Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator

https://www.2passeasy.com/dumps/NSE4_FGT_AD-7.6/

NEW QUESTION 1
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 2
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 3
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 4
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
```

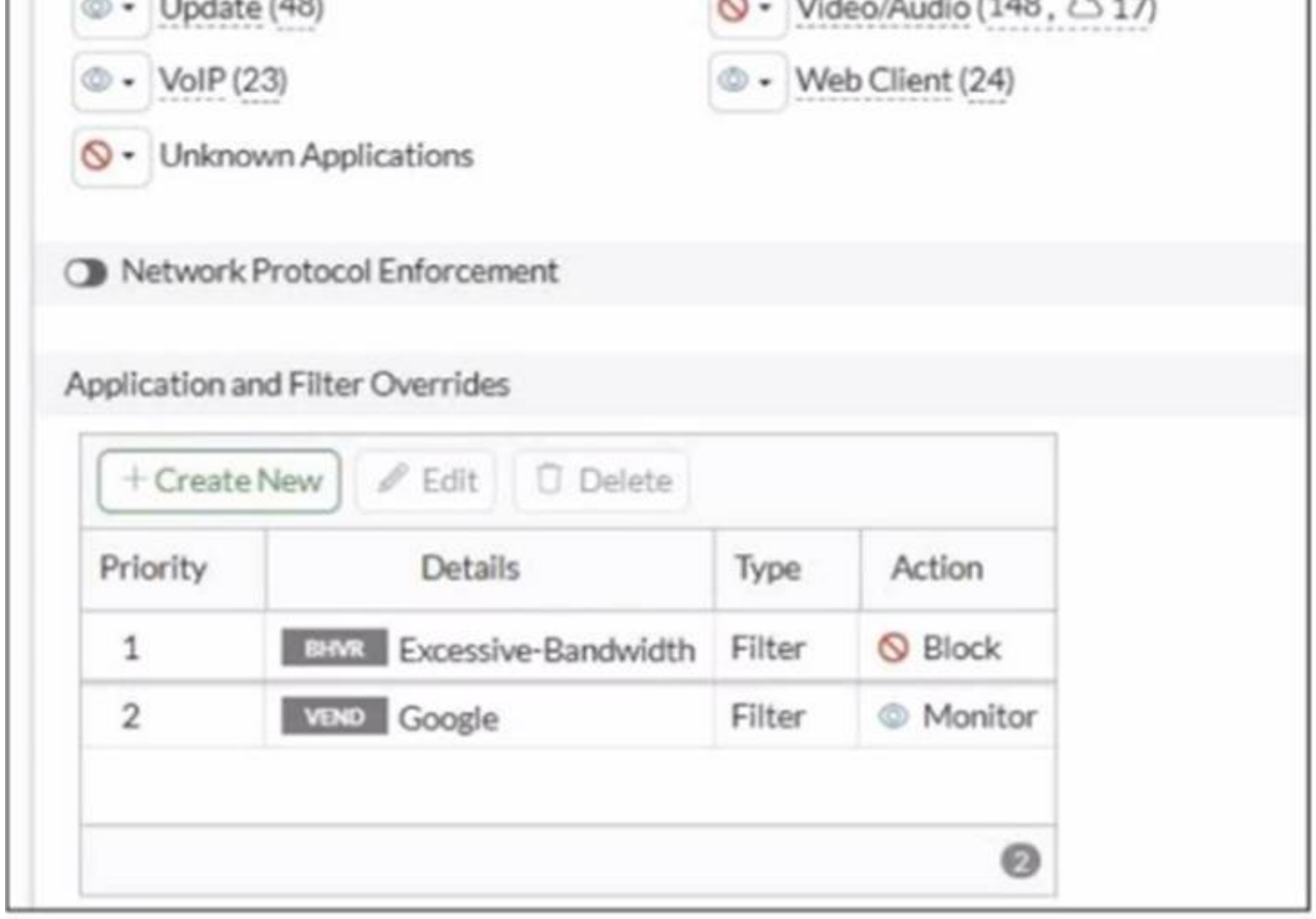
As an administrator you have created an IPS profile, but it is not performing as expected. While testing you got the output as shown in the exhibit What could be the possible reason of the diagnose output shown in the exhibit?

