Free Questions for FCP_FGT_AD-7.4 by certsinside

Shared by Strickland on 02-09-2024

For More Free Questions and Preparation Resources

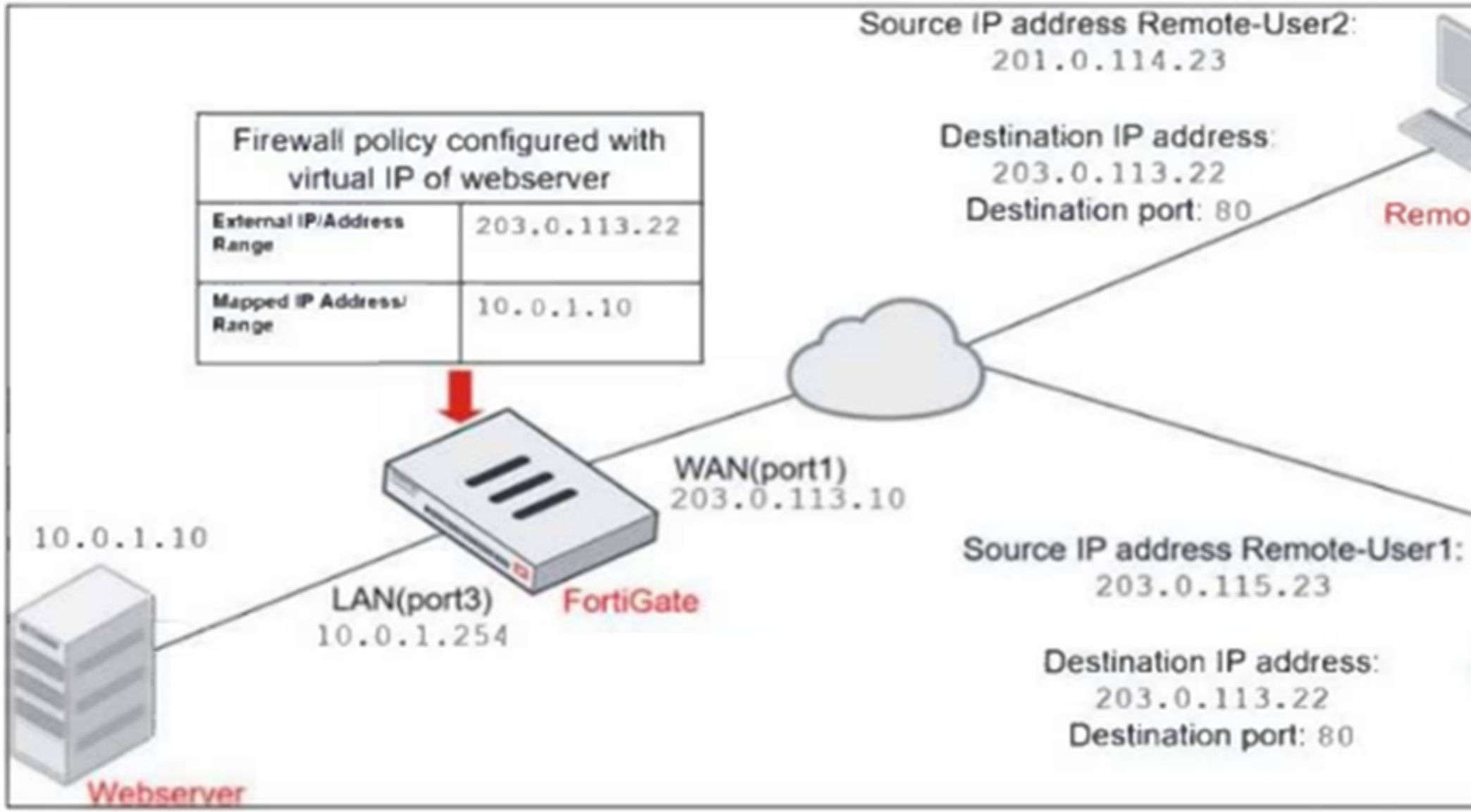
Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibits.

