Fortinet

Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator

NEW QUESTION 1
Refer to the exhibit.

```
FortiGate # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract
\
Num. of servers : 1
Protocol        : https
Port            : 8888
Anycast         : Disable
Default servers : Not included

-=- Server List (Wed Sep 20 09:22:42 2023) -=-

IP                    Weight    RTT Flags   TZ   FortiGuard-requests  Curr Lost Total Lost             Updated Time
10.0.1.241              -244      2 I        0                   122          0          0 Wed Sep 20 09:21:55 2023
```

Which two statements about the FortiGuard connection are true? (Choose two.)

A. The weight increases as the number of failed packets rises
B. You can configure unreliable protocols to communicate with FortiGuard Server.
C. FortiGate identified the FortiGuard Server using DNS lookup.
D. FortiGate is using the default port for FortiGuard communication.

Answer: AD

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-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 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 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 5
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 6
Refer to the exhibit.

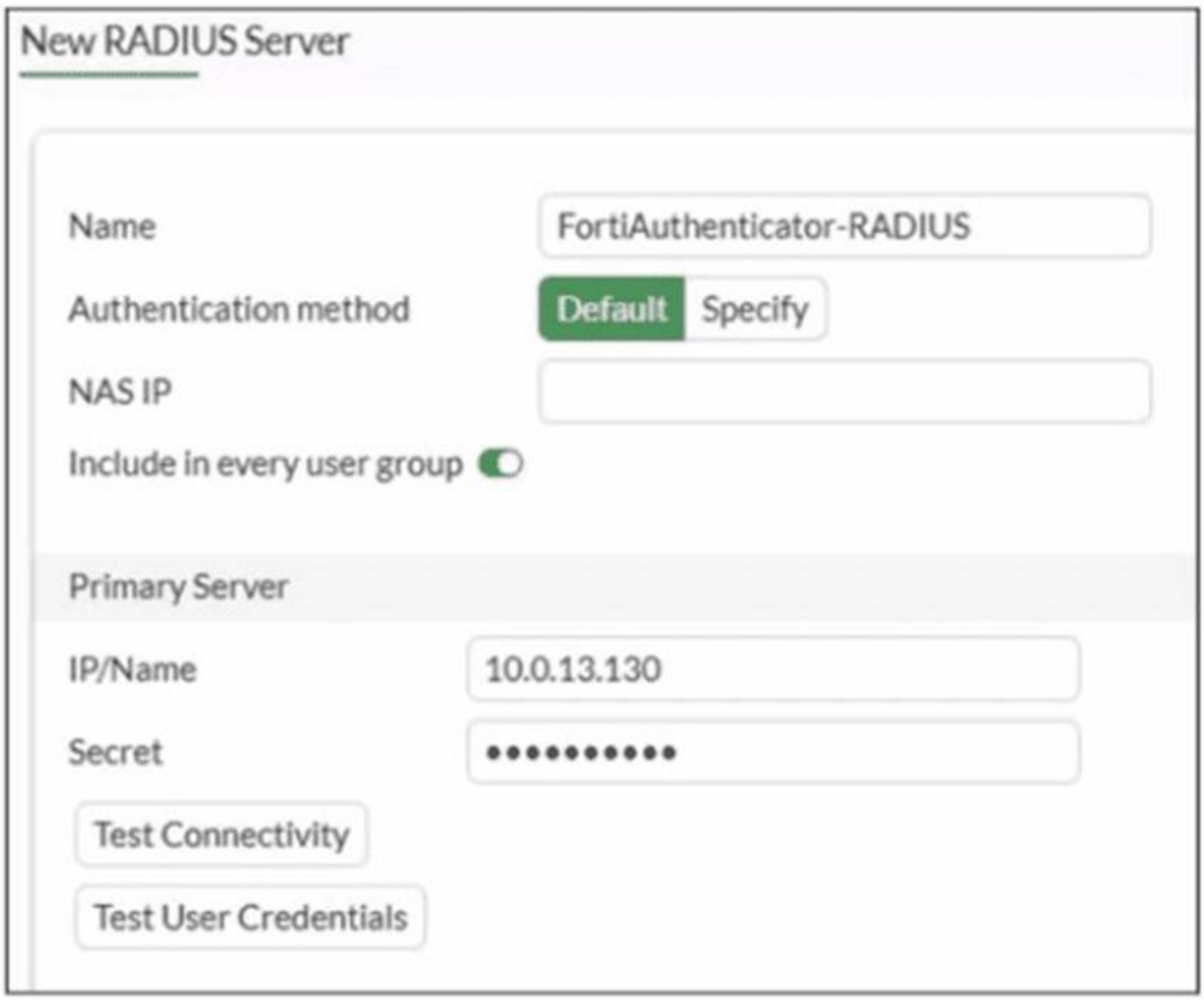
Profile Name
Monitoring_Access
NOC_Access
prof_admin
super_admin

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 7
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 8
Which two statements describe characteristics of automation stitches? (Choose two answers)

A. Actions involve only devices included in the Security Fabric.
B. An automation stitch can have multiple triggers.
C. Multiple actions can run in parallel.
D. Triggers can involve external connectors.

Answer: CD

NEW QUESTION 9
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.

