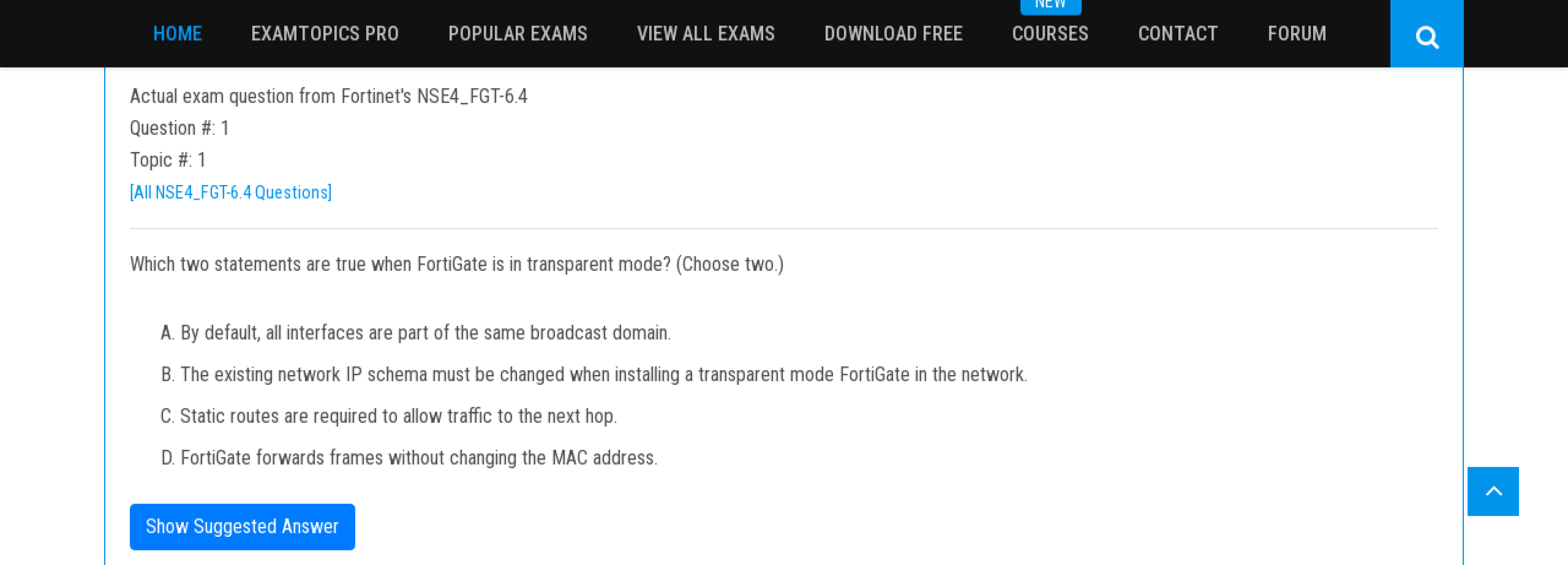


Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 1

Topic #: 1

[All NSE4_FGT-6.4 Questions]