Network diagram



Firewall address object

Firewall policies

ID	Name	Source	Destination	Schedule	Service
WAN (port1) → LAN (port3) 2					
4	Deny	Deny_IP	all	always	ALL
3	Allow_access	all	Webserver	always	ALL

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2.

The policy should work such that Remote-User1 must be able to access the Webserver while preventing Remote-User2 from accessing the Webserver.

Which two configuration changes can the administrator make to the policy to deny Webserver access for Remote-User2? (Choose two.)

Options:

A- Enable match-vip in the Deny policy.

B- Set the Destination address as Webserver in the Deny policy.

C- Disable match-vip in the Deny policy.

D- Set the Destination address as Deny_IP in the Allow_access policy.

Answer:

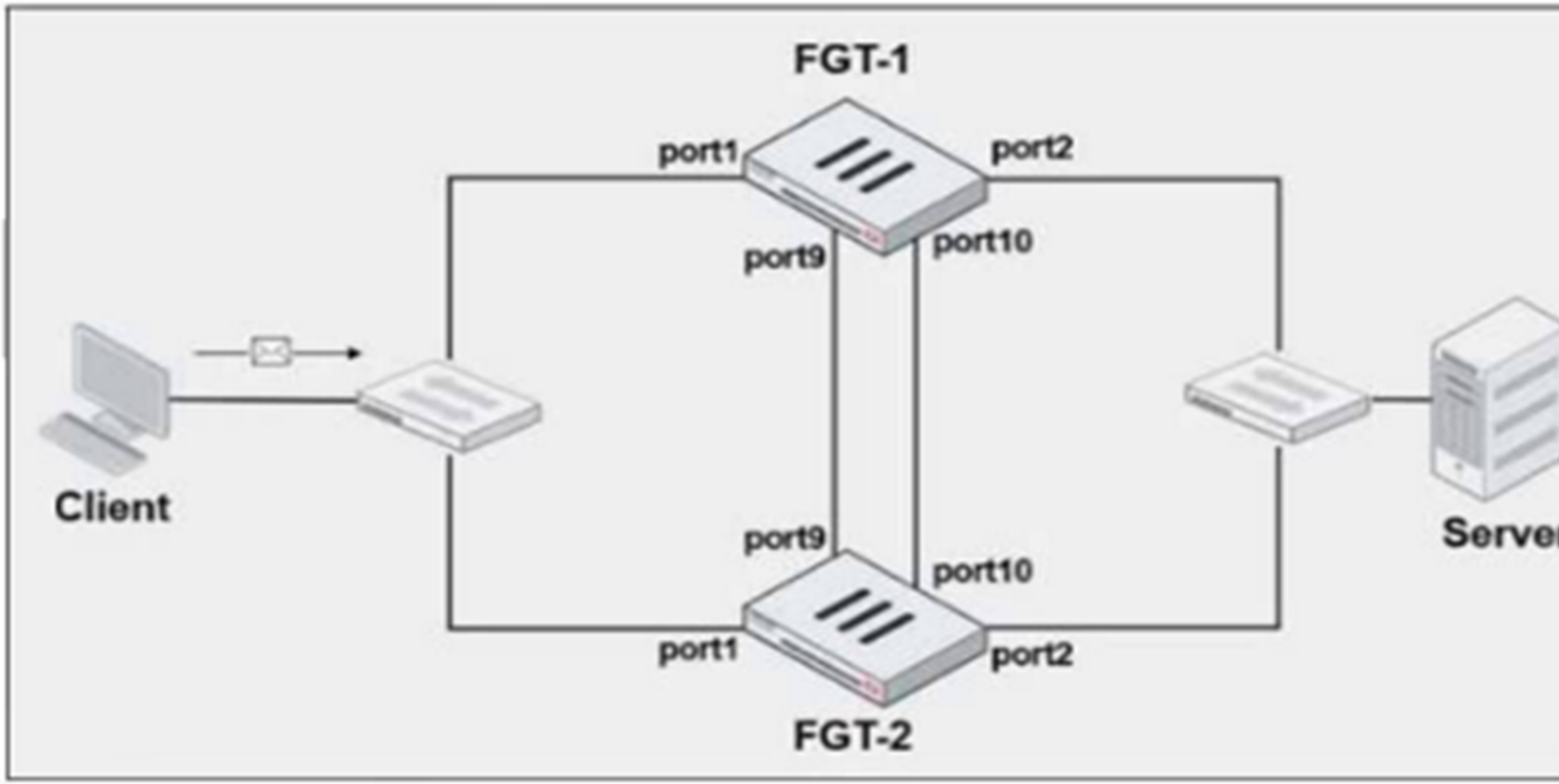
A, B

Question 2

Question Type: MultipleChoice

Refer to the exhibits.

