

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 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 3

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 4

You have configured the below commands on a FortiGate.

```
config system settings
set strict-src-check enable
end
```

```
Config system interface
edit port1
set src-check disable
next
end
```

What would be the impact of this configuration on FortiGate?

- A. FortiGate will enable strict RPF on all its interfaces and port1 will be exempted from RPF checks.
- B. FortiGate will enable strict RPF on all its interfaces and port1 will be enable for asymmetric routing.
- C. The global configuration will take precedence and FortiGate will enable strict RPF on all interfaces.
- D. Port1 will be enabled with flexible RP
- E. and all other interfaces will be enabled for strict RPF

Answer: A

NEW QUESTION 5

Which three strategies are valid SD-WAN rule strategies for member selection? (Choose three answers)

- A. Lowest Cost (SLA) without load balancing
- B. Manual with load balancing
- C. Lowest Quality (SLA) with load balancing
- D. Lowest Cost (SLA) with load balancing
- E. Best Quality with load balancing

Answer: ABD

NEW QUESTION 6

Refer to the exhibit.

A RADIUS server configuration is shown.

New RADIUS Server

Name

Authentication method Default Specify

NAS IP

Include in every user group

Primary Server

IP/Name

Secret

An administrator added a configuration for a new RADIUS server. While configuring, the administrator enabled "Include in every user group". What is the impact of enabling "Include in every user group" in a RADIUS configuration?

- A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
- B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
- C. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.
- D. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.

Answer: A

NEW QUESTION 7

An administrator manages a FortiGate model that supports NTurbo. How does NTurbo acceleration enhance antivirus performance?

- A. For flow-based inspection
- B. NTurbo establishes a dedicated data path to redirect traffic between the IPS engine and FortiGate ingress and egress interfaces.
- C. For proxy-based inspection
- D. NTurbo creates two inspection sessions on the FortiGate device.
- E. For proxy-based inspection
- F. NTurbo offloads traffic to the content processor.
- G. For proxy-based inspection
- H. NTurbo buffers the whole file and then sends it to the antivirus engine.

Answer: A

NEW QUESTION 8

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 9

Refer to the exhibit.

IPsec tunnel configuration

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 two configuration changes will bring phase 2 up? (Choose two.)

- A. On BR1-FGT, set Remote Address to 10.0.11.0/255.255.255.0.
- B. On HQ-NGF
- C. enable Diffie-Hellman Group 2.
- D. On BR1-FG
- E. set Seconds to 43200
- F. On HQ-NGF
- G. set Encryption to AES256.

Answer: AD

NEW QUESTION 10

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 10

Which two statements are correct when FortiGate enters conserve mode? (Choose two answers)

- A. FortiGate continues to run critical security actions, such as quarantine.
- B. FortiGate refuses to accept configuration changes.
- C. FortiGate halts complete system operation and requires a reboot to regain available resources.
- D. FortiGate continues to transmit packets without IPS inspection when the fail-open global setting in IPS is enabled.

