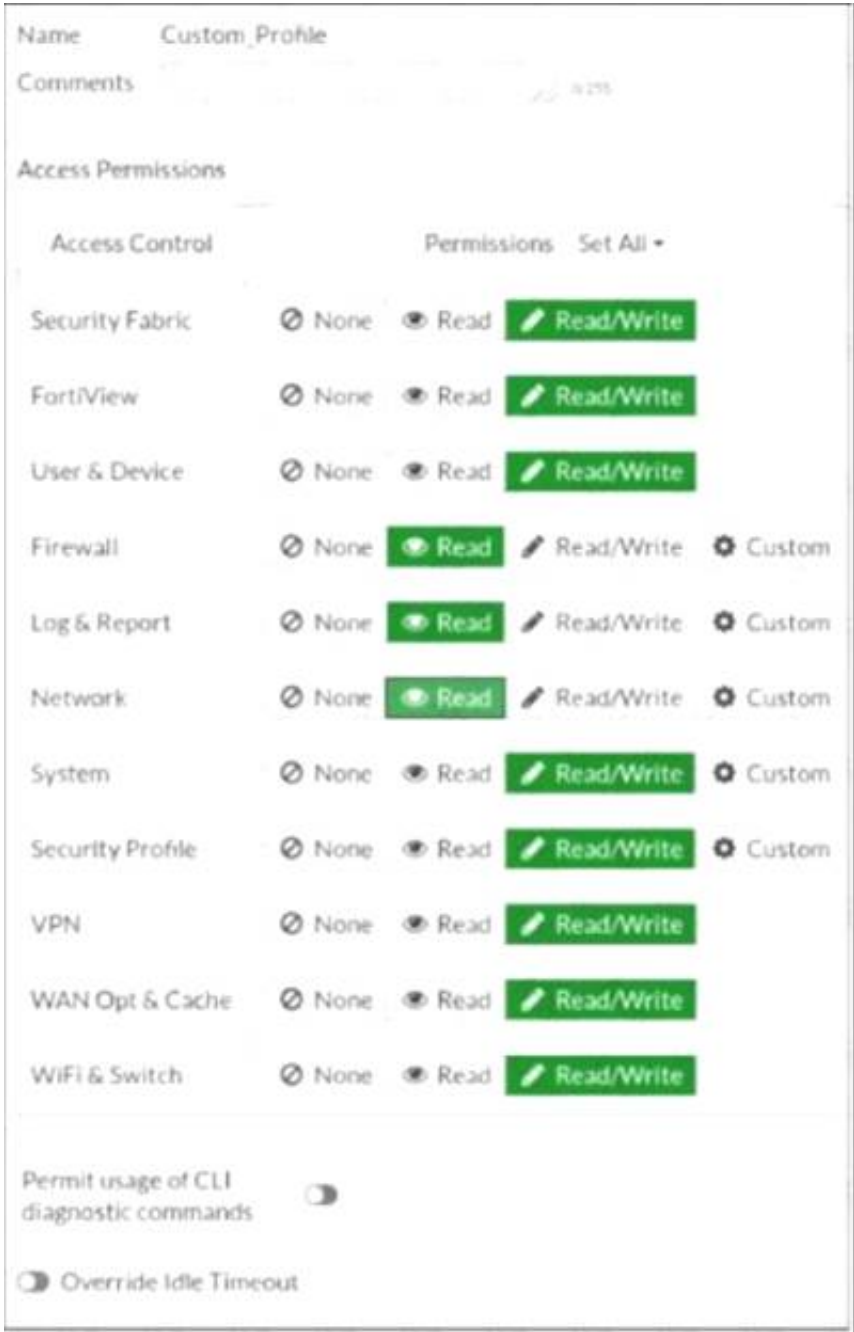
A. DNS
B. ping
C. udp-echo
D. TWAMP

Answer: CD

NEW QUESTION 95
- (Exam Topic 2)
Refer to the exhibit.

Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?