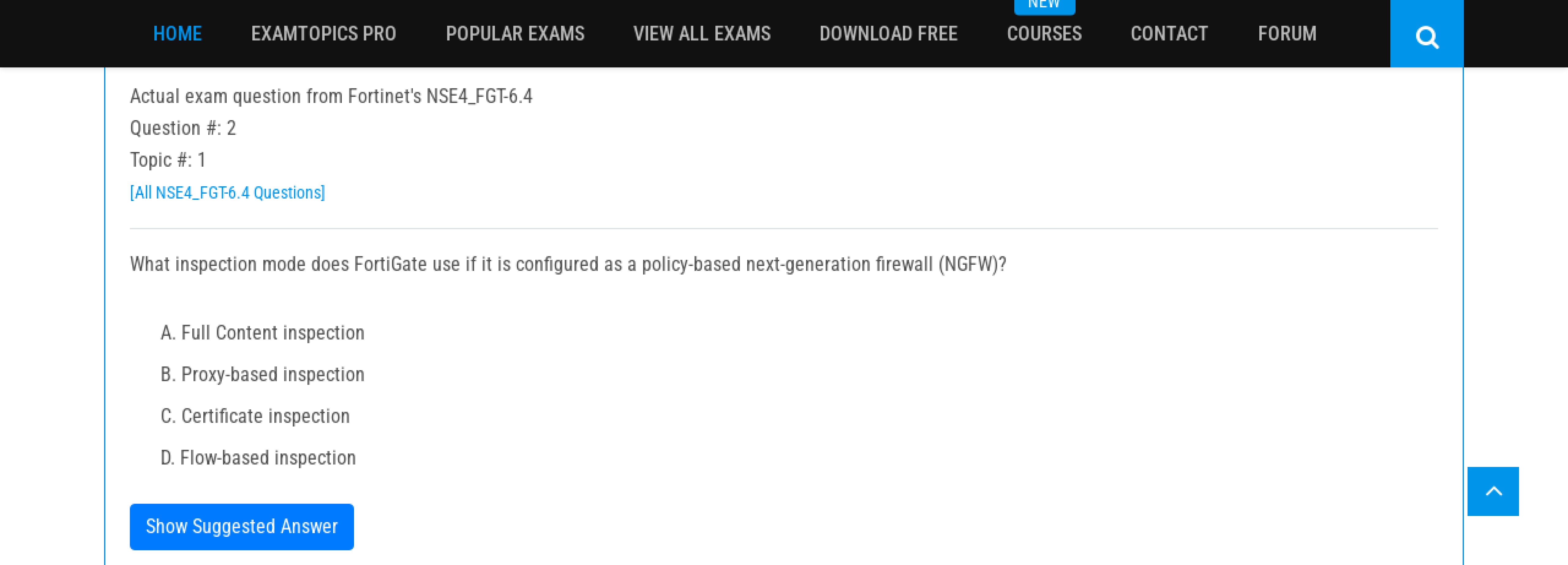
Which two statements are true when FortiGate is in transparent mode? (Choose two.)

A. By default, all interfaces are part of the same broadcast domain.

B. The existing network IP schema must be changed when installing a transparent mode FortiGate in the network.

C. Static routes are required to allow traffic to the next hop.

D. FortiGate forwards frames without changing the MAC address.



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 2

Topic #: 1

[All NSE4_FGT-6.4 Questions]

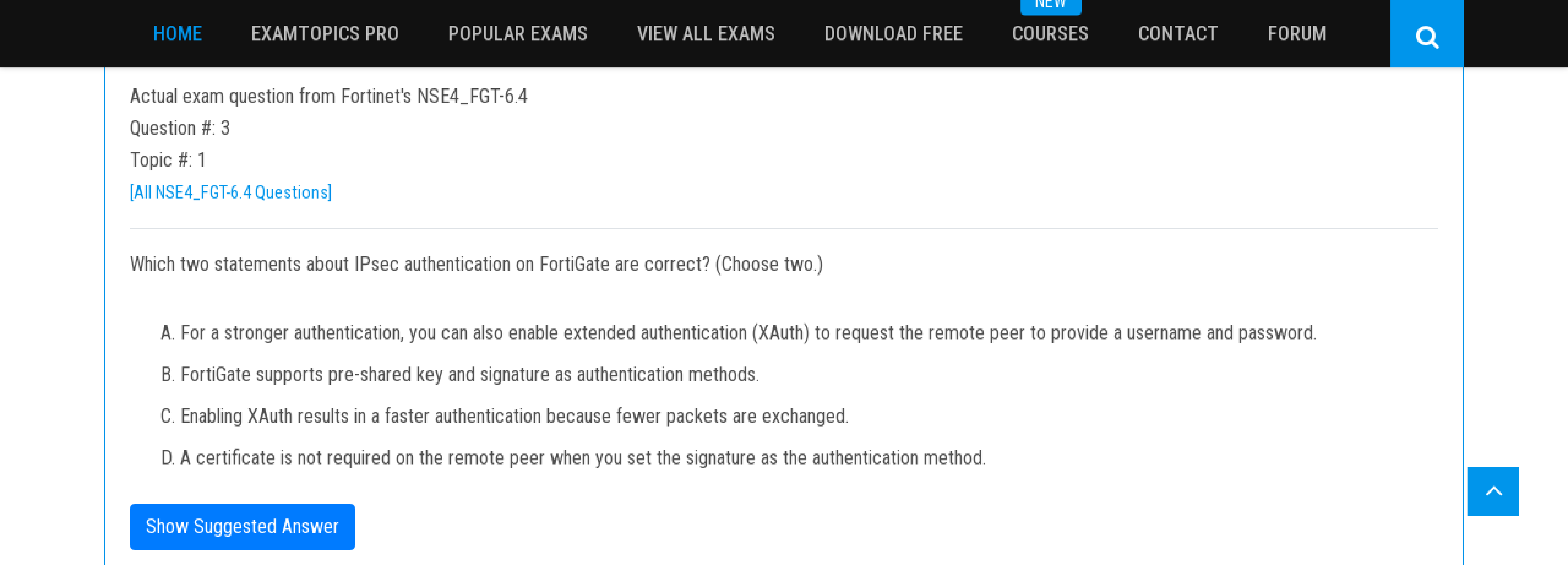
What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