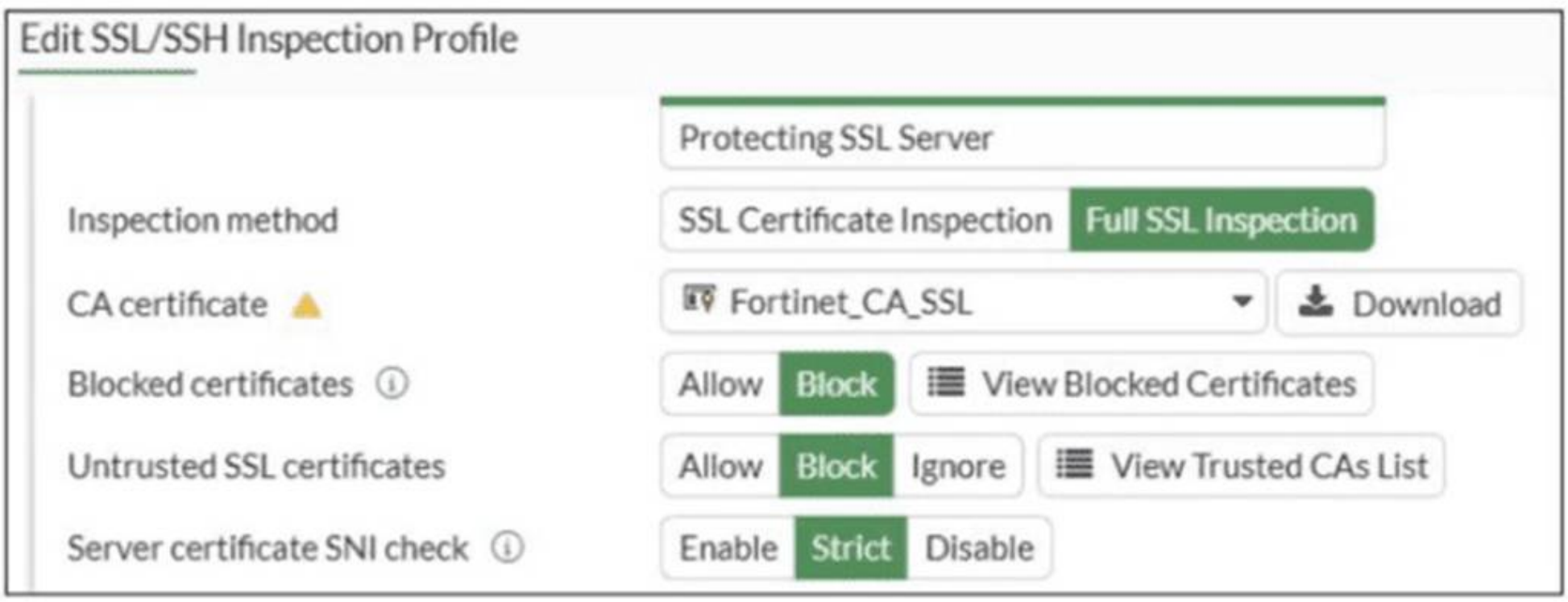
Answer: A

NEW QUESTION 10
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 exhibit.



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

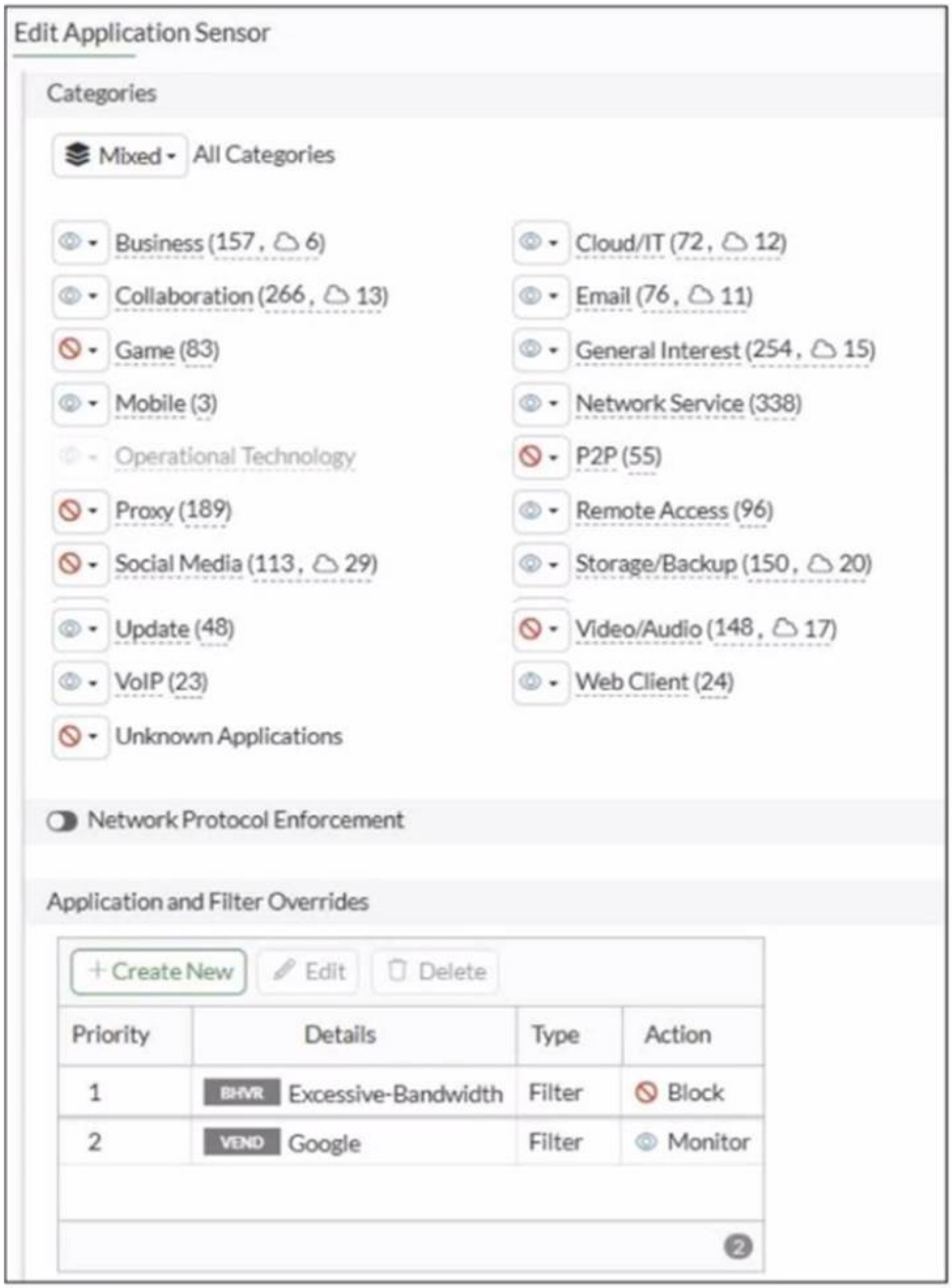
NEW QUESTION 11
Which two statements are correct when FortiGate enters conserve mode? (Choose two answers)

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.

