

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
Refer to the exhibit showing a debug flow output.

Debug Flow output

```
vd-root:0 received a packet(proto=1, 10.0.11.50:3->100.65.0.254:2048) tun_id=0.0.0.0 from port4. type=8,
code=0, id=3, seq=5.

allocate a new session-00000721

in-[port4], out-[]

len=0

result: skb_flags-02000000, vid-0, ret-no-match, act-accept, flag-00000000

find a route: flag=00000000 gw-0.0.0.0 via port2

in-[port4], out-[port2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0

gnum-100004, use addr/intf hash, len=3

checked gnum-100004 policy-2, ret-matched, act-accept

ret-matched

gnum-4e20, check-fffffffa002c9c7

checked gnum-4e20 policy-6, ret-no-match, act-accept

gnum-4e20 check result: ret-no-match, act-accept, flag-00000000, flag2-00000000

policy-2 is matched, act-drop

after iprobe_captive_check(): is_captive-0, ret-matched, act-drop, idx-2

Denied by forward policy check (policy 2)
```

Which two conclusions can you make from the debug flow output? (Choose two answers)

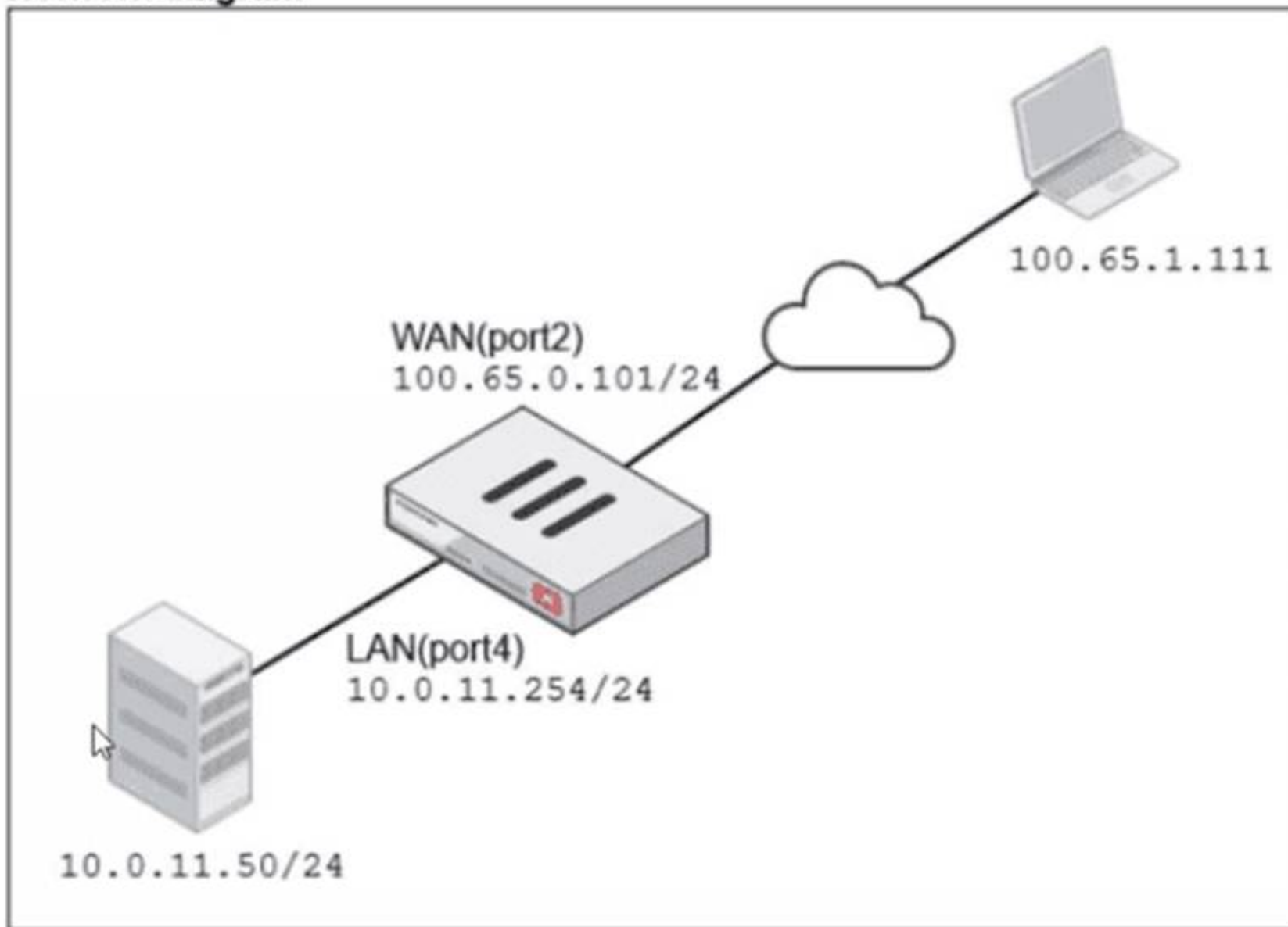
- A. The default gateway is configured on port2.
- B. The RPF check fails.
- C. The debug flow is for UDP traffic.
- D. The matching firewall policy denies the traffic.

