Fortinet

Exam Questions NSE4_FGT_AD-7.6

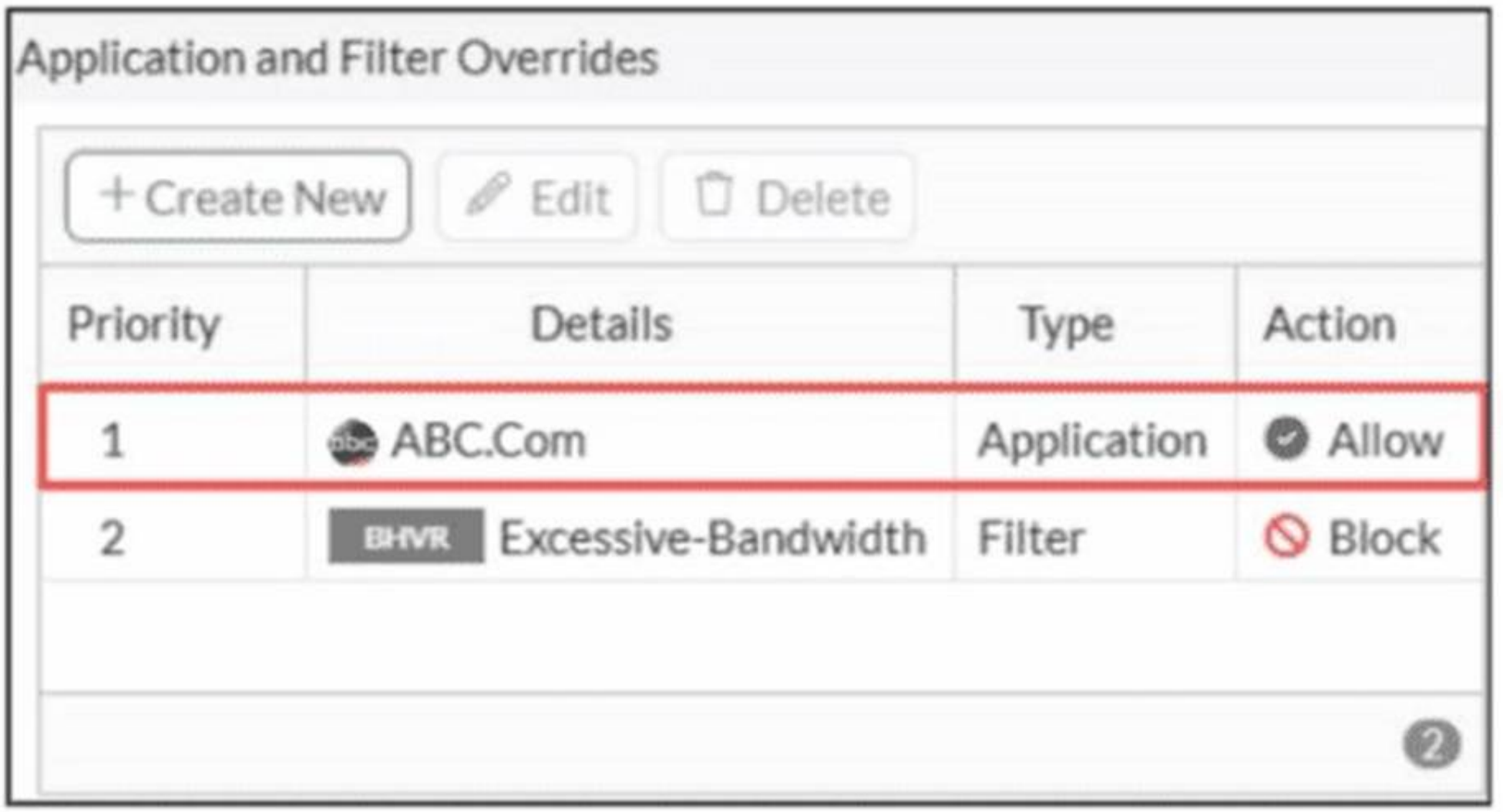
Fortinet NSE 4 - FortiOS 7.6 Administrator

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.

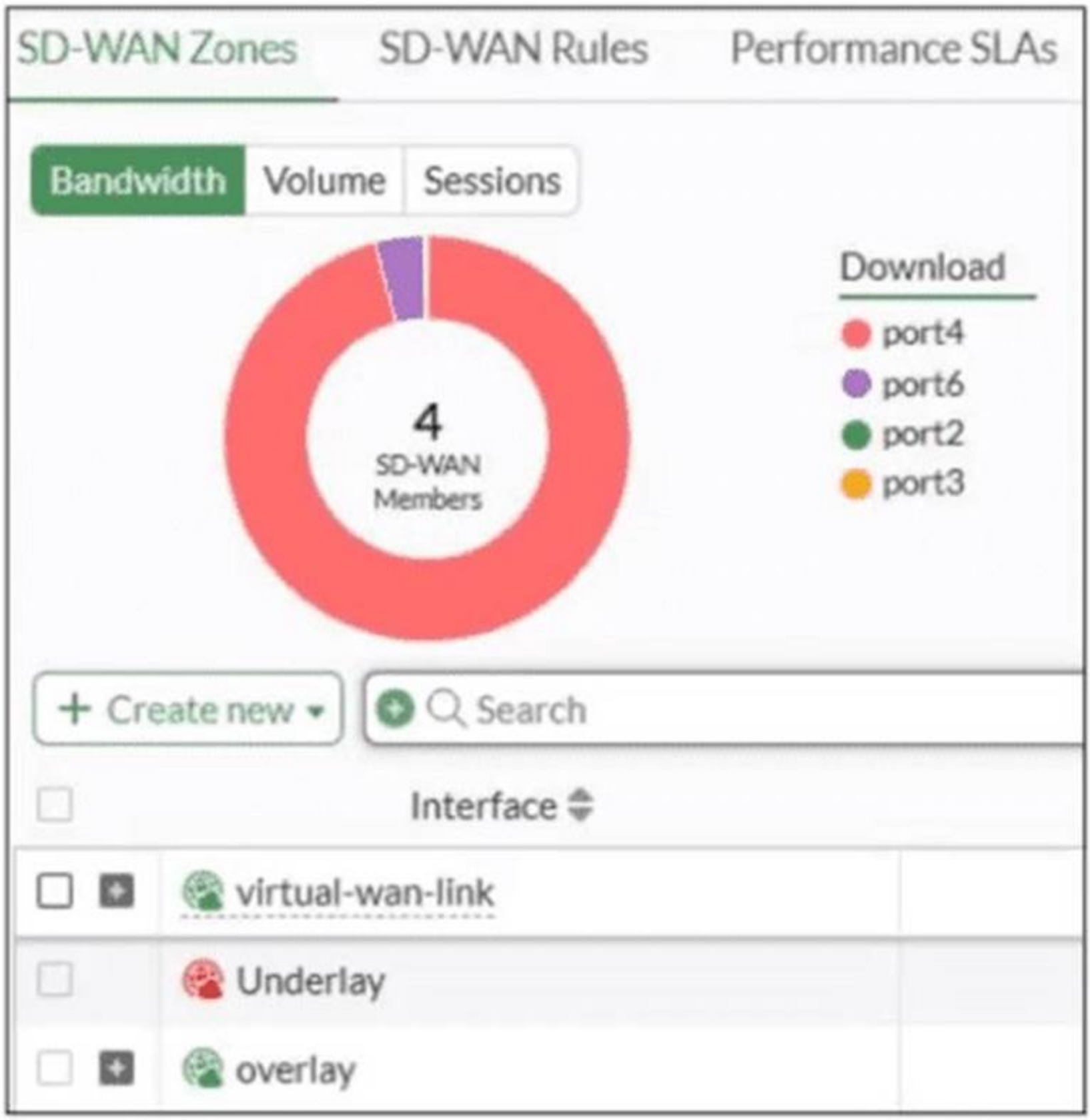


An administrator has configured an Application Overrides for the ABC.Com application signature and set the Action to Allow This application control profile is then applied to a firewall policy that is scanning all outbound traffic. Logging is enabled in the firewall policy. To test the configuration,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



