Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

https://www.2passeasy.com/dumps/NSE4_FGT-7.0/

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)
A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.
* All traffic must be routed through the primary tunnel when both tunnels are up
* The secondary tunnel must be used only if the primary tunnel goes down
* In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover
Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two,)

A. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
B. Enable Dead Peer Detection.
C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
D. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

Answer: BC

Explanation:
B - because the customer requires the tunnels to notify when a tunnel goes down. DPD is designed for that purpose. To send a packet over a firewall to determine a failover for the next tunnel after a specific amount of time of not receiving a response from its peer.
C - remember when it comes to choosing a route with regards to Administrative Distance. The route with the lowest distance for that particular route will be chosen. So, by configuring a lower routing distance on the primary tunnel, means that the primary tunnel will be chosen to route packets towards their destination.

NEW QUESTION 3
- (Exam Topic 1)
An administrator wants to configure Dead Peer Detection (DPD) on IPSEC VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.

Which DPD mode on FortiGate will meet the above requirement?

A. Disabled
B. On Demand
C. Enabled
D. On Idle

Answer: D

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD40813

NEW QUESTION 4
- (Exam Topic 1)
Refer to the exhibit.

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic. Why is FortiGate not sending probes to 4.2.2.2 and 4.2.2.1 servers? (Choose two.)

A. The Detection Mode setting is not set to Passive.
B. Administrator didn't configure a gateway for the SD-WAN members, or configured gateway is not valid.
C. The configured participants are not SD-WAN members.
D. The Enable probe packets setting is not enabled.

Answer: BD

NEW QUESTION 5
- (Exam Topic 1)
Which two statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.
C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Answer: BC

Explanation:
An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM—something that no device has in the real world. Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

NEW QUESTION 6
- (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 7
- (Exam Topic 1)
Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

Which two statements about the debug flow output are correct? (Choose two.)

A. The debug flow is of ICMP traffic.
B. A firewall policy allowed the connection.
C. A new traffic session is created.
D. The default route is required to receive a reply.

Answer: AC

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/54688/debugging-the-packet-flow

NEW QUESTION 8
- (Exam Topic 1)
An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.168.1.0/24 and the remote quick mode selector is 192.168.2.0/24.
Which subnet must the administrator configure for the local quick mode selector for site B?

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

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
Which two statements are true about the FGCP protocol? (Choose two.)

A. Not used when FortiGate is in Transparent mode
B. Elects the primary FortiGate device

C. Runs only over the heartbeat links
D. Is used to discover FortiGate devices in different HA groups

Answer: BC

Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/564712/fgcp-fortigate-clustering-protocol

NEW QUESTION 10
- (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 10
- (Exam Topic 1)
Refer to the exhibit.

Examine the intrusion prevention system (IPS) diagnostic command.
Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

A. The IPS engine was inspecting high volume of traffic.
B. The IPS engine was unable to prevent an intrusion attack.
C. The IPS engine was blocking all traffic.
D. The IPS engine will continue to run in a normal state.

Answer: A

Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/232929/troubleshooting-high-cpu-usage