Answer: AD

NEW QUESTION 3

Refer to the exhibits.

Network diagram



Name

VIP-WEB-SERVER

Comments

Write a comment...

0/255

Color

Change

Network

Interface

WAN (port2)

Type

Static NAT

External IP address/range ⓘ

100.65.0.200

Map to

IPv4 address/range

10.0.11.50

☐ Optional Filters

☒ Port Forwarding

Protocol

TCP

UDP

SCTP

ICMP

Port Mapping Type

One to one

Many to many

External service port ⓘ

443

Map to IPv4 port

4443

Firewall policies

A diagram of a FortiGate device connected to the network VIP object and firewall policy configurations are shown.

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.

If the host 100.65.1.111 sends a TCP SYN packet on port 443 to 100.65.0.200. what will the source address, destination address, and destination port of the packet be at the time FortiGate forwards the packet to the destination?

A. 10.0.11.254, 100.65.0.200. and 443, respectively

B. 10.0.11.254, 10.0.15.50, and 4443. respectively

C. 100.65.1. ill, 10.0.11.50, and 4443. respectively

D. 100.65.1.111, 10.0.11.50. and 443. respectively

Answer: C

NEW QUESTION 4

Refer to the exhibits.

System Performance output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-extreme 89
    set memory-use-threshold-green 82
    set memory-use-threshold-red 88
end
```

The system performance output and default configuration of high memory usage thresholds on a FortiGate device are shown. Based on the system performance output, what are the two possible outcomes? (Choose two.)

- A. Administrators can access FortiGate only through the console port.
- B. FortiGate has entered conserve mode.
- C. FortiGate drops new sessions.
- D. Administrators can change the configuration.

Answer: BD

NEW QUESTION 5

Refer to the exhibit.