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 4
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-ffffffffa002c9c7
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 5
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 6
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 porti will be exempted from RPF checks.
B. FortiGate will enable strict RPF on all its interfaces and porti 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 7
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

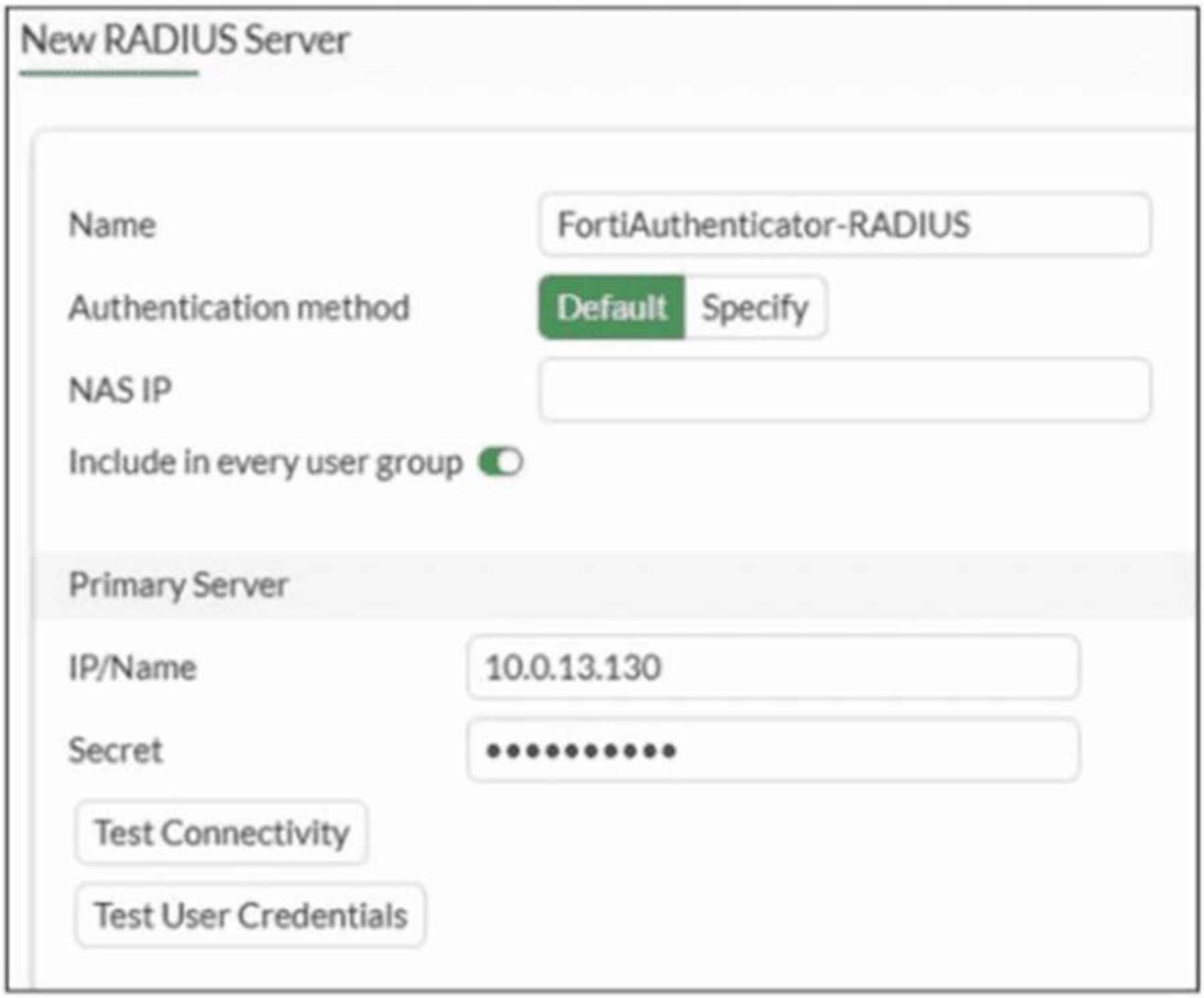
Answer: ABD

NEW QUESTION 8
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 9
Refer to the exhibit.
A RADIUS server configuration is shown.



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 10
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