A. Full Content inspection

B. Proxy-based inspection

C. Certificate inspection

D. Flow-based inspection



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 3

Topic #: 1

[All NSE4_FGT-6.4 Questions]

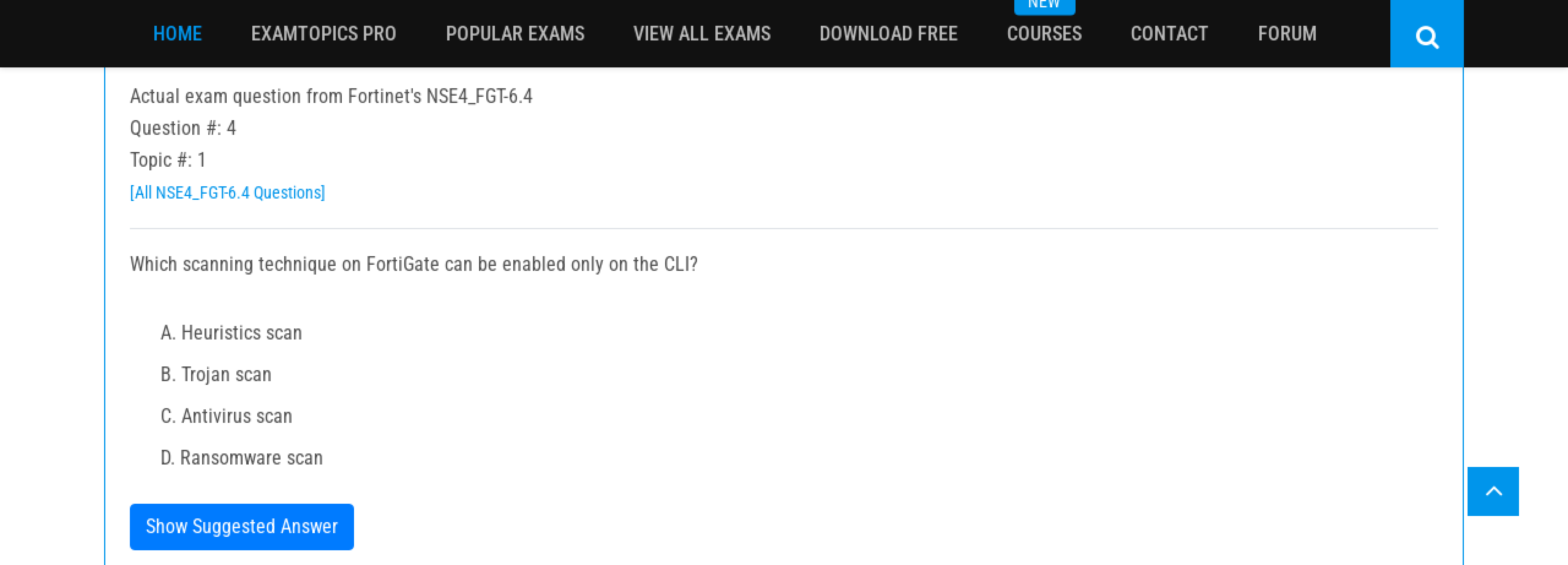
Which two statements about IPsec authentication on FortiGate are correct? (Choose two.)

A. For a stronger authentication, you can also enable extended authentication (XAuth) to request the remote peer to provide a username and password.

B. FortiGate supports pre-shared key and signature as authentication methods.

C. Enabling XAuth results in a faster authentication because fewer packets are exchanged.

D. A certificate is not required on the remote peer when you set the signature as the authentication method.



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 4

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which scanning technique on FortiGate can be enabled only on the CLI?

