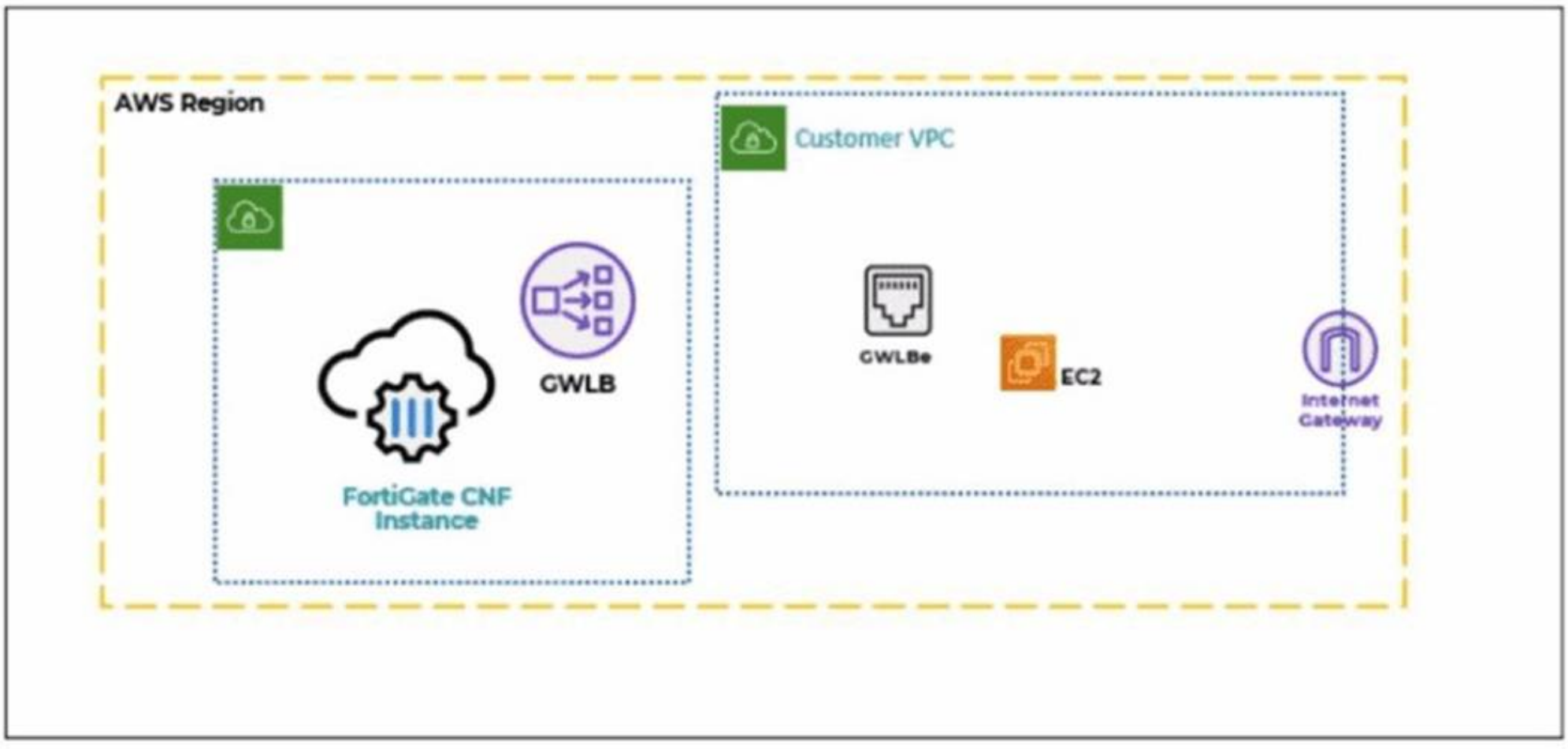
Fortinet

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.



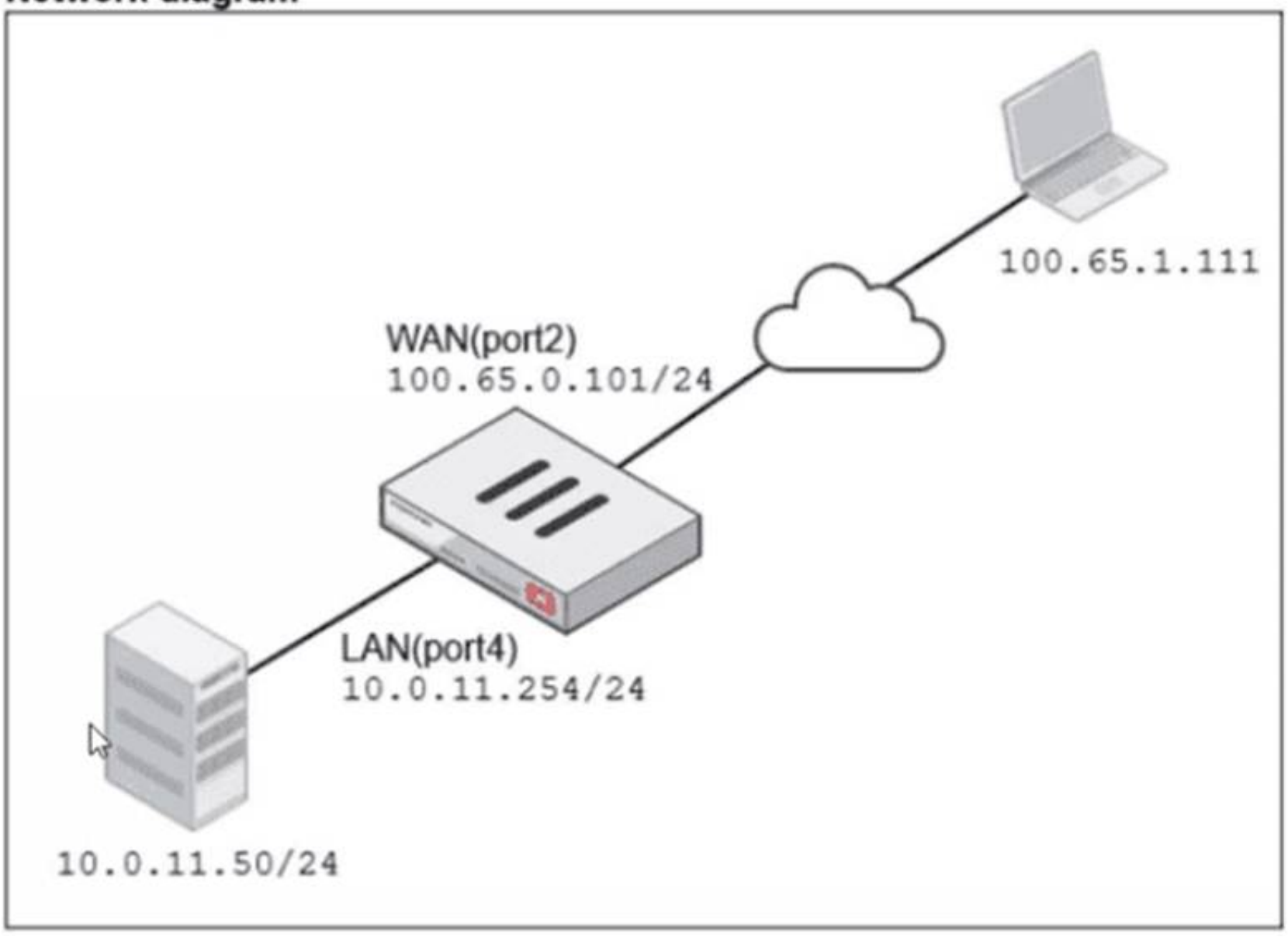
You deployed a FortiGate Cloud-Native Firewall (CNF) in AWS.
During the deployment, which components must the FortiGate CNF create to handle traffic from the EC2 instance?