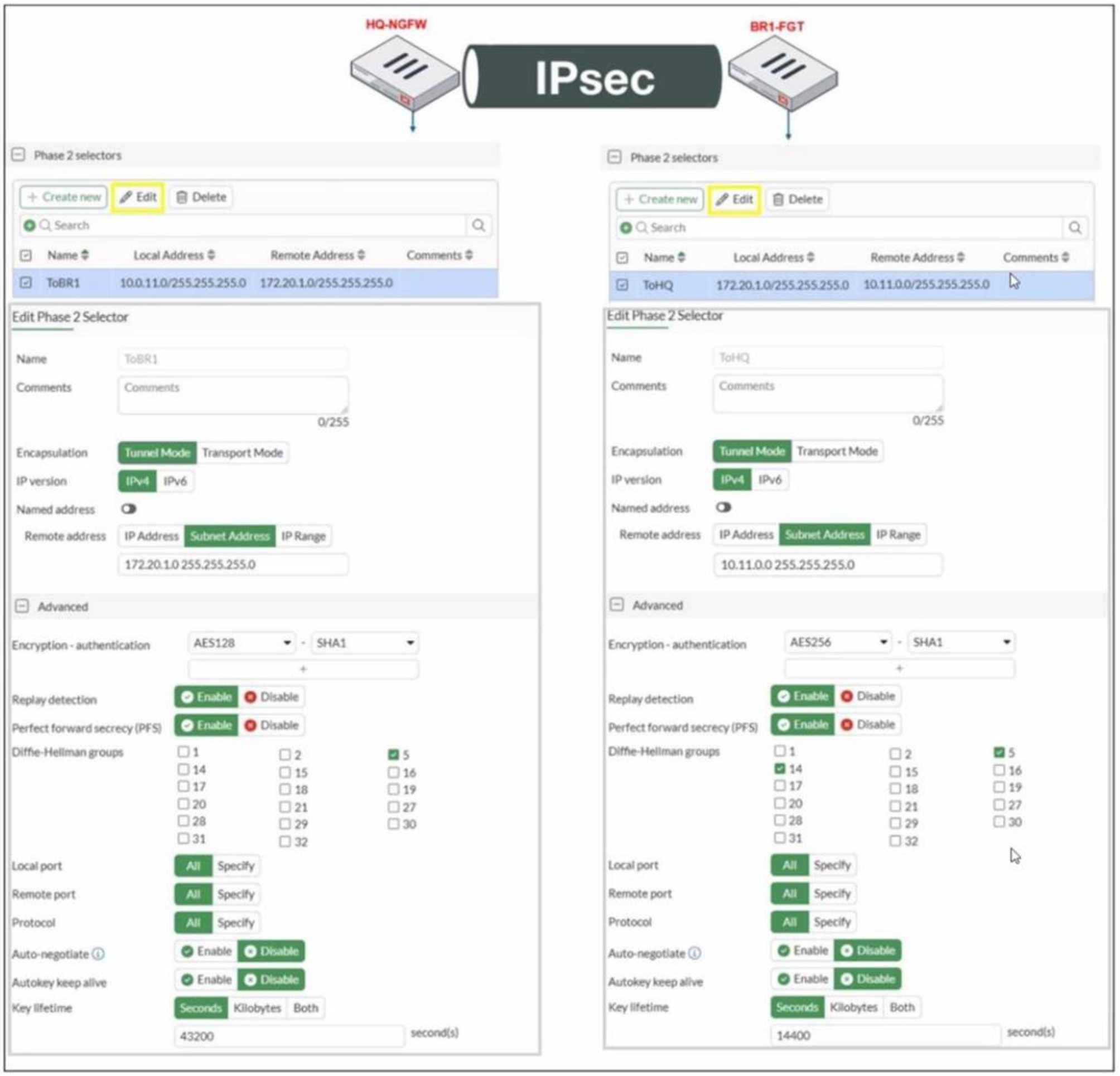
Answer: B

NEW QUESTION 10
An administrator manages a FortiGate model that supports NTurbo How does NTurbo acceleration enhance antivirus performance?

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

Answer: A

NEW QUESTION 12
Refer to the exhibit.



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.

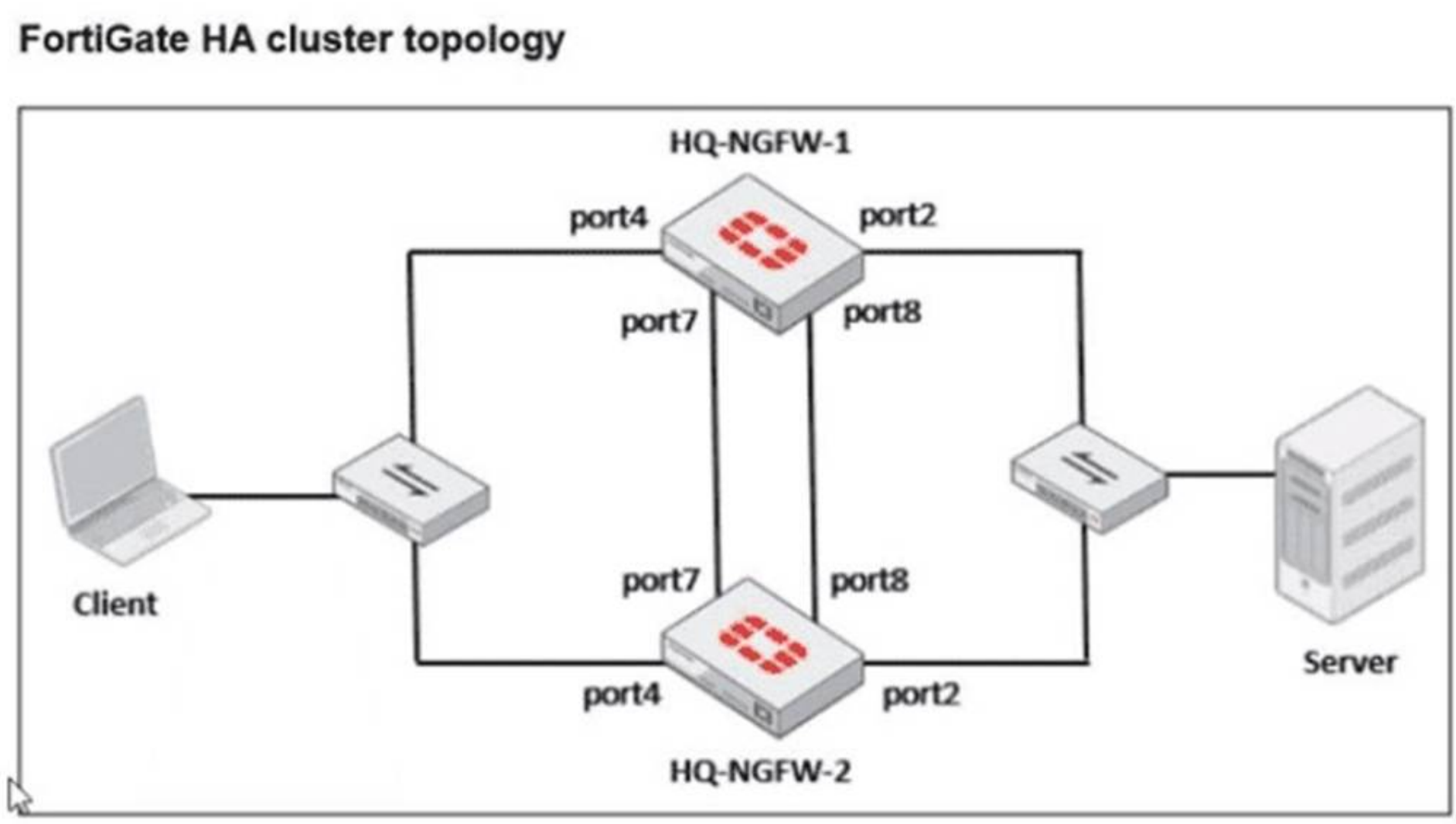
Answer: AD

NEW QUESTION 15
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 20
Refer to the exhibits.



