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
Refer to the exhibits.
Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.
The WAN (port1) interface has the IP address 10.200.1.1/24.
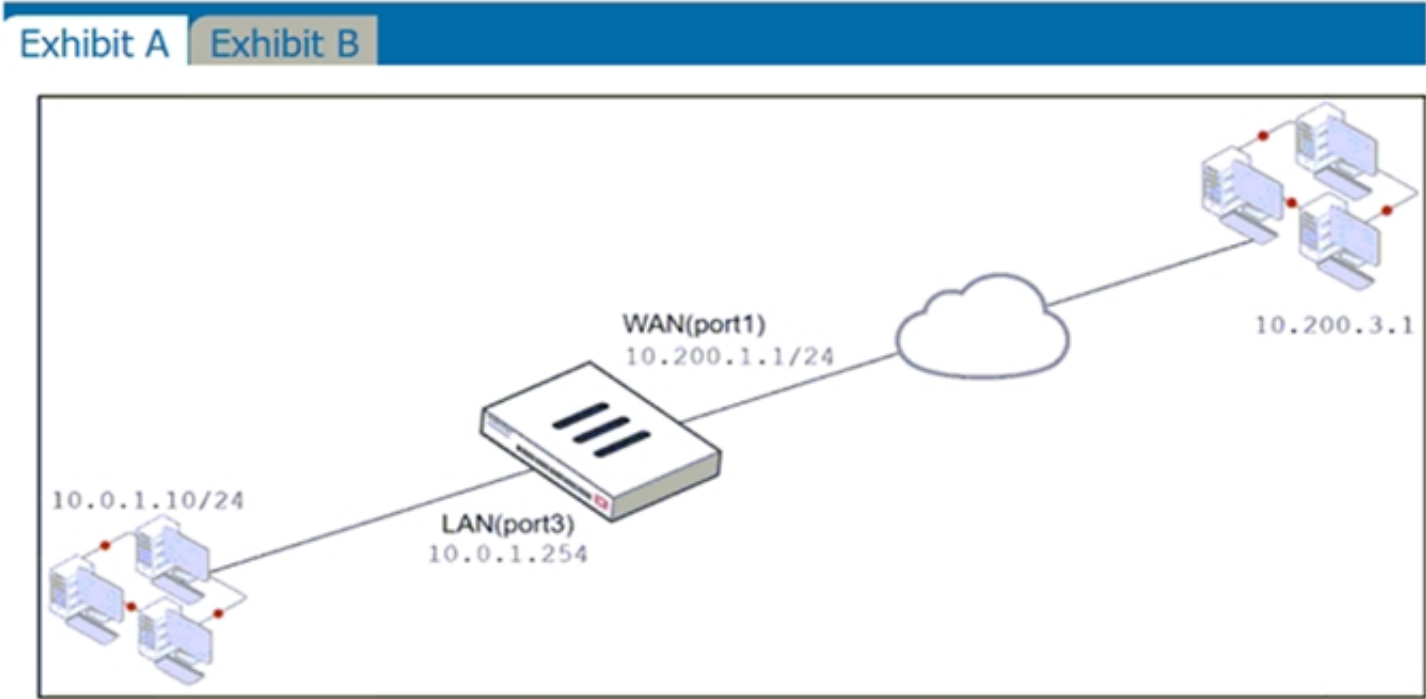The LAN (port3) interface has the IP address 10.0.1.254/24.

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

A. 10.0.1.254, 10.0.1.10, and 443, respectively
B. 10.0.1.254, 10.0.1.10, and 10443, respectively
C. 10.200.3.1, 10.0.1.10, and 443, respectively

Answer: C

NEW QUESTION 3
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 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
Which three statements explain a flow-based antivirus profile? (Choose three.)

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

Answer: ADE

NEW QUESTION 6
Which two statements are true about the FGCP protocol? (Choose two.)

A. FGCP elects the primary FortiGate device.
B. FGCP is not used when FortiGate is in transparent mode.
C. FGCP runs only over the heartbeat links.
D. FGCP is used to discover FortiGate devices in different HA groups.

Answer: AD

NEW QUESTION 7
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 8
FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.
In this scenario, what are two requirements for the VLAN ID? (Choose two.)

A. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.
B. The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs.

C. The two VLAN subinterfaces must have different VLAN IDs.
D. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

Answer: CD

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 exhibit.

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

A. The signature setting uses a custom rating threshold.
B. The signature setting includes a group of other signatures.
C. Traffic matching the signature will be allowed and logged.
D. Traffic matching the signature will be silently dropped and logged.

Answer: D

Explanation:
Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

NEW QUESTION 10
Which of the following statements about central NAT are true? (Choose two.)