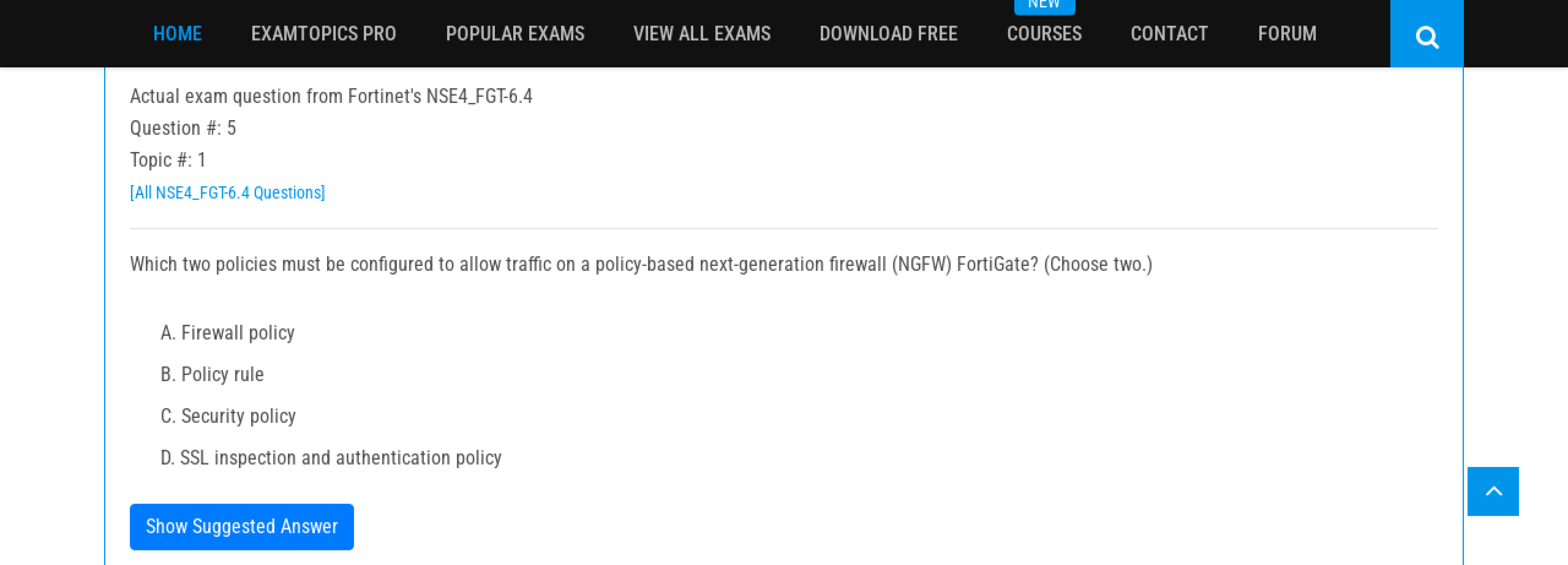
A. Heuristics scan

B. Trojan scan

C. Antivirus scan

D. Ransomware scan

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 5

Topic #: 1

[All NSE4_FGT-6.4 Questions]