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 21
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 26

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

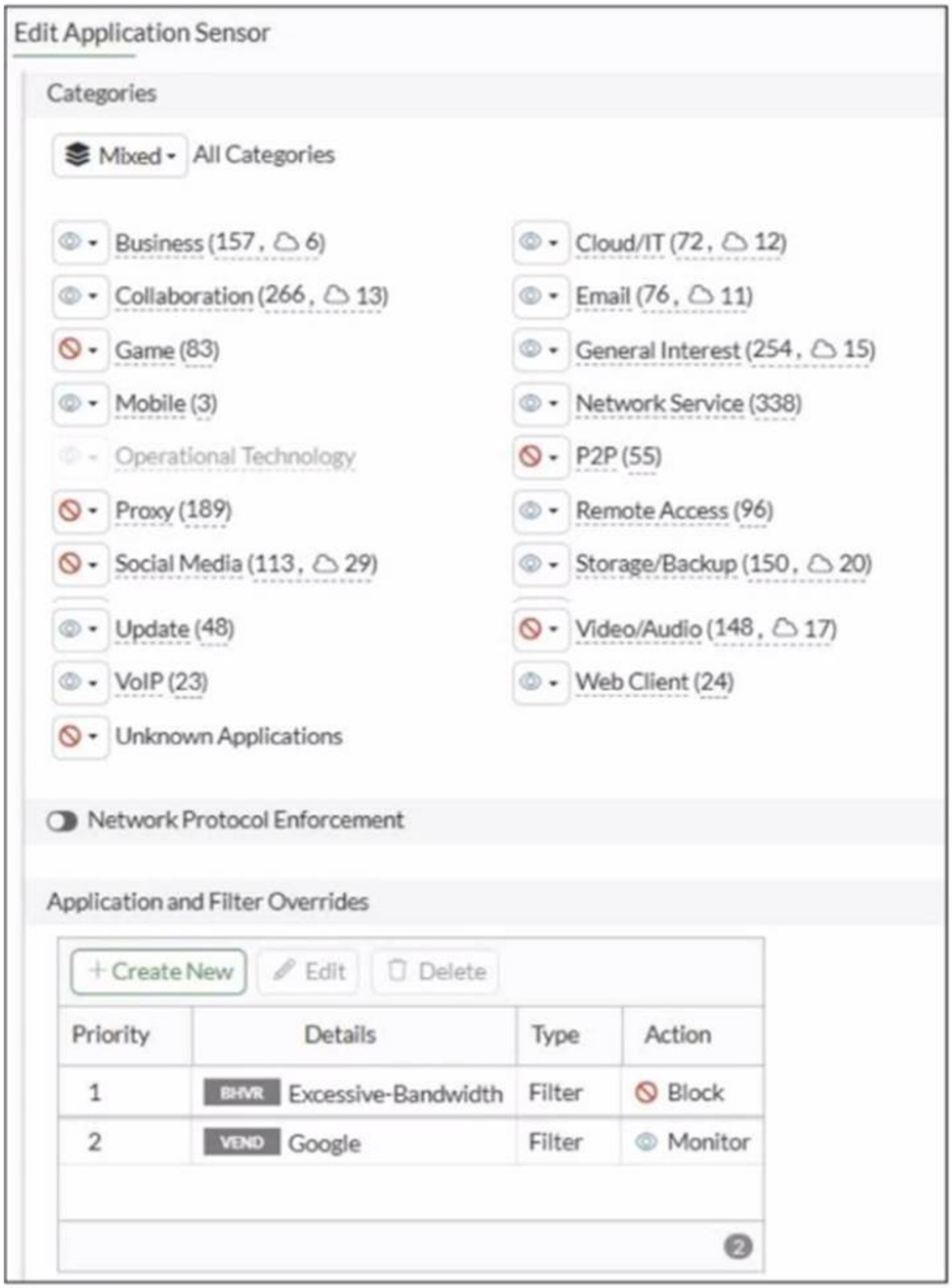
Based on the routing table shown in the exhibit, which two statements are true? (Choose two.)

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.

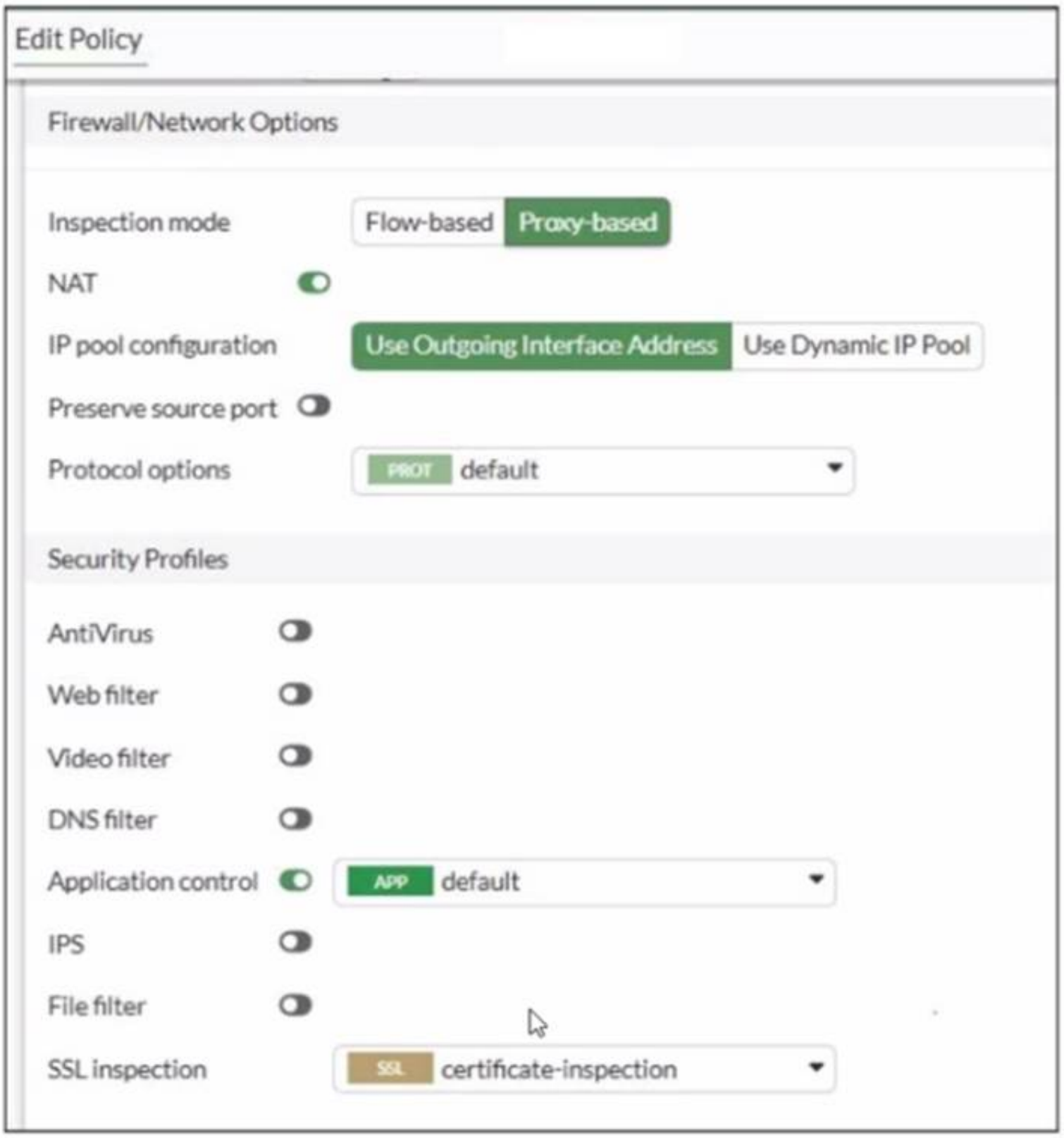
Answer: AC

NEW QUESTION 27
Refer to the exhibits.