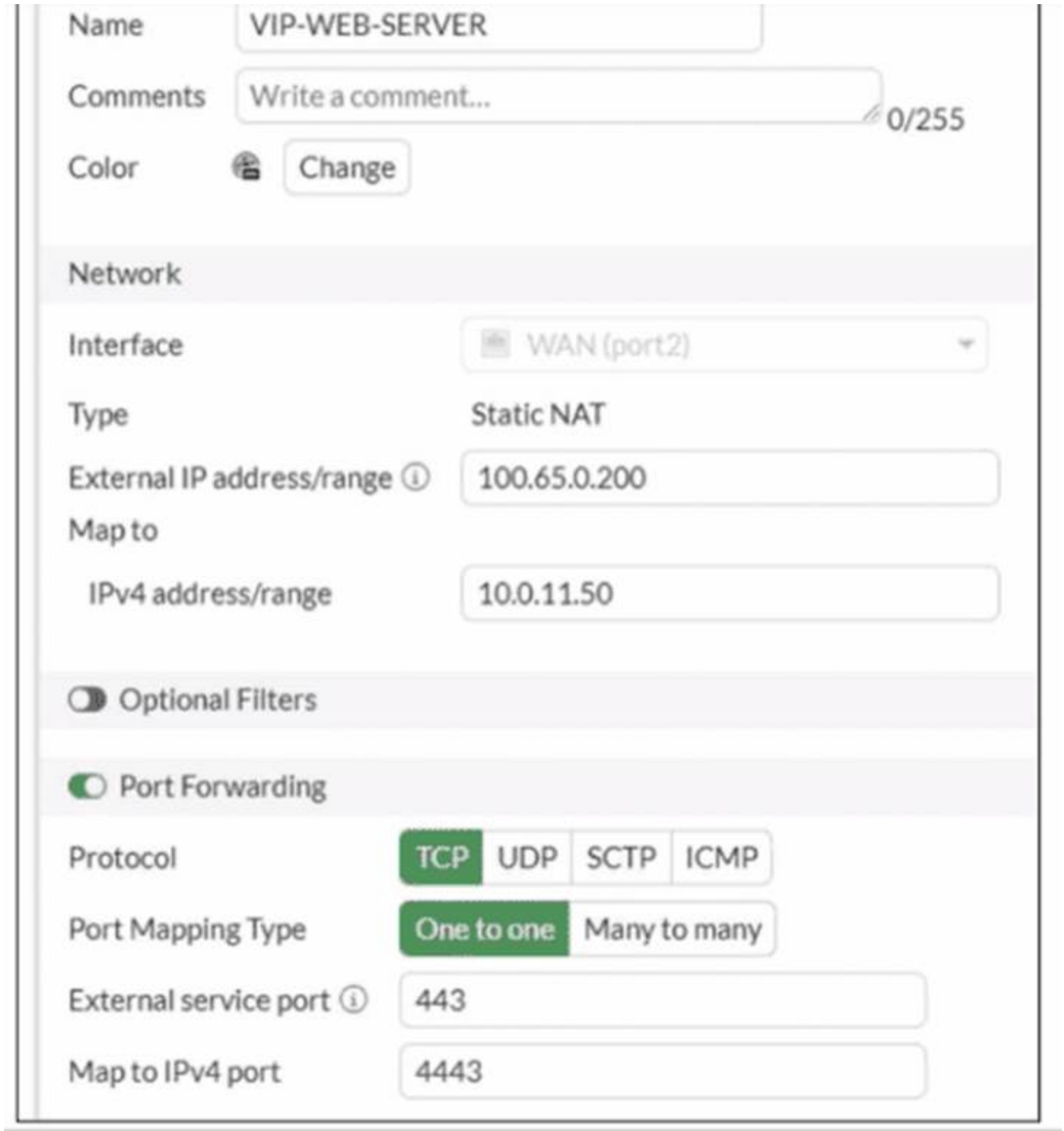
A. The customer VPC and GWLBe
B. The gateway load balancer endpoint (GWLBe) in the customer virtual private cloud (VPC)
C. The CNF VP
D. customer VP
E. and GWLB
F. The GWL
G. GWLBe, and the internet gateway (IGW) in the customer VPC

Answer: B

NEW QUESTION 2
Refer to the exhibits.