A. IP tool references must be removed from existing firewall policies before enabling central NAT .
B. Central NAT can be enabled or disabled from the CLI only.
C. Source NAT, using central NAT, requires at least one central SNAT policy.
D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

Answer: AB

NEW QUESTION 15
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.
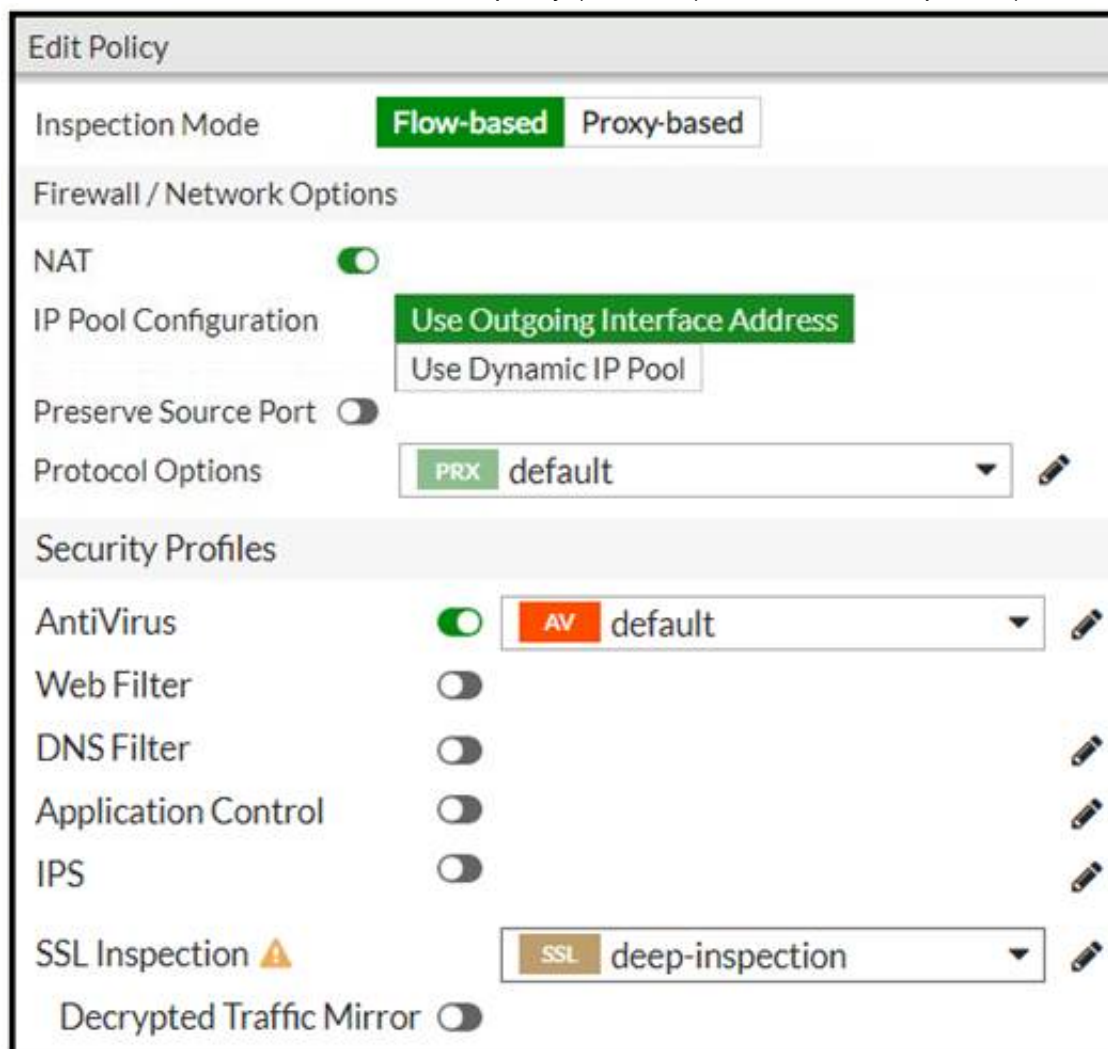

Based on the phase 2 configuration shown in the exhibit, which configuration change will bring phase 2 up?

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

Answer: B

NEW QUESTION 19
Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Edit AntiVirus Profile

Name	default
Comments	Scan files and block viruses. 29/255
Detect Viruses	**Block** Monitor
Feature set	**Flow-based** Proxy-based

Inspected Protocols

HTTP ⬤

SMTP ⬤

POP3 ⬤

IMAP ⬤

FTP ⬤

CIFS ◯

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ⬤

Include Mobile Malware Protection ⬤

Virus Outbreak Prevention ⓘ

Use FortiGuard Outbreak Prevention Database ◯

Use External Malware Block List ⓘ ⚠ ◯

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 24
Refer to the exhibits.
Exhibit A shows a topology for a FortiGate HA cluster that performs proxy-based inspection on traffic. Exhibit B shows the HA configuration and the partial output of the get system ha status command.