A. Custom permission for Network
B. Read/Write permission for Log & Report
C. CLI diagnostics commands permission
D. Read/Write permission for Firewall

Answer: C

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220

NEW QUESTION 98
- (Exam Topic 2)
Refer to the exhibit.

```
1: date=2020-08-14 time=06:28:24 logid= "0316013056" type= "utm" subtype= "webfilter"
eventtype= "ftgd_blk" level= "warning" vd= "root" eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= "port3" srci ntfrole=
"undefined" dstip=159.65.216.232 dstport=443 dstintf= "port1" dstintfrole= "wan" proto=6
service= "HTTPS" hostname= "etp-experiment-1.dummytracker.org" profile= "default"
action= "blocked" reqtype= "direct" url= "https://etp-experiment-1.dumytracker.org/"
sentbyte=517 rcvdbyte=0 direction= "outgoing" msg= "URL belongs to a denied category in
policy" method= "domain" cat=26 catdesc= "Malicious Websites" crscore=30 craction=
4194304 crlevel= "high"
```

Based on the raw log, which two statements are correct? (Choose two.)

A. Traffic is blocked because Action is set to DENY in the firewall policy.
B. Traffic belongs to the root VDOM.
C. This is a security log.
D. Log severity is set to error on FortiGate.

Answer: AC

NEW QUESTION 101
- (Exam Topic 2)
Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

A. Web filter in flow-based inspection
B. Antivirus in flow-based inspection
C. DNS filter
D. Web application firewall
E. Application control

Answer: ABE

NEW QUESTION 104
- (Exam Topic 2)
In an explicit proxy setup, where is the authentication method and database configured?

A. Proxy Policy
B. Authentication Rule
C. Firewall Policy
D. Authentication scheme

Answer: D

NEW QUESTION 109
- (Exam Topic 2)
Which Security rating scorecard helps identify configuration weakness and best practice violations in your network?

A. Fabric Coverage
B. Automated Response
C. Security Posture
D. Optimization

Answer: C

Explanation:
Reference:
https://www.fortinet.com/content/dam/fortinet/assets/support/fortinet-recommended-security-bestpractices.pdf

NEW QUESTION 114
- (Exam Topic 2)
What is the primary FortiGate election process when the HA override setting is disabled?

A. Connected monitored ports > System uptime > Priority > FortiGate Serial number
B. Connected monitored ports > HA uptime > Priority > FortiGate Serial number
C. Connected monitored ports > Priority > HA uptime > FortiGate Serial number
D. Connected monitored ports > Priority > System uptime > FortiGate Serial number

Answer: B

Explanation:
Reference: http://myitmicroblog.blogspot.com/2018/11/what-should-you-know-about-ha-override.html

NEW QUESTION 115
- (Exam Topic 2)
A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser
does not report errors.
What is the reason for the certificate warning errors?

A. The browser requires a software update.
B. FortiGate does not support full SSL inspection when web filtering is enabled.
C. The CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.
D. There are network connectivity issues.

Answer: C

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD41394

NEW QUESTION 119
- (Exam Topic 2)
Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

A. This is known as many-to-one NAT.
B. Source IP is translated to the outgoing interface IP.
C. Connections are tracked using source port and source MAC address.
D. Port address translation is not used.

Answer: BD

NEW QUESTION 121
- (Exam Topic 2)
Refer to the exhibit.

```
config firewall policy                    FIREWALL POLICIES
    edit 1
        set name "INTERNET"
        set uuid b11ac58c-791b-51e7-4600-12f829a689d9
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "LOCAL_SUBNET"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set http-policy-redirect enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set logtraffic all
        set logtraffic-start enable
        set ippool enable
        set poolname "ProxyPool"
        set nat enable
    next
end

config firewall proxy-address              PROXY ADDRESS
    edit "EICAR"
        set uuid 5a24bdaa-c792-51ea-2c89-a9f79e2bdc96
        set type host-regex
        set host-regex ".*eicar\\.org"
    next
end
```

```
config firewall
    edit 1
        set uuid 6491d12b-c79b-51ea-13f9-4ad84b543a8e
        set proxy transparent-web
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "EICAR"
        set service "webproxy"
        set action accept
        set schedule "always"
        set logtraffic all
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
    next
    edit 2
        set uuid 6a1c74c6-c794-51ea-e646-4f78ae2bc5f9
        set proxy transparent-web
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set service "webproxy"
        set action accept
        set status disable
        set schedule "always"
        set logtraffic disable
        set ssl-ssh-profile "certificate-inspection"
    next
    edit 3
        set uuid 818fb8b6-c797-51ea-d848-a7c2952ceea9
        set proxy transparent-web
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set service "webproxy"
        set action accept
        set status disable
        set schedule "always"
        set logtraffic all
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
    next
end
```