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.

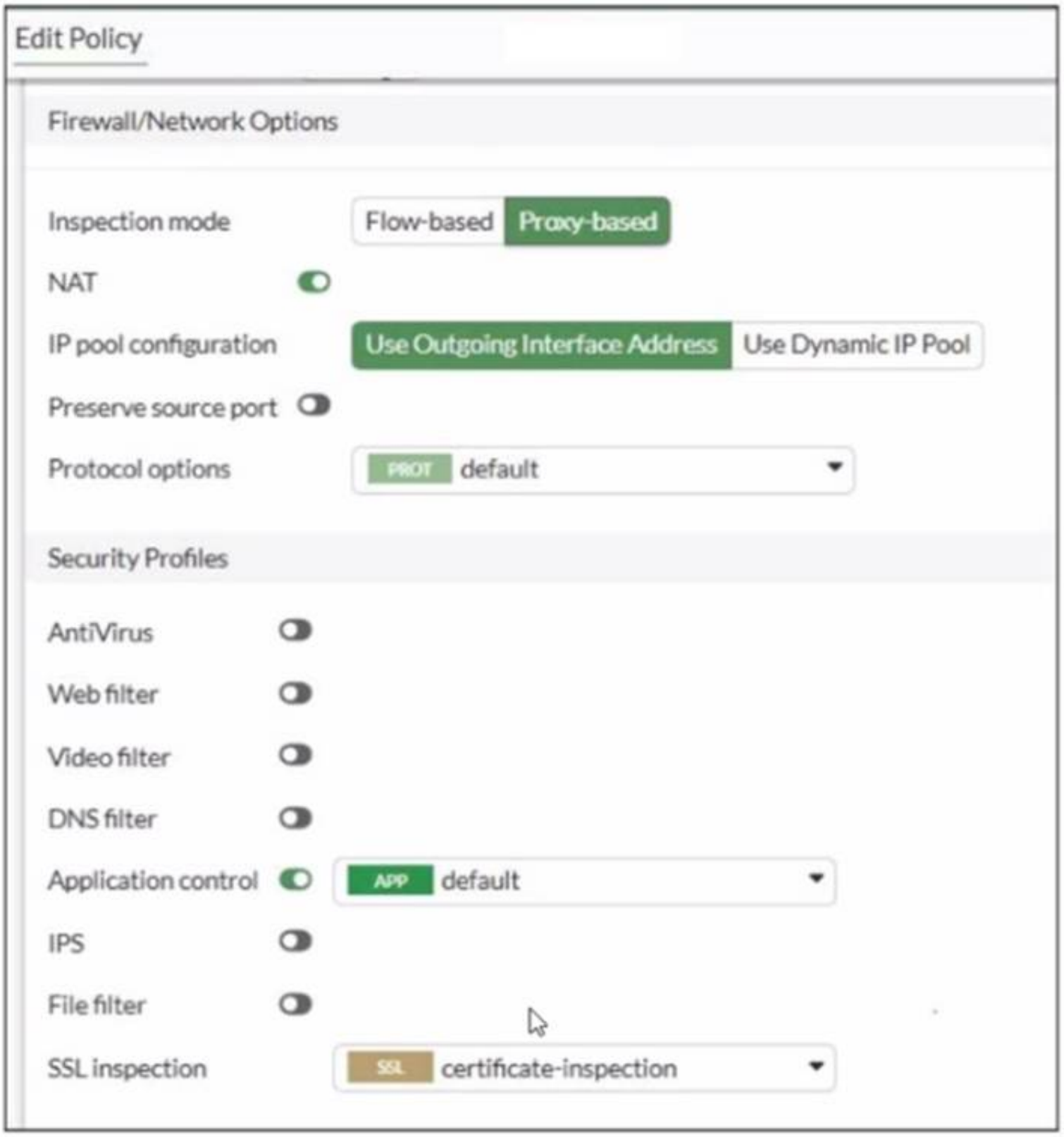
Answer: A

NEW QUESTION 5
Refer to the exhibits.

Application sensor



Firewall policy



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 6
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 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
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.