```
HQ-NGFW-1 # diagnose test application ipsmonitor 1
pid = 2044, engine count = 0 (+1)
0 - pid:2074:2074 cfg:1 master:0 run:1
```

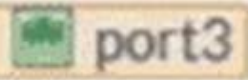
As an administrator you have created an IPS profile, but it is not performing as expected. While testing you got the output as shown in the exhibit What could be the possible reason of the diagnose output shown in the exhibit?

- A. There is a no firewall policy configured with an IPS security profile.
- B. Administrator entered the command diagnose test application ipsmonitor 5.
- C. FortiGate entered into IPS fail open state.
- D. Administrator entered the command diagnose test application ipsmonitor 99.

Answer: A

NEW QUESTION 6

Refer to the exhibit.

Destination ⇅	Gateway IP ⇅	Interface ⇅	Status ⇅
0.0.0.0/0	100.65.0.254	 port2	✓ Enabled
10.10.10.0/24	100.66.0.254	 port3	✓ Enabled
10.0.13.0/24	10.0.13.125	 port6	✓ Enabled

Based on the routing table shown in the exhibit, which two statements are true? (Choose two.)

- A. A packet with the source IP address 10.0.13.10 arriving on port2 is allowed if strict RPF is disabled.
- B. A packet with the source IP address 10.100.110.10 arriving on port2 is allowed if strict RPF is enabled.