Application sensor



Firewall policy



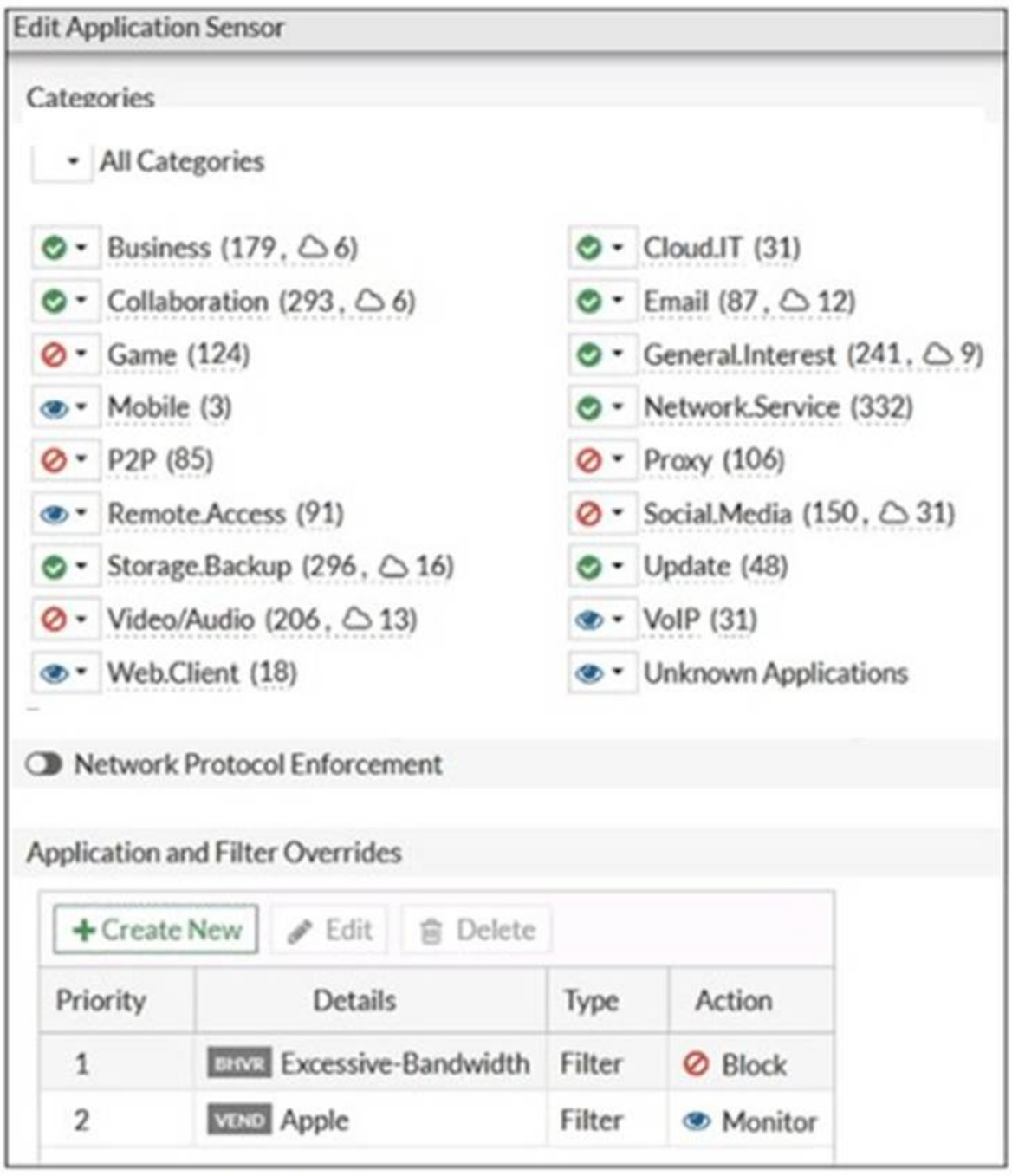
You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits.
You cannot access any of the Google applications, but you are able to access www.fortinet.com.
Which two actions would you take to resolve the issue? (Choose two.)

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

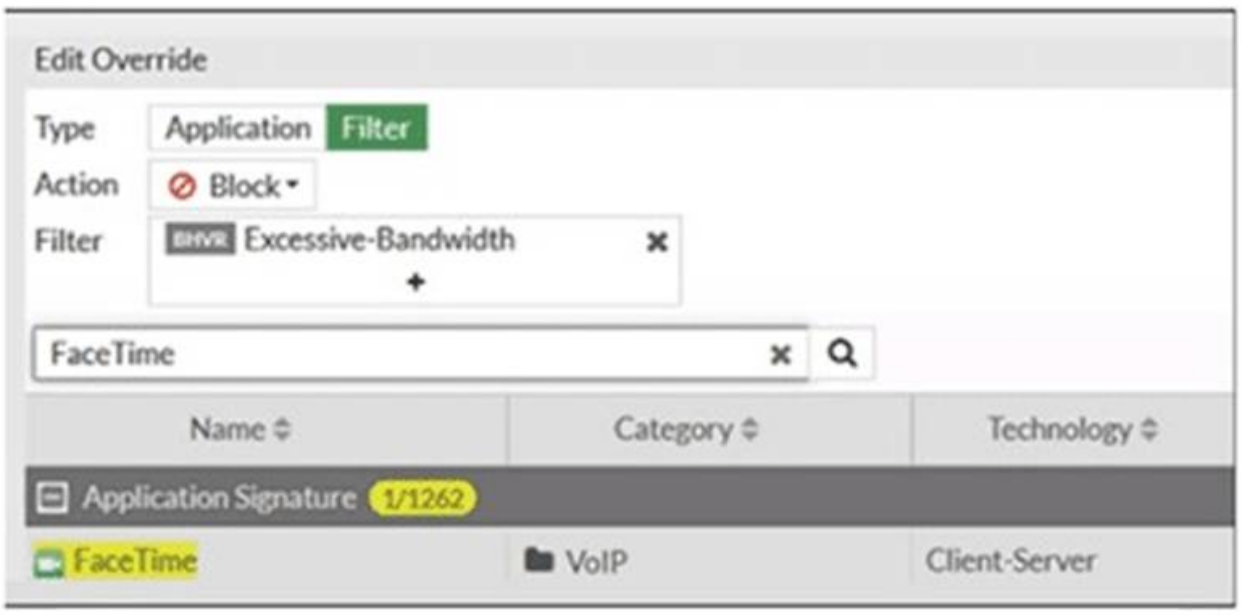
Answer: BE

NEW QUESTION 30
Refer to the exhibits.