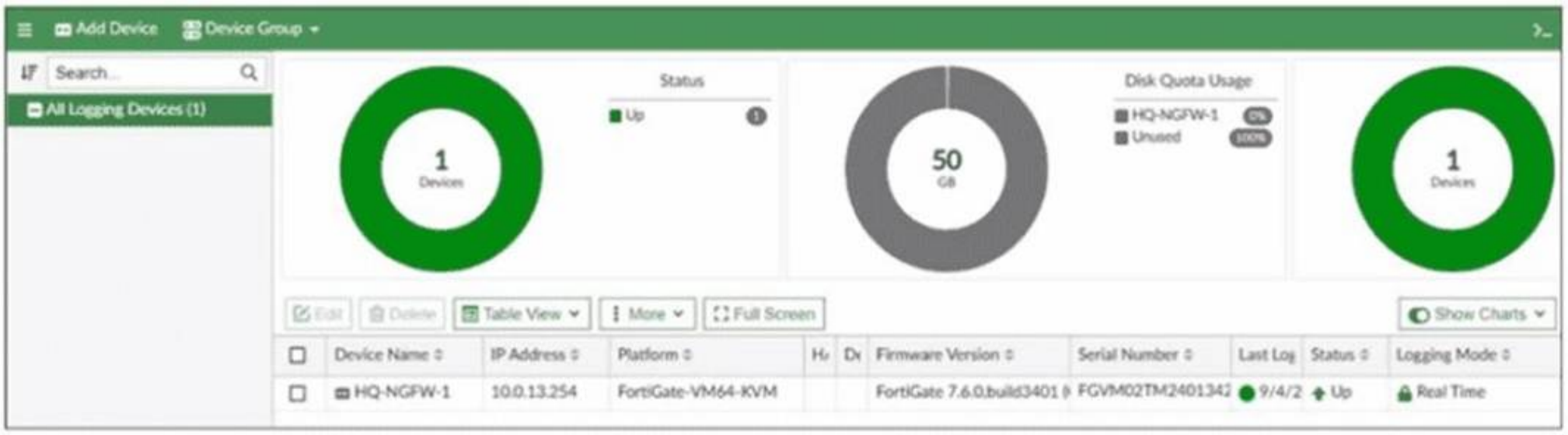
Answer: CDE

NEW QUESTION 9
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

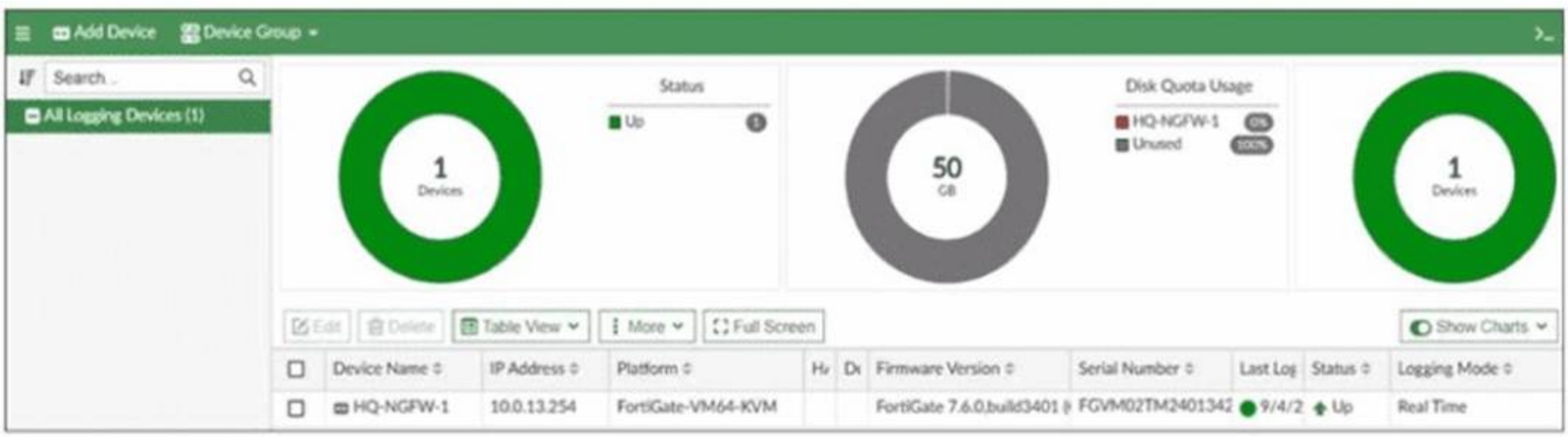
NEW QUESTION 10
The FortiGate device HQ-NGFW-1 with the IP address 10.0.13.254 sends logs to the FortiAnalyzer device with the IP address 10.0.13.125. The administrator wants to verify that reliable logging is enabled on HQ-NGFW-1.
