

Fortinet

Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator



NEW QUESTION 1

A network administrator is reviewing firewall policies in both Interface Pair View and By Sequence View. The policies appear in a different order in each view. Why is the policy order different in these two views?

- A. By Sequence View groups policies based on rule priority, while Interface Pair View always follows the order of traffic logs.
- B. The firewall dynamically reorders policies in Interface Pair View based on recent traffic patterns, but By Sequence View remains static.
- C. Interface Pair View sorts policies based on matching interfaces, while By Sequence View shows the actual processing order of rules.
- D. Policies in Interface Pair View are prioritized by security levels, while By Sequence View strictly follows the administrator's manual ordering.

Answer: C

NEW QUESTION 2

Refer to the exhibit.

Priority	Details	Type	Action
1	ABC.Com	Application	Allow
2	Excessive-Bandwidth	Filter	Block

An administrator has configured an Application Overrides for the ABC.Com application signature and set the Action to Allow. This application control profile is then applied to a firewall policy that is scanning all outbound traffic. Logging is enabled in the firewall policy. To test the configuration, the administrator accessed the ABC.Com web site several times.

Why are there no logs generated under security logs for ABC.Com?

- A. The ABC Com is hitting the category Excessive-Bandwidth.
- B. The ABC.Com Type is set as Application instead of Filter.
- C. The ABC.Com is configured under application profile, which must be configured as a web filter profile.
- D. The ABC Com Action is set to Allow

Answer: D

NEW QUESTION 3

Refer to the exhibit.

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-filter
Status      : Enable
License     : Contract
\
Num. of servers : 1
Protocol    : https
Port        : 8888
Anycast     : Disable
Default servers : Not included

