

Fortinet

Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator



NEW QUESTION 1
 Refer to the exhibit.

FortiGate SD-WAN zone configuration



An SD-WAN zone configuration on the FortiGate GUI is shown. Based on the exhibit, which statement is true?

- A. The Underlay zone contains no member.
- B. The virtual-wan-link and overlay zones can be deleted
- C. The Underlay zone is the zone by default.
- D. port2 and port3 are not assigned to a zone.

Answer: A

NEW QUESTION 2

There are multiple dialup IPsec VPNs configured in aggressive mode on the HQ FortiGate. The requirement is to connect dial-up users to their respective department VPN tunnels.

Which phase 1 setting you can configure to match the user to the tunnel?

- A. Local Gateway
- B. Dead Peer Detection
- C. Peer ID
- D. IKE Mode Config

Answer: C

NEW QUESTION 3

Which two statements describe characteristics of automation stitches? (Choose two answers)

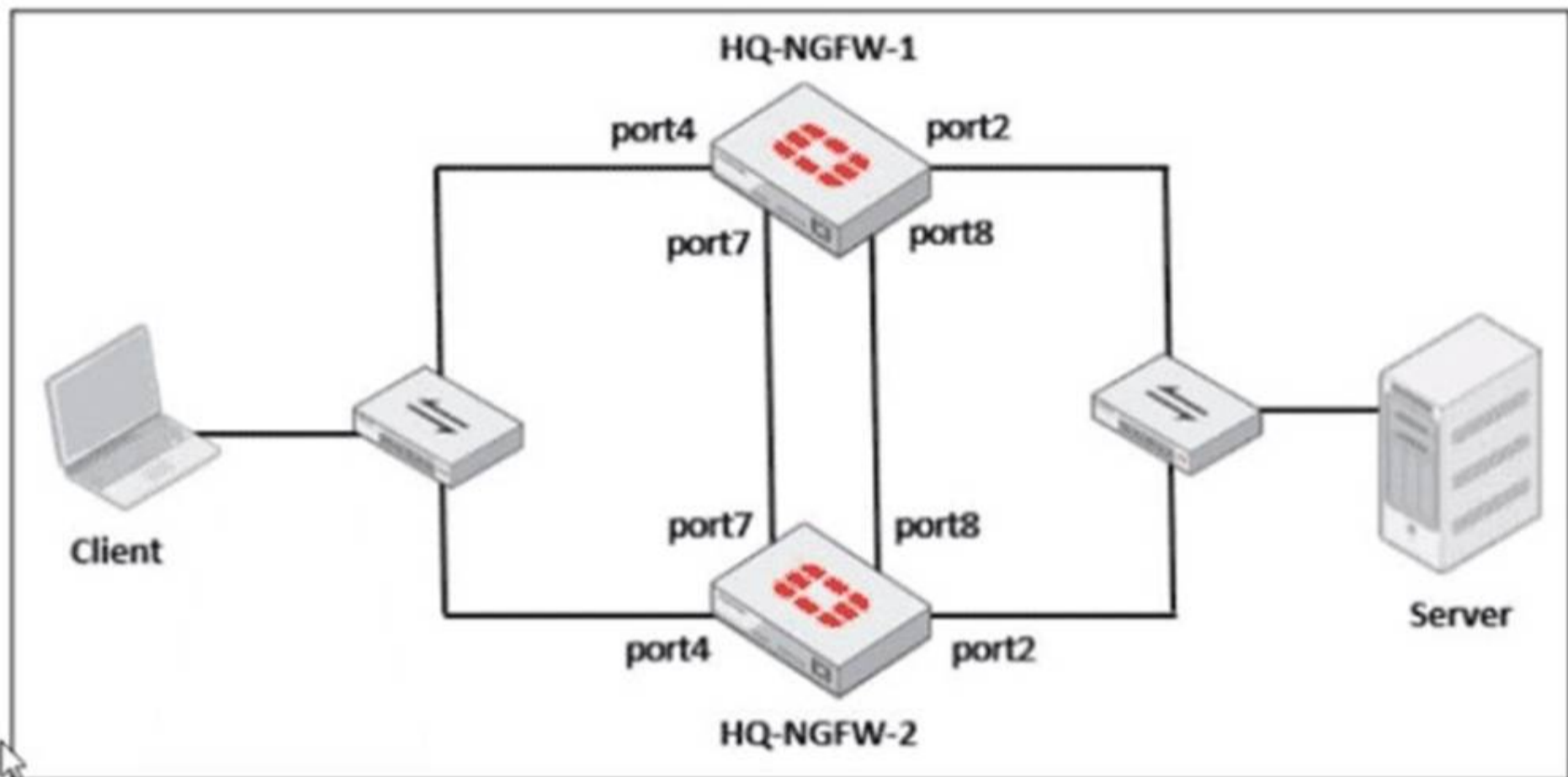
- A. Actions involve only devices included in the Security Fabric.
- B. An automation stitch can have multiple triggers.
- C. Multiple actions can run in parallel.
- D. Triggers can involve external connectors.