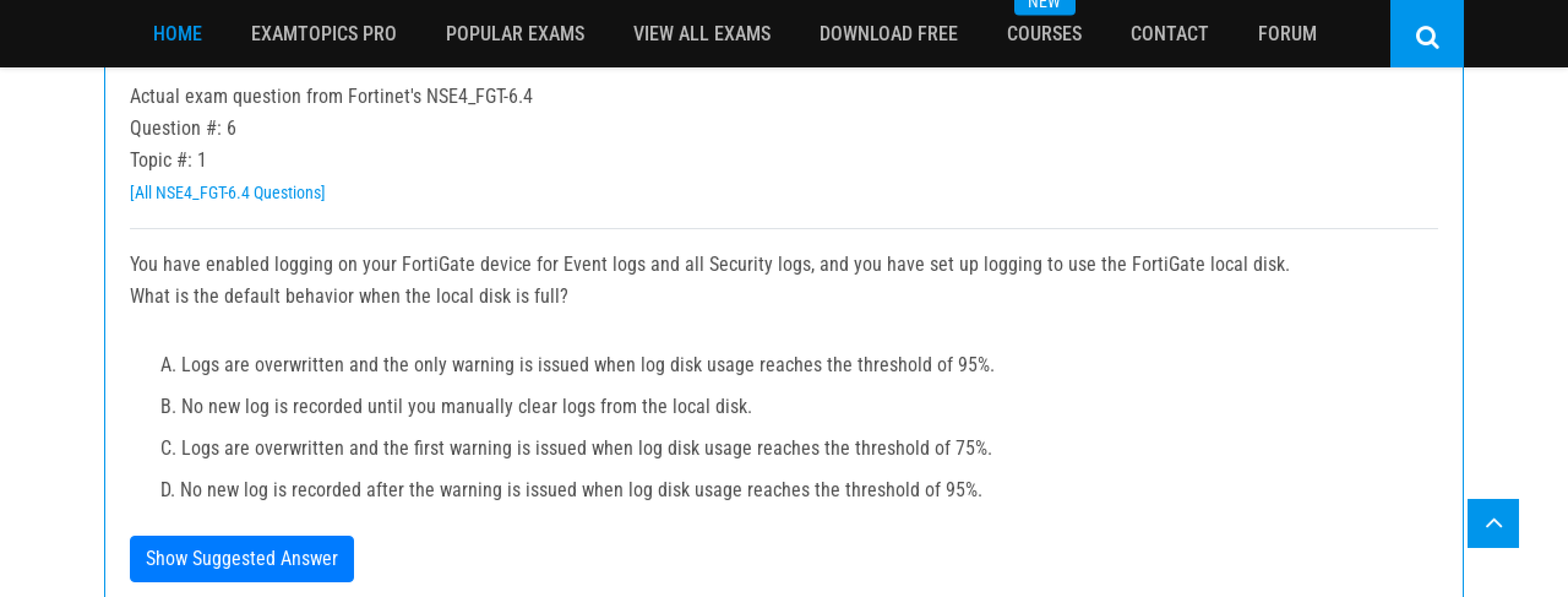
Which two policies must be configured to allow traffic on a policy-based next-generation firewall (NGFW) FortiGate? (Choose two.)

A. Firewall policy

B. Policy rule

C. Security policy

D. SSL inspection and authentication policy



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 6

Topic #: 1

[All NSE4_FGT-6.4 Questions]

You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk.

What is the default behavior when the local disk is full?

A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of 95%.

B. No new log is recorded until you manually clear logs from the local disk.

C. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of 75%.

D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of 95%.

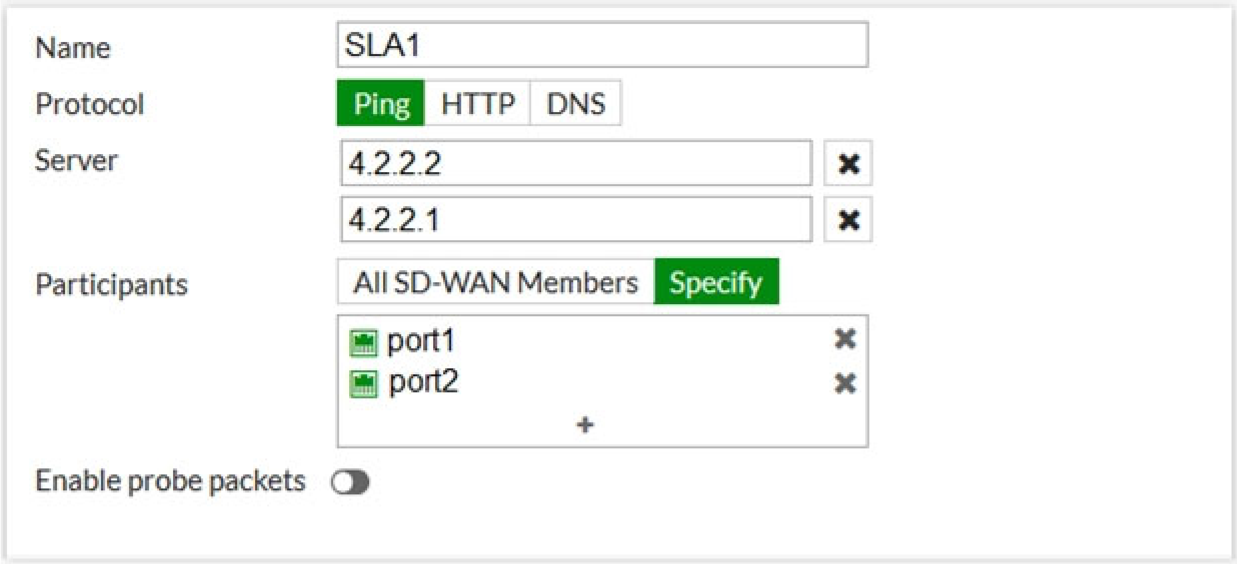
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 7

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit, which contains a Performance SLA configuration.



