

Fortinet

Exam Questions NSE4_FGT_AD-7.6

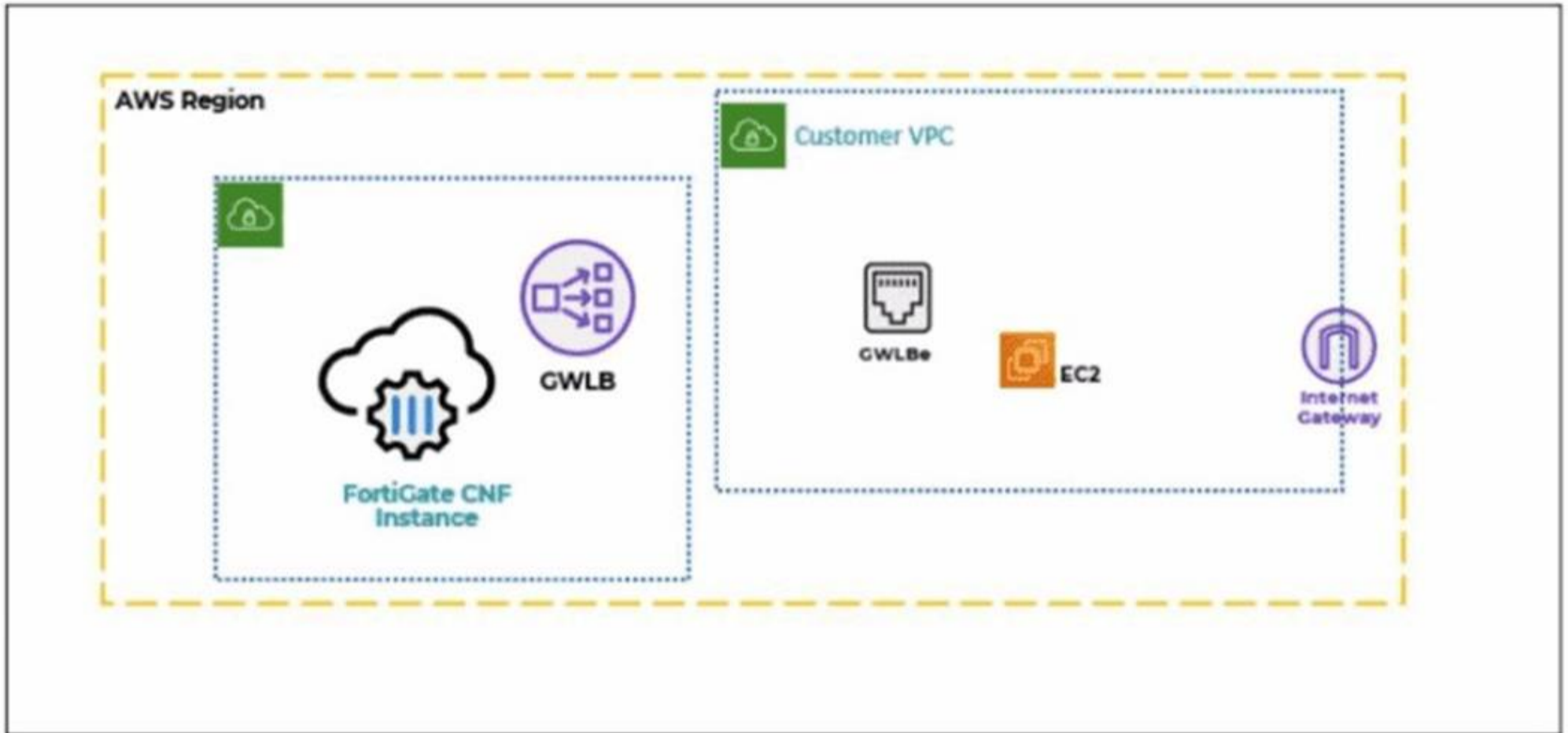
Fortinet NSE 4 - FortiOS 7.6 Administrator



NEW QUESTION 1

Refer to the exhibit.

A partial cloud topology is shown.



You deployed a FortiGate Cloud-Native Firewall (CNF) in AWS.

During the deployment, which components must the FortiGate CNF create to handle traffic from the EC2 instance?

- A. The customer VPC and GWLB
- B. The gateway load balancer endpoint (GWLBe) in the customer virtual private cloud (VPC)
- C. The CNF VP
- D. customer VP
- E. and GWLB
- F. The GWL
- G. GWLBe, and the internet gateway (IGW) in the customer VPC

Answer: B

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?