--- Server List (Wed Sep 20 09:22:42 2023) ---
IP           Weight  RTT  Flags  TZ  FortiGuard-requests  Curr Lost Total Lost  Updated Time
10.0.1.241   -244   2 I    0    122      0      0      0 Wed Sep 20 09:21:55 2023
```

Which two statements about the FortiGuard connection are true? (Choose two.)

- A. The weight increases as the number of failed packets rises

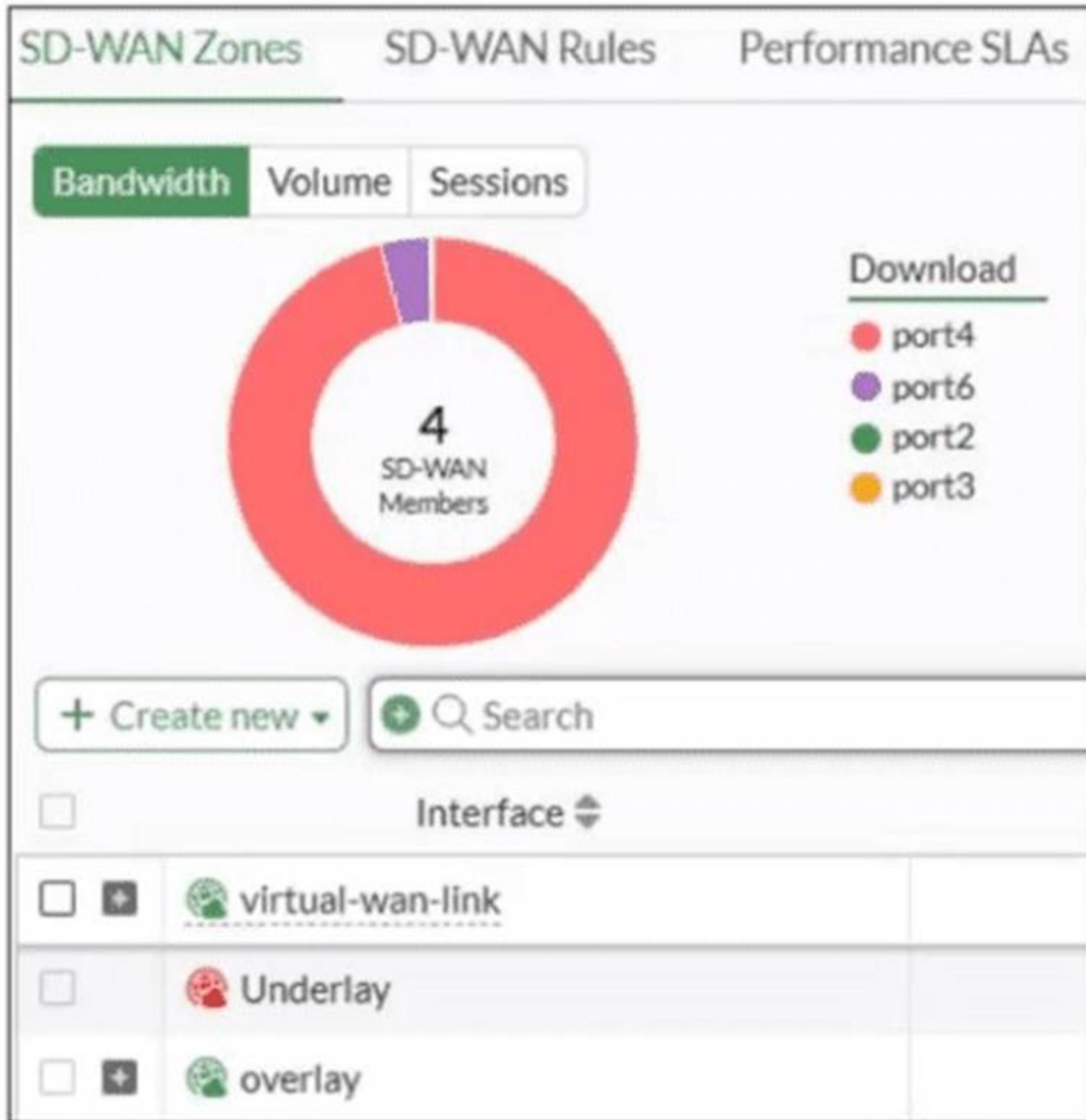
- B. You can configure unreliable protocols to communicate with FortiGuard Server.
- C. FortiGate identified the FortiGuard Server using DNS lookup.
- D. FortiGate is using the default port for FortiGuard communication.

Answer: AD

NEW QUESTION 4

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 5

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 iprope_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 6

An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic.
 Which DPD mode on FortiGate meets this requirement?

- A. On Demand
- B. Enabled
- C. On Idle
- D. Usabled

Answer: A

NEW QUESTION 7

What are two features of FortiGate FSSO agentless polling mode? (Choose two.)

- A. FortiGate uses the AD server as the collector agent.
- B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- C. FortiGate does not support workstation check.