FortiGate HA cluster topology



Current HA status

```
# get system ha status
...
Configuration Status:
    FGVM010000064692(updated 4 seconds ago): in-sync
    FGVM010000064692 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
    FGVM010000065036(updated 4 seconds ago): in-sync
    FGVM010000065036 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
...
Primary      : FGT-1, FGVM010000064692, HA cluster index = 1
Secondary    : FGT-2, FGVM010000065036, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1
```

New FortiGate HA configuration

```
FGT-1
#config system ha
    set group-id 3
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port9" 50 "port10" 50
    set session-pickup enable
    set override disable
    set priority 90
    set monitor port3

FGT-2
#config system ha
    set group-id 3
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port9" 50 "port10" 50
    set session-pickup enable
    set override enable
    set priority 110
    set monitor port3
```

FGT-1 and FGT-2 are updated with HA configuration commands shown in the exhibit.

What would be the expected outcome in the HA cluster?

Options:

A- FGT-1 will remain the primary because FGT-2 has lower priority.

B- FGT-2 will take over as the primary because it has the override enable setting and higher priority than FGT-1.

C- FGT-1 will synchronize the override disable setting with FGT-2.

D- The HA cluster will become out of sync because the override setting must match on all HA members.

Answer:

B

Question 3

Question Type: MultipleChoice

Refer to the exhibits, which show the firewall policy and an antivirus profile configuration.


Edit Antivirus Profile
Name
default
Comments
Scan files and block viruses.
29/255
AntiVirus scan
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
Send files to FortiSandbox for inspection
Send files to FortiNDR for inspection

Why is the user unable to receive a block replacement message when downloading an infected file for the first time?

Options:

A- The intrusion prevention security profile must be enabled when using flow-based inspection mode.

B- The option to send files to FortiSandbox for inspection is enabled.

C- The firewall policy performs a full content inspection on the file.

D- Flow-based inspection is used, which resets the last packet to the user.

Answer:

D

Question 4

Question Type: MultipleChoice

An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings.

What is true about the DNS connection to a FortiGuard server?

Options:

A- It uses UDP 8888.

B- It uses DNS over HTTPS.

C- It uses DNS over TLS.

D- It uses UDP 53.

Answer:

C

Question 5

Question Type: **MultipleChoice**

What are two features of collector agent advanced mode? (Choose two.)

Options:

A- In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.

B- Advanced mode supports nested or inherited groups.

C- In advanced mode, security profiles can be applied only to user groups, not individual users.

D- Advanced mode uses the Windows convention ---NetBios: Domain\Username.

Answer:

A, B

Question 6

Question Type: MultipleChoice

Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two.)

Options:

A- If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.

B- If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.

C- If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP

D- If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.

Answer:

B, C

Question 7

Question Type: MultipleChoice

Which three methods are used by the collector agent for AD polling? (Choose three.)

Options:

A- WinSecLog

B- WMI

C- NetAPI

D- FSSO REST API

E- FortiGate polling

Answer:

C, D, E

Question 8

Question Type: MultipleChoice

Refer to the exhibit.

FortiGate is configured for firewall authentication. When attempting to access an external website, the user is not presented with a login prompt.

What is the most likely reason for this situation?

Options:

A- The Service DNS is required in the firewall policy.

B- The user is using an incorrect user name.

C- The Remote-users group is not added to the Destination.

D- No matching user account exists for this user.

Answer:

B

Question 9

Question Type: MultipleChoice

A network administrator has configured an SSL/SSH inspection profile defined for full SSL inspection and set with a private CA certificate. The firewall policy that allows the traffic uses this profile for SSL inspection and performs web filtering. When visiting any HTTPS websites, the browser reports certificate warning errors.