- C. A packet with the source IP address 10.100.110.10 arriving on port3 is allowed if strict RPF is disabled.
- D. A packet with the source IP address 10.10.10.10 arriving on port2 is allowed if strict RPF is enabled.

Answer: AC

NEW QUESTION 7

Which three statements explain a flow-based antivirus profile? (Choose three answers)

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

Answer: ABD

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?

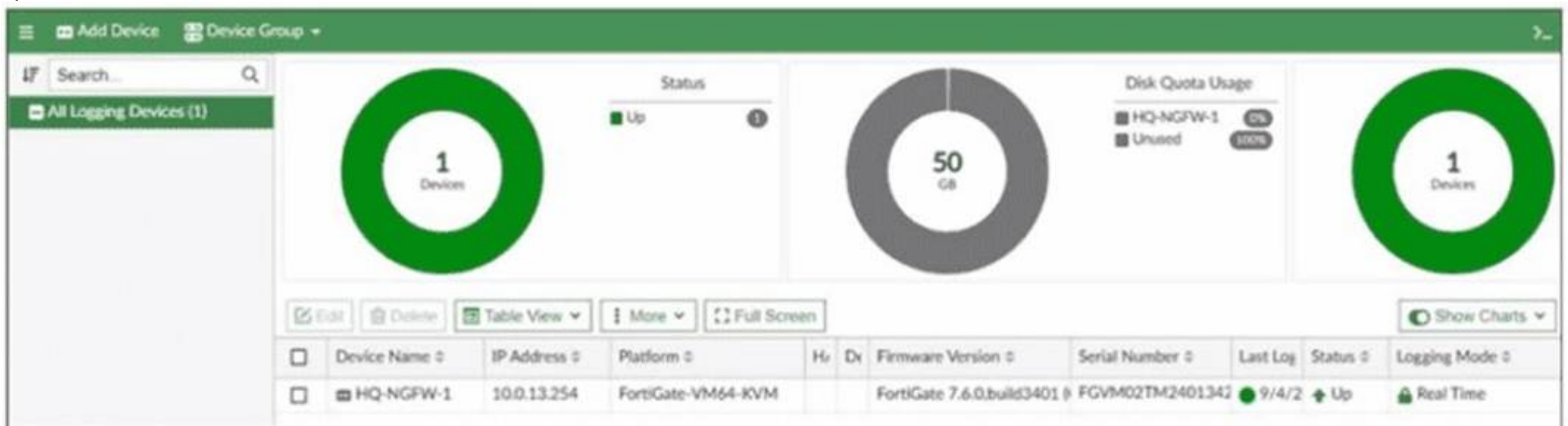
- A. Use IPS group signatures, set rate-mode 60.
- B. Use IPS packet logging option with periodical filter option.
- C. Use IPS signatures, rate-mode periodical option.
- D. Use IPS filter, rate-mode periodical option.

Answer: D

NEW QUESTION 9

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?

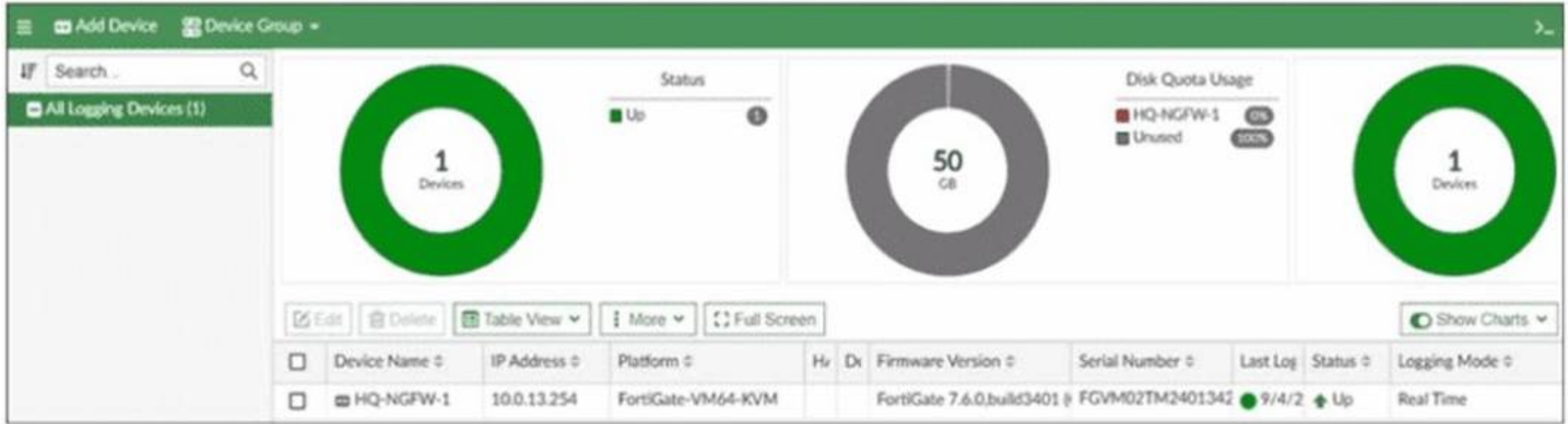
A)



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
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:

Allow downstream device REST API access: ☒

Management IP/FQDN: ☐ Use WAN IP ☒ Specify

Management port: ☐ Use Admin Port ☒ Specify

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 10