Network diagram





Firewall policies

	Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
☐	Internet (1)	LAN (port4)	WAN (port2)	all	all	always	ALL	✓ ACCEPT		NAT
☐	Web_Server_Access (2)	WAN (port2)	LAN (port4)	all	VIP-WEB-SERVER	always	HTTPS	✓ ACCEPT		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. ill, 10.0.11.50, and 4443. respectively
D. 100.65.1.111, 10.0.11.50. and 443. respectively

Answer: C

NEW QUESTION 3
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 4
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 5
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 6
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 7
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
```

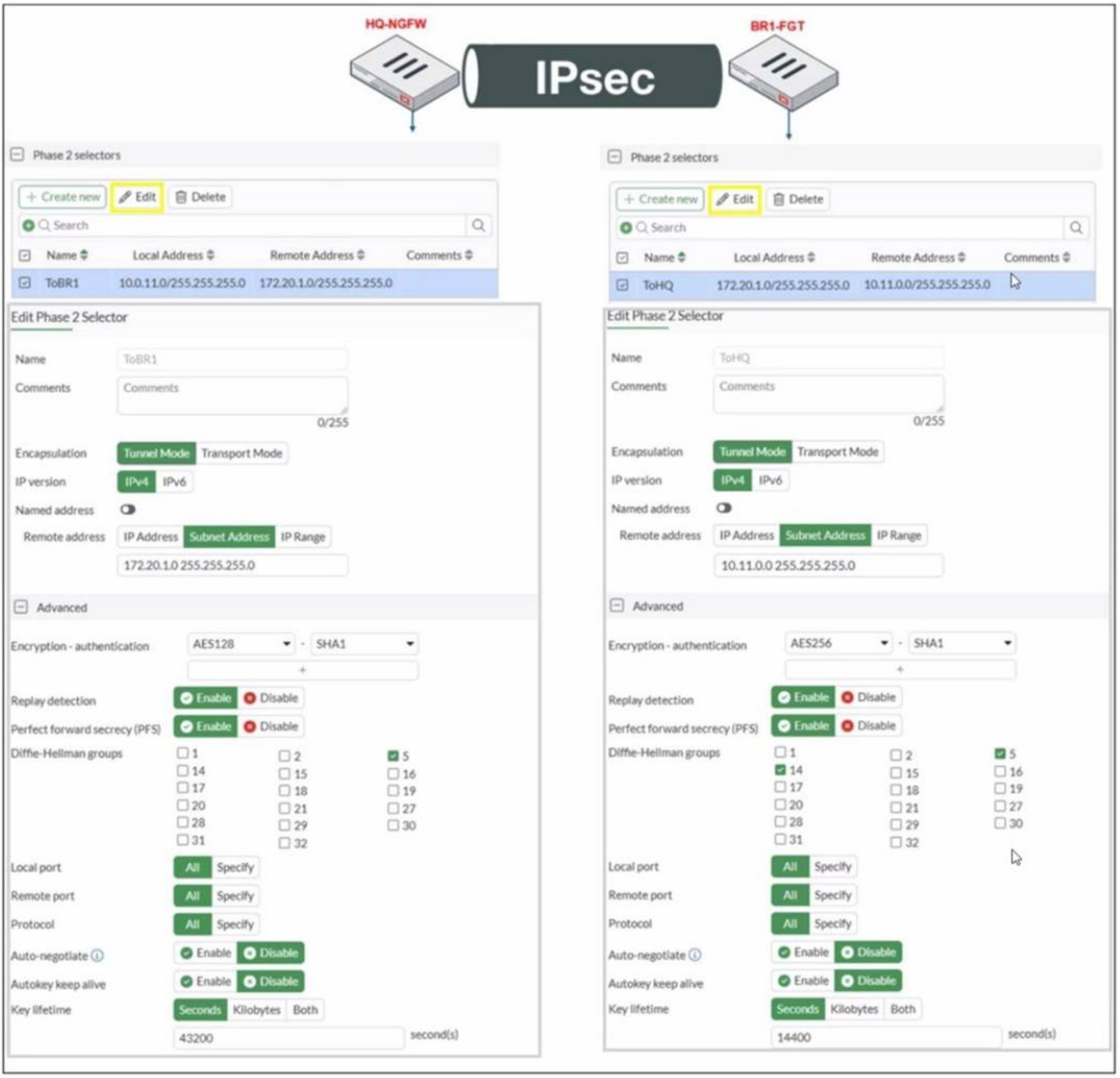
As an administrator you have created an IPS profile, but it is not performing as expected. While testing you got the output as shown in the exhibit What could be the possible reason of the diagnose output shown in the exhibit?

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 8
Refer to the exhibit.

IPsec tunnel configuration



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.