What is the reason for the certificate warning errors?

Options:

A- The SSL cipher compliance option is not enabled on the SSL inspection profile. This setting is required when the SSL inspection profile is defined with a private CA certificate.

B- The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.

C- The browser does not recognize the certificate in use as signed by a trusted CA.

D- With full SSL inspection it is not possible to avoid certificate warning errors at the browser level.

Answer:

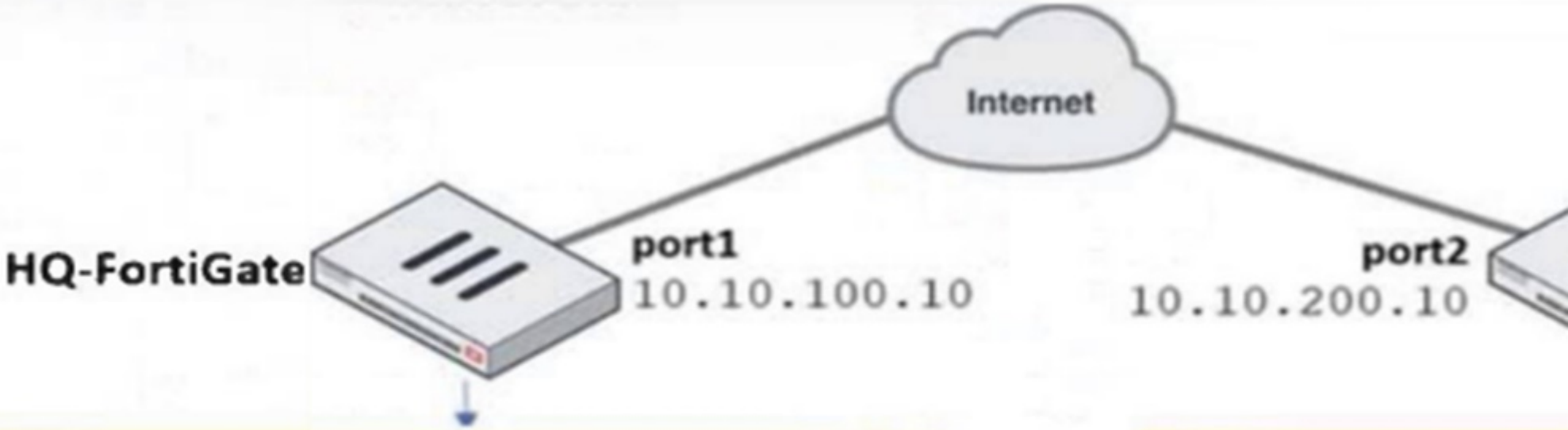
C

Question 10

Question Type: **MultipleChoice**

Refer to the exhibit.

IPsec tunnel configuration



Network

IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	10.10.200.10
Interface	port1
Local Gateway	
Mode Config	
NAT Traversal	Enable / Disable / Forced
Keepalive Frequency	10
Dead Peer Detection	Disable / On Idle / On Demand
DPD retry count	3
DPD retry interval	20 s
Forward Error Correction	Egress / Ingress

Network

IP Version	
Remote Gateway	
IP Address	
Interface	
Local Gateway	
Mode Config	
NAT Traversal	
Keepalive Frequency	
Dead Peer Detection	
DPD retry count	
DPD retry interval	

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 failed 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 can the administrator make to bring phase 1 up? (Choose two.)

Options:

A- On HQ-FortiGate, disable Diffie-Helman group 2.

B- On Remote-FortiGate, set port2 as Interface.

C- On both FortiGate devices, set Dead Peer Detection to On Demand.

D- On HQ-FortiGate, set IKE mode to Main (ID protection).