Exhibit A | Exhibit B
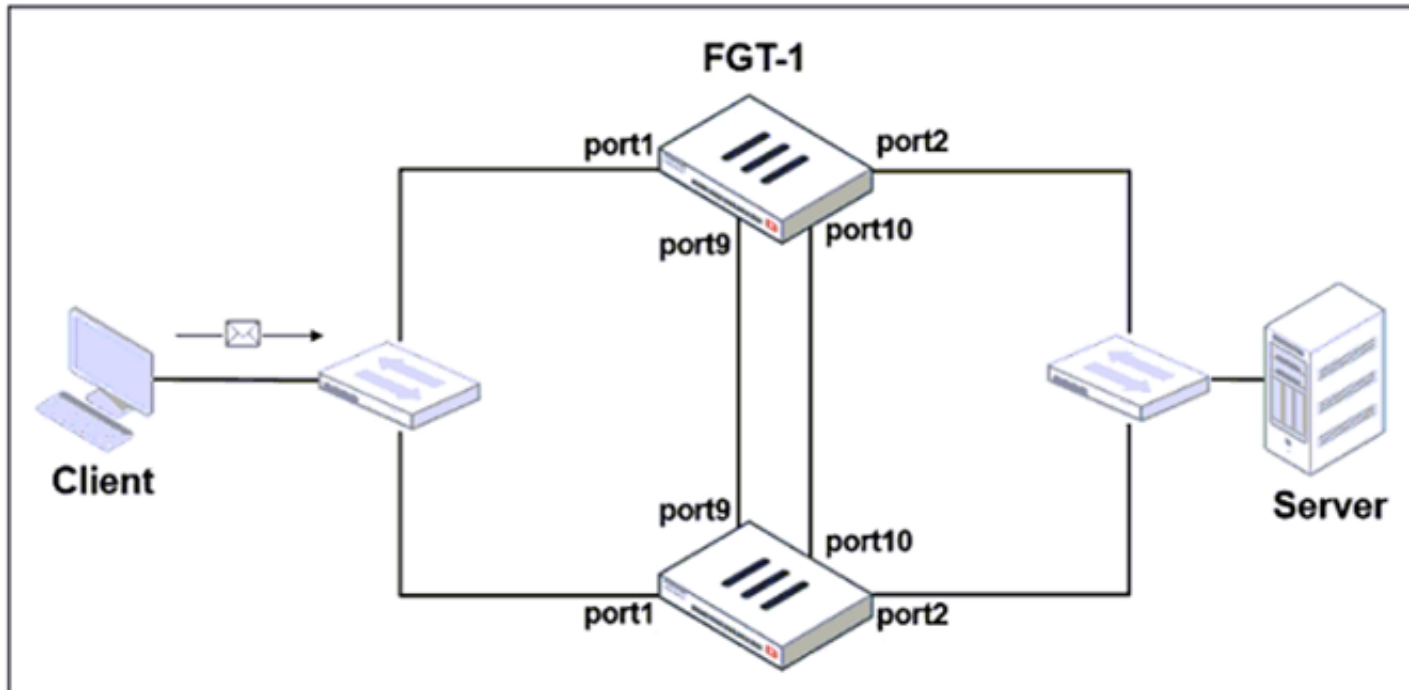

Exhibit A | Exhibit B

```
        set group-id 3
        set group-name "NSE"
        set mode a-a
        set password *
        set hbdev "port9" 50 "port10" 50
        set session-pickup enable
        set override disable
        set monitor port3
    end

    # get system ha status
    ...
    Primary    : FGT-2, FGVM010000065036, HA cluster index = 1
    Secondary  : FGT-1, FGVM010000064692, HA cluster index = 0
    number of vcluster: 1
    vcluster 1: work 169.254.0.2
    Primary: FGVM010000065036, HA operating index = 1
    Secondary: FGVM010000064692, HA operating index = 0
```

Based on the exhibits, which two statements about the traffic passing through the cluster are true? (Choose two.)

A. For non-load balanced connections, packets forwarded by the cluster to the server contain the virtual MAC address of port2 as source.
B. The traffic sourced from the client and destined to the server is sent to FGT-1.
C. The cluster can load balance ICMP connections to the secondary.
D. For load balanced connections, the primary encapsulates TCP SYN packets before forwarding them to the secondary.