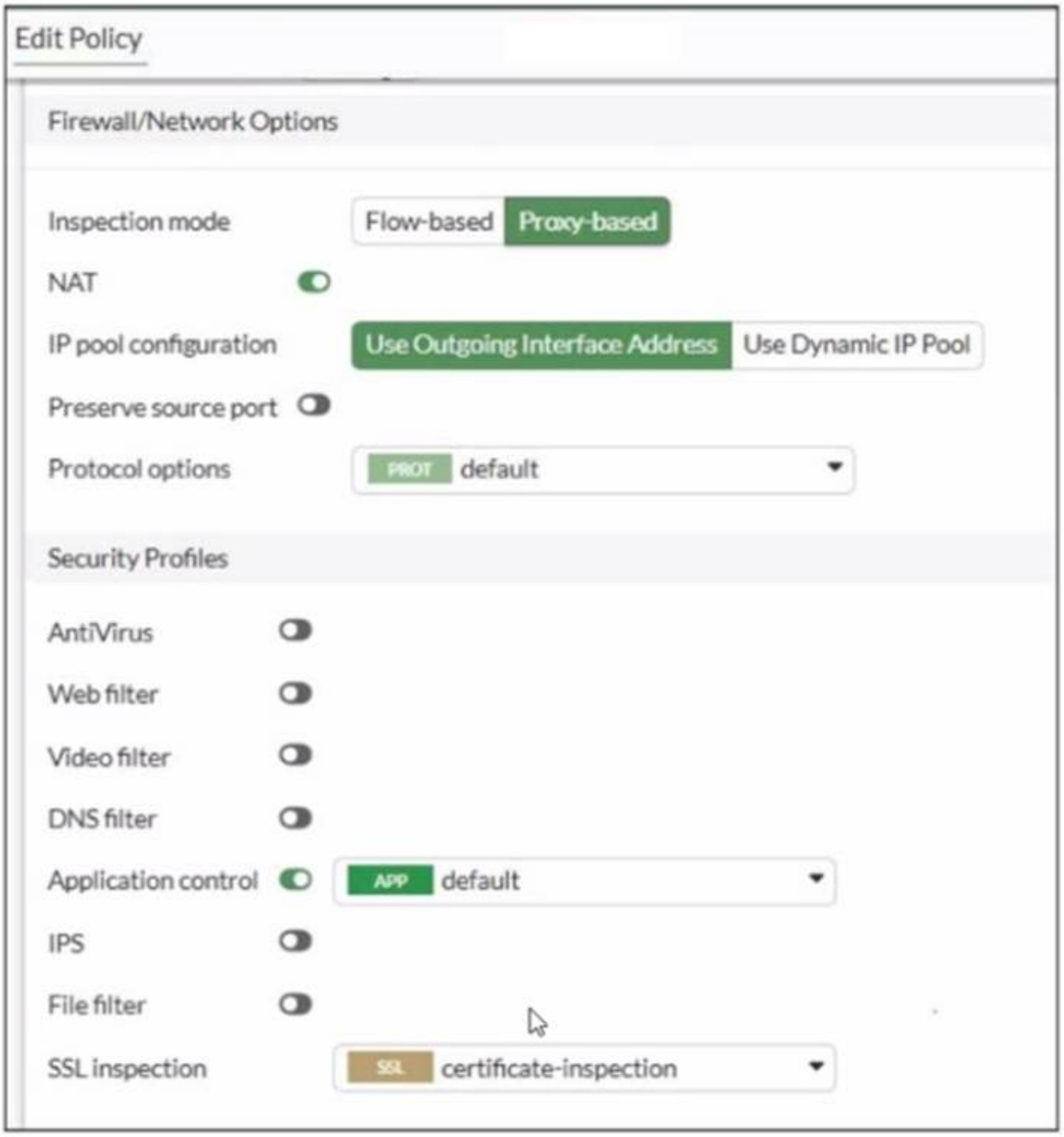
Answer: BD

NEW QUESTION 16
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 19
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.

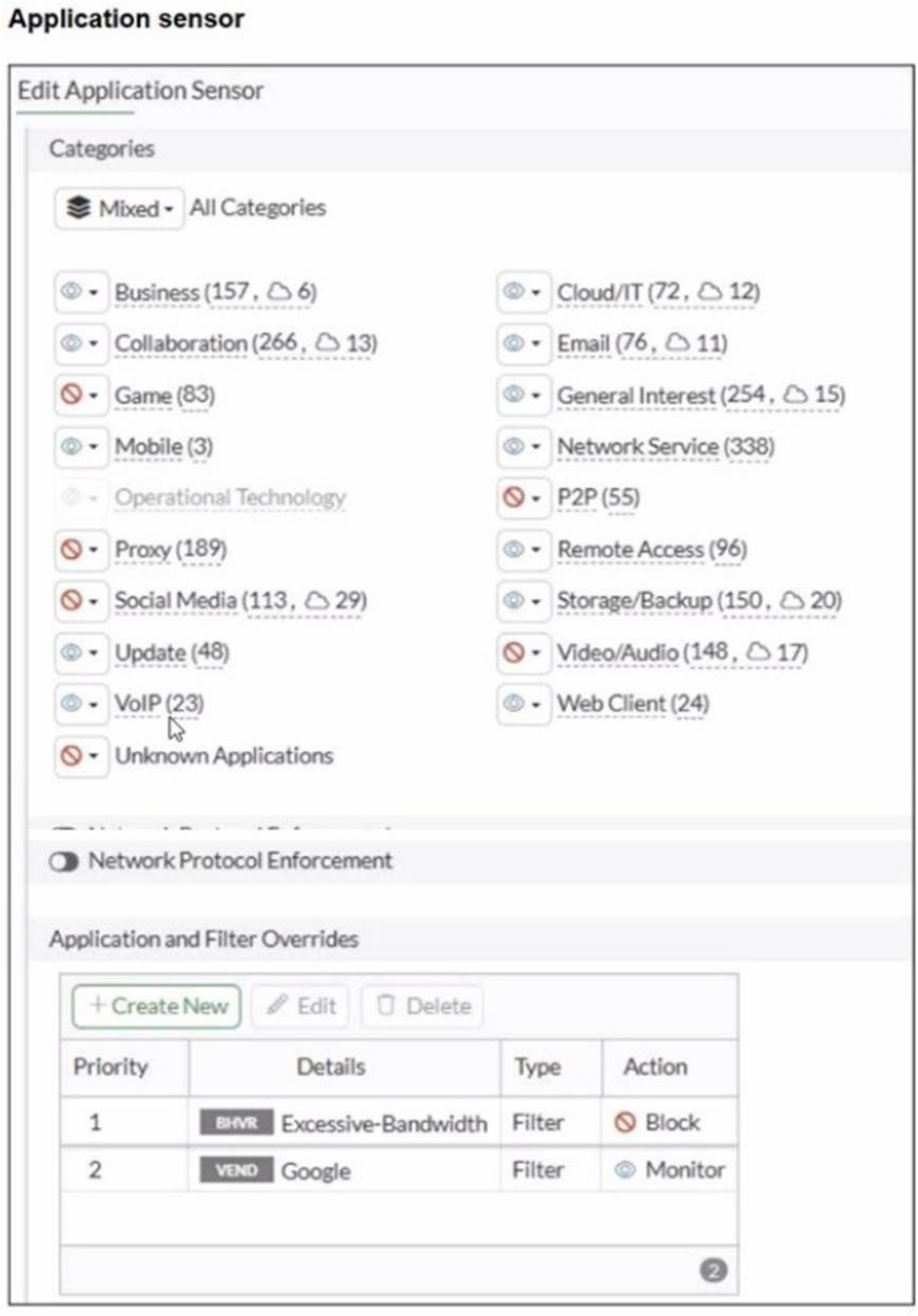
Answer: ABD

NEW QUESTION 23
Which three statements about SD-WAN performance SLAs are true? (Choose three.)