Answer: BD

NEW QUESTION 14

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

+ Create New
Edit
Delete

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

Application override configuration

Edit Override

Type: Application Filter

Action: Block

Filter: BIVR Excessive-Bandwidth x

+

FaceTime x Q

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

Filter override configuration

Edit Override

Type: Application Filter

Action: Monitor

Filter: VEND Apple x

+

FaceTime x Q

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

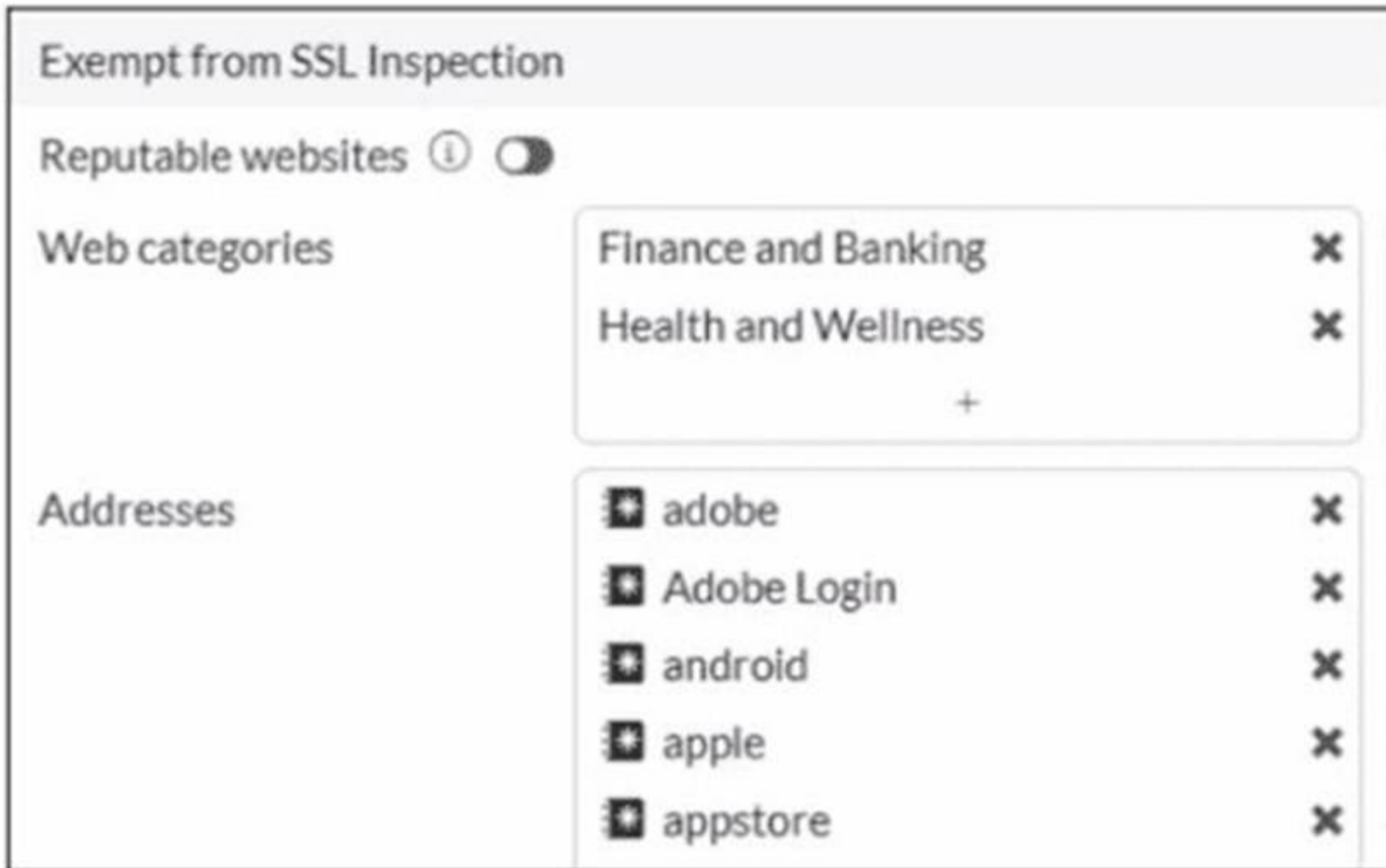
The exhibits show the application sensor configuration and the Excessive-Bandwidth and Apple filter details. Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming? (Choose one answer)

- 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 16

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 21

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 26

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 31

Which three statements about SD-WAN performance SLAs are true? (Choose three.)

- A. They rely on session loss and jitter.
- B. They monitor the state of the FortiGate device.
- C. All the SLA targets can be configured.
- D. They are applied in a SD-WAN rule lowest cost strategy.
- E. They can be measured actively or passively.

Answer: CDE

NEW QUESTION 35

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 37

Refer to the exhibit.



The NOC team connects to the FortiGate GUI with the NOC_Access admin profile. They request that their GUI sessions do not disconnect too early during inactivity. What must the administrator configure to answer this specific request from the NOC team?

- A. Increase the admintimeout value under config system accprofile noc Access.
- B. increase the of line value of the override idle Timeout parameter in the NOC_Access admin profile.
- C. Move NOC_Access to the top of the list to ensure all profile settings take effect.
- D. Ensure that all NOC_Access users are assigned the super_admin role to guarantee access.

Answer: B

NEW QUESTION 40

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?