Answer: CD

NEW QUESTION 4

Refer to the exhibits.

FortiGate HA cluster topology



Current HA status

```
HQ-NGFW-1 # get system ha status
...
Configuration Status:
  FGVM02TM24013423(updated 0 seconds ago): in-sync
  FGVM02TM24013423 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
  FGVM02TM24013501(updated 4 seconds ago): in-sync
  FGVM02TM24013501 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
...
number of member: 2
HQ-NGFW-1      , FGVM02TM24013423, HA cluster index = 1
HQ-NGFW-2      , FGVM02TM24013501, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM02TM24013423, HA operating index = 0
Secondary: FGVM02TM24013501, HA operating index = 1
```

New FortiGate HA configuration

```
HQ-NGFW-1
# config system ha
  set group-id 5
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port7" 50 "port8" 60
  set session-pick enable
  set override disable
  set priority 90
  set monitor "port3"

HQ-NGFW-2
# config system ha
  set group-id 5
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port7" 50 "port8" 60
  set session-pick enable
  set override enable
  set priority 110
  set monitor "port3"
```

Based on the current HA status, an administrator updates the override and priority parameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibits. What would be the expected outcome in the HA cluster?

- A. HQ-NGFW-2 will take over as the primary because it has the override enable setting and higher priority than HQ-NGFW-1.
- B. HQ-NGFW-1 will remain the primary because HQ-NGFW-2 has lower priority
- C. The HA cluster will become out of sync because the override setting must match on all HA members.
- D. HQ-NGFW-1 will synchronize the override disable setting with HQ-NGFW-2.

Answer: A

NEW QUESTION 5

Which two components are part of the secure internet access (SIA) agent-based mode on FortiSASE? (Choose two.)

- A. FortiSASE Firewall-as-a-Service (FWaaS)
- B. The proxy auto-configuration (PAC) file
- C. VPN policies
- D. FortiExtender

Answer: AC

NEW QUESTION 6

Refer to the exhibits.

Application sensor configuration

Edit Application Sensor

Categories

- All Categories
- Business (179, 6)
- Collaboration (293, 6)
- Game (124)
- Mobile (3)
- P2P (85)
- Remote.Access (91)
- Storage.Backup (296, 16)
- Video/Audio (206, 13)
- Web.Client (18)
- Cloud.IT (31)
- Email (87, 12)
- General.Interest (241, 9)
- Network.Service (332)
- Proxy (106)
- Social.Media (150, 31)
- Update (48)
- VoIP (31)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	Excessive-Bandwidth	Filter	Block
2	Apple	Filter	Monitor

Application override configuration

Edit Override

Type: Application **Filter**

Action: Block

Filter: Excessive-Bandwidth

FaceTime

Name	Category	Technology
Application Signature 1/1262		
FaceTime	VoIP	Client-Server

Filter override configuration

Edit Override

Type: Application **Filter**

Action: Monitor

Filter: Apple

FaceTime

Name	Category	Technology
Application Signature 1/33		
FaceTime	VoIP	Client-Server

The exhibits show the application sensor configuration and the Excessive-Bandwidth and Apple filter details. Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming? (Choose one answer)

- A. Apple FaceTime will be allowed, based on the Video/Audio category configuration.
- B. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.
- C. Apple FaceTime will be allowed, based on the Apple filter configuration.
- D. Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.