Which exhibit helps with the verification?
A)



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

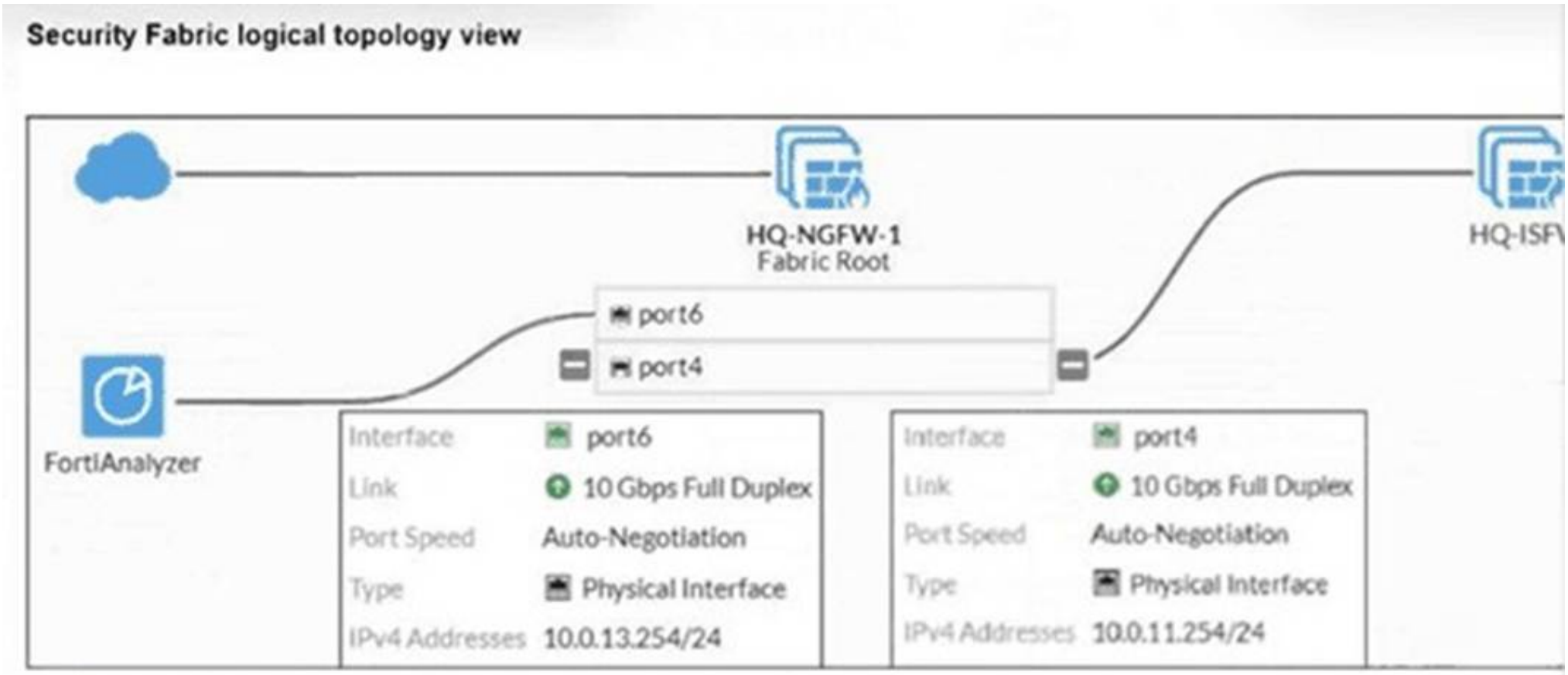
Answer: B

NEW QUESTION 10
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?