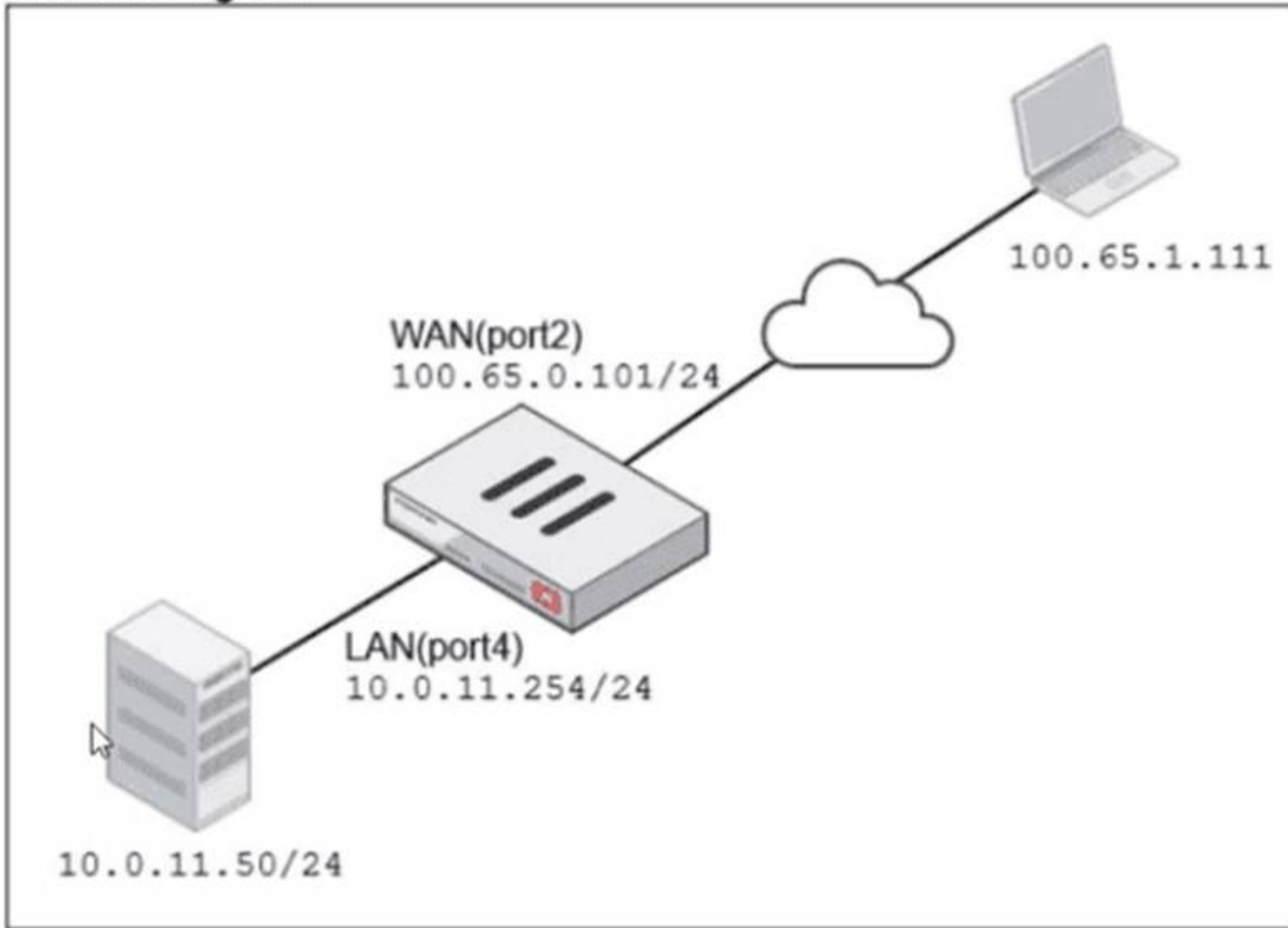
- A. Local Gateway
- B. Dead Peer Detection
- C. Peer ID
- D. IKE Mode Config

Answer: C

NEW QUESTION 4


Refer to the exhibits.