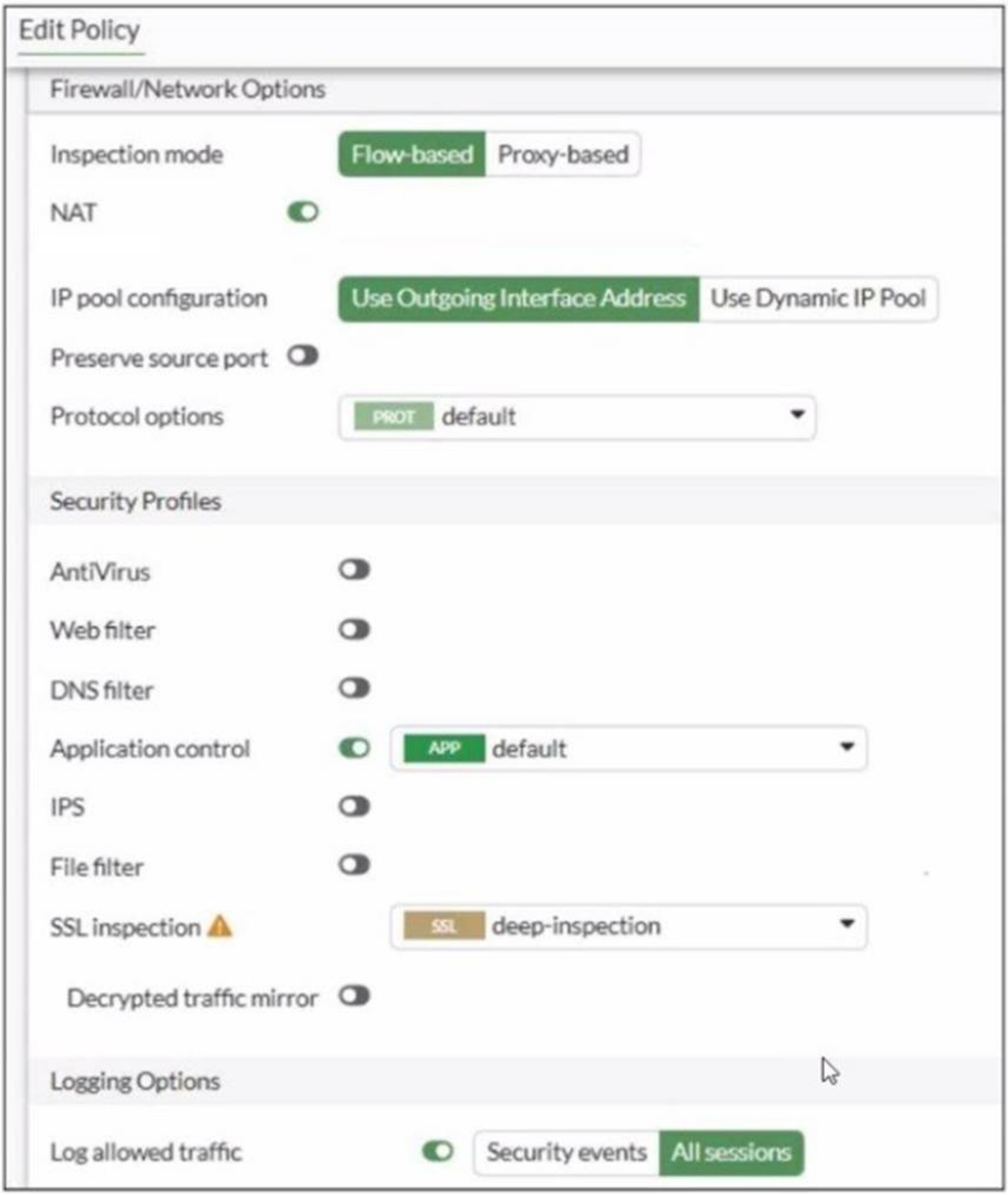
A. They rely on session loss and jitter.
B. They monitor the state of the FortiGate device.
C. All the SLA targets can be configured.
D. They are applied in a SD-WAN rule lowest cost strategy.
E. They can be measured actively or passively.

Answer: CDE

NEW QUESTION 26
Refer to the exhibits.



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 28
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.

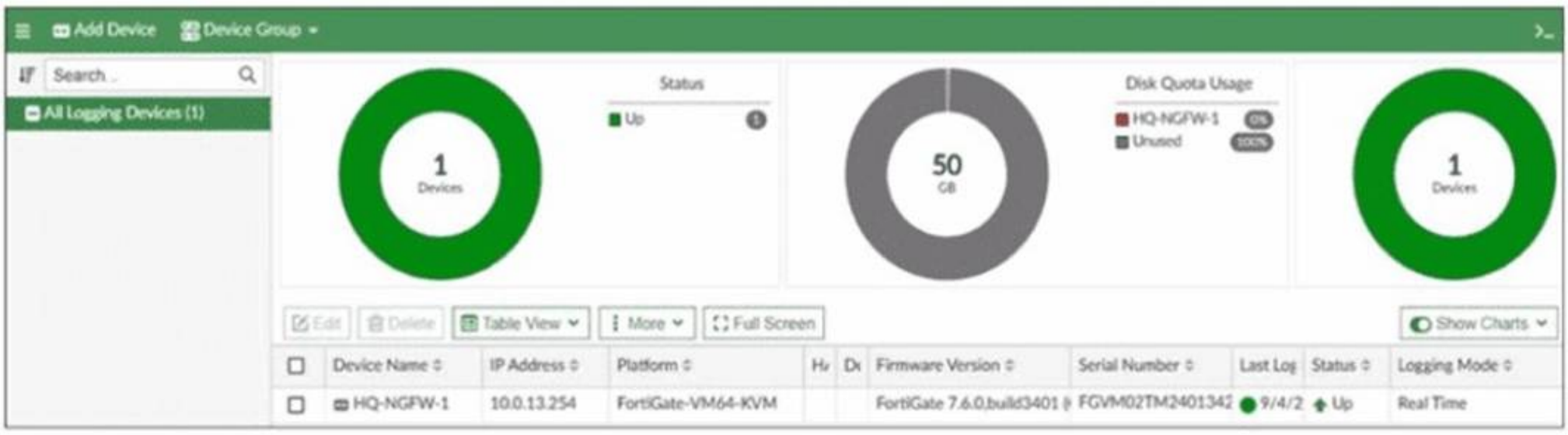
Answer: D

NEW QUESTION 31
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 35
What is the primary FortiGate election process when the HA override setting is enabled? (Choose one answer)

A. Connected monitored ports > Priority > HA uptime > FortiGate serial number
B. Connected monitored ports > Priority > System uptime > FortiGate serial number
C. Connected monitored ports > HA uptime > Priority > FortiGate serial number
D. Connected monitored ports > System uptime > Priority > FortiGate serial number