Application sensor configuration



Application override configuration



Filter override configuration

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

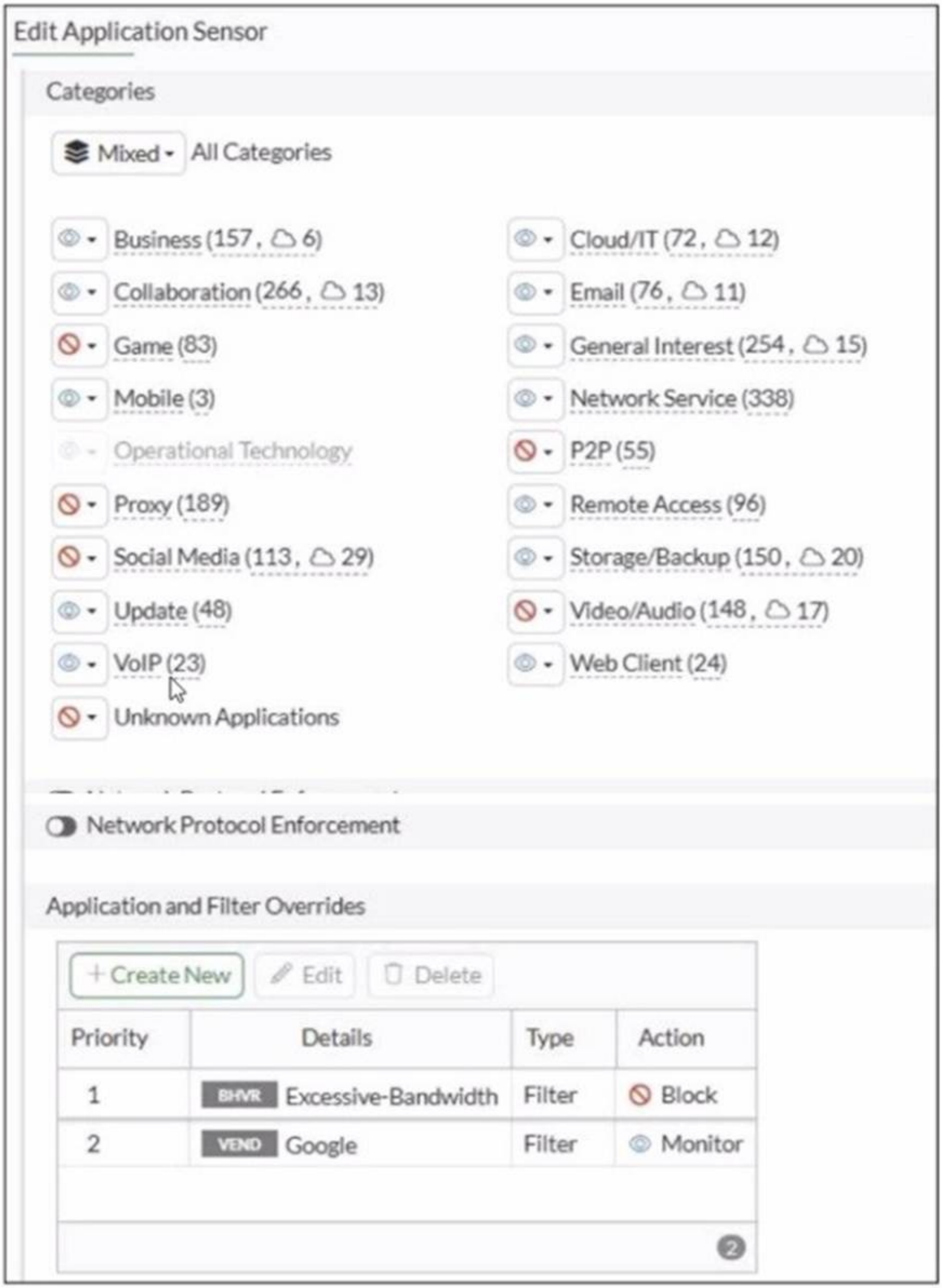
NEW QUESTION 35
Which two statements are true about an HA cluster? (Choose two answers)

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.

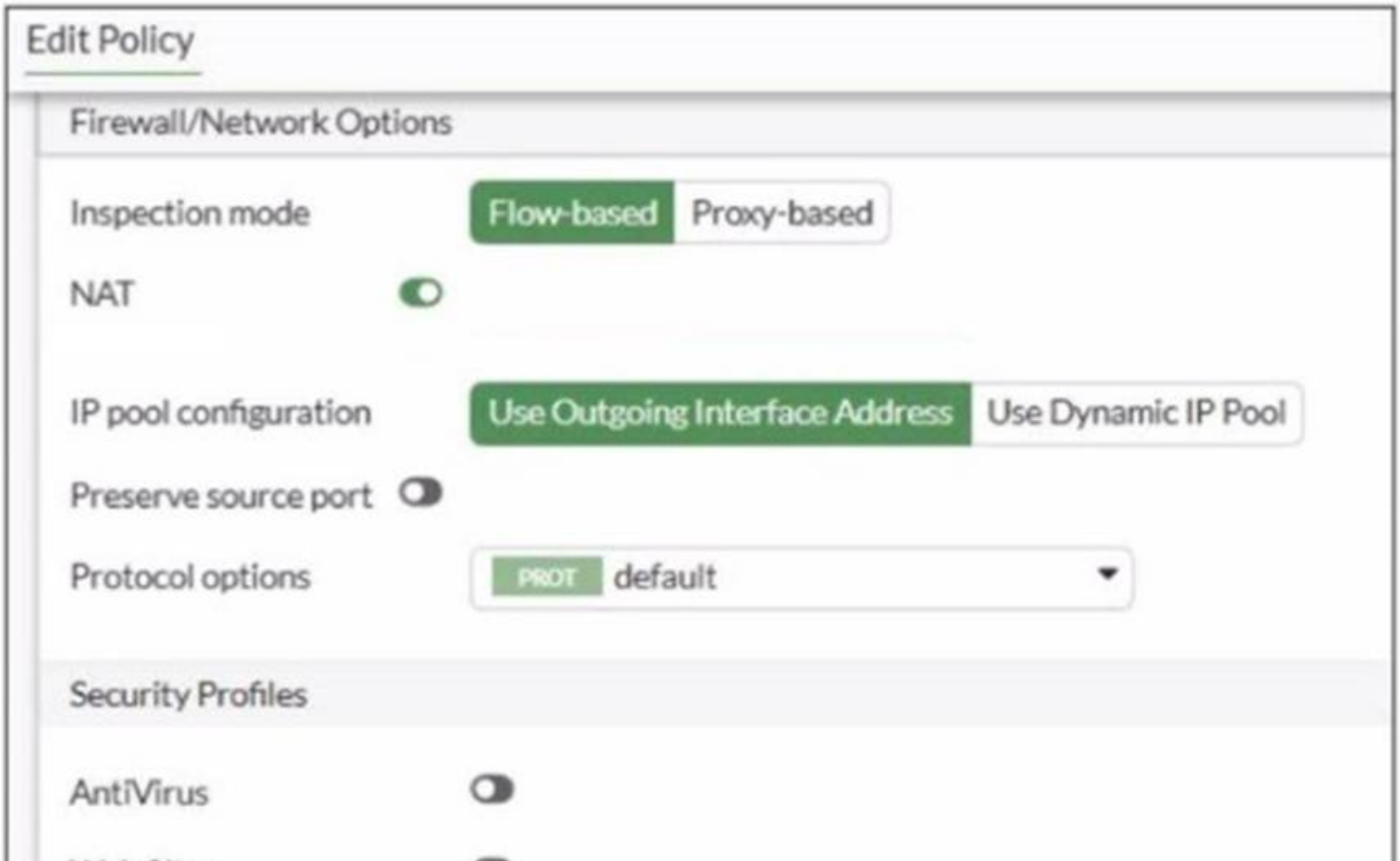
Answer: BD

NEW QUESTION 36
Refer to the exhibits.