Answer: AB

NEW QUESTION 29
Refer to the exhibit.

```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

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

NEW QUESTION 30
An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings. What is true about the DNS connection to a FortiGuard server?

A. It uses UDP 8888.
B. It uses UDP 53.
C. It uses DNS over HTTPS.
D. It uses DNS overTLS.

Answer: B

NEW QUESTION 35
You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk . What is the default behavior when the local disk is full?

A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of 95%.
B. No new log is recorded until you manually clear logs from the local disk .
C. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of 75%.
D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of 95%.

Answer: C

NEW QUESTION 40
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 44
Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

A. FortiCache
B. FortiSIEM
C. FortiAnalyzer
D. FortiSandbox
E. FortiCloud

Answer: BCE

NEW QUESTION 49
What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

A. It limits the scope of application control to the browser-based technology category only.
B. It limits the scope of application control to scan application traffic based on application category only.
C. It limits the scope of application control to scan application traffic using parent signatures only
D. It limits the scope of application control to scan application traffic on DNS protocol only.
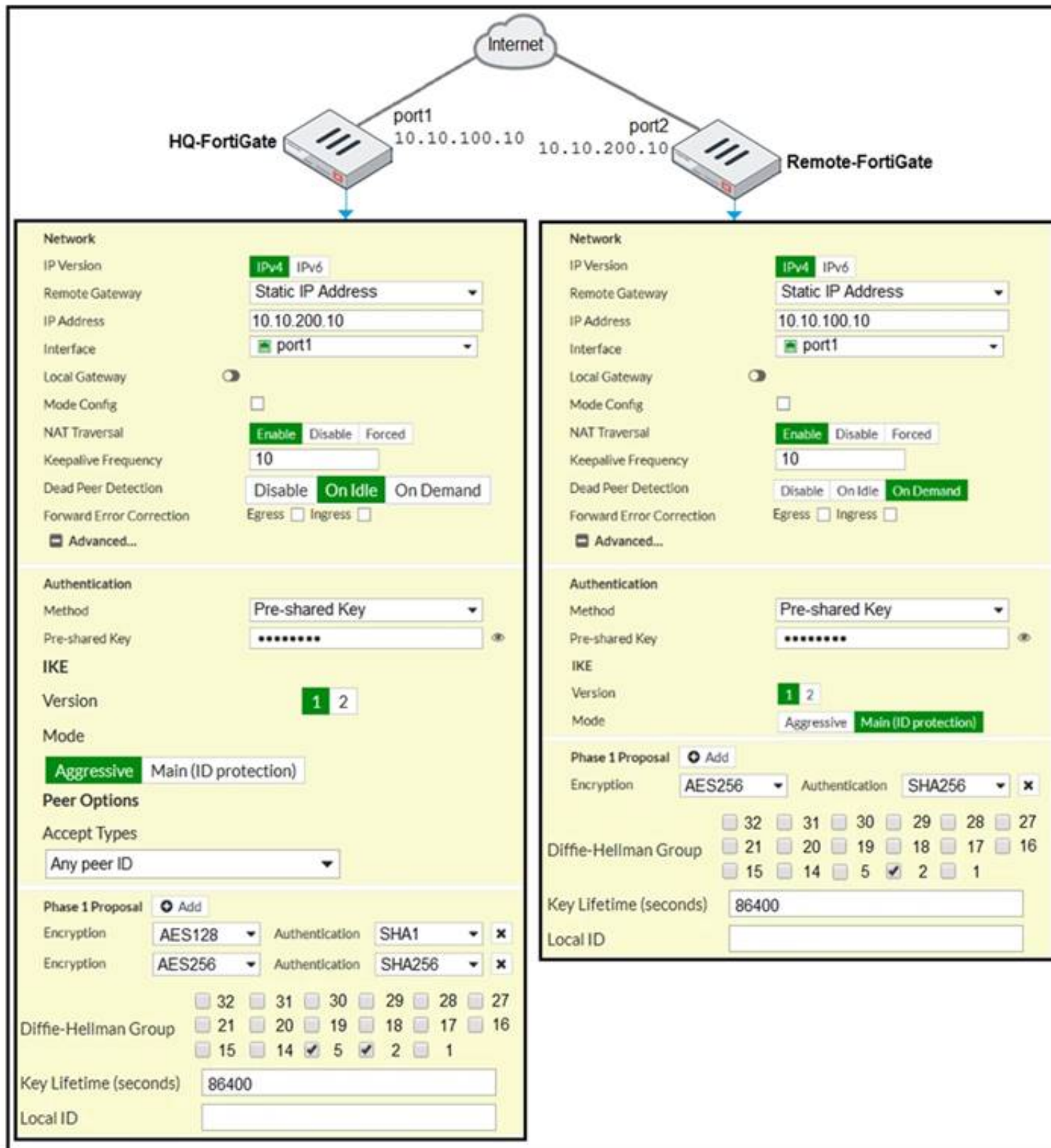
Answer: B

NEW QUESTION 51
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

NEW QUESTION 55
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 56
......

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](#)