Answer: A

NEW QUESTION 40
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 42
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

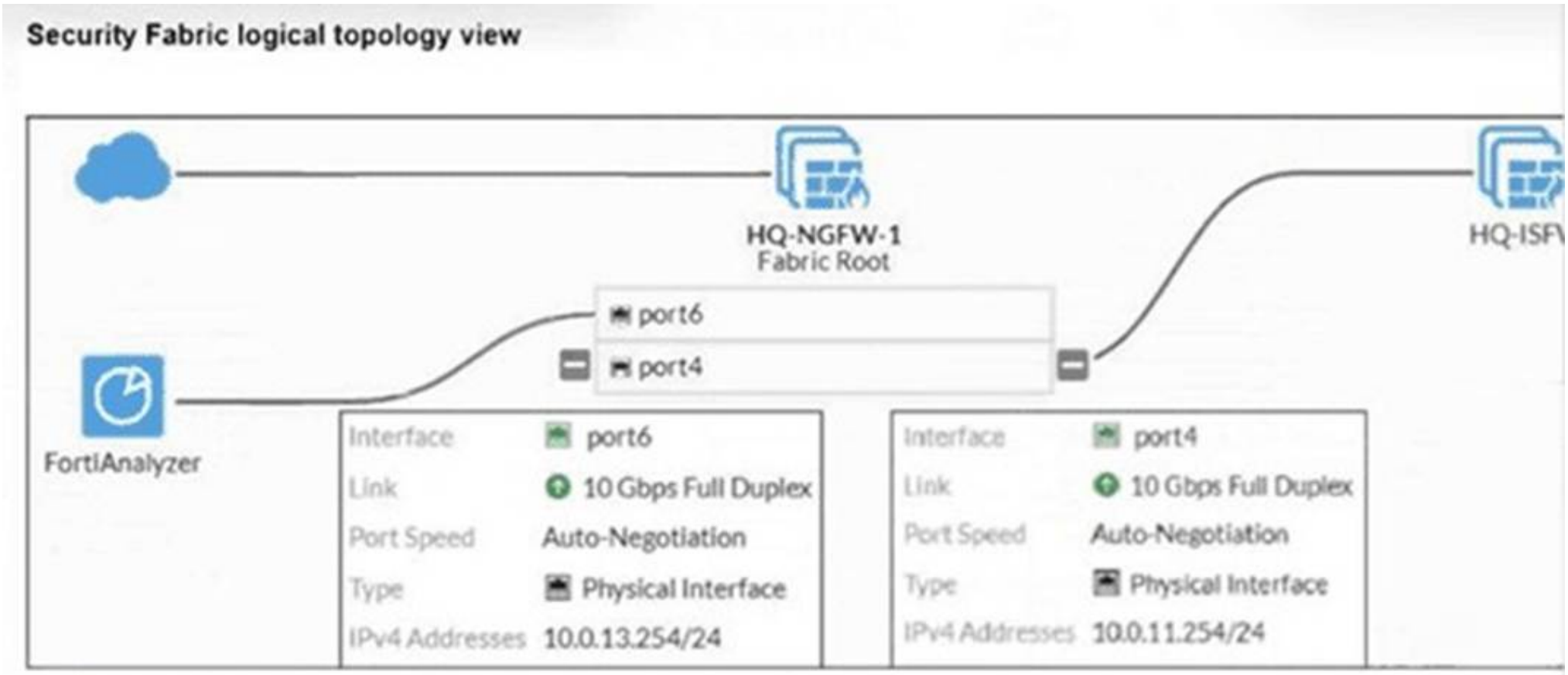
```
HQ-NGFW-2 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k 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?

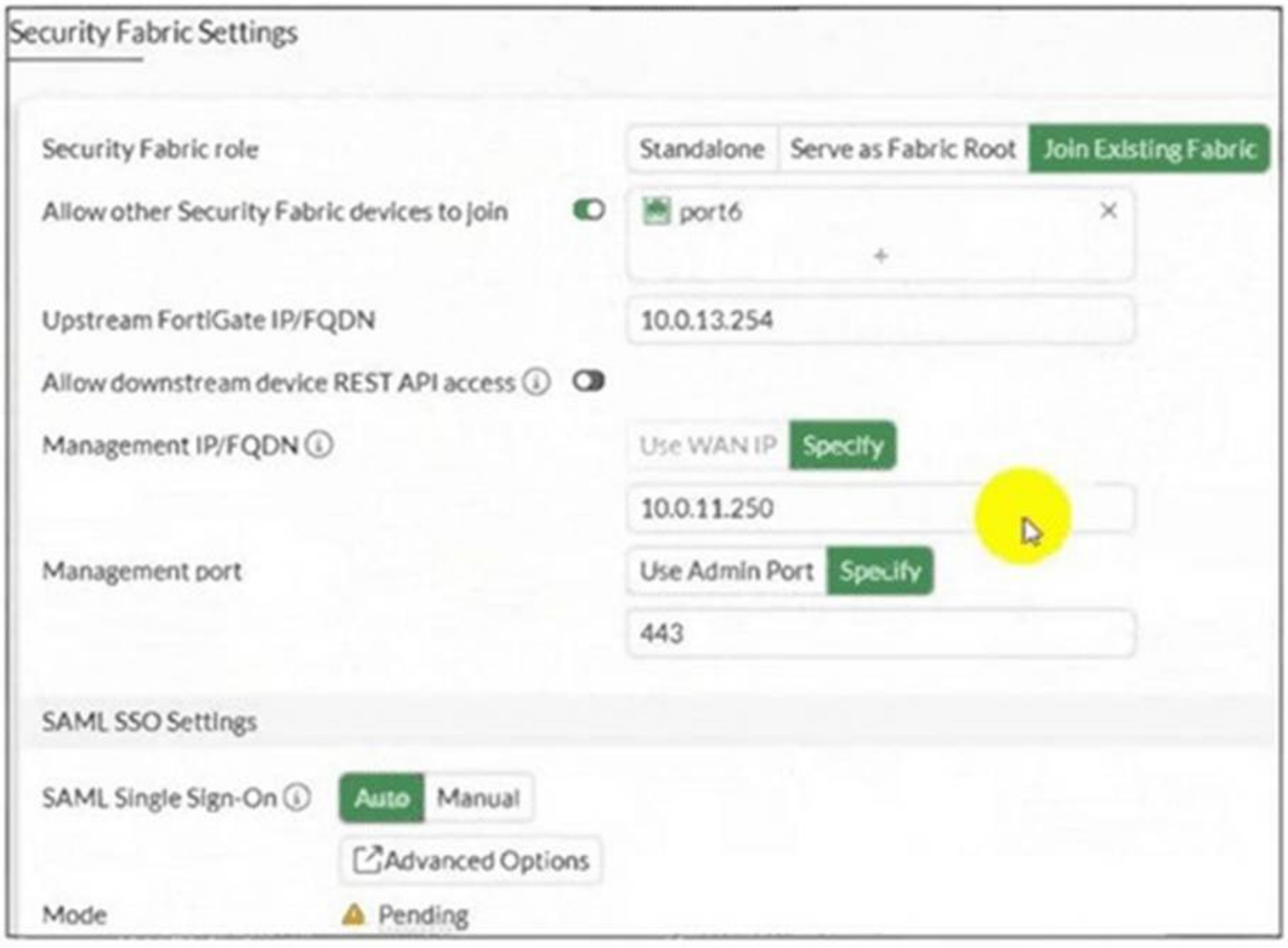
A. HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting
B. HQ-NGFW-2 with the parameter priority setting