NEW QUESTION 13
- (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?
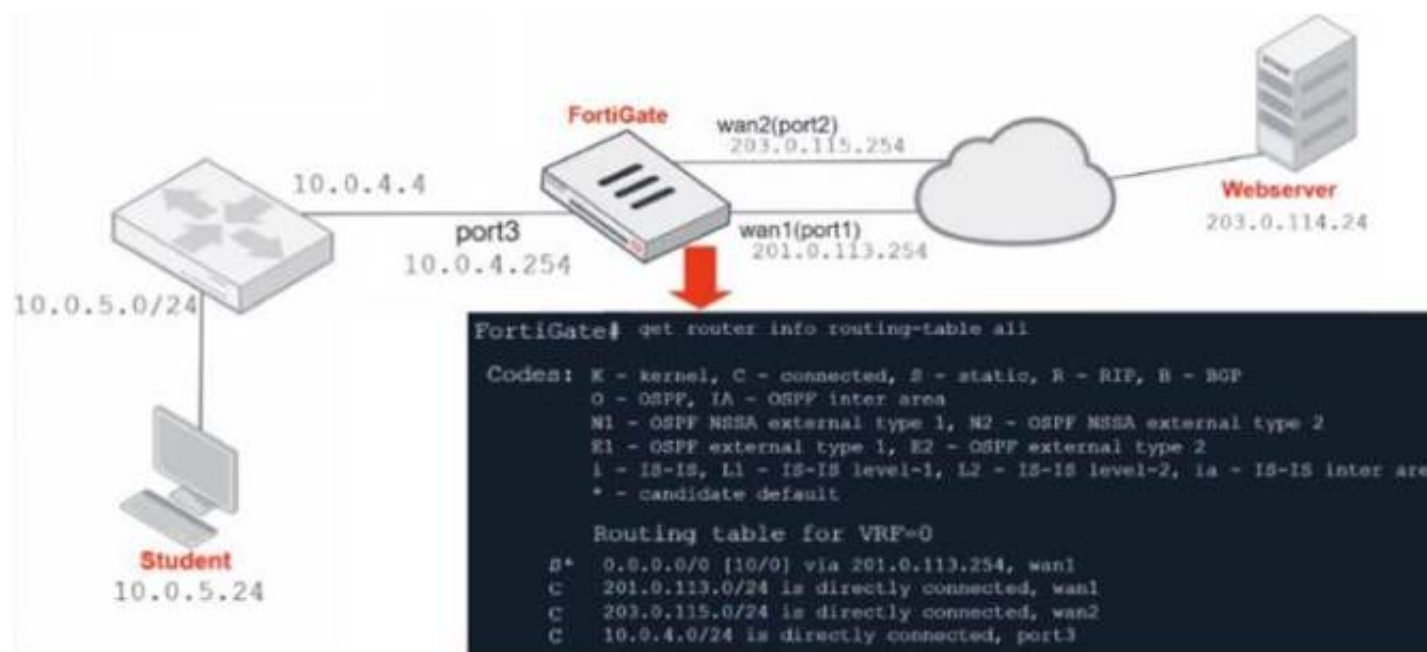
A. 192.168.3.0/24
B. 192.168.2.0/24
C. 192.168.1.0/24
D. 192.168.0.0/8

Answer: B

NEW QUESTION 14
- (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 16
- (Exam Topic 2)
In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

A. The IP version of the sources and destinations in a firewall policy must be different.
B. The Incoming Interfac
C. Outgoing Interfac
D. Schedule, and Service fields can be shared with both IPv4 and IPv6.
E. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
F. The IP version of the sources and destinations in a policy must match.
G. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Answer: BDE