Network diagram



Name: VIP-WEB-SERVER

Comments: Write a comment... 0/255

Color: 

Network

Interface:

Type: Static NAT

External IP address/range:

Map to:

IPv4 address/range:

Optional Filters

Port Forwarding













Protocol: TCP UDP SCTP ICMP

Port Mapping Type: One to one Many to many

External service port:

Map to IPv4 port:

Firewall policies

Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
<input type="checkbox"/> Internet (1)	 LAN (port4)	 WAN (port2)	 all	 all	 always	 ALL	<input checked="" type="checkbox"/> ACCEPT		<input checked="" type="checkbox"/> NAT
<input type="checkbox"/> Web_Server_Access (2)	 WAN (port2)	 LAN (port4)	 all	 VIP-WEB-SERVER	 always	 HTTPS	<input checked="" type="checkbox"/> ACCEPT		<input checked="" type="checkbox"/> Disabled

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. 100.65.1.111, 10.0.11.50, and 4443. respectively
- D. 100.65.1.111, 10.0.11.50. and 443. respectively

Answer: C

NEW QUESTION 5

Refer to the exhibit.

Profile Name
Monitoring_Access
NOC_Access
prof_admin
super_admin

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? (Choose one answer)

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

Answer: D

NEW QUESTION 6

Refer to the exhibit.

A RADIUS server configuration is shown.

New RADIUS Server

Name: FortiAuthenticator-RADIUS

Authentication method: Default Specify

NAS IP:

Include in every user group:

Primary Server

IP/Name: 10.0.13.130

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

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 8

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 9

FortiGate is integrated with FortiAnalyzer and FortiManager.

When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?

- A. Universally Unique Identifier
- B. Policy ID
- C. Sequence ID
- D. Log ID

Answer: A

NEW QUESTION 10

Refer to the exhibits.

Application sensor

Edit Application Sensor

Categories

Mixed ▾
All Categories

Business (157, 6)

Cloud/IT (72, 12)

Collaboration (266, 13)

Email (76, 11)

Game (83)

General Interest (254, 15)

Mobile (3)

Network Service (338)

Operational Technology

P2P (55)

Proxy (189)

Remote Access (96)

Social Media (113, 29)

Storage/Backup (150, 20)

Update (48)

Video/Audio (148, 17)

VoIP (23)

Web Client (24)

Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New
 Edit
 Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	Block
2	VEND Google	Filter	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:

Video filter:

DNS filter:

Application control: APP default

IPS:

File filter:

SSL inspection: SSL certificate-inspection

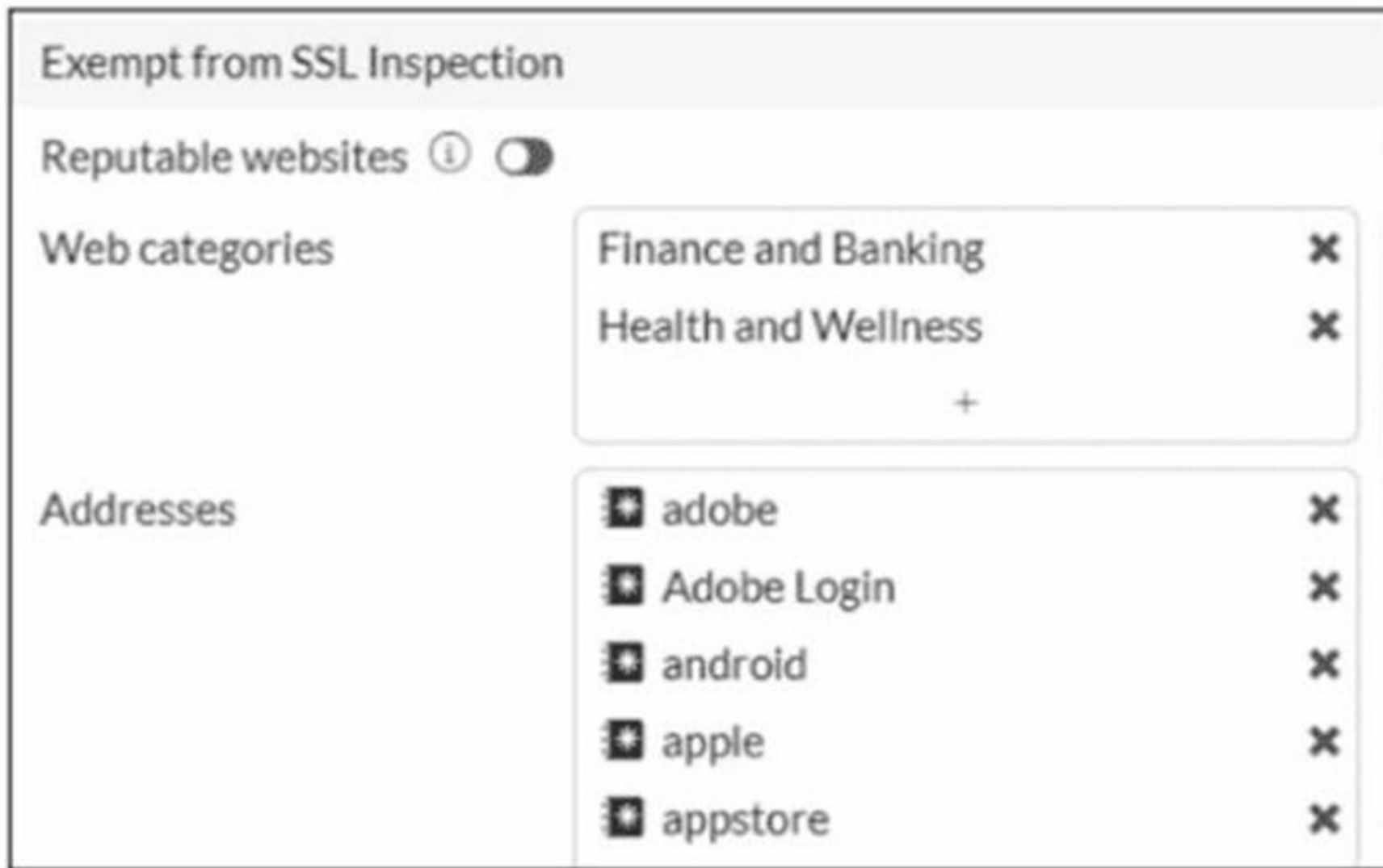
You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. You cannot access any of the Google applications, but you are able to access www.fortinet.com. Which two actions would you take to resolve the issue? (Choose two.)

