Fortinet

Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

NEW QUESTION 1
Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

A. FTM
B. SSH
C. HTTPS
D. FortiTelemetry

Answer: BC

NEW QUESTION 2
A network administrator enabled antivirus and selected an SSL inspection profile on a firewall policy. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and does not block the file, allowing it to be downloaded.
The administrator confirms that the traffic matches the configured firewall policy.
What are two reasons for the failed virus detection by FortiGate? (Choose two.)

A. The website is exempted from SSL inspection.
B. The EICAR test file exceeds the protocol options oversize limit.
C. The selected SSL inspection profile has certificate inspection enabled.
D. The browser does not trust the FortiGate self-signed CA certificate.

Answer: AD

NEW QUESTION 3
Which statement is correct regarding the use of application control for inspecting web applications?

A. Application control can identify child and parent applications, and perform different actions on them.
B. Application control signatures are organized in a nonhierarchical structure.
C. Application control does not require SSL inspection to identify web applications.
D. Application control does not display a replacement message for a blocked web application.

Answer: A

NEW QUESTION 4
A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.
Which type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

A. Pre-shared key
B. Dialup user
C. Dynamic DNS
D. Static IP address

Answer: D

NEW QUESTION 5
Refer to the exhibit.
The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.
When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.
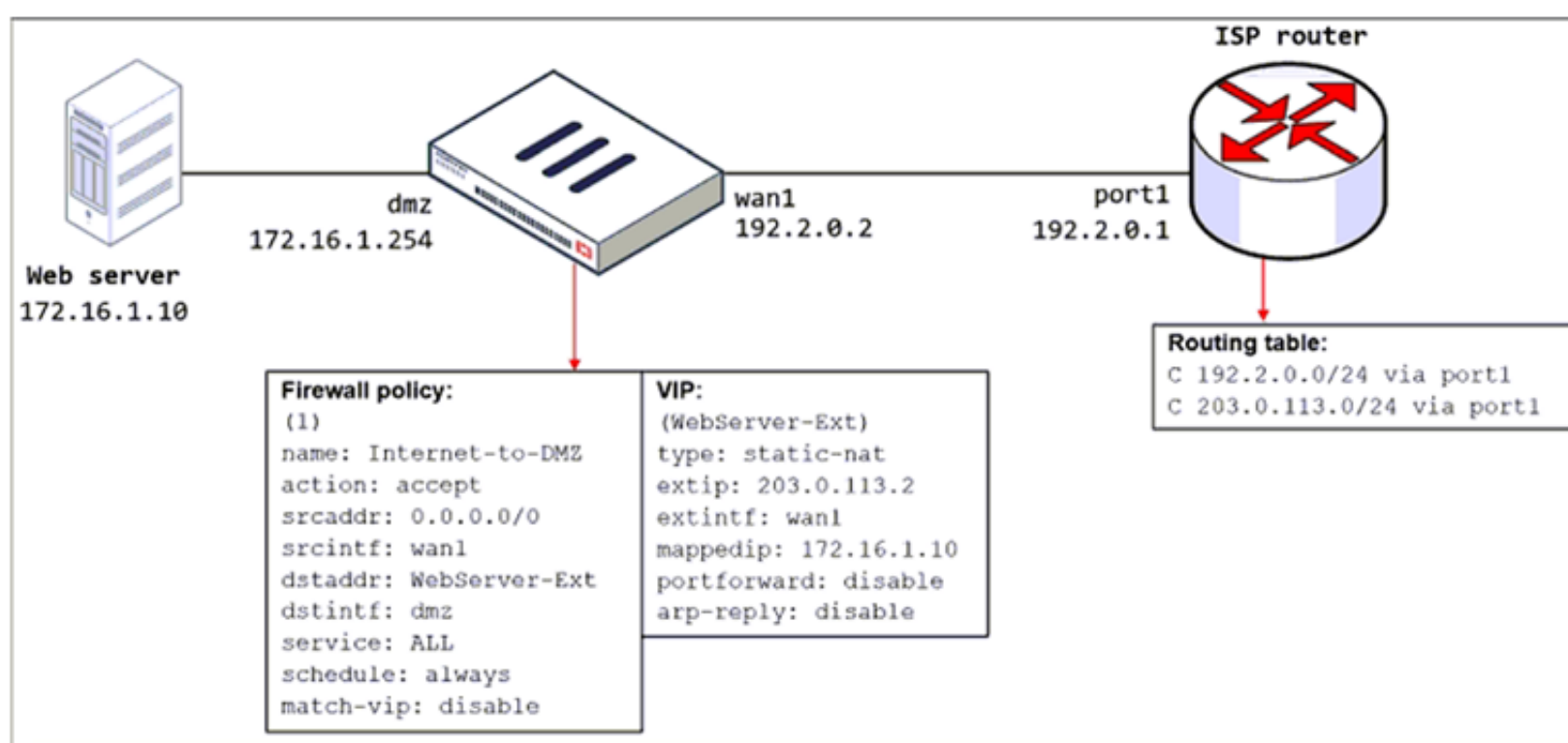
Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