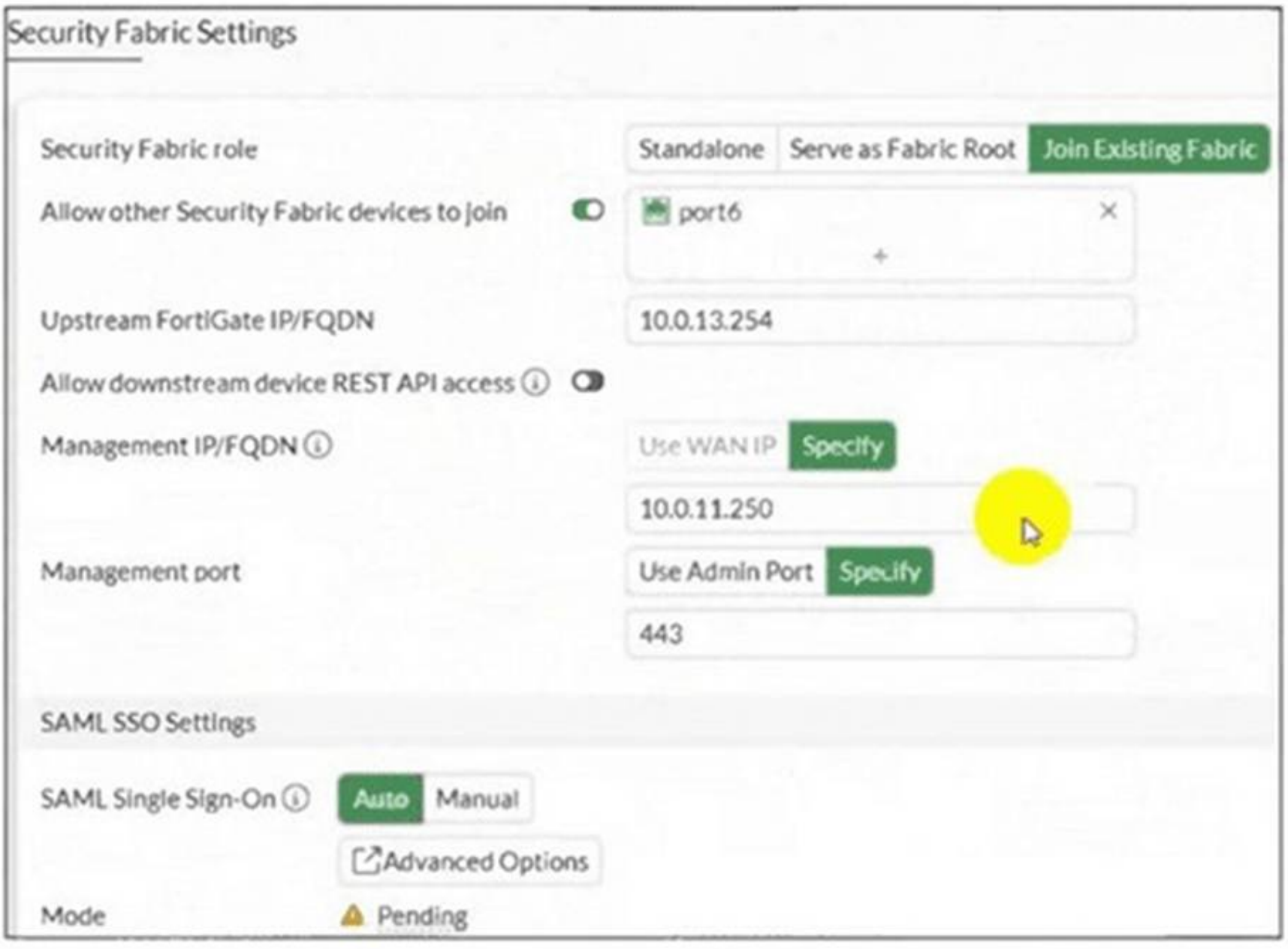
A. The web filter profile is already referenced in another firewall policy.
B. The firewall policy is in no-inspection mode instead of deep-inspection.
C. The naming convention used in the web filter profile is restricting it in the firewall policy.
D. The inspection mode in the firewall policy is not matching with web filter profile feature set.

Answer: D

NEW QUESTION 12
Refer to the exhibits.