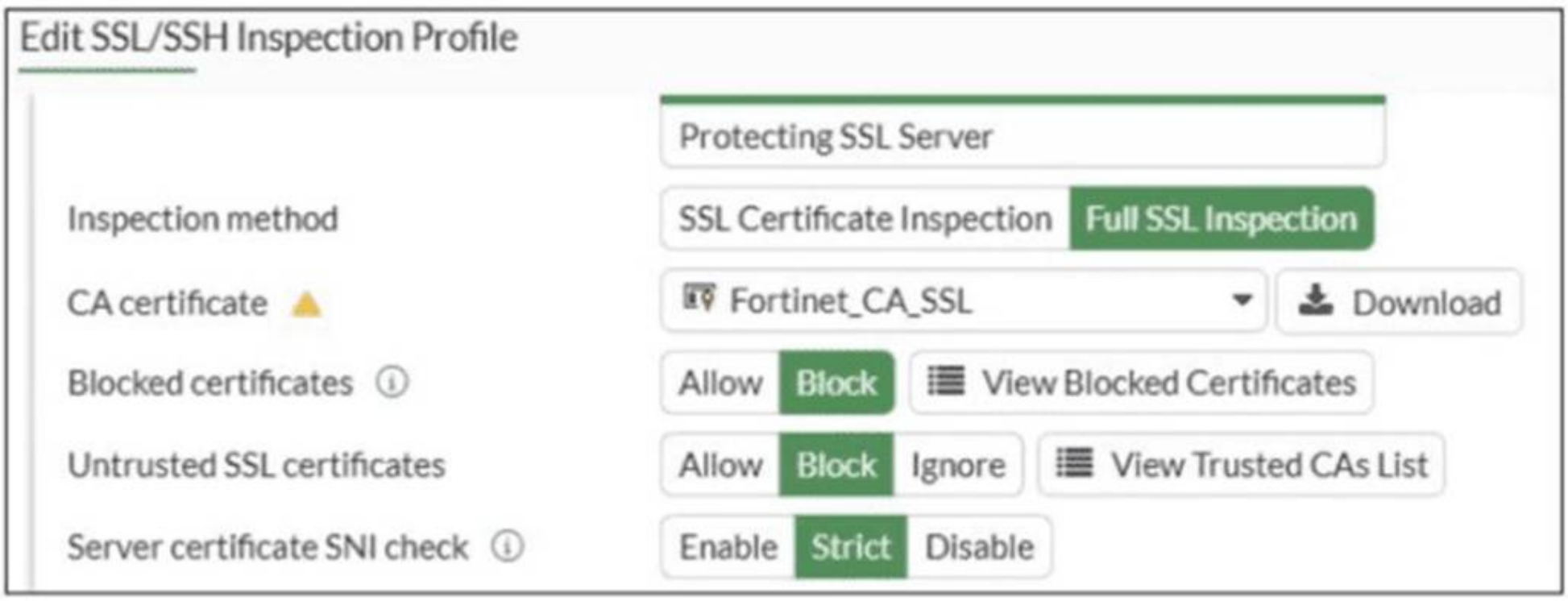
Answer: AD

NEW QUESTION 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 exhibit.



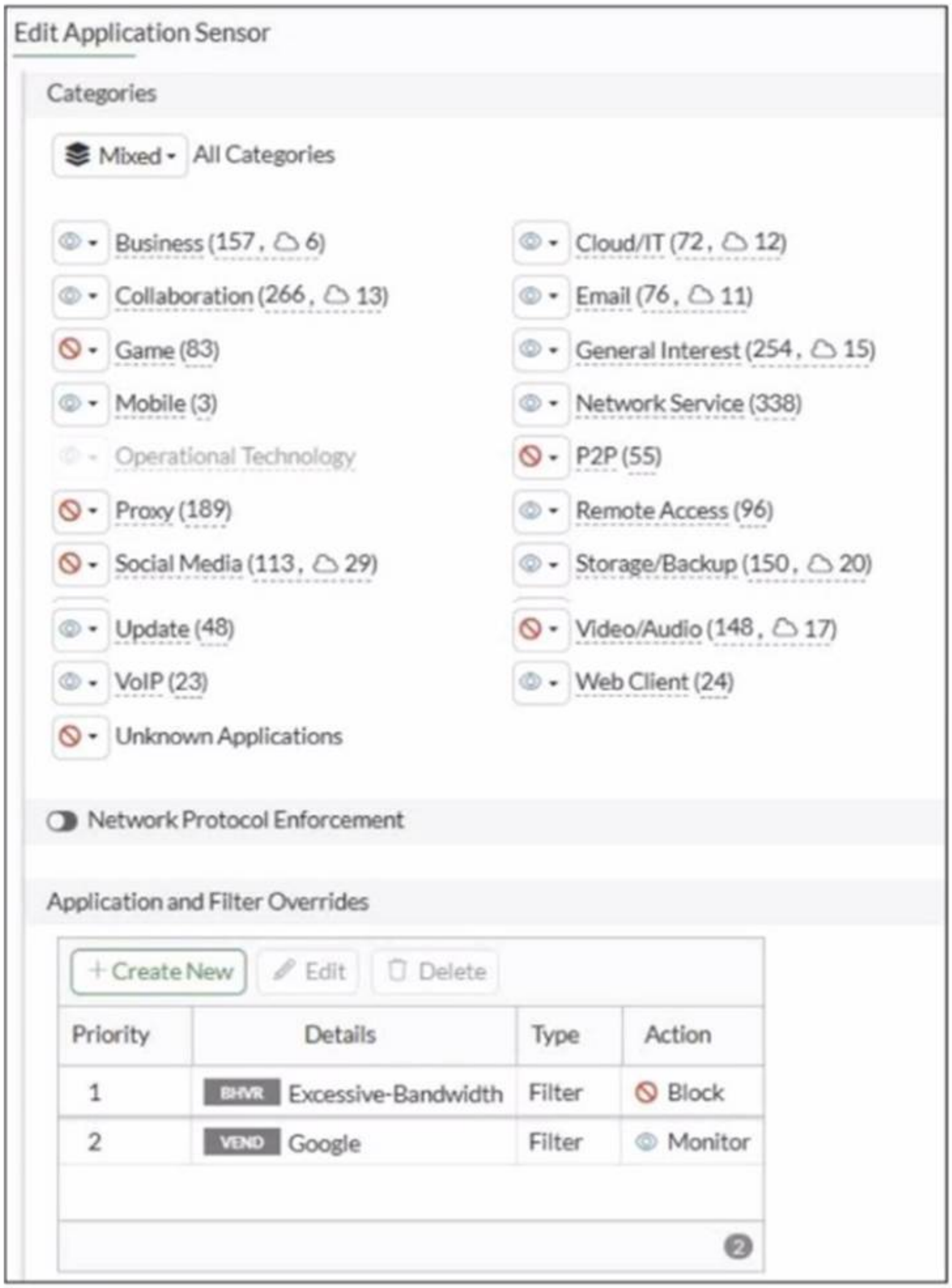
What would be the impact of these settings on the Server certificate SNI check configuration on FortiGate?

