

NSE4_FGT_AD-7.6 Dumps

Fortinet NSE 4 - FortiOS 7.6 Administrator

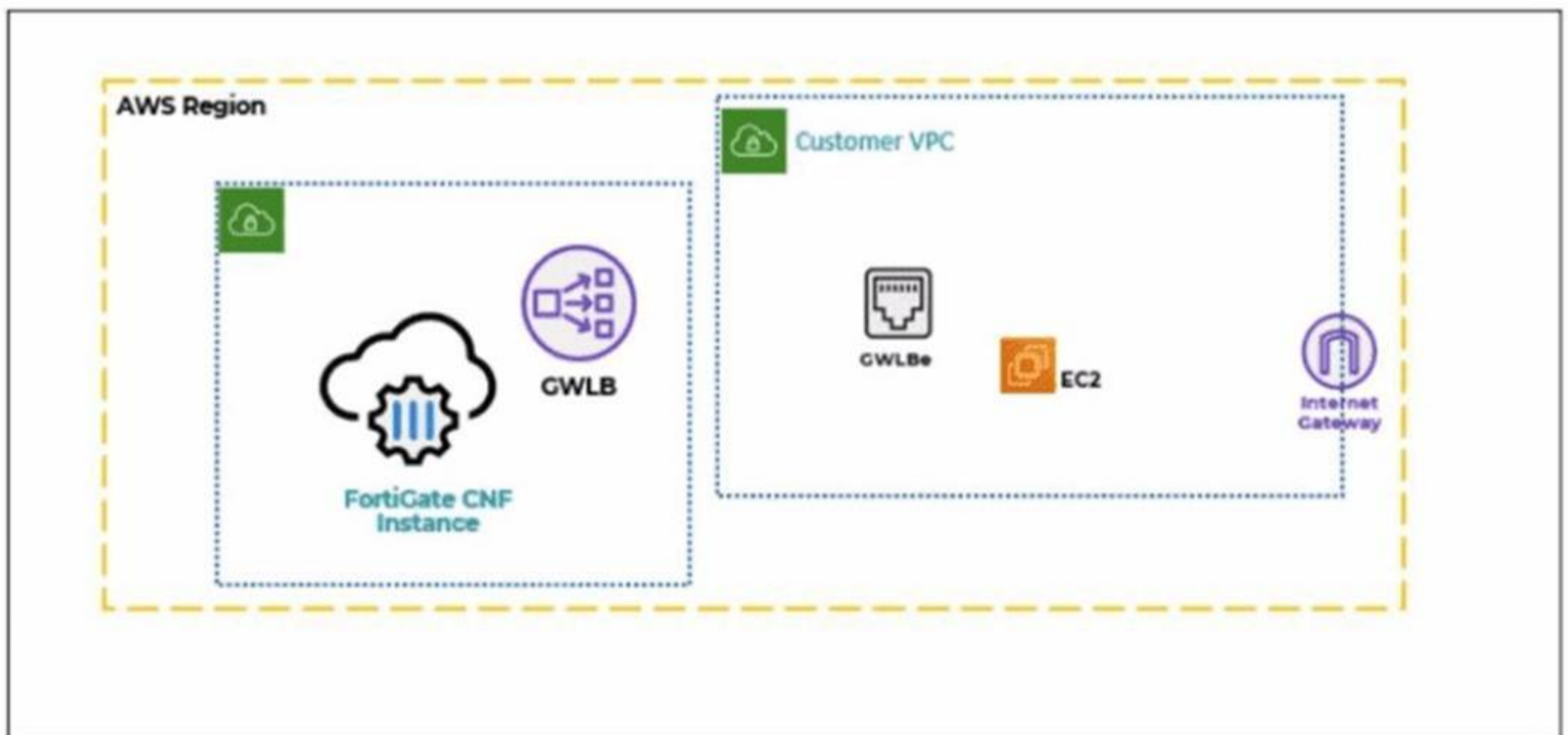
https://www.certleader.com/NSE4_FGT_AD-7.6-dumps.html



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 GWLBe
- 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

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 3

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 4

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 5

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 6

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 7

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 8

Refer to the exhibit.

Edit SSL/SSH Inspection Profile

Protecting SSL Server

Inspection method: SSL Certificate Inspection **Full SSL Inspection**

CA certificate: Fortinet_CA_SSL Download

Blocked certificates: Allow Block View Blocked Certificates

Untrusted SSL certificates: Allow Block Ignore View Trusted CAs List

Server certificate SNI check: Enable Strict Disable

What would be the impact of these settings on the Server certificate SNI check configuration on FortiGate?