A. Configure a loopback interface with address 203.0.113.2/32.
B. In the VIP configuration, enable arp-reply.
C. Enable port forwarding on the server to map the external service port to the internal service port.
D. In the firewall policy configuration, enable match-vip.

Answer: D

NEW QUESTION 6
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"
```

What two conclusions can you make from the debug flow output? (Choose two.)

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

Answer: AC

NEW QUESTION 7
Refer to the exhibits.
The exhibits show the firewall policies and the objects used in the firewall policies.
The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.

Exhibit A | Exhibit B

Address Object

Name	Details
IP Range/Subnet **10**	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN **2**	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services **1.635**		
Facebook-Web	Destination	26.578

IP	Port	Protocol	Status
1.9.91.17 - 1.9.91.18	80 443 8443	TCP	✅ Enabled
1.9.91.17 - 1.9.91.18	443	UDP	✅ Enabled
1.9.91.30	443	UDP	✅ Enabled

Firewall Policies

ID	From	To	Source	Destination	Shedule	Service	Action	NAT
3	port3	port1	LOCAL_CLIENT	facebook.com	always	ULL_UDP	✔ ACCEPT	✅ Enabled
1	port1	port3	facebook.com	LOCAL_CLIENT	always	ULL_UDP	✔ ACCEPT	✅ Enabled
4	port4	port1	LOCAL_CLIENT	all	always	HTTP DNS HTTPS	✔ ACCEPT	✅ Enabled
5	port3	port1	LOCAL_CLIENT	Facebook-Web	always	Internet Service	✔ ACCEPT	✅ Enabled
2	port3	port1	all	all	always	ALL	✔ ACCEPT	✅ Enabled

Exhibit A | **Exhibit B**

Policy Lookup

Incoming Interface	![] port3 ▼
IP Version	IPv4 ▼
Protocol	TCP ▼
Source	10.0.1.10
Source Port	Optional (1-65535) ⌄
Destination	facebook.com
Destination Port	443 ⌄

[Search]   [Close]

Which policy will be highlighted, based on the input criteria?

A. Policy with ID 4.
B. Policy with ID 5.
C. Policies with ID 2 and 3.
D. Policy with ID 4.

Answer: A

NEW QUESTION 8
Refer to the exhibit.

Network Diagram
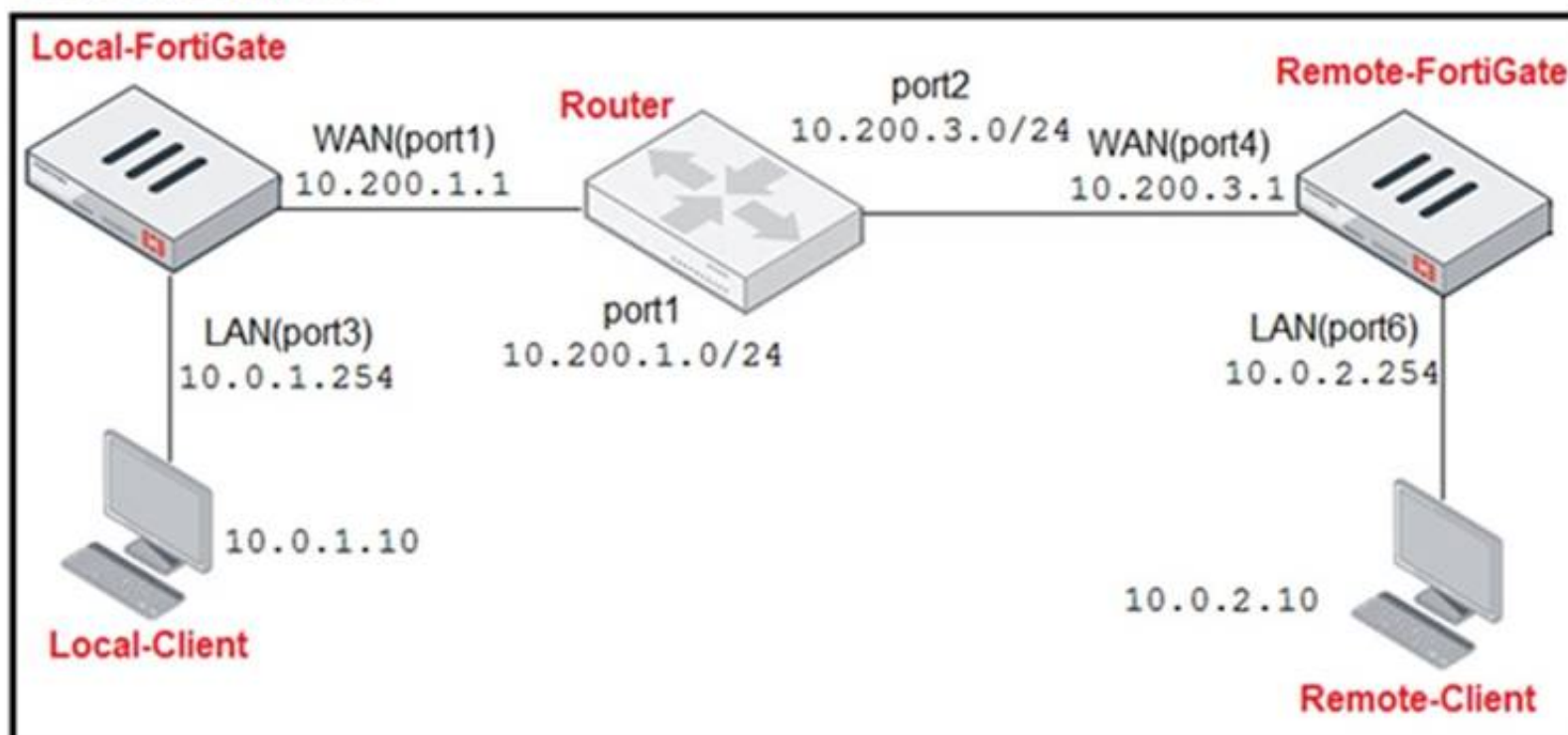
Central SNAT Policies Local-FortiGate

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 9
Refer to the exhibit.