What are two characteristics of HA cluster heartbeat IP addresses in a FortiGate device? (Choose two.)

- A. Heartbeat IP addresses are used to distinguish between cluster members.
- B. The heartbeat interface of the primary device in the cluster is always assigned IP address 169.254.0.1.
- C. A change in the heartbeat IP address happens when a FortiGate device joins or leaves the cluster.
- D. Heartbeat interfaces have virtual IP addresses that are manually assigned.

Answer: AC

NEW QUESTION 13

When configuring firewall policies which of the following is true regarding the policy ID? (Choose two.)

- A. A firewall policy ID identifies the order of policy execution in firewall policies.
- B. A policy ID cannot be modified once a policy is created.
- C. You can create a policy in CLI with policy ID 0
- D. It is mandatory to provide a policy ID while creating a firewall policy regardless of GUI or CLI.

Answer: BC

NEW QUESTION 16

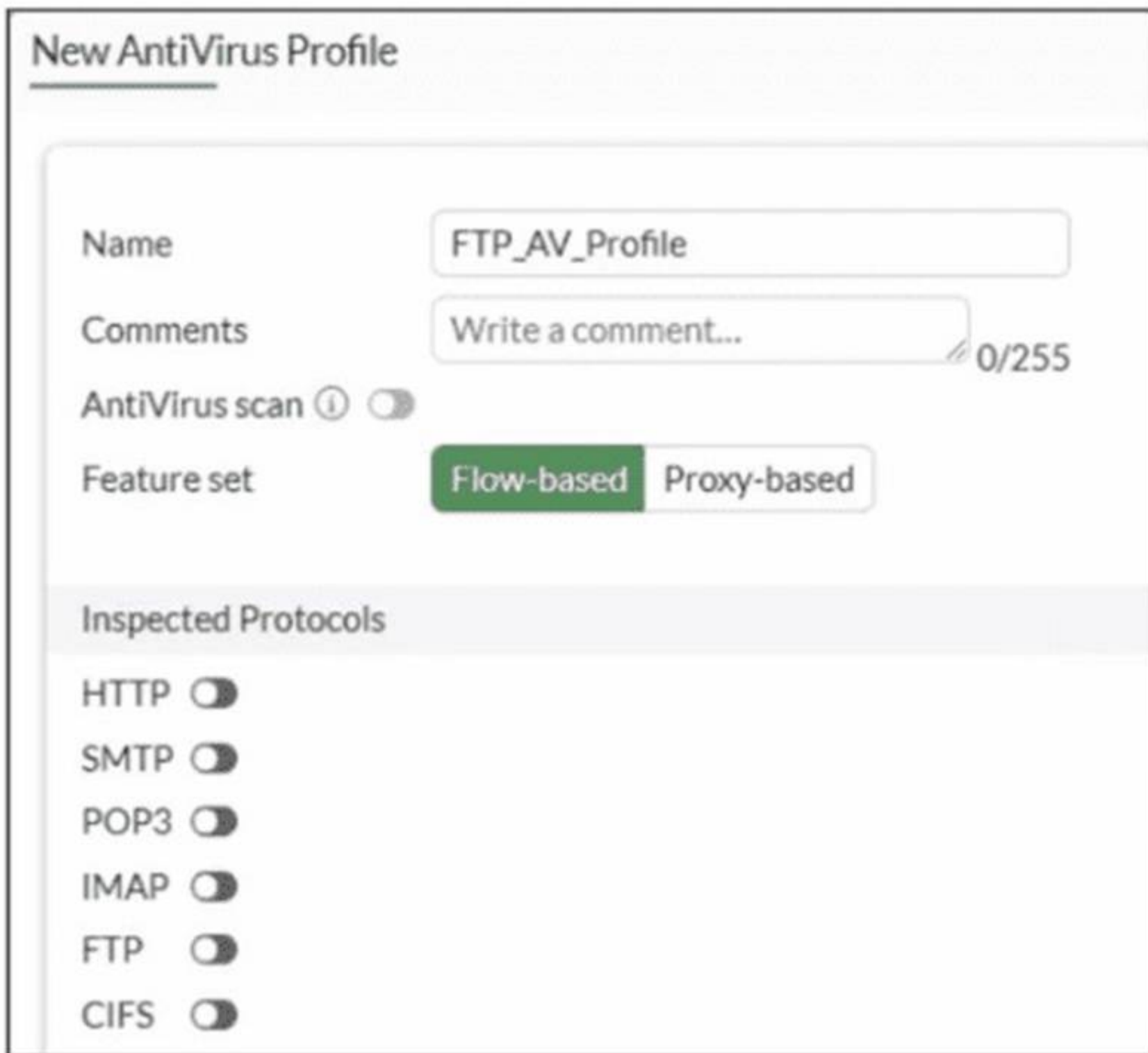
How does FortiExtender connect to FortiSASE in a site-based, remote internet access method?

- A. FortiExtender uses a Virtual Extensible LAN (VXLAN)-over-IPsec connection.