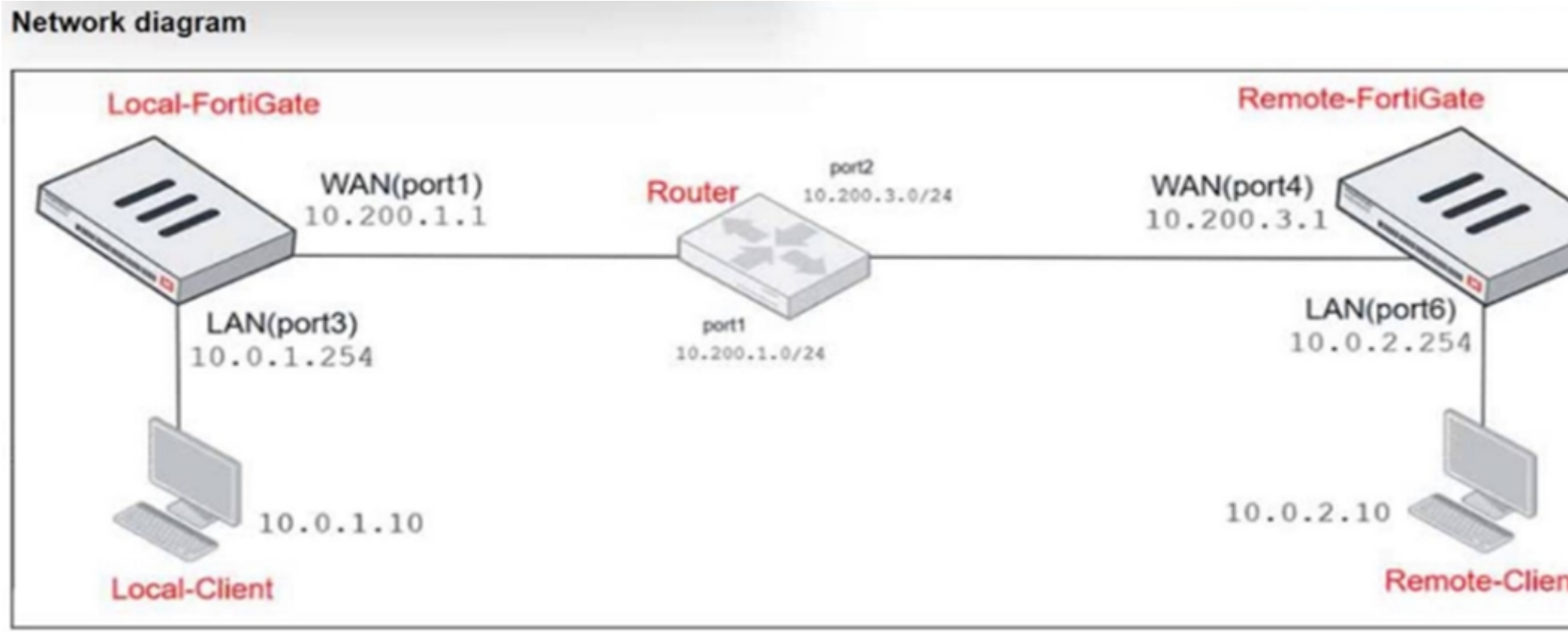
Answer:

B, D

Question 11

Question Type: MultipleChoice

Refer to the exhibits.



NAT IP pool configuration

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

Firewall policy

ID	Name	Source	Destination	Schedule	Service	Actio
LAN (port3) → WAN (port1)						
2	TCP traffic	all	REMOTE_FORTIGATE	always	ALL_TCP	ACC
6	PING traffic	all	all	always	PING	ACC
7	IGMP traffic	all	all	always	IGMP	ACC

The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects.

The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IPaddress 10.0.1.254/24.

Which IP address will be used to source NAT (SNAT) the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

Options:

A- 10.200.1.1

B- 10.200.1.149

C- 10.200.1.99

D- 10.200.1.49

Answer:

D

Question 12

Question Type: MultipleChoice

Refer to the exhibit, which shows a partial configuration from the remote authentication server.

Attribute	Value	Vendor	Actions
Fortinet-Group-Name	Training	Fortinet	

Why does the FortiGate administrator need this configuration?

Options:

A- To authenticate only the Training user group.

B- To set up a RADIUS server Secret

C- To authenticate and match the Training OU on the RADIUS server.

D- To authenticate Any FortiGate user groups.

Answer:

C