- A. Set SSL inspection to deep-content inspection.
- B. Move up Google in the Application and Filter Overrides section to set its priority lot
- C. Add "Google".com to the URL category in the security profile.
- D. Change the Inspection mode to Flow-based
- E. Set the action for Google in the Application and Filter Overrides section to Allow

Answer: BE

NEW QUESTION 10

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 11

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 13

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 14

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 16

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 20

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

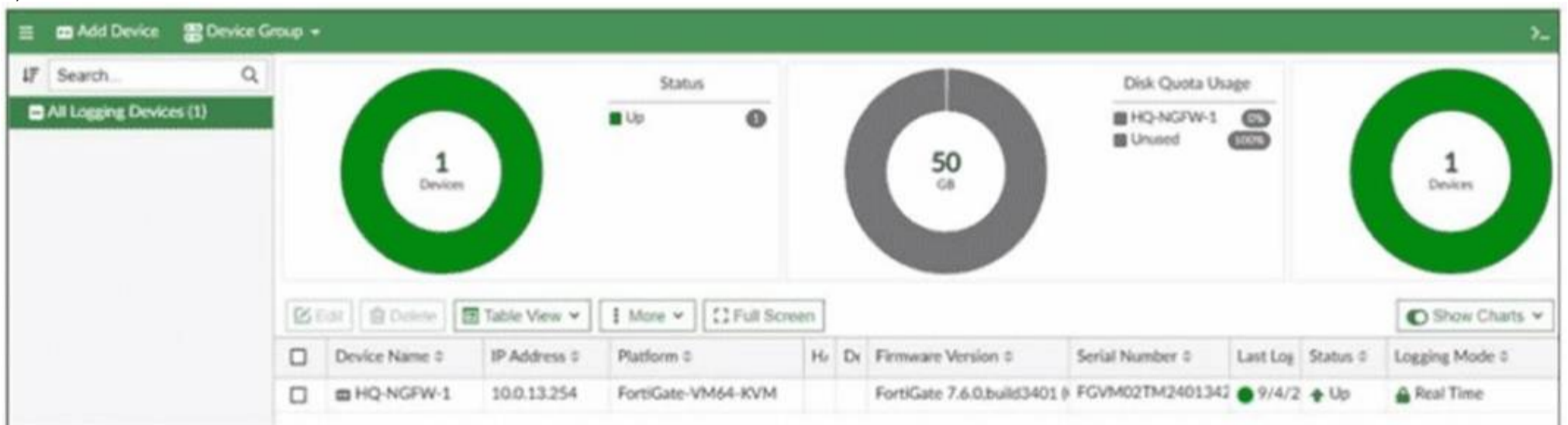
- A. They must have the same hard drive configuration.
- B. They must have the same number of configured VDOMs.
- C. They must have the heartbeat interfaces in the same subnet
- D. They must have the same HA group ID.