Answer: B

NEW QUESTION 7

Refer to the exhibits.

Application sensor

Edit Application Sensor

Categories

Mixed ▾ All Categories

Business (157, ☁ 6)

Collaboration (266, ☁ 13)

Game (83)

Mobile (3)

Operational Technology

Proxy (189)

Social Media (113, ☁ 29)

Update (48)

VoIP (23)

Unknown Applications

Cloud/IT (72, ☁ 12)

Email (76, ☁ 11)

General Interest (254, ☁ 15)

Network Service (338)

P2P (55)

Remote Access (96)

Storage/Backup (150, ☁ 20)

Video/Audio (148, ☁ 17)

Web Client (24)

Network Protocol Enforcement

Application and Filter Overrides

+ Create New
 Edit
 Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	<input checked="" type="checkbox"/> Block
2	VEND Google	Filter	<input checked="" type="checkbox"/> Monitor
2			

Firewall policy

Edit Policy

Firewall/Network Options

Inspection mode: Flow-based Proxy-based

NAT:

IP pool configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Preserve source port:

Protocol options: PROT default

Security Profiles

AntiVirus:


Web filter:

DNS filter:

Application control: APP default

IPS:

File filter:

SSL inspection : SSL deep-inspection

Decrypted traffic mirror:

Logging Options

Log allowed traffic: Security events All sessions

You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. Which two factors can you observe from these configurations? (Choose two.)

- A. YouTube access is blocked based on Excessive-Bandwidth Application and Filter override settings.
- B. Facebook access is blocked based on the category filter settings.
- C. Facebook access is allowed but you cannot play Facebook videos based on Video/Audio category filter settings.
- D. YouTube search is allowed based on the Google Application and Filter override settings.

Answer: AB

NEW QUESTION 8

An administrator wanted to configure an IPS sensor to block traffic that triggers the signature set number of times during a specific time period. How can the administrator achieve the objective?

- A. Use IPS group signatures, set rate-mode 60.
- B. Use IPS packet logging option with periodical filter option.
- C. Use IPS signatures, rate-mode periodical option.
- D. Use IPS filter, rate-mode periodical option.

Answer: D

NEW QUESTION 9

An administrator wants to form an HA cluster using the FGCP protocol.
 Which two requirements must the administrator ensure both members fulfill? (Choose two.)

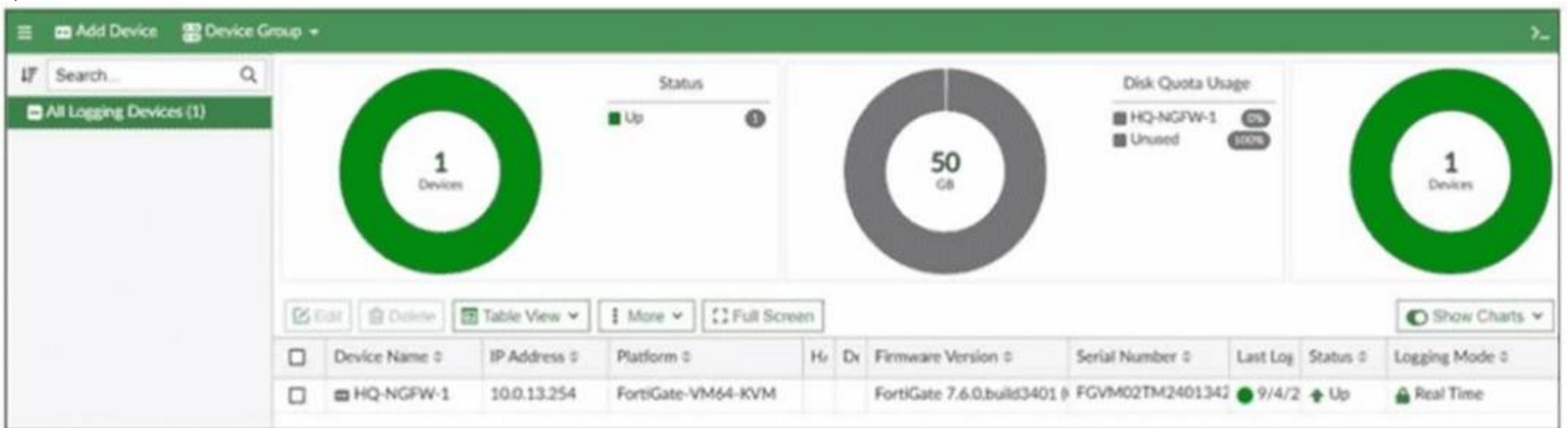
- A. They must have the same hard drive configuration.
- B. They must have the same number of configured VDOMs.
- C. They must have the heartbeat interfaces in the same subnet
- D. They must have the same HA group ID.