NEW QUESTION 21
- (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.
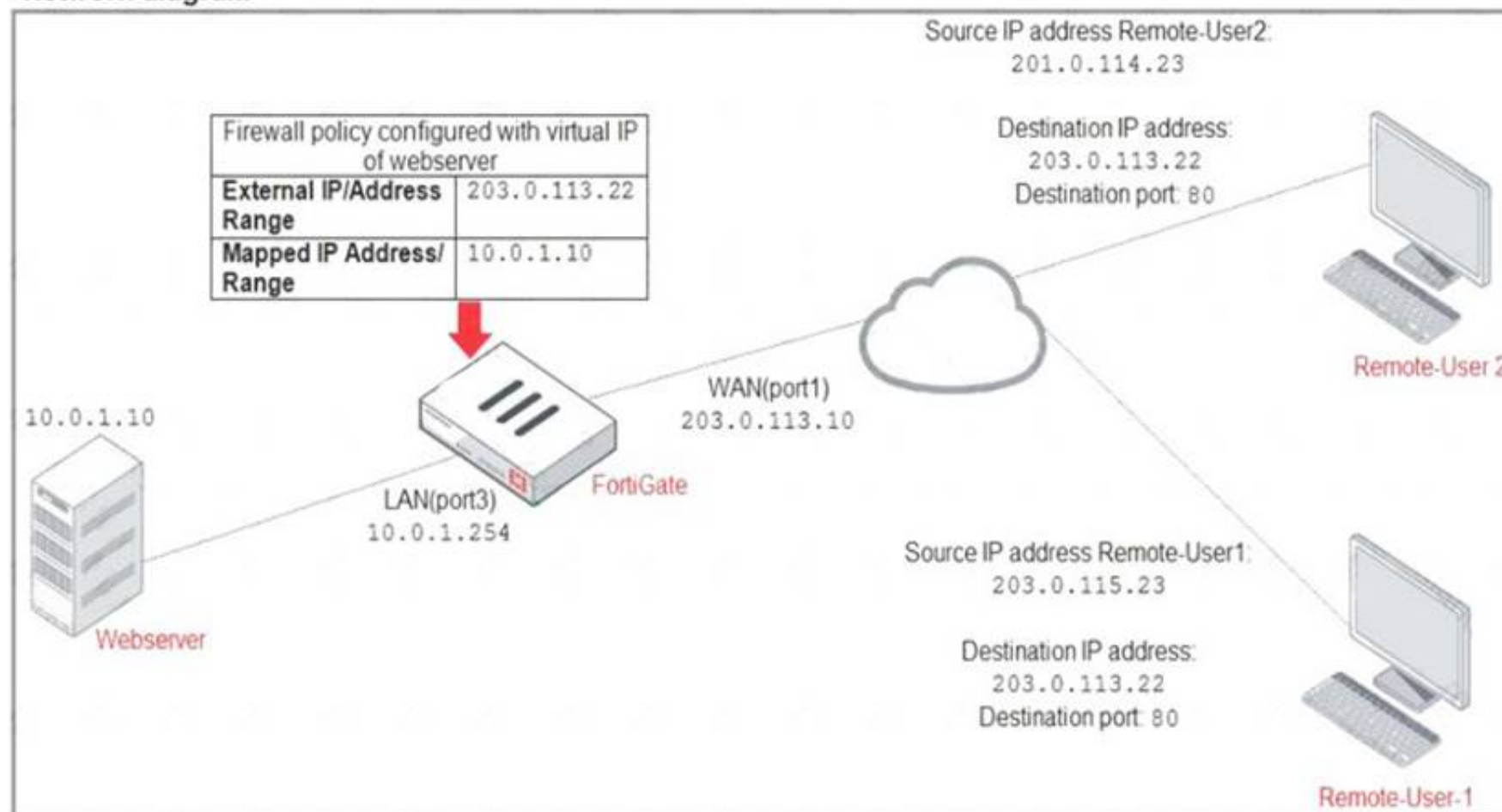
Answer: AD

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

NEW QUESTION 25
- (Exam Topic 2)
Refer to the exhibit.

Network diagram

Firewall policy configured with virtual IP of webserver

| External IP/Address Range | 203.0.113.22 |
| Mapped IP Address/ Range | 10.0.1.10 |

Source IP address Remote-User2:
201.0.114.23

Destination IP address:
203.0.113.22
Destination port: 80

Remote-User 2

10.0.1.10

WAN(port1)
203.0.113.10

FortiGate

LAN(port3)
10.0.1.254

Webserver

Source IP address Remote-User1:
203.0.115.23

Destination IP address:
203.0.113.22
Destination port: 80

Remote-User-1

ID	Name	Source	Destination	Schedule	Service	Action
☐ ▦ WAN(port1) → ▦ LAN(port3) ❷						
2	Deny	🖭 Deny_IP	🖥 all	🕓 always	📇 ALL	⊘ DENY
3	Allow_access	🖥 all	🖷 Web_server	🕓 always	📇 ALL	✔ ACCEPT