- A. FortiGate will accept and use the CN in the server certificate for URL filtering if the SNI does not match the CN or SAN fields.
- B. FortiGate will accept the connection with a warning if the SNI does not match the CN or SAN fields.
- C. FortiGate will close the connection if the SNI does not match the CN or SAN fields.
- D. FortiGate will close the connection if the SNI does not match the CN and SAN fields

Answer: C

NEW QUESTION 9

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 10

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

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

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

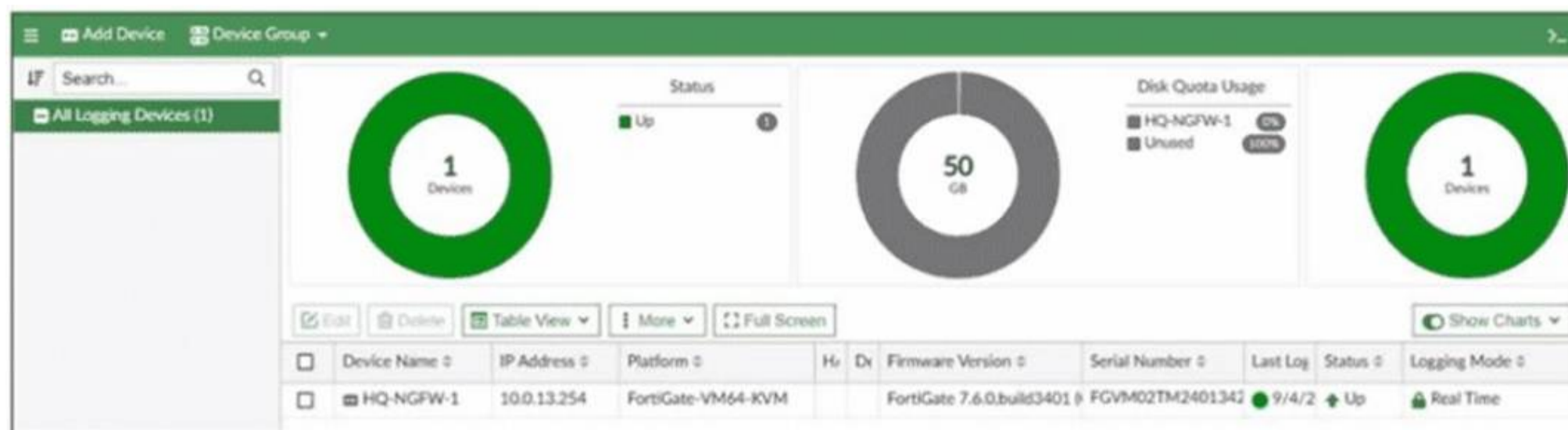
Answer: BE

NEW QUESTION 10

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?

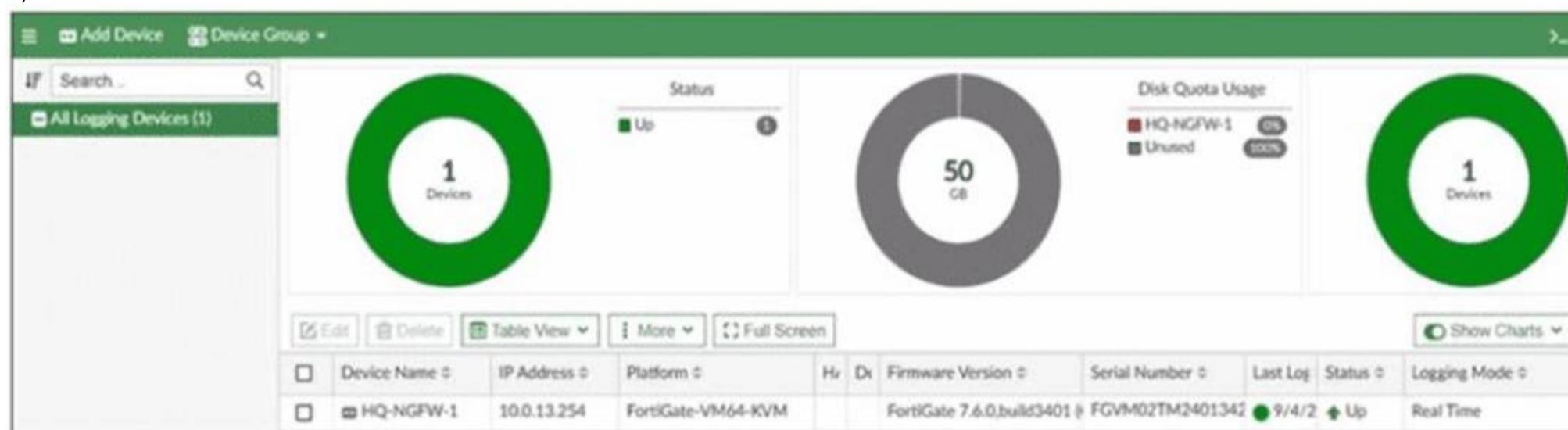
A)