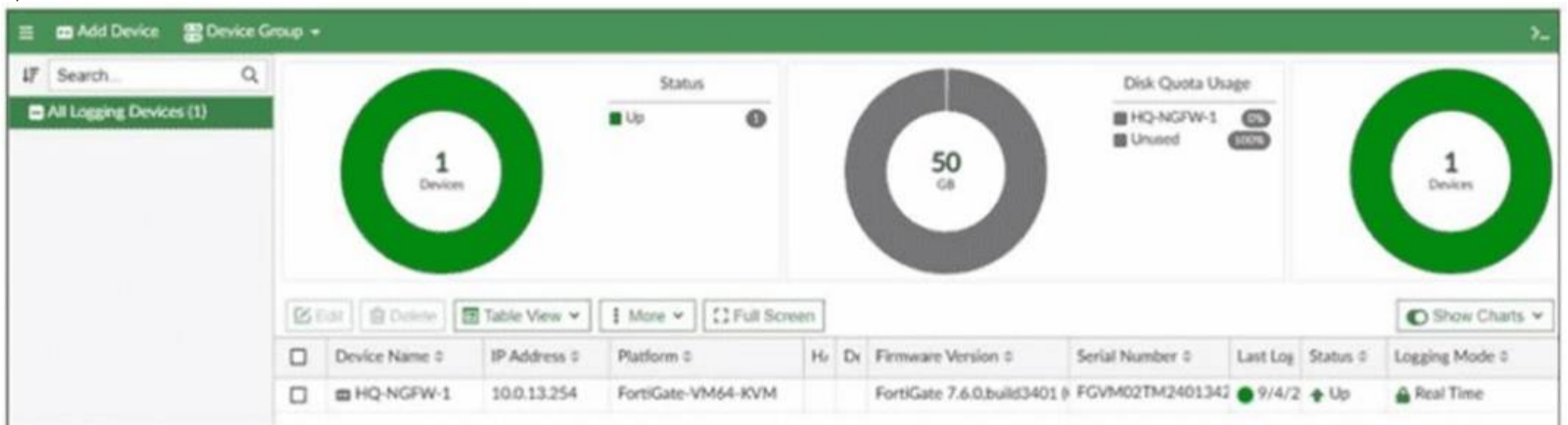
- A. Use IPS group signatures, set rate-mode 60.
- B. Use IPS packet logging option with periodical filter option.
- C. Use IPS signatures, rate-mode periodical option.
- D. Use IPS filter, rate-mode periodical option.

Answer: D

NEW QUESTION 41

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)