Security Fabric settings on HQ-ISFW-2



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 14
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.

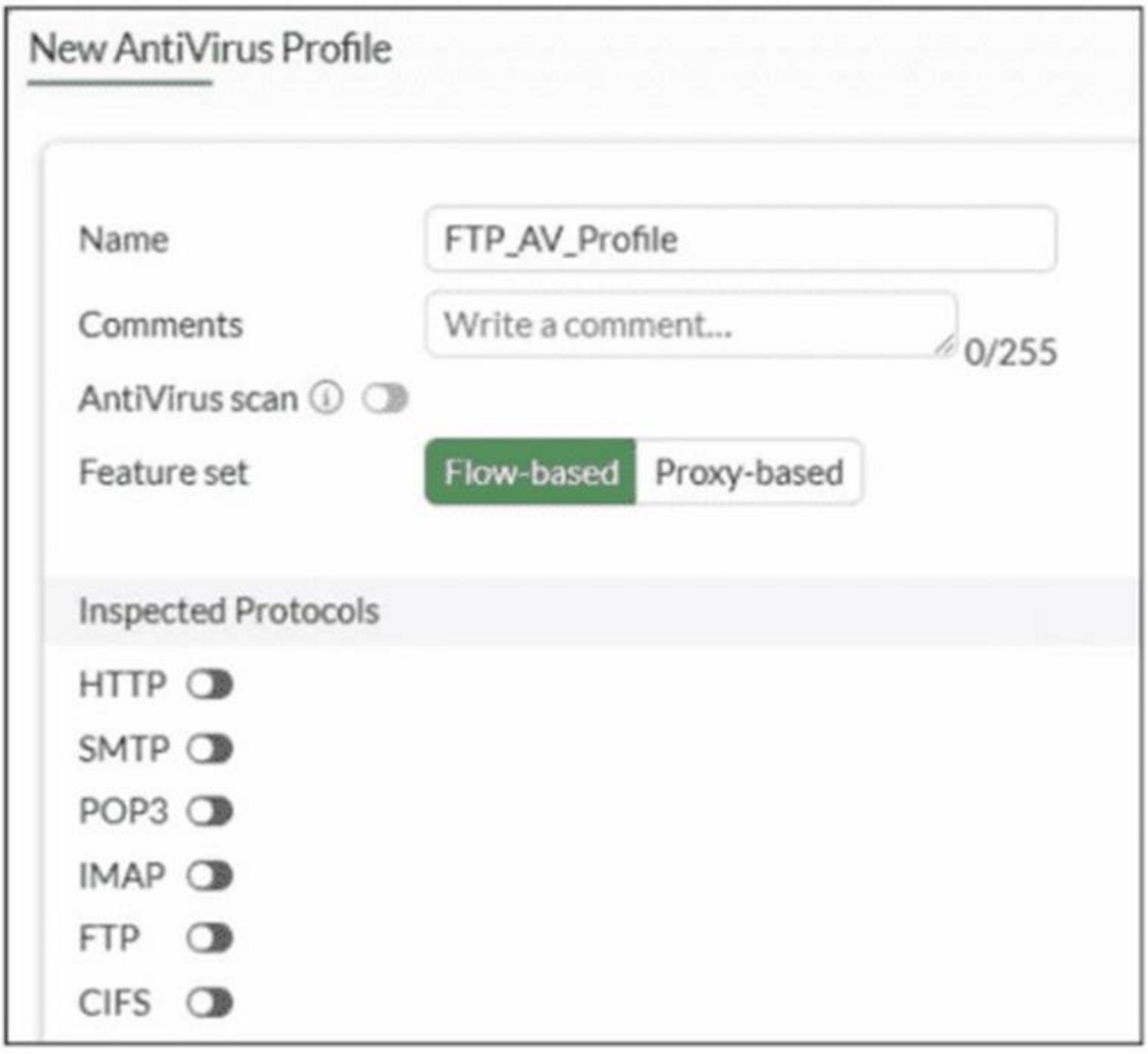
Answer: CD

NEW QUESTION 15
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 20
Refer to the exhibit.