- D. FortiGate directs the collector agent to use a remote LDAP server.

Answer: BC

NEW QUESTION 8

You have configured an application control profile, set peer-to-peer traffic to Block under the Categories tab. and applied it to the firewall policy. However, your peer-to-peer traffic on known ports is passing through the FortiGate without being blocked. What FortiGate settings should you check to resolve this issue?

- A. FortiGuard category ratings
- B. Network Protocol Enforcement
- C. Replacement Messages for UDP-based Applications
- D. Application and Filter Overrides

Answer: B

NEW QUESTION 9

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 10

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 10

A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode. Which step is not part of the expected process?

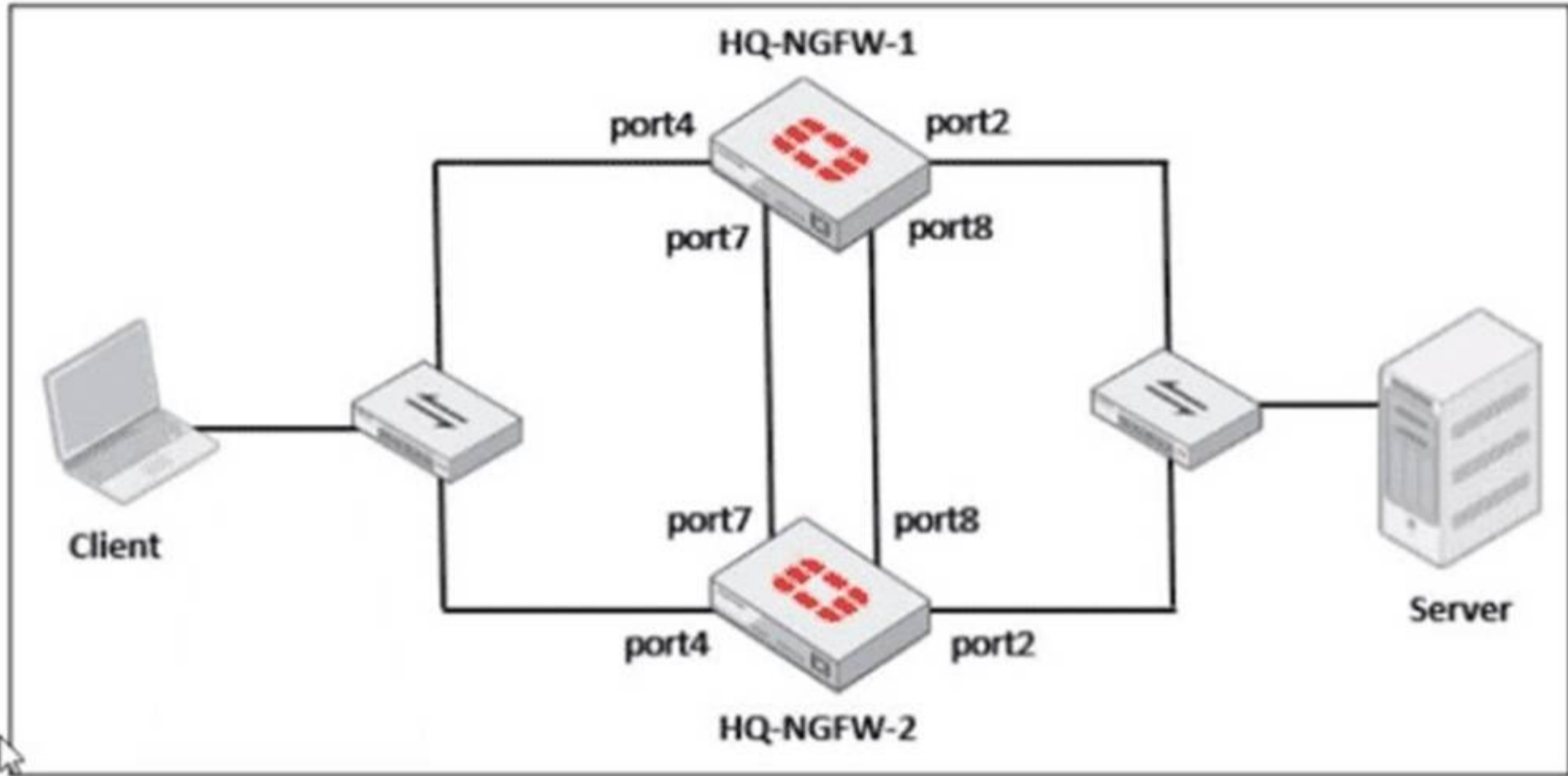
- A. The DC agent sends login event data directly to FortiGate.
- B. FortiGate determines user identity based on the IP address in the FSSO list.
- C. The collector agent forwards login event data to FortiGate.
- D. The user logs into the windows domain.

Answer: A

NEW QUESTION 14

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"
```