Answer: BD

NEW QUESTION 10

The FortiGate device HQ-NGFW-1 with the IP address 10.0.13.254 sends logs to the FortiAnalyzer device with the IP address 10.0.13.125. The administrator wants to verify that reliable logging is enabled on HQ-NGFW-1.
 Which exhibit helps with the verification?

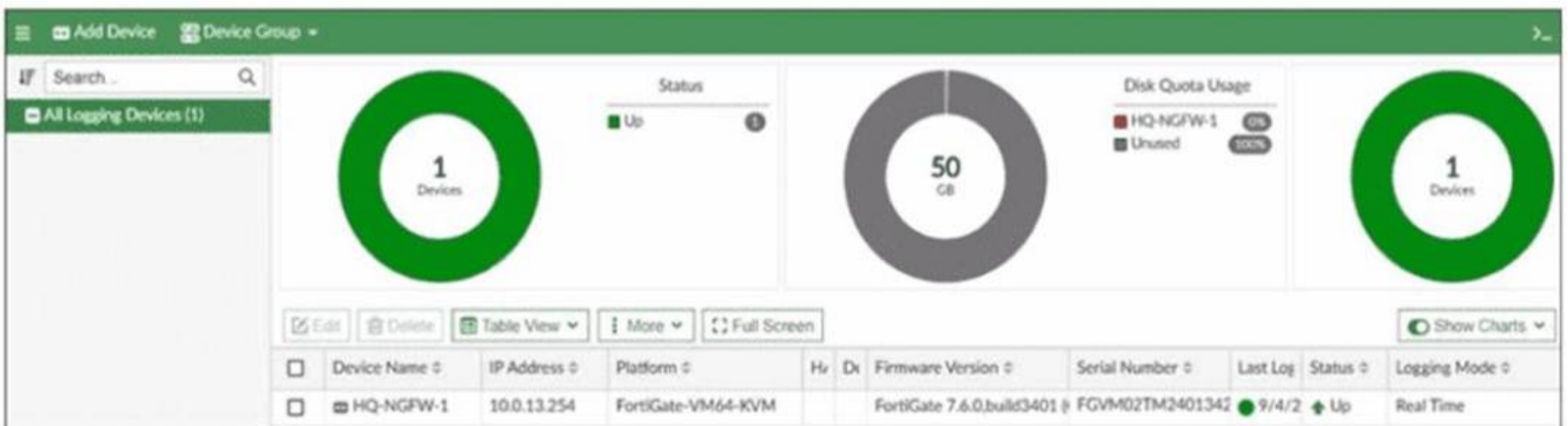
A)



B)

```
config log fortianalyzer setting
  set status enable
  set server "10.0.13.125"
  set serial "FAZ-VMTM24012176"
  set enc-algorithm high-medium
  set upload-option realtime
end
```

C)