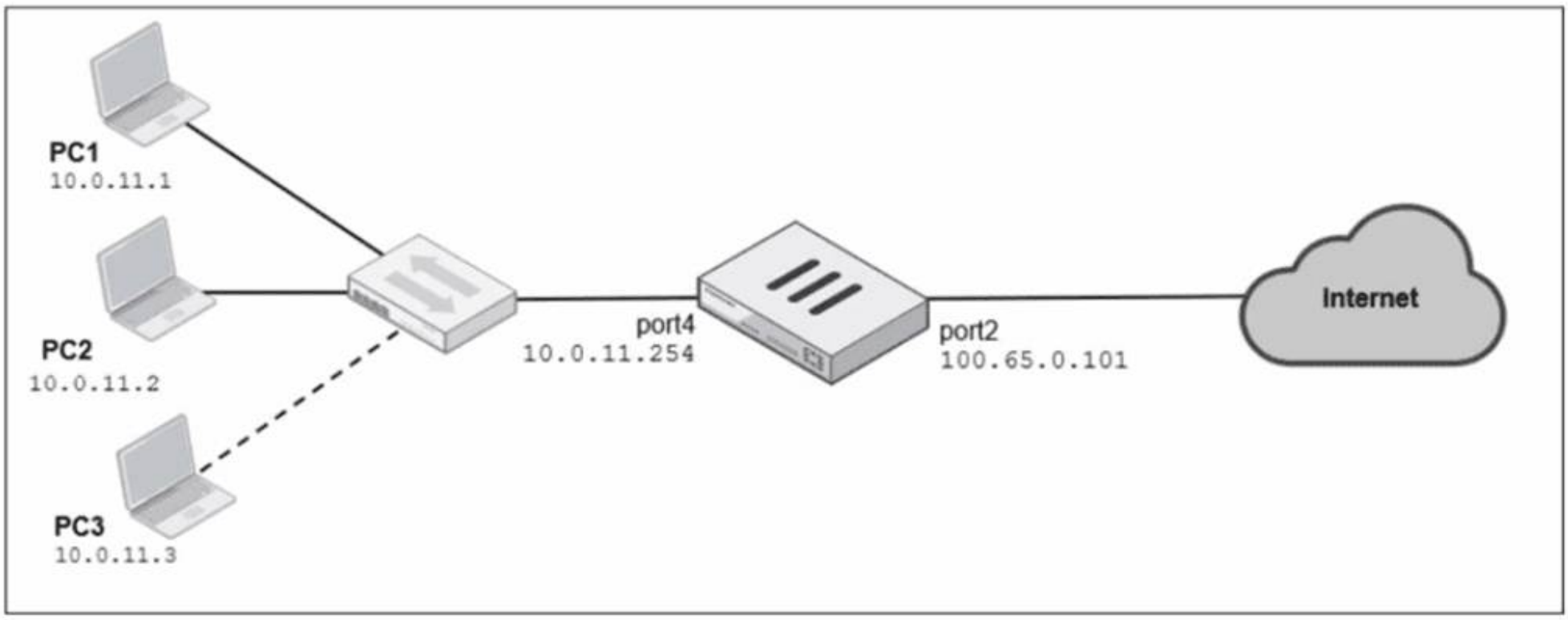
Why is the Antivirus scan switch grayed out when you are creating a new antivirus profile for FTP?

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.