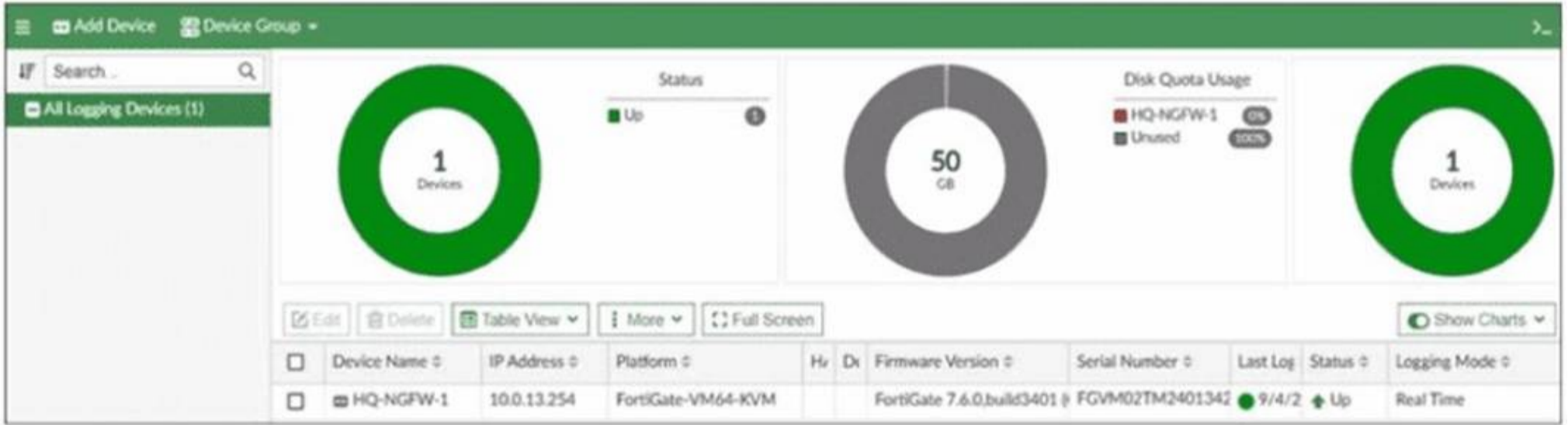


B)

```

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 46

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 51

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 52

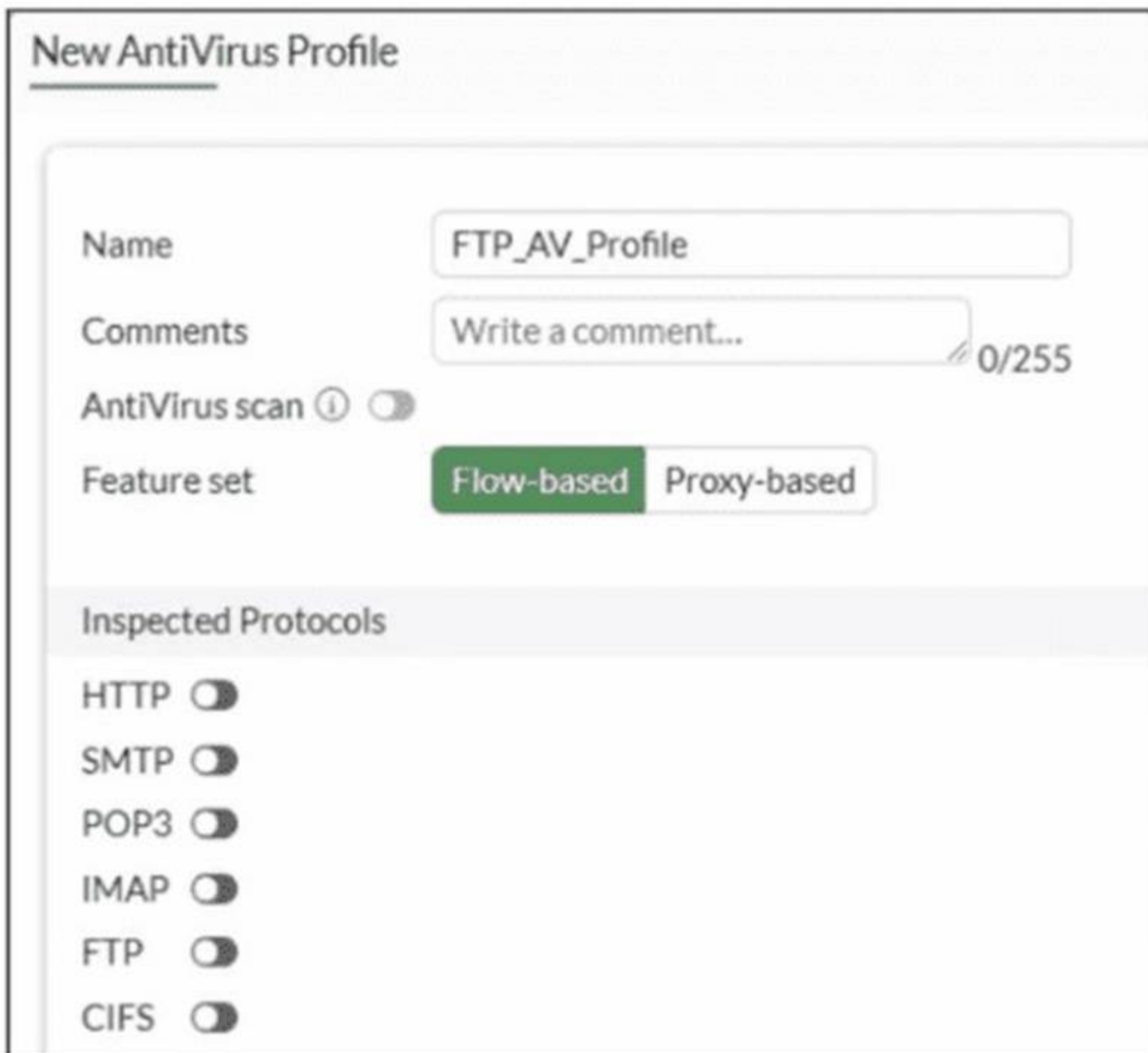
When configuring firewall policies which of the following is true regarding the policy ID? (Choose two.)

- 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 57

Refer to the exhibit.



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 61

Refer to the exhibit.