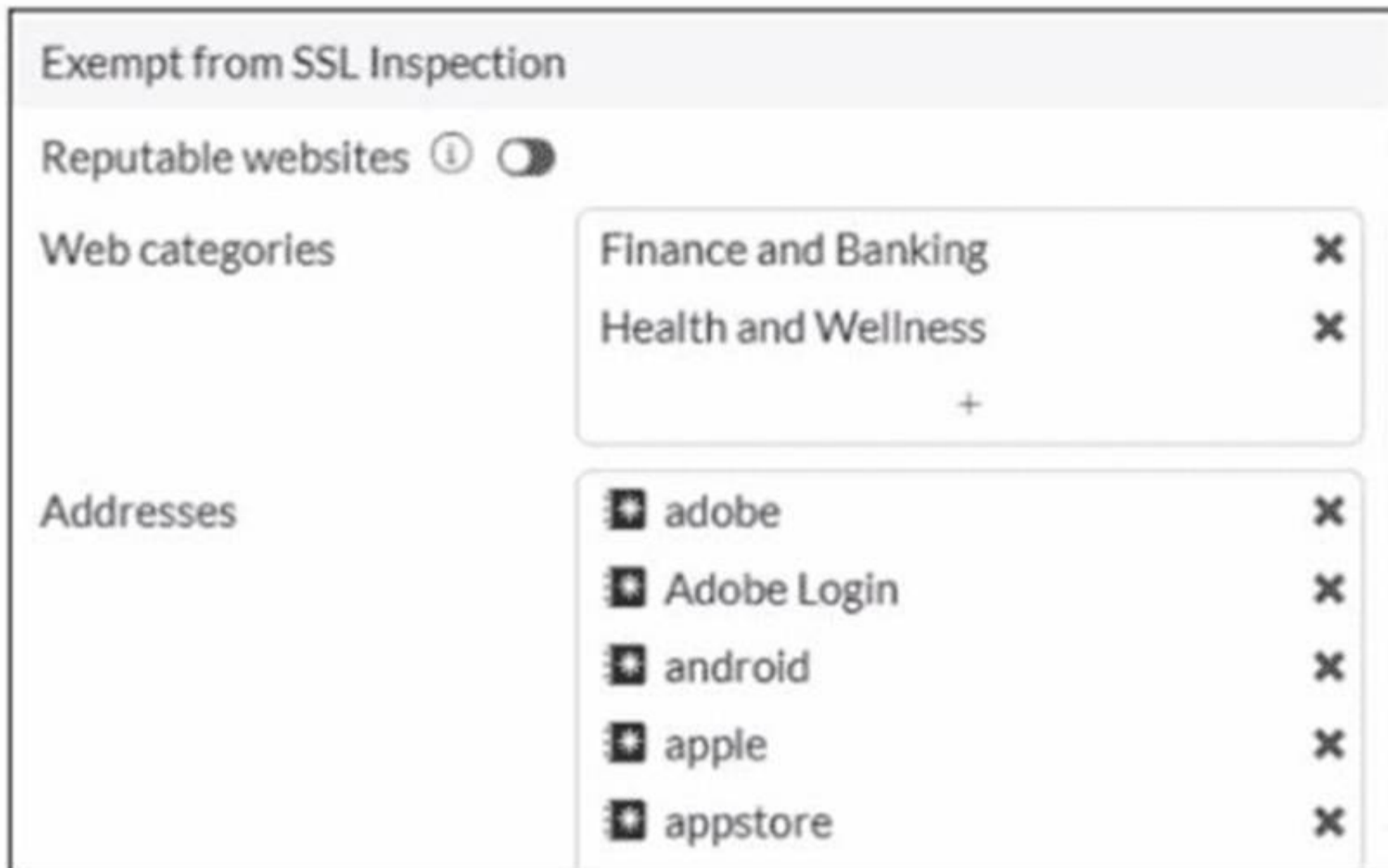
Based on the current HA status, an administrator updates the override and priority parameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibits. What would be the expected outcome in the HA cluster?