Firewall address object

Edit Address

Name	Deny_IP
Color	🖭 Change
Type	Subnet ▼
IP/Netmask	201.0.114.23/32
Interface	▦ WAN(port1) ▼
Static route configuration	◯
Comments	Deny webserver access. 22/255

The exhibit contains a network diagram, firewall policies, and a firewall address object configuration.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-user2. Remote-user2 is still able to access Webserver.
Which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

A. Disable match-vip in the Deny policy.
B. Set the Destination address as Deny_IP in the Allow-access policy.
C. Enable match vip in the Deny policy.
D. Set the Destination address as Web_server in the Deny policy.

Answer: CD

NEW QUESTION 27
- (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 30
- (Exam Topic 2)
An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

A. Configure Source IP Pools.
B. Configure split tunneling in tunnel mode.
C. Configure different SSL VPN realms.
D. Configure host check.

Answer: D

NEW QUESTION 32
- (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 34
- (Exam Topic 2)
NGFW mode allows policy-based configuration for most inspection rules. Which security profile's configuration does not change when you enable policy-based inspection?

A. Web filtering
B. Antivirus
C. Web proxy
D. Application control

Answer: B

NEW QUESTION 35
- (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 38
- (Exam Topic 2)
Which two statements about IPsec authentication on FortiGate are correct? (Choose two.)

A. For a stronger authentication, you can also enable extended authentication (XAuth) to request the remote peer to provide a username and password
B. FortiGate supports pre-shared key and signature as authentication methods.
C. Enabling XAuth results in a faster authentication because fewer packets are exchanged.
D. A certificate is not required on the remote peer when you set the signature as the authentication method.
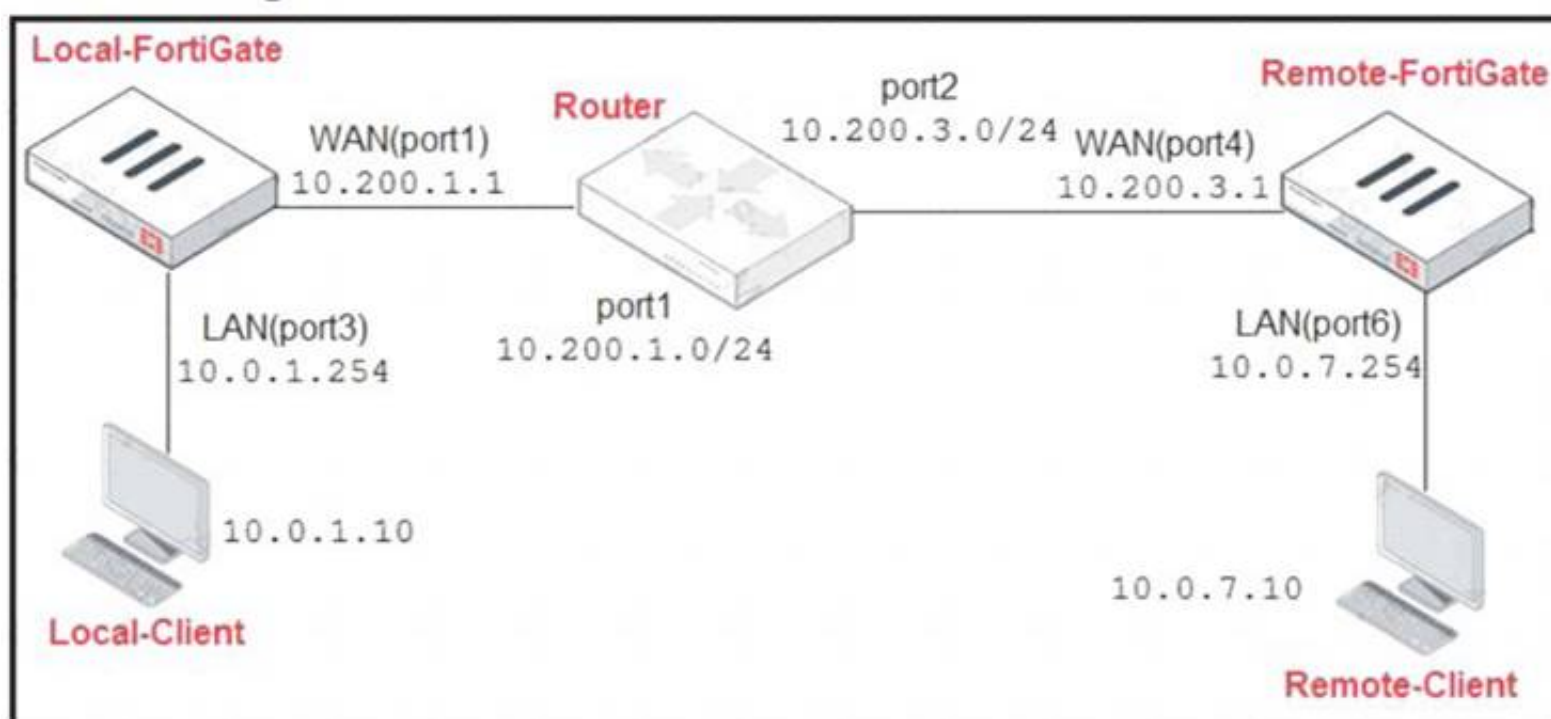
Answer: AB

Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/913287/ipsec-vpn-authenticating-aremote-fortigate

NEW QUESTION 41
- (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 44
- (Exam Topic 2)
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

A. diagnose wad session list
B. diagnose wad session list | grep hook-pre&&hook-out
C. diagnose wad session list | grep hook=pre&&hook=out
D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: A

NEW QUESTION 49
- (Exam Topic 2)
Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

A. diagnose sys top
B. execute ping
C. execute traceroute
D. diagnose sniffer packet any
E. get system arp

Answer: BCD

NEW QUESTION 51
- (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 54
- (Exam Topic 2)
Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

A. The public key of the web server certificate must be installed on the browser.
B. The web-server certificate must be installed on the browser.
C. The CA certificate that signed the web-server certificate must be installed on the browser.
D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Answer: C

NEW QUESTION 56
- (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 57
- (Exam Topic 2)
Refer to the exhibit.

Name	Custom_Profile			
Comments				

Access Permissions

Access Control	Permissions	Set All ▾		
Security Fabric	⊘ None	◉ Read	✎ Read/Write	
FortiView	⊘ None	◉ Read	✎ Read/Write	
User & Device	⊘ None	◉ Read	✎ Read/Write	
Firewall	⊘ None	◉ Read	✎ Read/Write	⚙ Custom
Log & Report	⊘ None	◉ Read	✎ Read/Write	⚙ Custom
Network	⊘ None	◉ Read	✎ Read/Write	⚙ Custom
System	⊘ None	◉ Read	✎ Read/Write	⚙ Custom
Security Profile	⊘ None	◉ Read	✎ Read/Write	⚙ Custom
VPN	⊘ None	◉ Read	✎ Read/Write	
WAN Opt & Cache	⊘ None	◉ Read	✎ Read/Write	
WiFi & Switch	⊘ None	◉ Read	✎ Read/Write	

Permit usage of CLI diagnostic commands ◯▪

◯▪ Override Idle Timeout

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 62
- (Exam Topic 2)
What types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

A. Traffic to botnetservers
B. Traffic to inappropriate web sites
C. Server information disclosure attacks
D. Credit card data leaks
E. SQL injection attacks

Answer: CDE

NEW QUESTION 64
- (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 68
- (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 71
- (Exam Topic 2)
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