Application sensor



Firewall policy



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 41
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 44
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 48
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 53
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 54
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.

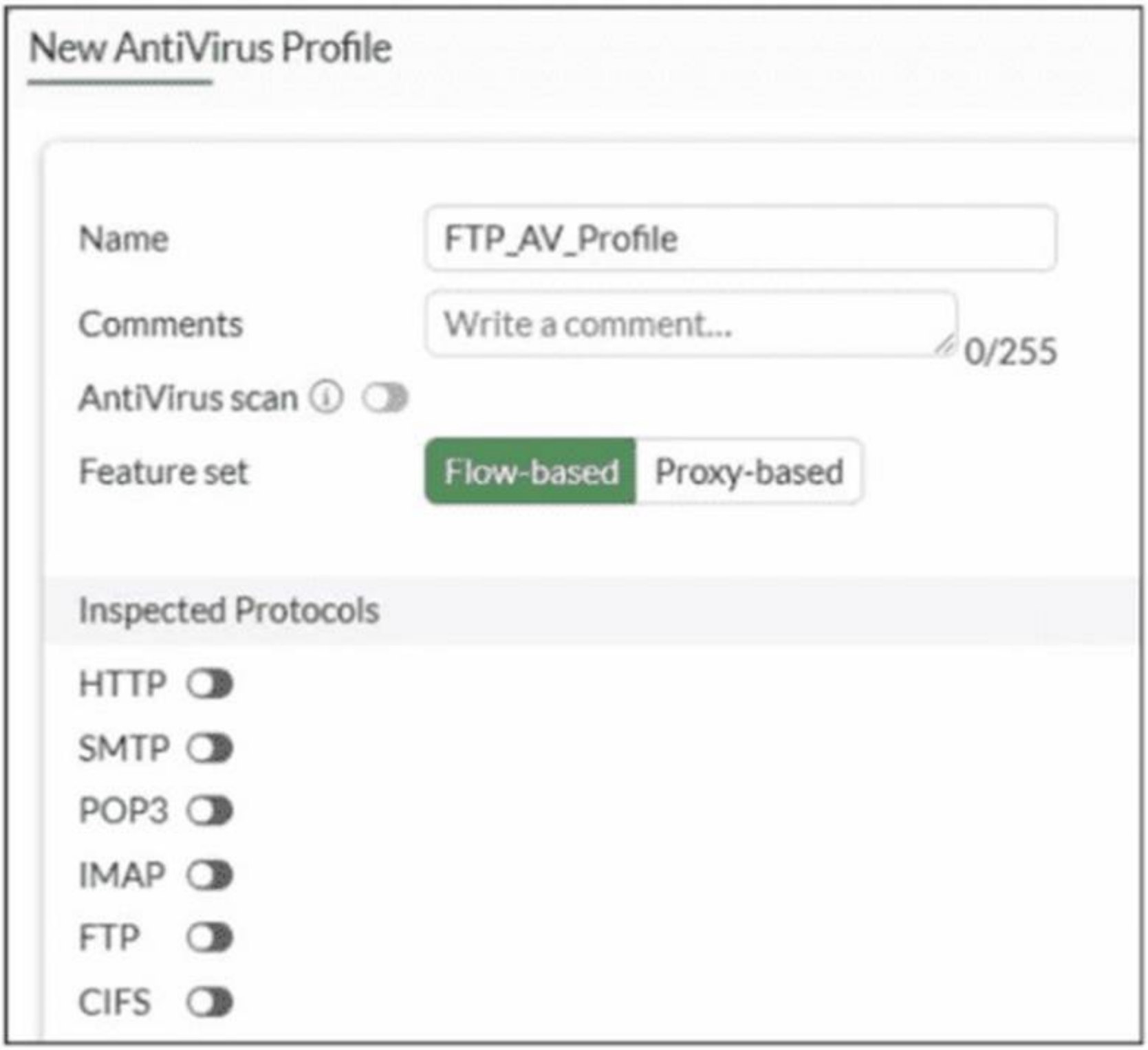
Answer: AC

NEW QUESTION 58
A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.
What is the reason for the certificate warning errors?

A. The option invalid SSL certificates is set to allow on the SSL/SSH inspection profile.
B. The matching firewall policy is set to proxy inspection mode.
C. The browser does not trust the certificate used by FortiGate for SSL inspection.
D. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.

Answer: C

NEW QUESTION 60
Refer to the exhibit.



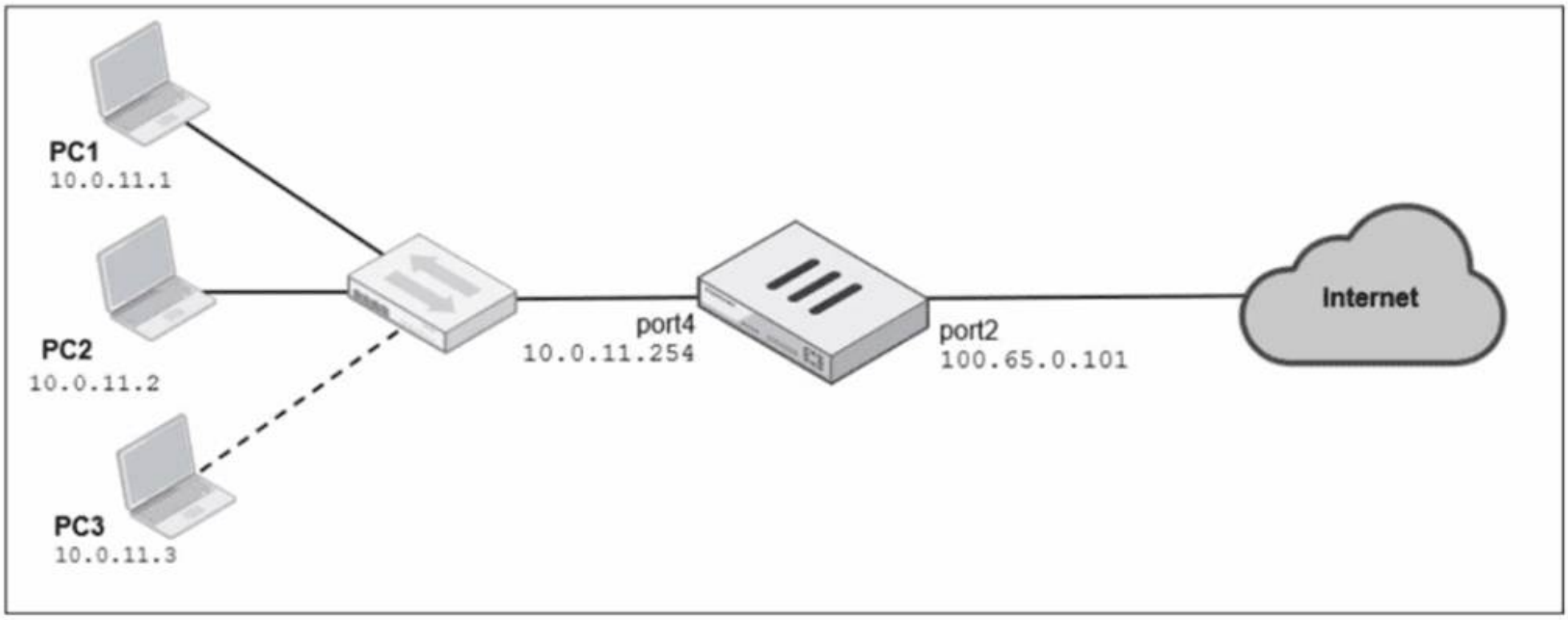
Why is the Antivirus scan switch grayed out when you are creating a new antivirus profile for FTP?