- 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 19

Refer to the exhibit.



The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories from SSL inspection, as shown in the exhibit For which two reasons are these web categories exempted? (Choose two.)

- A. The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.
- B. The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.
- C. These websites are in an allowlist of reputable domain names maintained by FortiGuard.
- D. The FortiGate temporary certificate denies the browser's access to websites that use HTTP Strict Transport Security.

Answer: BC

NEW QUESTION 22

Which two statements are true about an HA cluster? (Choose two answers)

- A. An HA cluster cannot have both in-band and out-of-band management interfaces at the same time.
- B. Link failover triggers a failover if the administrator sets the interface down on the primary device.
- C. When sniffing the heartbeat interface, the administrator must see the IP address 169.254.0.2.
- D. HA incremental synchronization includes FIB entries and IPsec SAs.

Answer: BD

NEW QUESTION 27

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 28

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 30

What is the primary FortiGate election process when the HA override setting is enabled? (Choose one answer)

- A. Connected monitored ports > Priority > HA uptime > FortiGate serial number

- B. Connected monitored ports > Priority > System uptime > FortiGate serial number
- C. Connected monitored ports > HA uptime > Priority > FortiGate serial number
- D. Connected monitored ports > System uptime > Priority > FortiGate serial number

Answer: A

NEW QUESTION 33

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 38

Refer to the exhibits.

HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
    set group-id 5
    set group-name "Training"
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output

```
HQ-NGFW-1 # 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
```

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # 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, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32 kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions in 10 minutes, 13 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, 10 hours, 50 minutes
```

An administrator has observed the performance status outputs on an HA cluster for 55 seconds. Which FortiGate is the primary?

- A. HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting
- B. HQ-NGFW-2 with the parameter priority setting
- C. HQ-NGFW-1 with the parameter override setting
- D. HQ-NGFW-2 with the parameter memory-failover-threshold setting

Answer: D

NEW QUESTION 40

An administrator has configured a dialup IPsec VPN on FortiGate with add-route enabled. However, the static route is not showing in the routing table. Which two statements about this scenario are correct? (Choose two.)

- A. The administrator must use a policy route instead of a static route for add-route to work properly.
- B. The administrator must ensure phase 2 is successfully established
- C. The administrator must define the remote network correctly in the phase 2 selectors.
- D. The administrator must enable a dynamic routing protocol on the dialup interface.

Answer: BC

NEW QUESTION 42

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 46

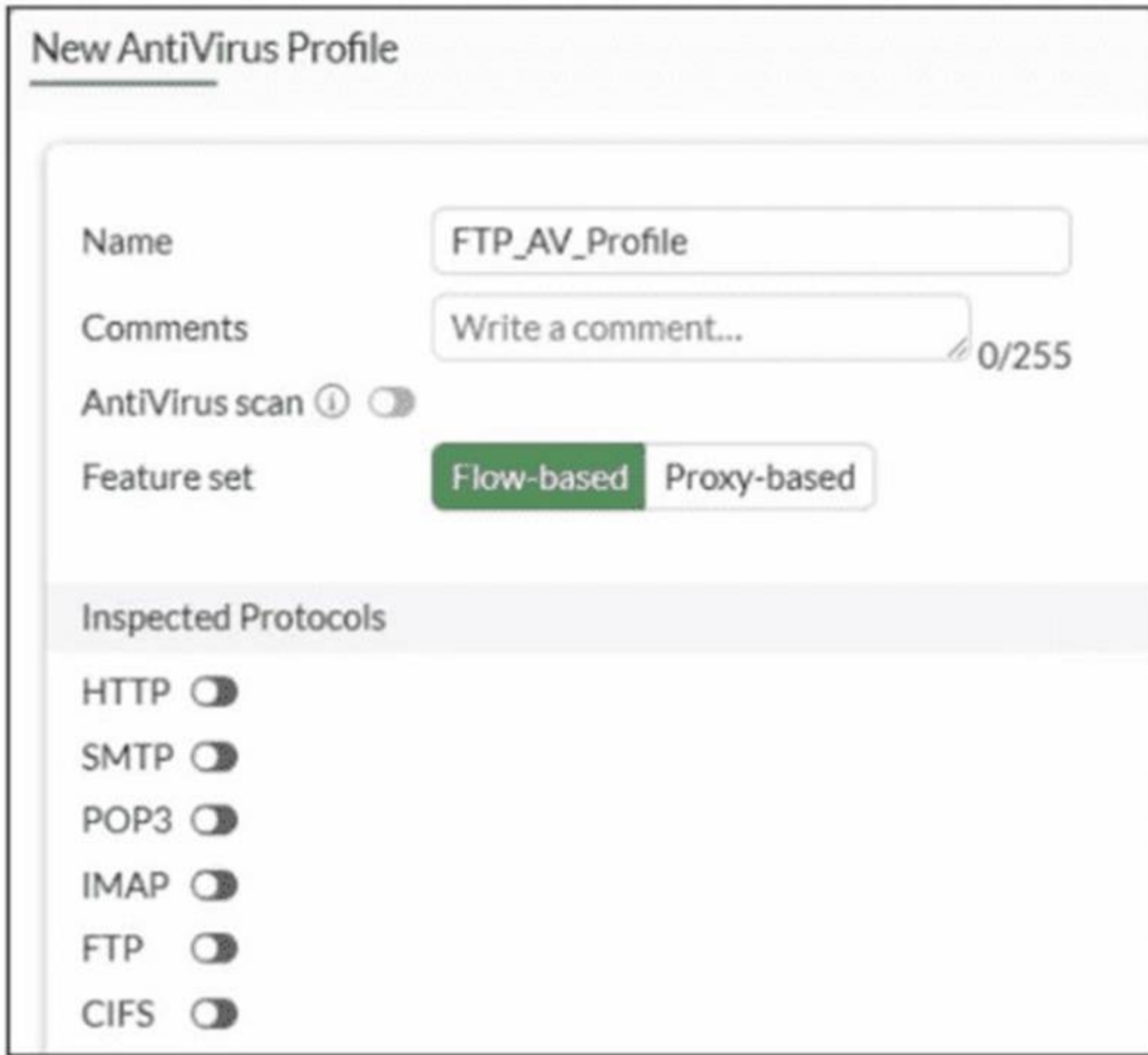
How does FortiExtender connect to FortiSASE in a site-based, remote internet access method?

- 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 51

Refer to the exhibit.



New AntiVirus Profile

Name:

Comments: 0/255

AntiVirus scan (disabled)