- B. FortiExtender establishes a secure SSL connection using FortiClient.
- C. FortiExtender first connects to a FortiGate LAN extension through a secure web gateway (SWG).
- D. FortiExtender uses the proxy auto-configuration (PAC) file and an explicit web proxy to connect.

Answer: A

NEW QUESTION 21

Refer to the exhibit.



New AntiVirus Profile

Name:

Comments: 0/255

AntiVirus scan ⓘ ☐

Feature set: Flow-based Proxy-based

Inspected Protocols

- HTTP ☐
- SMTP ☐
- POP3 ☐
- IMAP ☐
- FTP ☐
- CIFS ☐

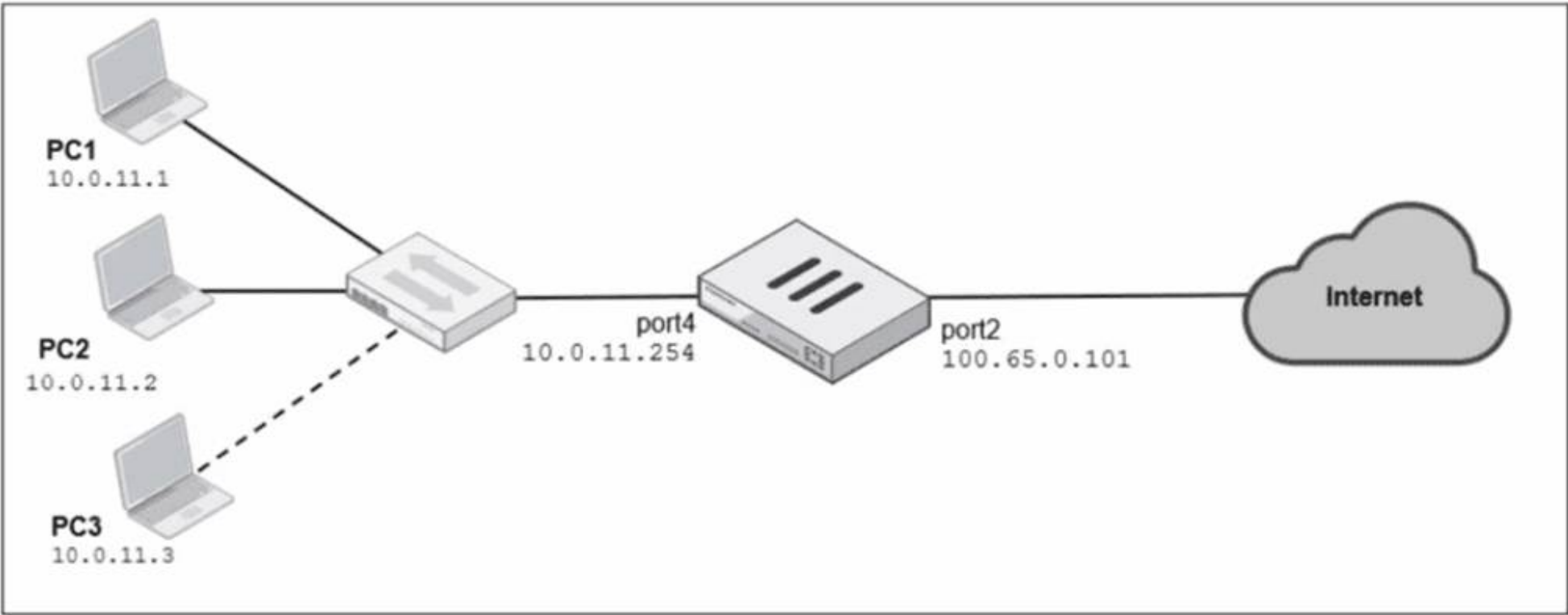
Why is the Antivirus scan switch grayed out when you are creating a new antivirus profile for FTP?

- A. Antivirus scan is disabled under System -> Feature visibility
- B. None of the inspected protocols are active in this profile.
- C. The Feature Set for the profile is Flow-based but it must be Proxy-based
- D. FortiGat
- E. with less than 2 GB RA
- F. does not support the Antivirus scan feature.

Answer: B

NEW QUESTION 26
Refer to the exhibits.

Network diagram



Dynamic IP pool

Edit Dynamic IP Pool

Name

Internet-pool

Comments

Write a comment...0/255

Type

One-to-One

External IP Range ⓘ