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 12

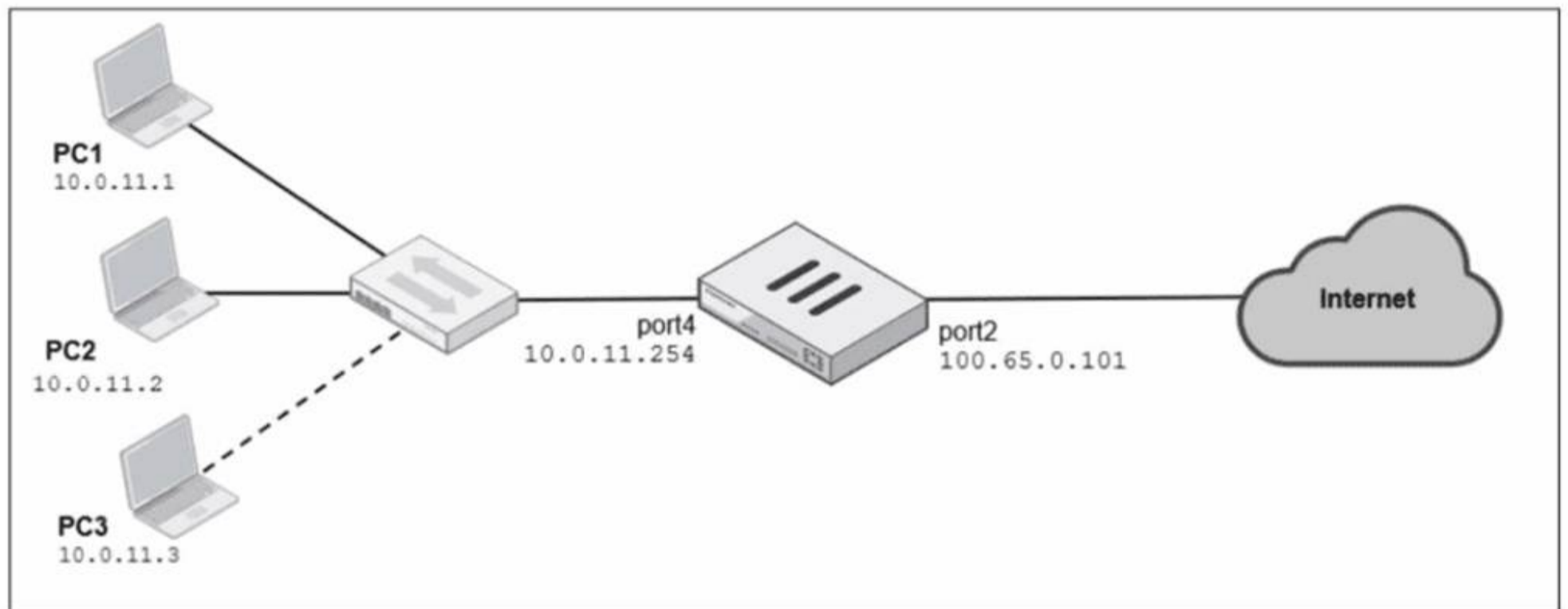
FortiGate is operating in NAT mode and has two physical interfaces connected to the LAN and DMZ networks respectively. Which two statements about the requirements of connected physical interfaces on FortiGate are true? (Choose two.)

- 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 13
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 18

Refer to the exhibit.

```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" eid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=706003401 type="utm" subtype="app-ctrl" level="warning" action="block" sessionid=510 policyid=1 srcip=
10.0.11.50 dstip=54.146.230.62 srcport=53398 dstport=80 proto=6 logid=1059028705 service="HTTP" eventtime=
1756915797391471958 incidentserialno=116391982 direction="outgoing" apprisk="elevated" appid=30220 srcintfrole="undefined"
dstintfrole="undefined" applist="default" appcat="Video/Audio" app="ABC.Com" hostname="abc.go.com" url="/favicon.ico"
eventtype="signature" srcintf="port4" dstintf="port2" msg="Video/Audio: ABC.Com" tz="-0700" policytype="policy"
srccountry="Reserved" dstcountry="United States" poluid="b11ac58c-791b-51e7-4600-12f829a689d9" agent="Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:142.0) Gecko/20100101 Firefox/142.0" httpmethod="GET" referralurl="http://abc.go.com/"
devid="FGVM02TM24013423" vd="root" dtime="2025-09-03 09:09:57" itime_t=1756915802 devname="HQ-NGFW-1"
```

Which two ways can you view the log messages shown in the exhibit? (Choose two.)

- A. By right clicking the implicit deny policy
- B. Using the FortiGate CLI command diagnose log test
- C. By filtering by policy universally unique identifier (UUID) and application name in the log entry
- D. In the Forward Traffic section

Answer: CD

NEW QUESTION 19

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 22

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 23

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE4_FGT_AD-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE4_FGT_AD-7.6-dumps.html