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

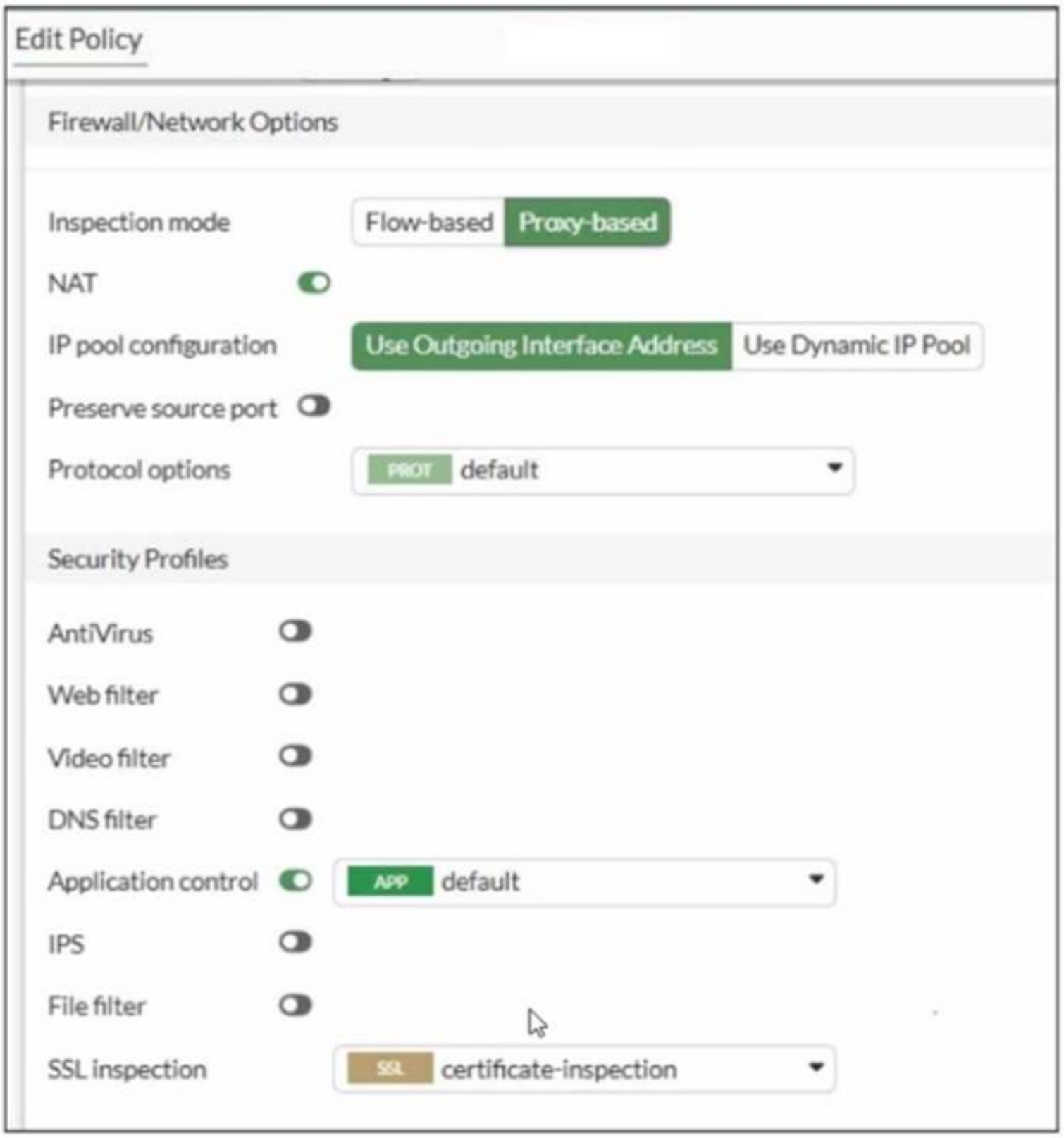
Answer: C

NEW QUESTION 10
Refer to the exhibits.