C. HQ-NGFW-1 with the parameter override setting
D. HQ-NGFW-2 with the parameter memory-failover-threshold setting

Answer: D

NEW QUESTION 46
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 47
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.

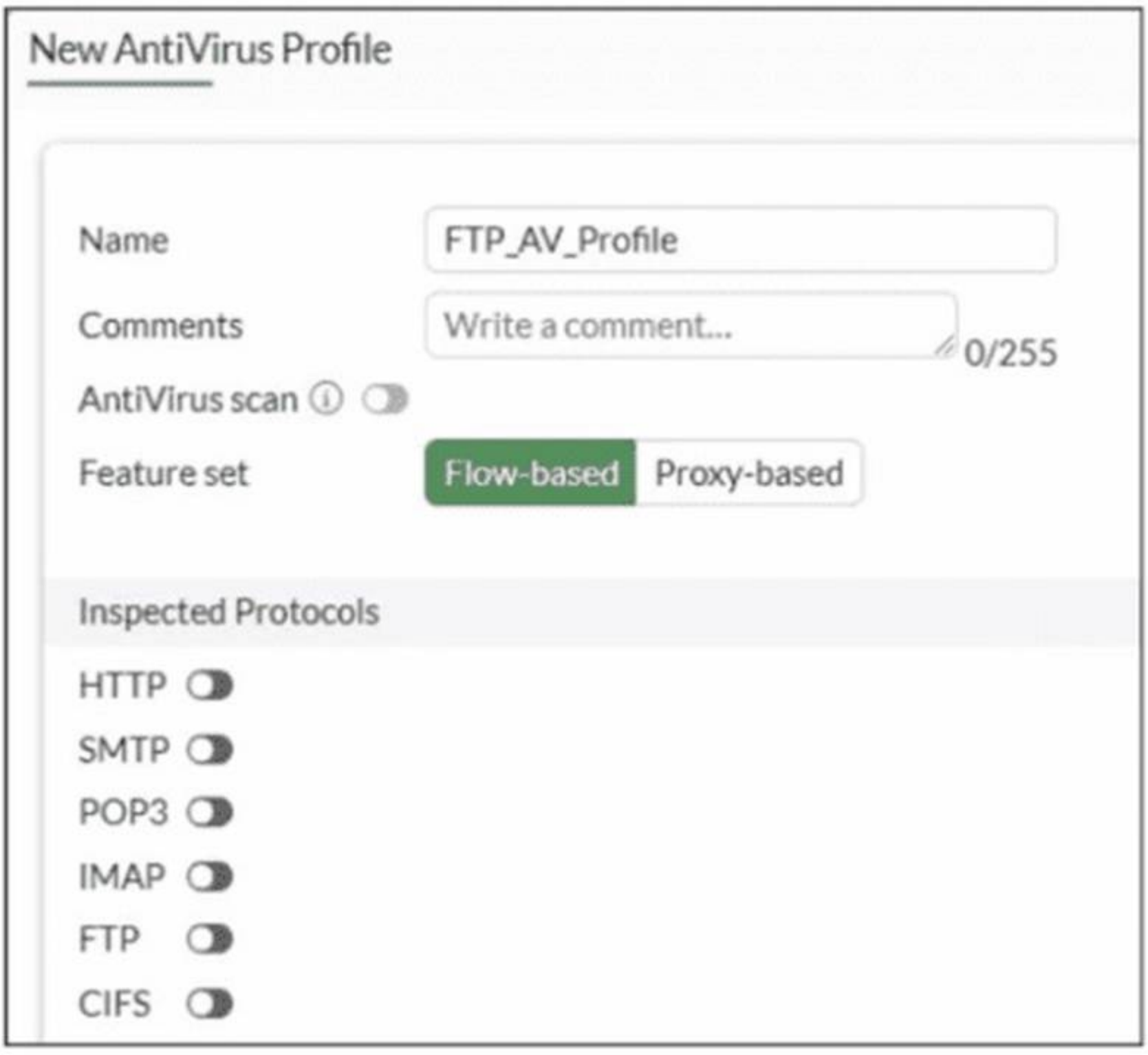
Answer: BC

NEW QUESTION 51
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 53
Refer to the exhibit.