D)

```
HQ-NGFW-1 # diagnose sniffer packet any "host 10.0.13.125" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.13.125]
2.173071 port6 out 10.0.13.254.14974 -> 10.0.13.125.514: udp 347
3.334638 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: psh 4017477514 ack 2638032500
3.335098 port6 in 10.0.13.125.514 -> 10.0.13.254.23054: psh 2638032500 ack 4017477548
3.335129 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: ack 2638032543
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 10

You have created a web filter profile named restrictmedia-profile with a daily category usage quota. When you are adding the profile to the firewall policy, the restrict_media-profile is not listed in the available web profile drop down. What could be the reason?

- A. The web filter profile is already referenced in another firewall policy.
- B. The firewall policy is in no-inspection mode instead of deep-inspection.
- C. The naming convention used in the web filter profile is restricting it in the firewall policy.
- D. The inspection mode in the firewall policy is not matching with web filter profile feature set.

Answer: D

NEW QUESTION 15

Refer to the exhibits.

Security Fabric logical topology view



Security Fabric settings on HQ-ISFW-2

Security Fabric Settings

Security Fabric role: Standalone | Serve as Fabric Root | **Join Existing Fabric**

Allow other Security Fabric devices to join: port6

Upstream FortiGate IP/FQDN: 10.0.13.254

Allow downstream device REST API access:

Management IP/FQDN: Use WAN IP **Specify**
 10.0.11.250

Management port: Use Admin Port **Specify**
 443

SAML SSO Settings

SAML Single Sign-On: **Auto** | Manual

Advanced Options

Mode: Pending

An administrator wants to add HQ-ISFW-2 in the Security Fabric. HQ-ISFW-2 is in the same subnet as HQ-ISFW. After configuring the Security Fabric settings on HQ-ISFW-2, the status stays Pending. What can be the two possible reasons? (Choose two answers)

- A. Upstream FortiGate IP must be set to 10.0.11.254.
- B. SAML Single Sign-On must be set to Manual.
- C. HQ-ISFW-2 must be authorized on HQ-ISFW.
- D. Management IP must be set to 10.0.13.254.

Answer: AC

NEW QUESTION 20

FortiGate is operating in NAT mode and has two physical interfaces connected to the LAN and DMZ networks respectively. Which two statements about the requirements of connected physical interfaces on FortiGate are true? (Choose two.)

- A. Both interfaces must have DHCP enabled and interfaces set to LAN and DMZ roles assigned.
- B. Both interfaces must have the interface role assigned.
- C. Both interfaces must have directly connected routes on the routing table.