Answer: BD

NEW QUESTION 23

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 24

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 28

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 33

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 35

Which two statements are correct when the FortiGate device enters conserve mode? (Choose two.)

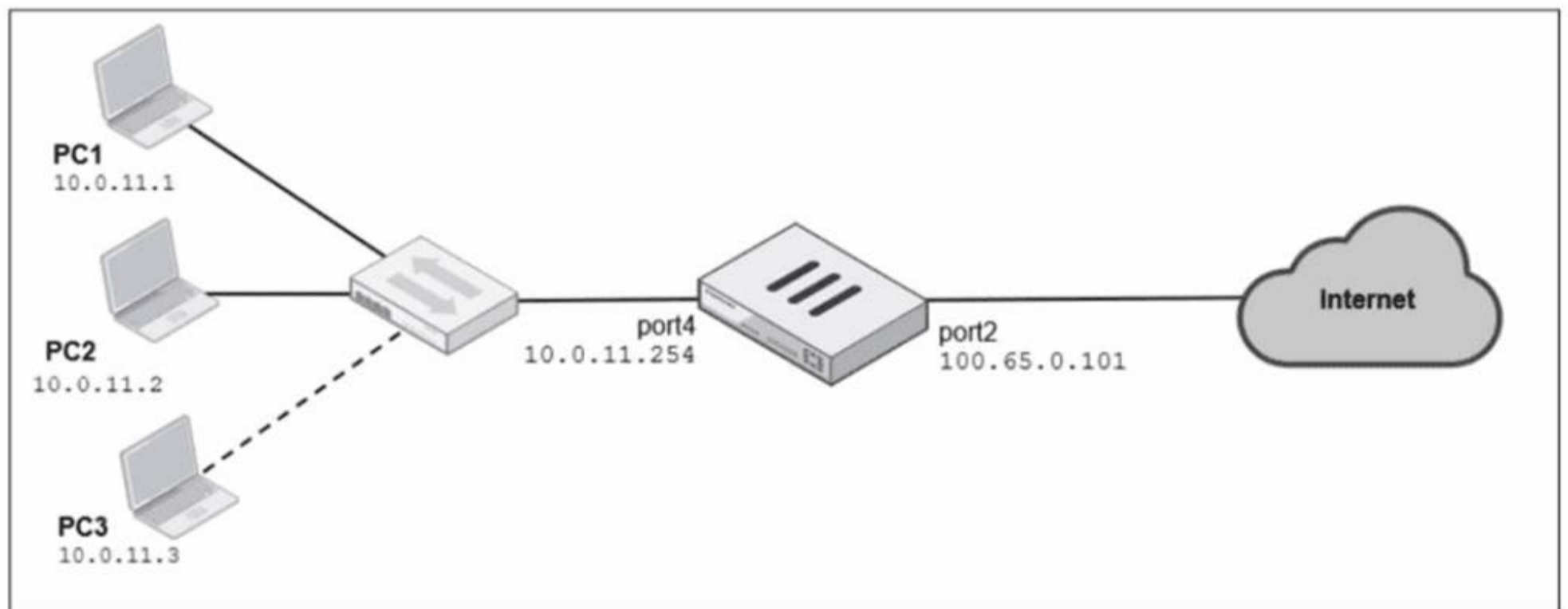
- A. FortiGate refuses to accept configuration changes.
- B. FortiGate halts complete system operation and requires a reboot to regain available resources.
- C. FortiGate continues to transmit packets without IPS inspection when the fail-open global setting in IPS is enabled.
- D. FortiGate continues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

Answer: AC

NEW QUESTION 40

Refer to the exhibits.

Network diagram



Dynamic IP pool

Edit Dynamic IP Pool

Name	<input type="text" value="Internet-pool"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Type	<input type="text" value="One-to-One"/>
External IP Range ⓘ	<input type="text" value="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

NAT

IP pool configuration

+

Preserve source port

Protocol options 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 41

.....

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](#)