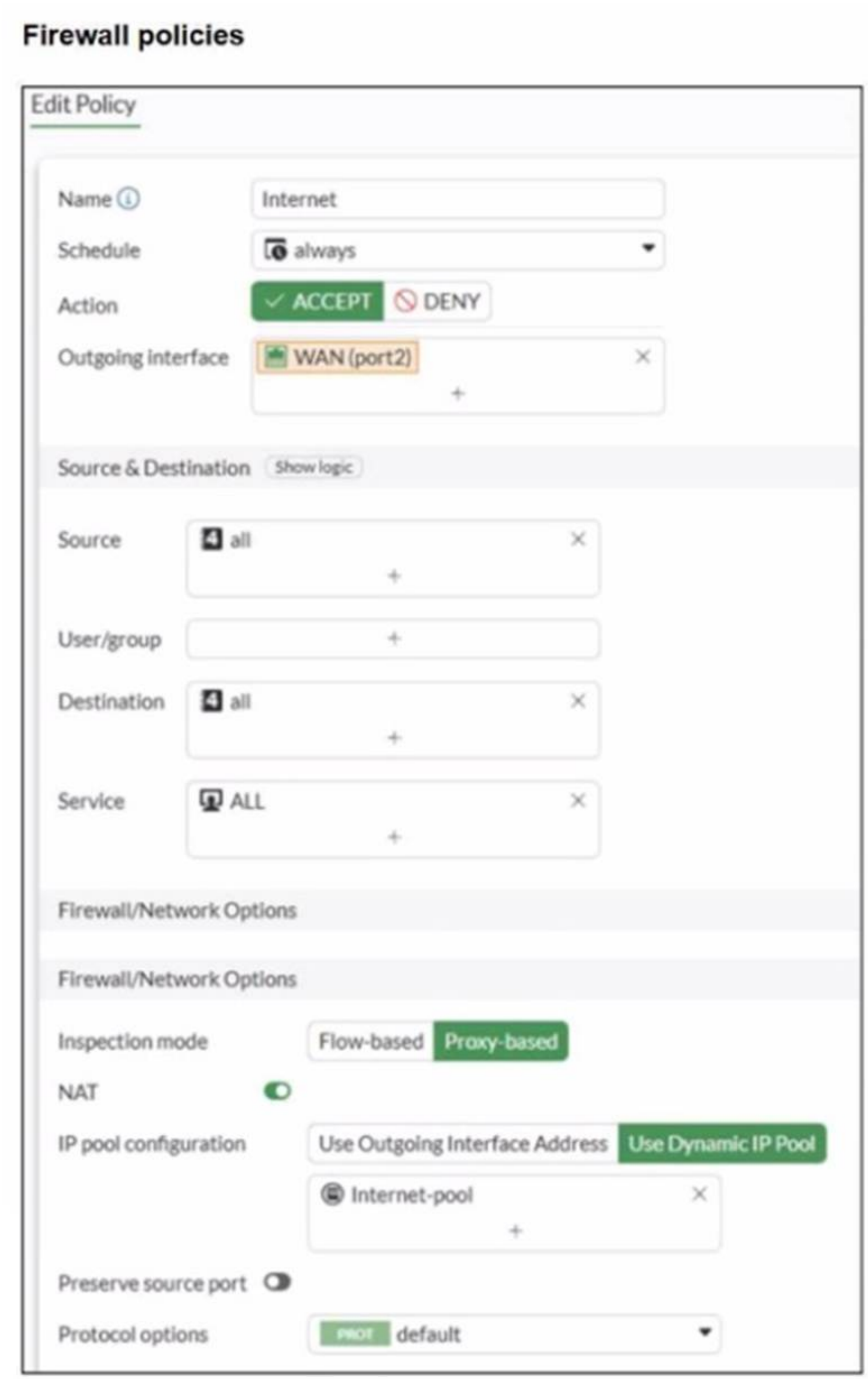
Answer: B

NEW QUESTION 23
Refer to the exhibits.

Network diagram



Dynamic IP pool



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 ipto 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 26
Refer to the exhibit.

```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" euid=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" poluuid="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 31
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 32
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The collector agent uses a Windows API to query DCs for user logins.
B. The NetSessionEnum function is used to track user logouts.
C. NetAPI polling can increase bandwidth usage in large networks.
D. The collector agent must search Windows application event logs.

Answer: B

NEW QUESTION 35
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 36
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4_FGT_AD-7.6 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4_FGT_AD-7.6 Product From:

https://www.2passeasy.com/dumps/NSE4_FGT_AD-7.6/

Money Back Guarantee

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