```
FGT1 # get router info routing-table database
Codes:  K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        > - selected route, * - FIB route, p - stale info

S       *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
        *>           [10/0] via 10.0.0.2, port2, [30/0]
S          0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C       *> 10.0.0.0/24 is directly connected, port2
S          172.13.24.0/24 [10.0] is directly connected, port4
C       *> 172.20.121.0/24 is directly connected, port1
S       *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C       *> 192.168.15.0/24 is directly connected, port3
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

A. The port3 default route has the highest distance.
B. The port3 default route has the lowest metric.
C. There will be eight routes active in the routing table.
D. The port1 and port2 default routes are active in the routing table.

Answer: AD

NEW QUESTION 10
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 10
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

NEW QUESTION 14
FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.
Which two syntaxes are correct to configure web rating for the home page? (Choose two.)

A. www.example.com:443
B. www.example.com
C. example.com
D. www.example.com/index.html

Answer: BC

Explanation:
When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names - no URLs or wildcard characters are allowed.
OK: google.com or www.google.com
NO OK: www.google.com/index.html or google.* FortiGate_Security_6.4 page 384
When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names-- "no URLs or wildcard characters are allowed".

NEW QUESTION 15
An administrator needs to increase network bandwidth and provide redundancy.
What interface type must the administrator select to bind multiple FortiGate interfaces?