The exhibit shows a CLI output of firewall policies, proxy policies, and proxy addresses.
How does FortiGate process the traffic sent to http://www.fortinet.com?

A. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 3.
B. Traffic will not be redirected to the transparent proxy and it will be allowed by firewall policy ID 1.
C. Traffic will be redirected to the transparent proxy and It will be allowed by proxy policy ID 1.
D. Traffic will be redirected to the transparent proxy and it will be denied by the proxy implicit deny policy.

Answer: D

NEW QUESTION 126
- (Exam Topic 2)
Which security feature does FortiGate provide to protect servers located in the internal networks from attacks such as SQL injections?

A. Denial of Service
B. Web application firewall
C. Antivirus
D. Application control

Answer: B

Explanation:
Reference: https://docs.fortinet.com/document/fortiweb/6.3.3/administration-guide/60895/introduction

NEW QUESTION 130
- (Exam Topic 2)
Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

A. Log downloads from the GUI are limited to the current filter view
B. Log backups from the CLI cannot be restored to another FortiGate.
C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
D. Log downloads from the GUI are stored as LZ4 compressed files.

Answer: AB

NEW QUESTION 134

- (Exam Topic 2)
An administrator has configured a route-based IPsec VPN between two FortiGate devices. Which statement about this IPsec VPN configuration is true?

A. A phase 2 configuration is not required.
B. This VPN cannot be used as part of a hub-and-spoke topology.
C. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.
D. The IPsec firewall policies must be placed at the top of the list.

Answer: C

Explanation:
In a route-based configuration, FortiGate automatically adds a virtual interface eith the VPN name (Infrastructure Study Guide, 206)

NEW QUESTION 137
- (Exam Topic 2)
Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

A. Heartbeat interfaces have virtual IP addresses that are manually assigned.
B. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.
C. Virtual IP addresses are used to distinguish between cluster members.
D. The primary device in the cluster is always assigned IP address 169.254.0.1.

Answer: BD

NEW QUESTION 139
- (Exam Topic 2)
An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

A. The interface has been configured for one-arm sniffer.
B. The interface is a member of a virtual wire pair.
C. The operation mode is transparent.
D. The interface is a member of a zone.
E. Captive portal is enabled in the interface.

Answer: ABC

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

NEW QUESTION 144
- (Exam Topic 2)
Examine this output from a debug flow:

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

A. The next-hop IP address is unreachable.
B. It failed the RPF check.
C. It matched an explicitly configured firewall policy with the action DENY.
D. It matched the default implicit firewall policy.

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=13900

NEW QUESTION 146
- (Exam Topic 2)
Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.
B. Only secondary FortiGate devices are rebooted.
C. Uninterruptable upgrade is enabled by default.
D. Traffic load balancing is temporaly disabled while upgrading the firmware.

Answer: CD

NEW QUESTION 150
- (Exam Topic 2)
When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

A. remote user's public IP address
B. The public IP address of the FortiGate device.
C. The remote user's virtual IP address.
D. The internal IP address of the FortiGate device.

Answer: D

Explanation:
Source IP seen by the remote resources is FortiGate's internal IP address and not the user's IP address

NEW QUESTION 151
- (Exam Topic 2)
How do you format the FortiGate flash disk?

A. Load a debug FortiOS image.
B. Load the hardware test (HQIP) image.
C. Execute the CLI command execute formatlogdisk.
D. Select the format boot device option from the BIOS menu.

Answer: D

NEW QUESTION 156
......

Relate Links

100% Pass Your NSE4_FGT-7.0 Exam with Exambible Prep Materials

https://www.exambible.com/NSE4_FGT-7.0-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/