D. Both interfaces must have IP addresses assigned.

Answer: CD

NEW QUESTION 21

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

- A. In advanced mode, security profiles can be applied only to user groups, not individual users.
- B. In advanced mod
- C. FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
- D. Advanced mode uses the Windows convention—NetBios: Domain\Username.
- E. Advanced mode supports nested or inherited groups.

Answer: BD

NEW QUESTION 26

Refer to the exhibit

A firewall policy to enable active authentication is shown.

Policy	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port4 → port2	Internet (1)	HQ_SUBNET Remote-users	always	ALL_ICMP HTTPS HTTP	ACCEPT	NAT	Standard	Category_Monitor certificate-inspection

When attempting to access an external website using an active authentication method, the user is not presented with a login prompt. What is the most likely reason for this situation?

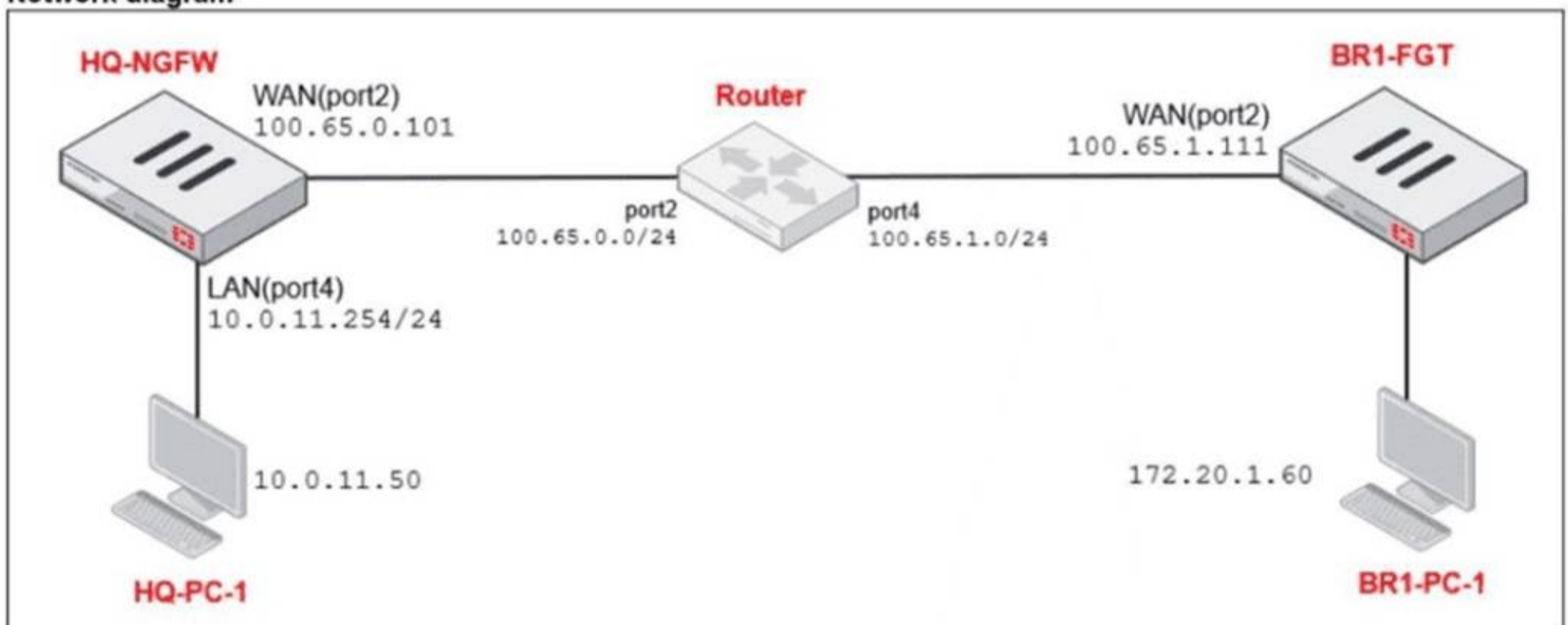
- A. No matching user account exists for this user.
- B. The Remote-users group must be set up correctly in the FSSO configuration.
- C. The Remote-users group is not added to the Destination
- D. The Service DNS is required in the firewall policy.

Answer: D

NEW QUESTION 30

Refer to the exhibits.

Network diagram



NAT IP pool configuration

Name	External IP Range	Type	ARP Reply
SNAT-Pool	100.65.0.49 - 100.65.0.49	Overload	Enabled
SNAT-Remote	100.65.0.149 - 100.65.0.149	Overload	Enabled
SNAT-Remote1	100.65.0.99 - 100.65.0.99	Overload	Enabled

Firewall policies

Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port4) → WAN (port2) 3							
TCP traffic (2)	all	BR1-FGT	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
PING traffic (3)	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
IGMP traffic (4)	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

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 (port2) interface has the IP address 100.65.0.101/24.

The LAN (port4) interface has the IP address 10.0.11.254/24.

Which IP address will be used to source NAT (SNAT) the traffic, if the user on HQ-PC-1 (10.0.11.50) pings the IP address of BR-FGT (100.65.1.111)?

- A. 100.65.0.101
- B. 100.65.0.49
- C. 100.65.0.149
- D. 100.65.0.99

Answer: D

NEW QUESTION 34

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

NSE4_FGT_AD-7.6 Practice Exam Features:

- * NSE4_FGT_AD-7.6 Questions and Answers Updated Frequently
- * NSE4_FGT_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4_FGT_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4_FGT_AD-7.6 Practice Test Here](#)