Application sensor



Firewall policy



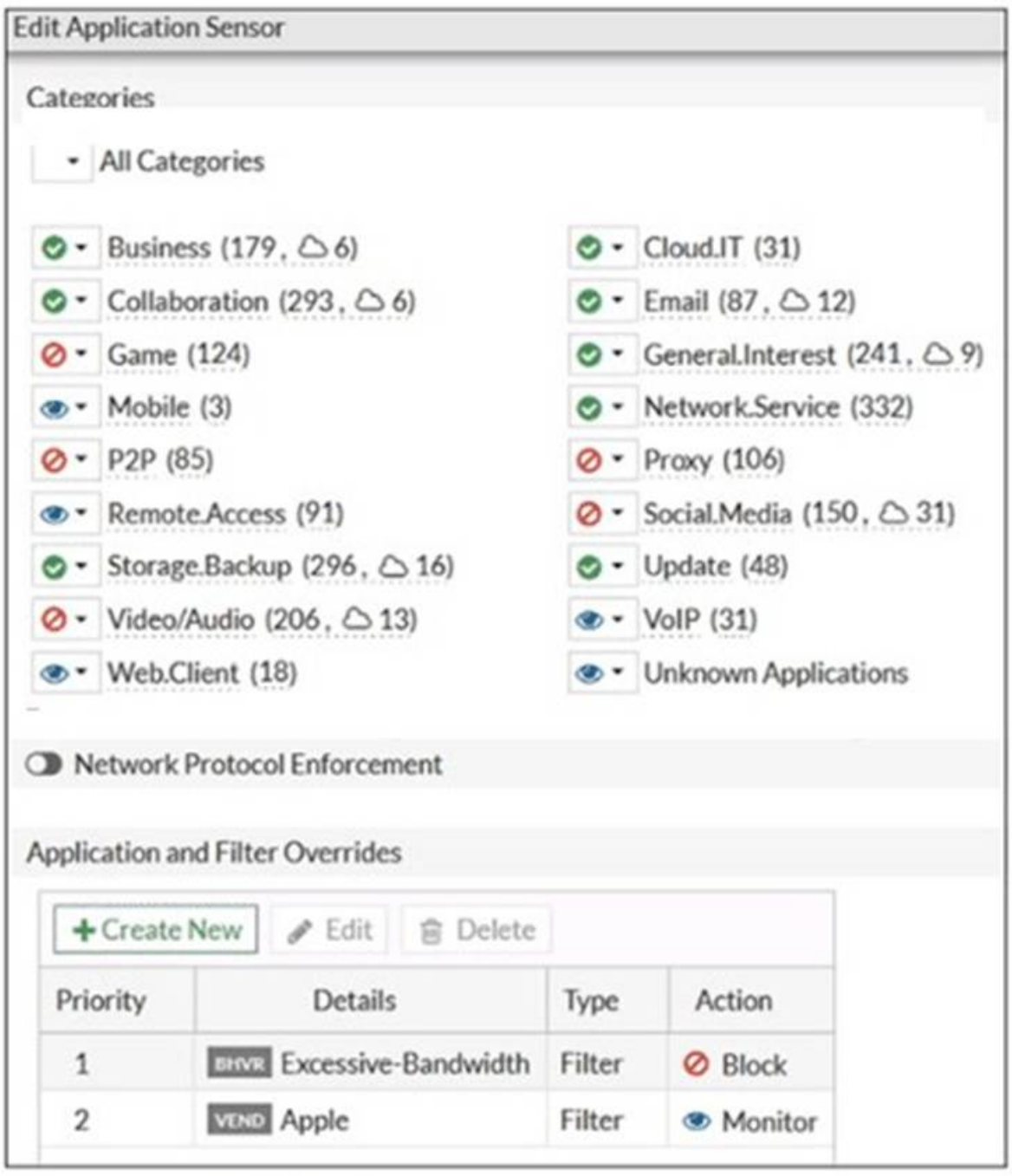
You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits.
You cannot access any of the Google applications, but you are able to access www.fortinet.com.
Which two actions would you take to resolve the issue? (Choose two.)

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

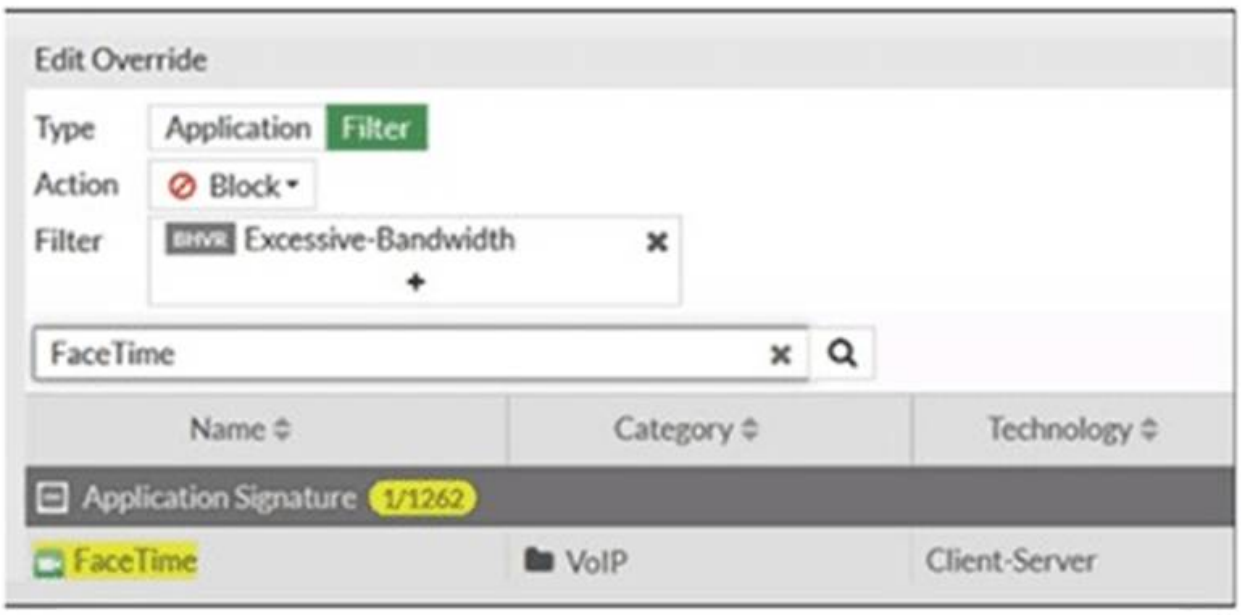
Answer: BE

NEW QUESTION 11
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

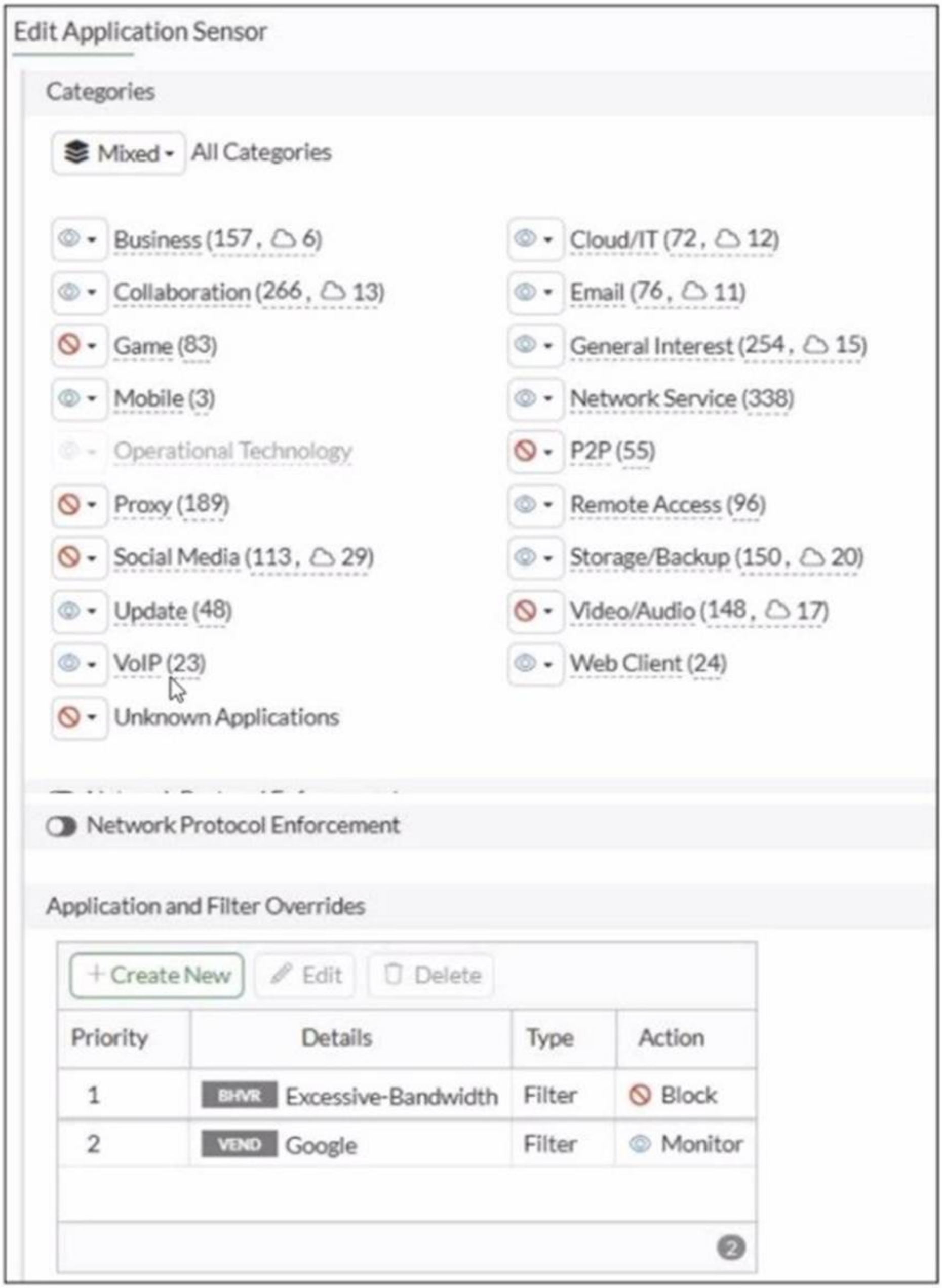
NEW QUESTION 16