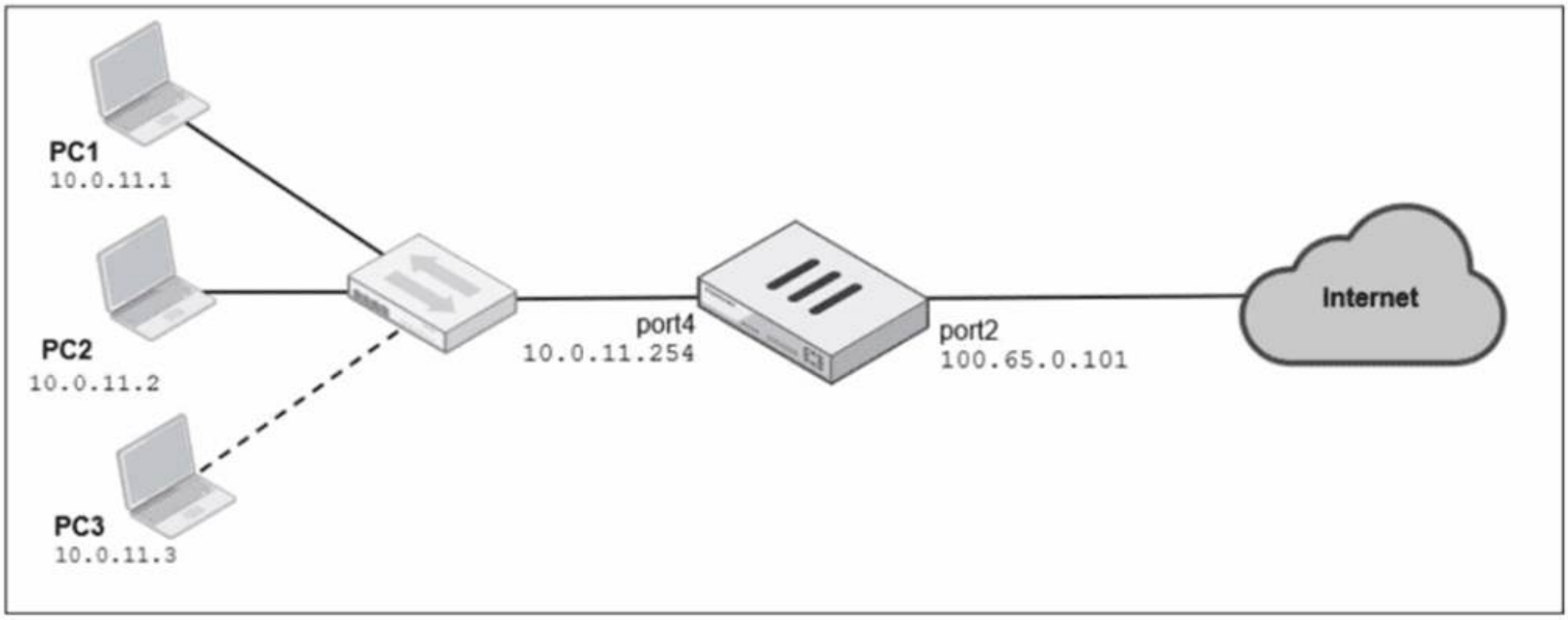
Why is the Antivirus scan switch grayed out when you are creating a new antivirus profile for FTP?

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.

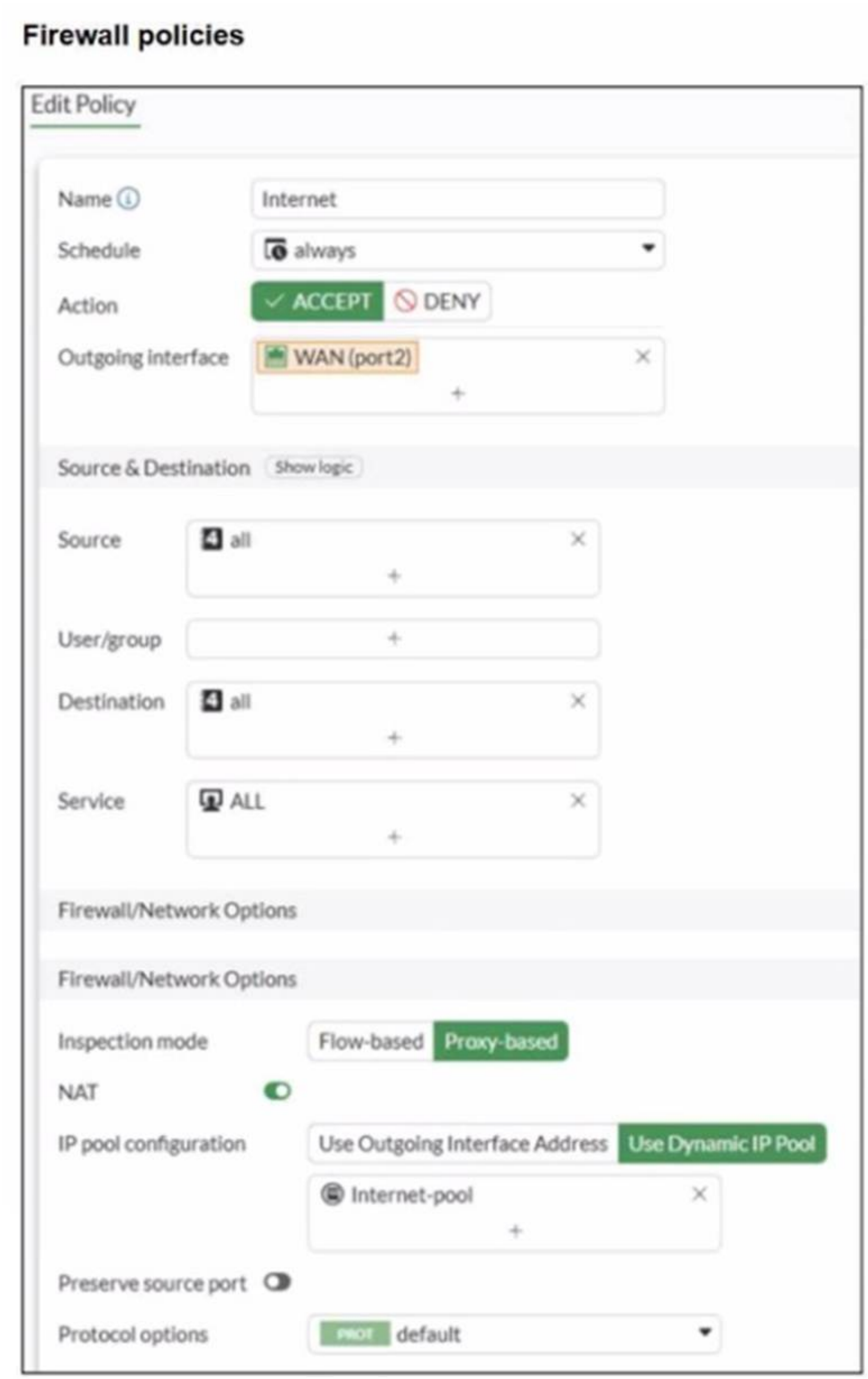
Answer: B

NEW QUESTION 56
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 60
Refer to the exhibit.

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

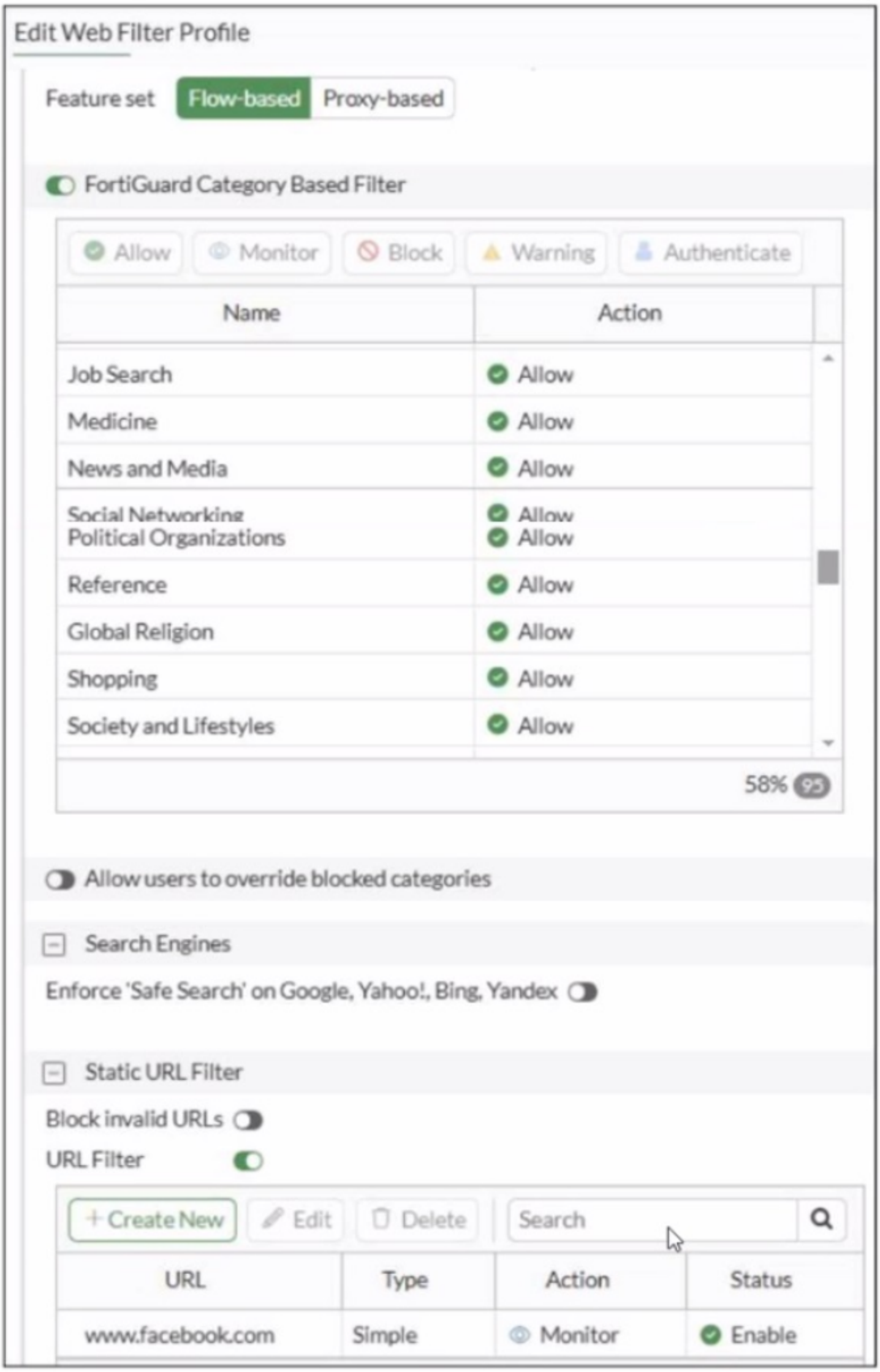
Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

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.

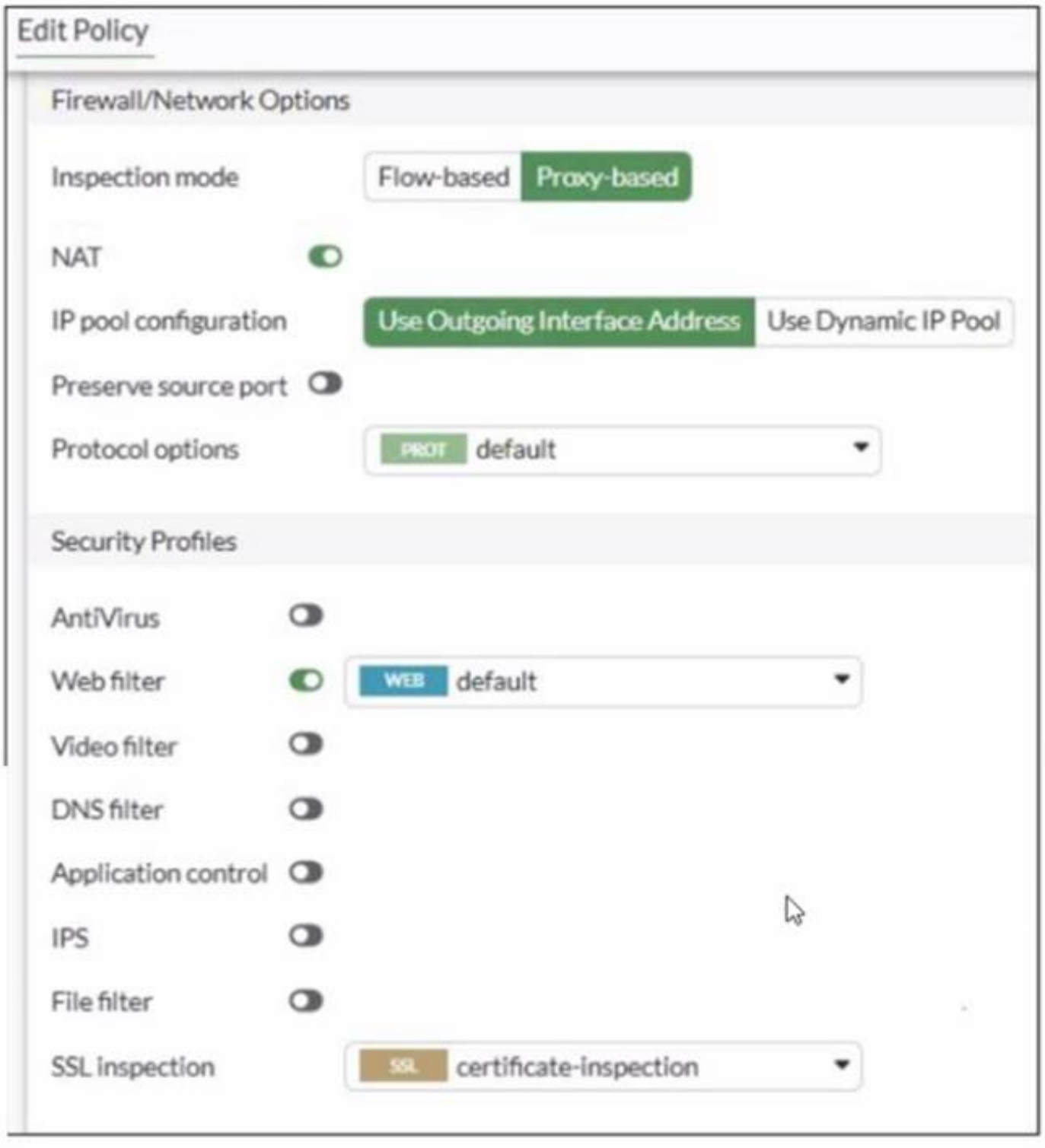
Answer: CD

NEW QUESTION 63
Refer to the exhibits.

Web filter profile configuration



Firewall policy configuration



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 67
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 72
.....

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