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?

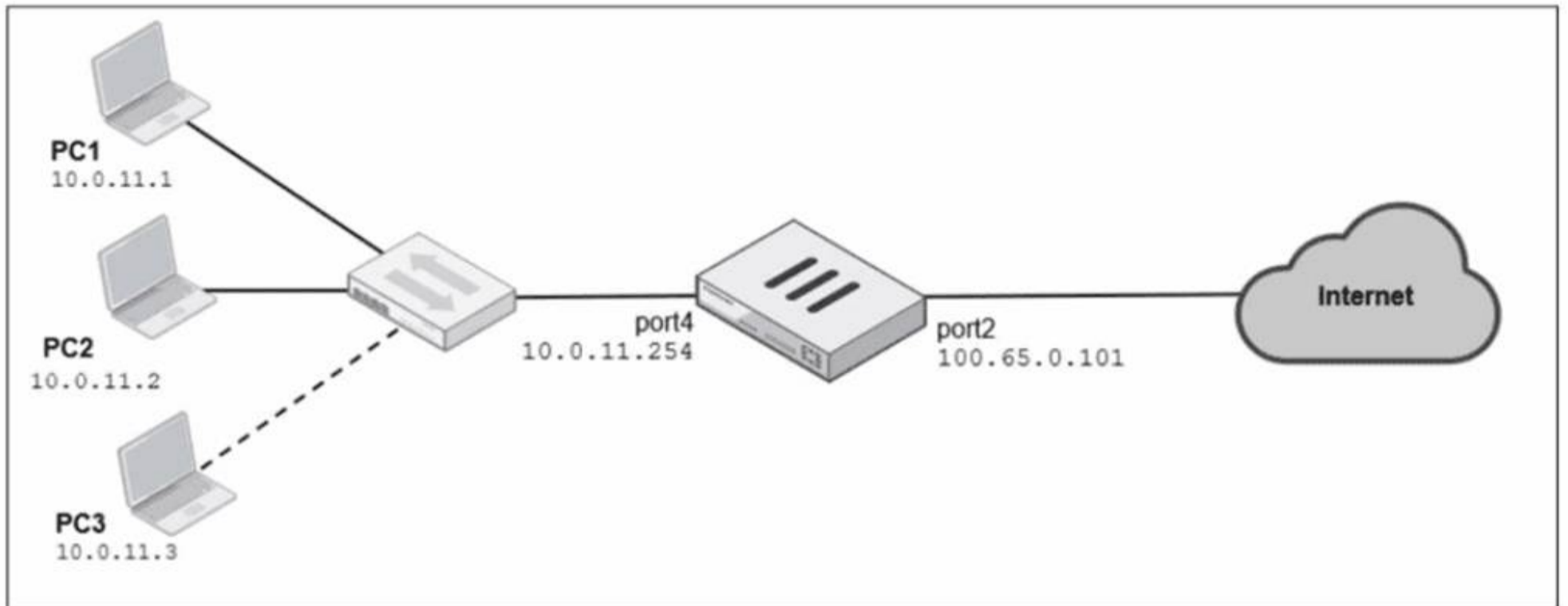
- A. Antivirus scan is disabled under System -> Feature visibility
- B. None of the inspected protocols are active in this profile.
- C. The Feature Set for the profile is Flow-based but it must be Proxy-based
- D. FortiGat
- E. with less than 2 GB RA
- F. does not support the Antivirus scan feature.

Answer: B

NEW QUESTION 55

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	<input type="checkbox"/>

Firewall policies

Edit Policy

Name (i)

Schedule

Action ACCEPT DENY

Outgoing interface ×

Source & Destination Show logic

Source ×

User/group

Destination ×

Service ×

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 PROXY 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.

- 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 58

Refer to the exhibit.
 A routing table is shown

Network	Gateway IP	Interfaces	Distance	Metric	Priority	Type
10.0.11.0/24	0.0.0.0	port4	0	0	0	Connected
10.0.12.0/24	0.0.0.0	port5	0	0	0	Connected
10.0.13.0/24	0.0.0.0	port6	0	0	0	Connected
100.65.0.0/24	0.0.0.0	port2	0	0	0	Connected
100.66.0.0/24	0.0.0.0	port3	0	0	0	Connected
172.20.1.0/24	100.66.0.254	port3	9	0	2	Static
192.168.0.0/16	0.0.0.0	port1	0	0	0	Connected

An administrator wants to create a new static route so the traffic to the subnet 172.20.1.0/24 is routed through port2 only. What are the two criteria that the administrator can use to achieve this objective? (Choose two.)

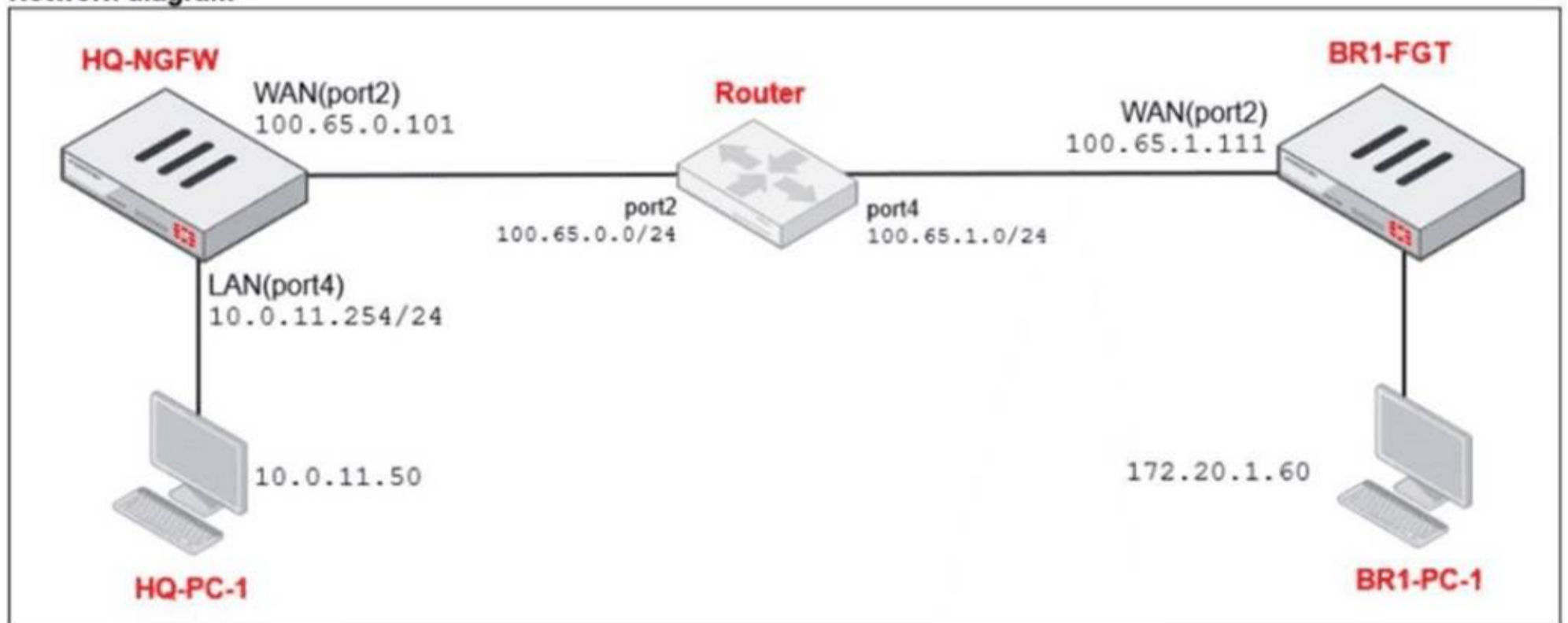
- A. The new static route must have the priority set to 3.
- B. The new static route must have the metric set to 1.
- C. The existing static route through port3 must have the distance set to 11.
- D. The new static route must have the distance set to 9

Answer: CD

NEW QUESTION 59

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 63

.....

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](#)