```
config system global
    set av-failopen one-shot
end
config ips global
    set fail-open enable
end
```

Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

- A. FortiGate drops new sessions requiring inspection.
- B. Administrators must restart FortiGate to allow new sessions.
- C. Administrators cannot change the configuration.
- D. FortiGate skips quarantine actions.

Answer: CD

NEW QUESTION 64

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 67

Refer to the exhibits.

Web filter profile configuration

Edit Web Filter Profile

Feature set Flow-based Proxy-based

FortiGuard Category Based Filter

Allow
 Monitor
 Block
 Warning
 Authenticate

Name	Action
Job Search	<input checked="" type="radio"/> Allow
Medicine	<input checked="" type="radio"/> Allow
News and Media	<input checked="" type="radio"/> Allow
Social Networking	<input checked="" type="radio"/> Allow
Political Organizations	<input checked="" type="radio"/> Allow
Reference	<input checked="" type="radio"/> Allow
Global Religion	<input checked="" type="radio"/> Allow
Shopping	<input checked="" type="radio"/> Allow
Society and Lifestyles	<input checked="" type="radio"/> Allow

58% 95

Allow users to override blocked categories

Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex

Static URL Filter

Block invalid URLs

URL Filter

+ Create New
 Edit
 Delete
Search

URL	Type	Action	Status
www.facebook.com	Simple	<input type="radio"/> Monitor	<input checked="" type="radio"/> Enable

Firewall policy configuration

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: WEB default

Video filter:

DNS filter:

Application control:

IPS:

File filter:

SSL inspection: SSL certificate-inspection

FortiGuard block page



A web filter profile configuration and firewall policy configuration are shown. You are trying to access www.facebook.com, but you are redirected to a FortiGuard web filtering block page. Based on the exhibits, what is the possible cause of the issue?

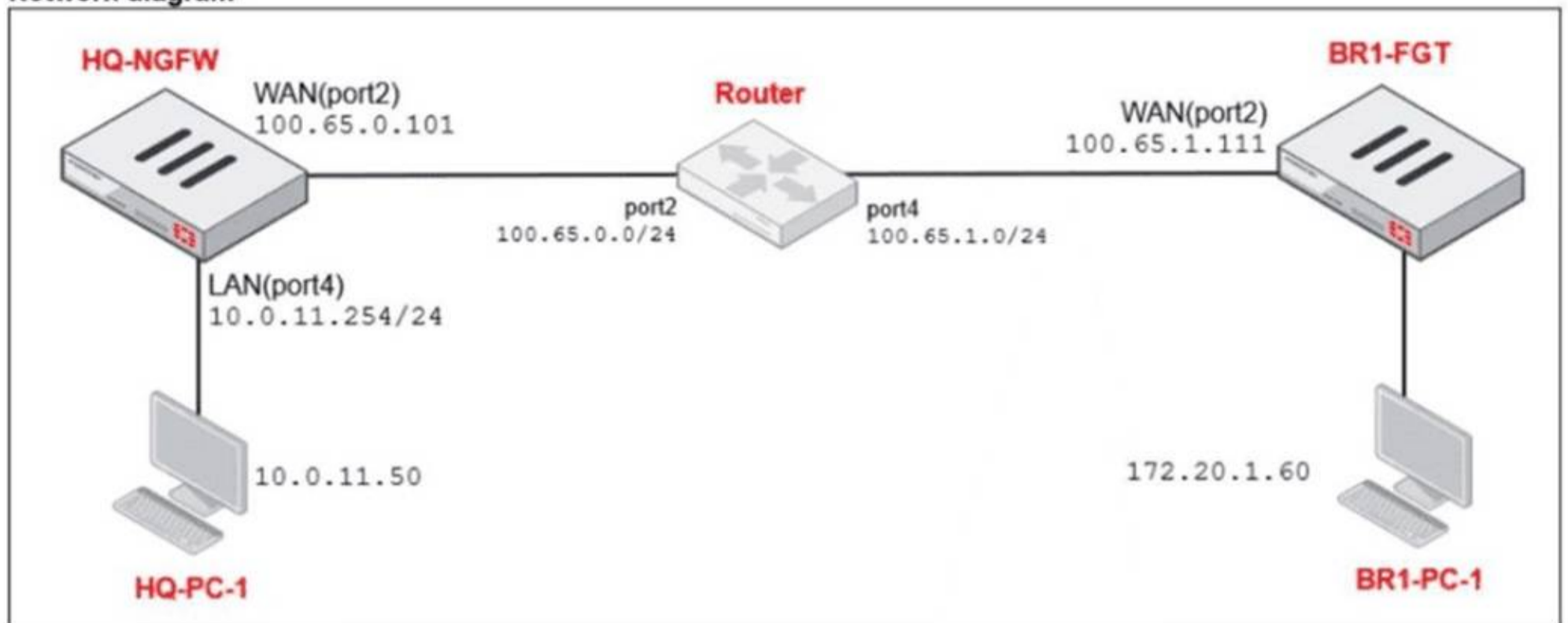
- A. The web rating override configuration is incorrect.
- B. The web filter profile feature set is configured incorrectly.
- C. The firewall policy inspection mode is incorrect.
- D. For ww
- E. faceboo
- F. co
- G. the URL filter action is incorrect.

Answer: C

NEW QUESTION 69

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 71

.....

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](#)