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.

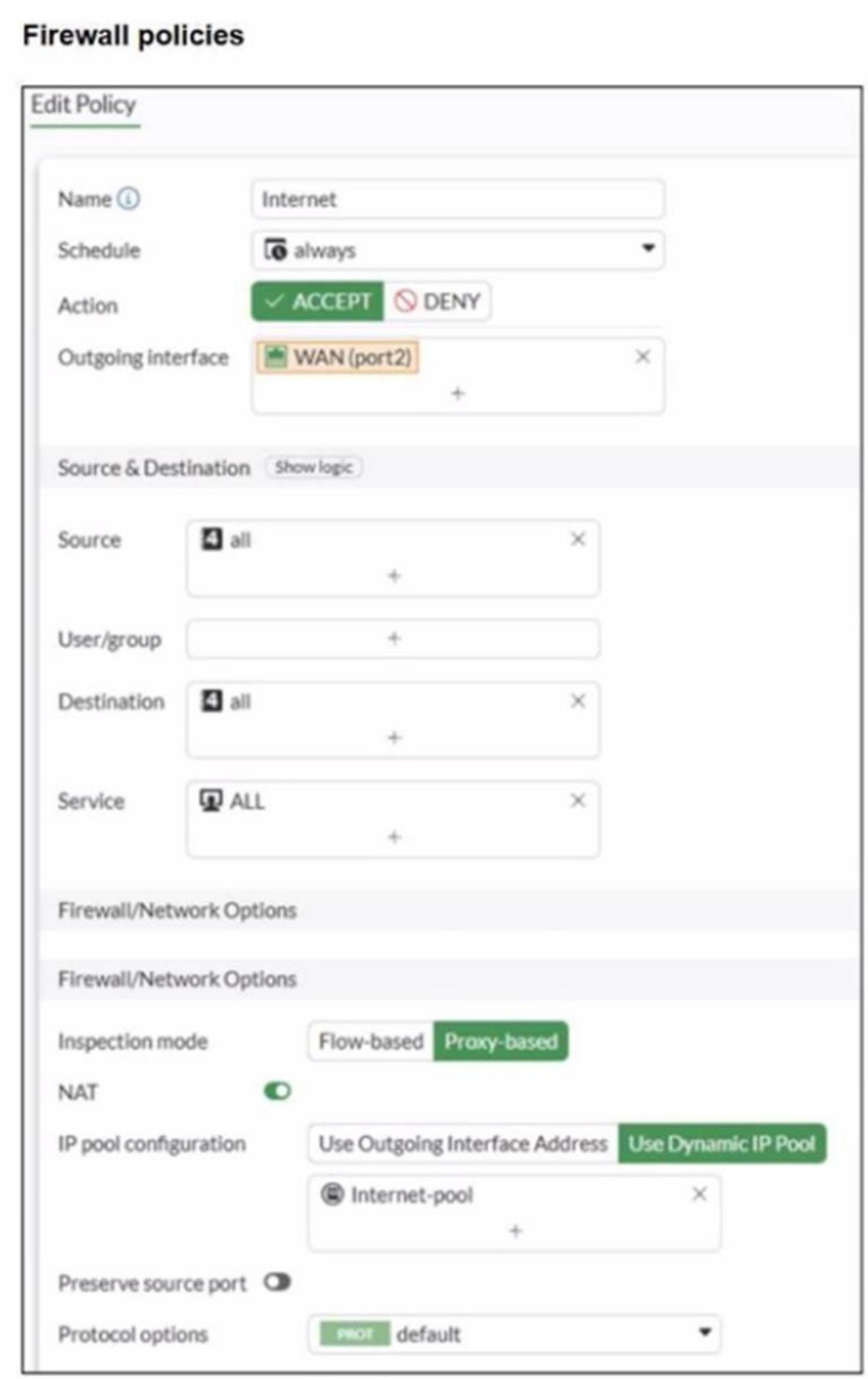
Answer: B

NEW QUESTION 65
Refer to the exhibits.

Network diagram



Dynamic IP pool



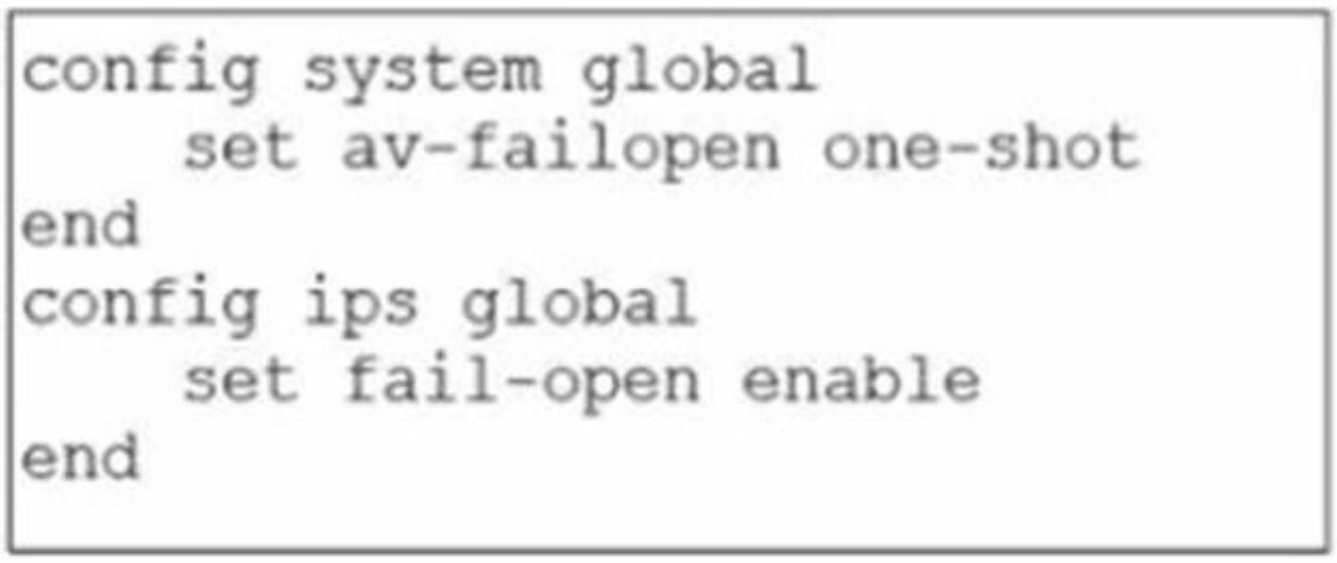
A diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device are shown.
Two PCs. PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (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 66
Refer to the exhibit.



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 67
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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