A. Warning
B. Exempt
C. Allow
D. Learn

Answer: AC

NEW QUESTION 75
- (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 80
- (Exam Topic 2)
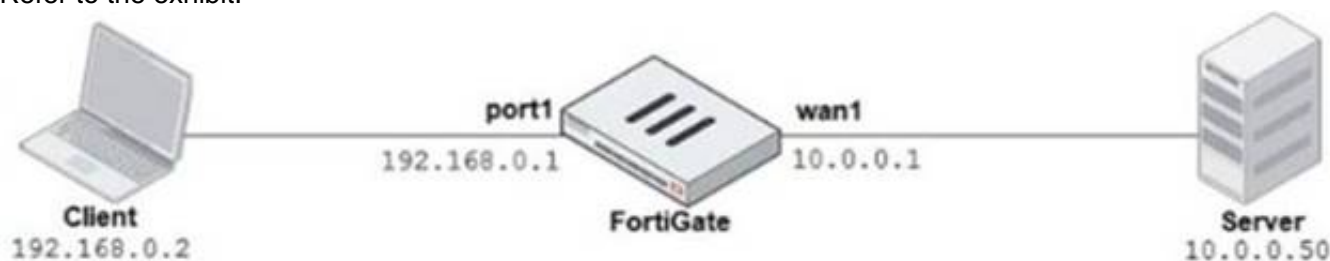Which three statements about security associations (SA) in IPsec are correct? (Choose three.)

A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.
B. An SA never expires.
C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.
D. Phase 2 SA expiration can be time-based, volume-based, or both.
E. Both the phase 1 SA and phase 2 SA are bidirectional.

Answer: ACD

NEW QUESTION 82
- (Exam Topic 2)
Refer to the exhibit.

Explicit Proxy

Explicit Web Proxy

Listen on Interfaces   port1   ✕
     +

HTTP Port   8080   -   8080

HTTPS Port   **Use HTTP Port**   Specify

FTP over HTTP

Proxy auto-config (PAC)

Proxy FQDN   default.fqdn

Max HTTP request length   8   KB

Max HTTP message length   32   KB

Unknown HTTP version   Best Effort **Reject**

Realm   default

Default Firewall Policy Action   Accept **Deny**

The exhibits show a network diagram and the explicit web proxy configuration.
In the command diagnose sniffer packet, what filter can you use to capture the traffic between the client and the explicit web proxy?

A. 'host 192.168.0.2 and port 8080'
B. 'host 10.0.0.50 and port 80'
C. 'host 192.168.0.1 and port 80'
D. 'host 10.0.0.50 and port 8080'

Answer: A

NEW QUESTION 86
- (Exam Topic 2)
Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)

A. Shut down/reboot a downstream FortiGate device.
B. Disable FortiAnalyzer logging for a downstream FortiGate device.
C. Log in to a downstream FortiSwitch device.
D. Ban or unban compromised hosts.

Answer: AB

NEW QUESTION 90
- (Exam Topic 2)
Examine the following web filtering log.

```
Date=2016-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk level=warning
vd=root policyid=1 sessionid=149645 user= " " scrip=10.0.1.10 srcport=52919 srcintf= "port3"
dstip=54.230.128.169 dstport=80 dstintf= "port1" proto=6 service="HTTP" hostname= "miniclip.com"
profile= "default" action=blocked reqtype=direct url= "/" sentbyte=286 rcvdbyte=0 direction=outgoing msg= "URL
belongs to a category with warnings enabled" method=domain cat=20 catdesc="Games" crscore=30 crlevel=high
```

Which statement about the log message is true?

A. The action for the category Games is set to block.
B. The usage quota for the IP address 10.0.1.10 has expired
C. The name of the applied web filter profile is default.
D. The web site miniclip.com matches a static URL filter whose action is set to Warning.

Answer: C

NEW QUESTION 93
......

NSE4_FGT-7.0 Practice Exam Features:

* NSE4_FGT-7.0 Questions and Answers Updated Frequently

* NSE4_FGT-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE4_FGT-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE4_FGT-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year