Which two statements are true about an HA cluster? (Choose two answers)

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.

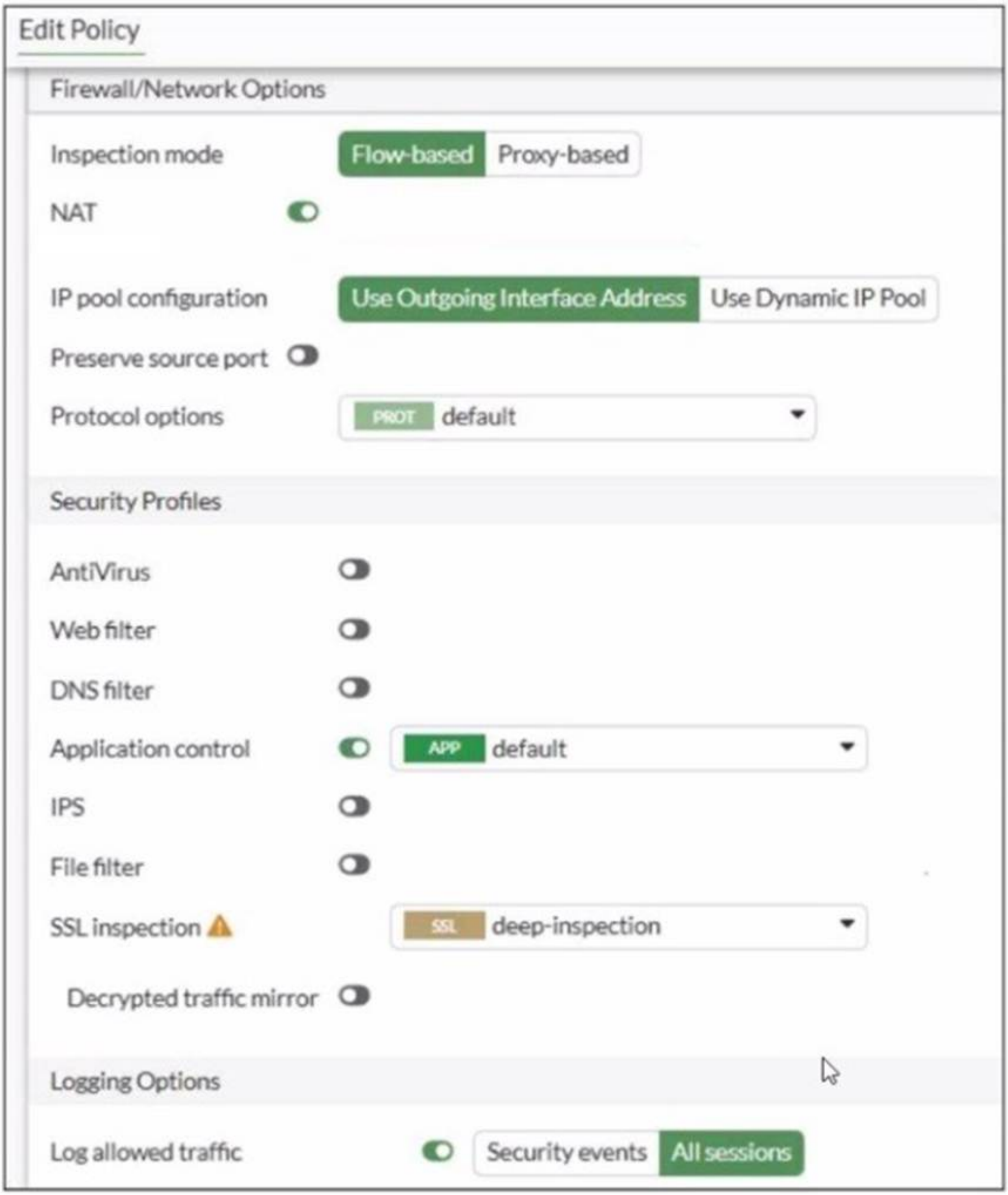
Answer: BD

NEW QUESTION 19
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

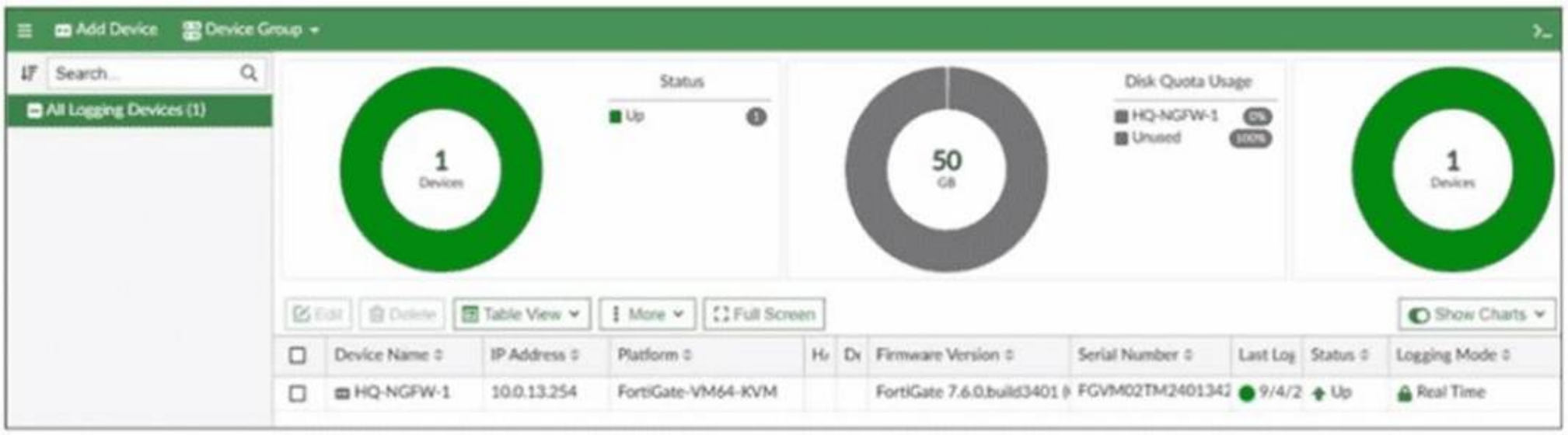
NEW QUESTION 22
Refer to the exhibit.

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

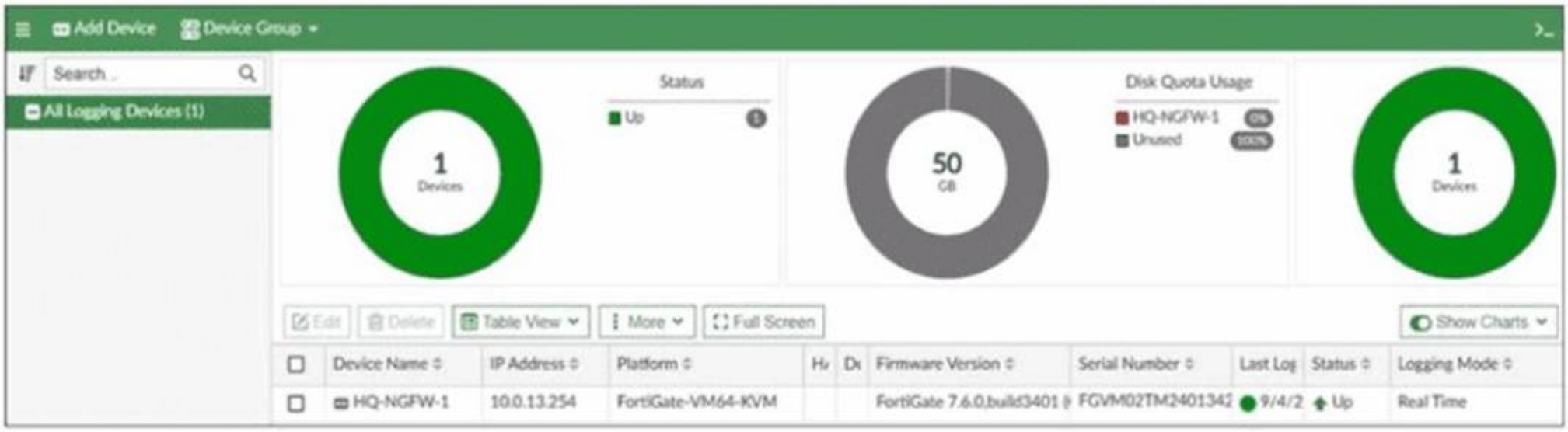
NEW QUESTION 24
The FortiGate device HQ-NGFW-1 with the IP address 10.0.13.254 sends logs to the FortiAnalyzer device with the IP address 10.0.13.125. The administrator wants to verify that reliable logging is enabled on HQ-NGFW-1.
Which exhibit helps with the verification?
A)



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 28
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 30
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 34
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 36
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 38
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 39
.....

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