A. VLAN interface
B. Software Switch interface
C. Aggregate interface
D. Redundant interface

Answer: C

NEW QUESTION 18
A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.
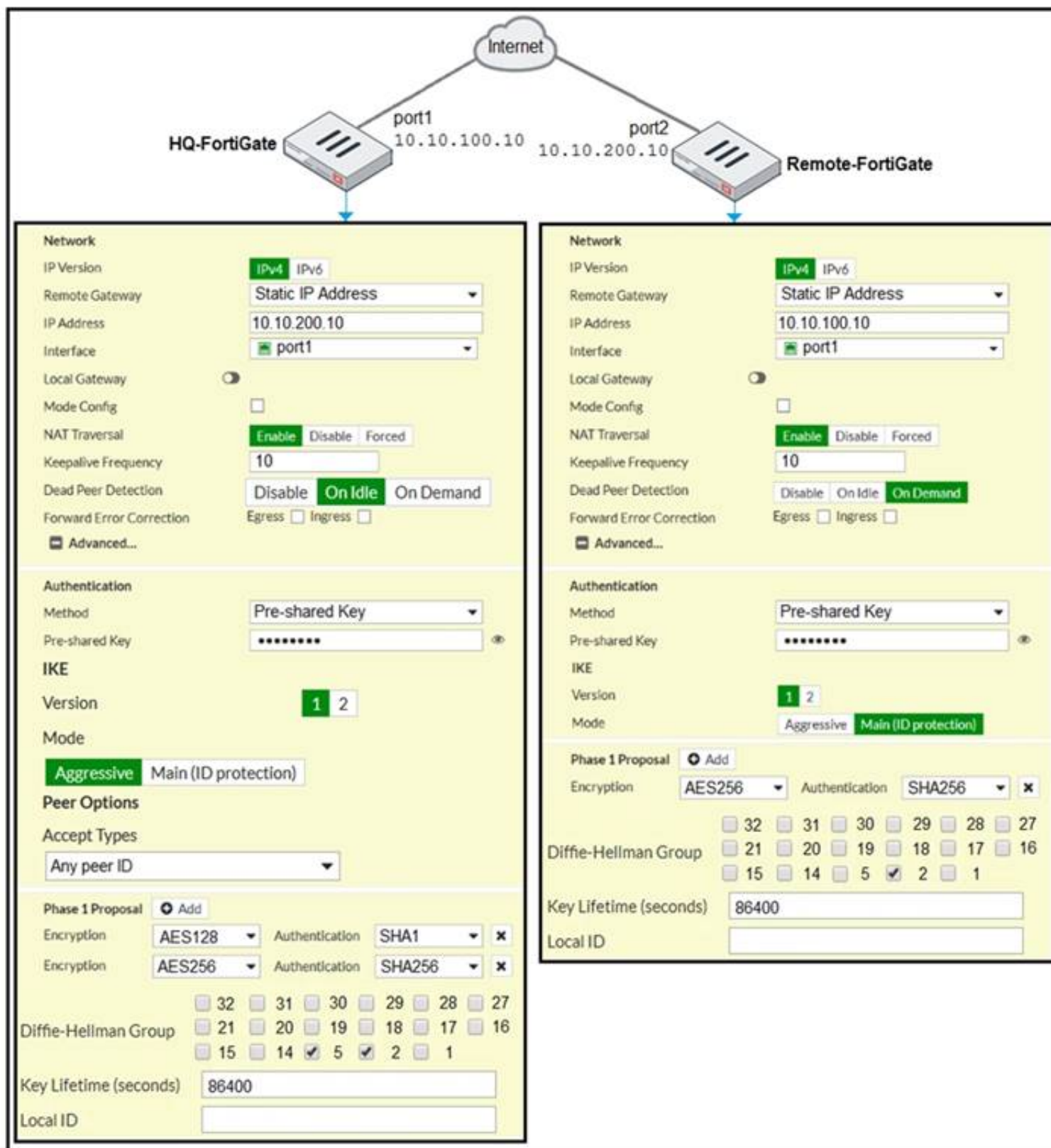
Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

A. On HQ-FortiGate, set IKE mode to Main (ID protection).
B. On both FortiGate devices, set Dead Peer Detection to On Demand.
C. On HQ-FortiGate, disable Diffie-Helman group 2.
D. On Remote-FortiGate, set port2 as Interface.

Answer: AD

NEW QUESTION 23
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 24
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE4_FGT-7.2 Practice Exam Features:

* NSE4_FGT-7.2 Questions and Answers Updated Frequently

* NSE4_FGT-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE4_FGT-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE4_FGT-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4_FGT-7.2 Practice Test Here](#)