100.65.0.110-100.65.0.111

ARP Reply

☐

Firewall policies

Edit Policy

Name

Internet

Schedule

always

Action

ACCEPT

DENY

Outgoing interface

WAN (port2)

Source & Destination

Show logic

Source

all

User/group

Destination

all

Service

ALL

Firewall/Network Options

Inspection mode

Flow-based

Proxy-based

NAT

IP pool configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Internet-pool

Preserve source port

Protocol options

PROT

default

A diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device are shown. Two PCs. PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet. Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)

A. In the system settings, set Multiple Interface Policies to enable.
B. in the IP pool configuration, set end ip to 100.65.0.112.

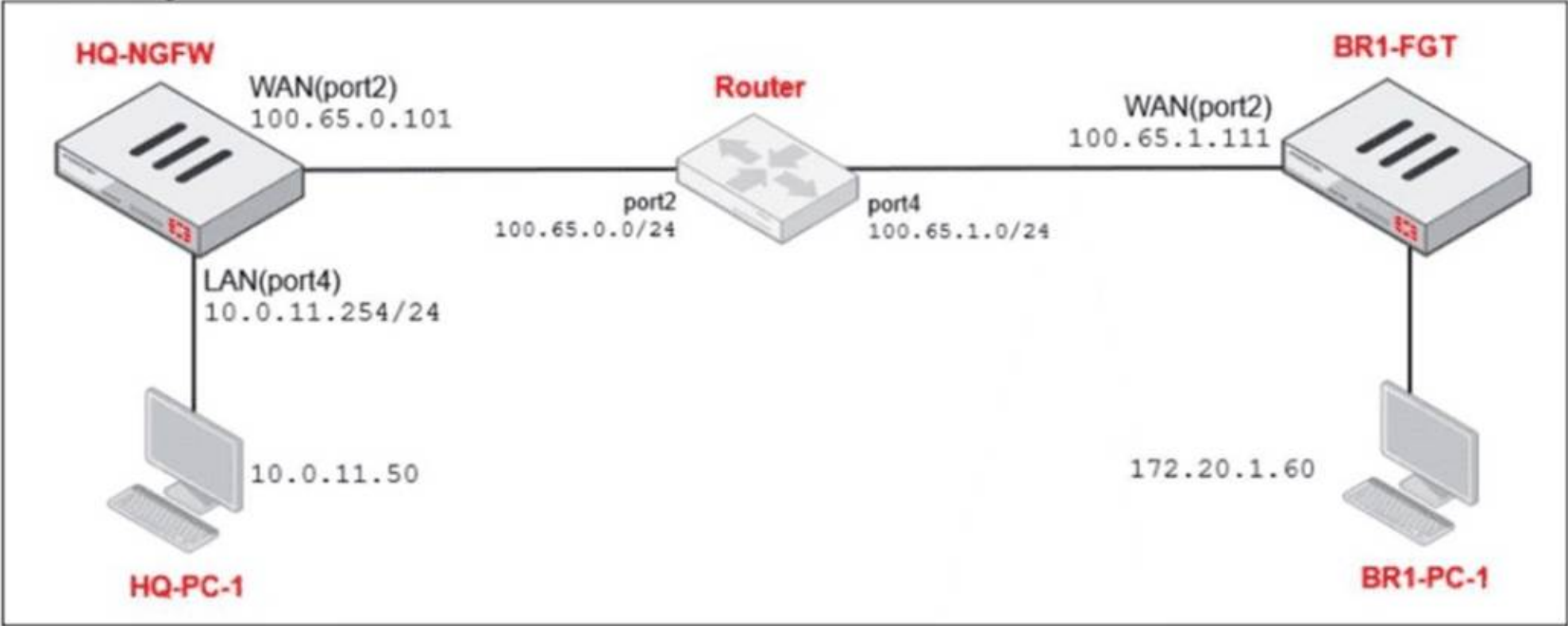
Passing Certification Exams Made Easy visit - <https://www.surepassexam.com>

- C. In the firewall policy, set match-vip to enable using CLI.
- D. In the IP pool configuration, set type to overload.

Answer: BD

NEW QUESTION 27
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 30
.....

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](#)