Name SLA1

Protocol [✓ Ping] HTTP DNS

Server 4.2.2.2 ✖

4.2.2.1 ✖

Participants All SD-WAN Members [✓ Specify]

port1 ✖

port2 ✖

+

Enable probe packets ○

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic.

Why is FortiGate not generating any traffic for the performance SLA?

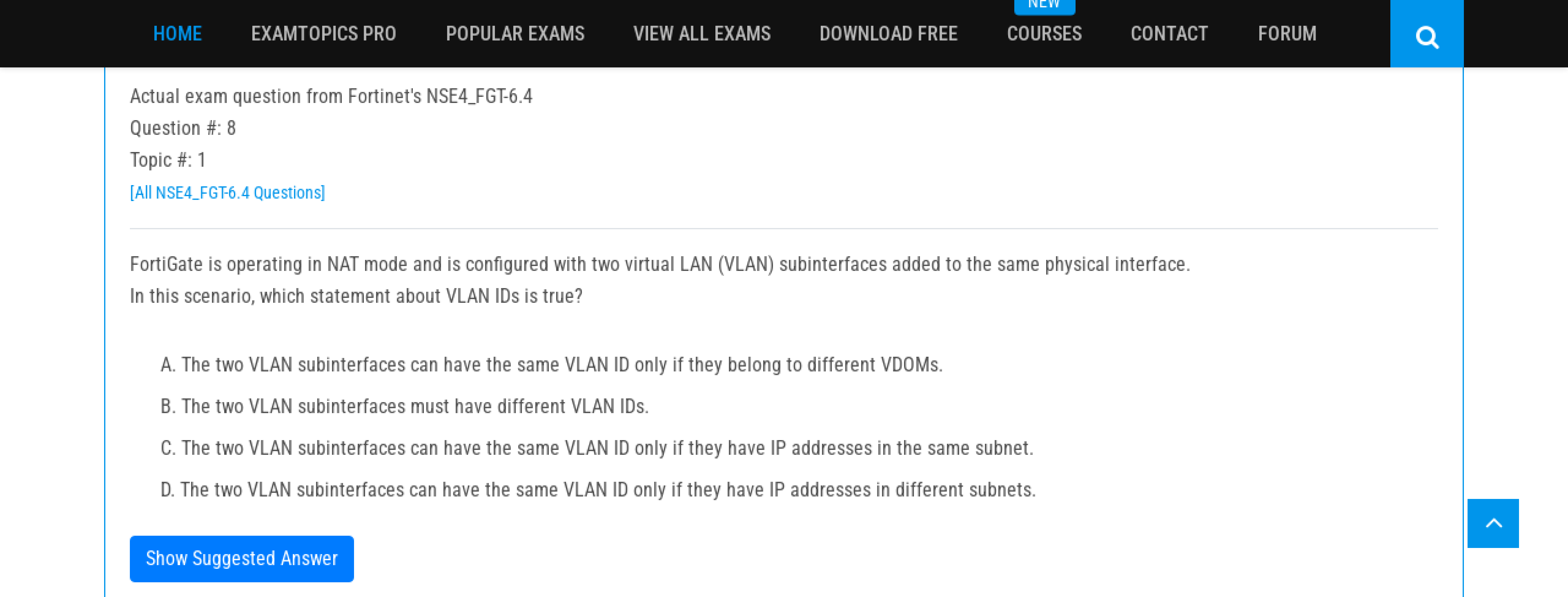
A. There may not be a static route to route the performance SLA traffic.

B. You need to turn on the Enable probe packets switch.

C. The Ping protocol is not supported for the public servers that are configured.

D. Participants configured are not SD-WAN members.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 8

Topic #: 1

[All NSE4_FGT-6.4 Questions]

FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.

In this scenario, which statement about VLAN IDs is true?

A. The two VLAN subinterfaces can have the same VLAN ID only if they belong to different VDOMs.

B. The two VLAN subinterfaces must have different VLAN IDs.

C. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in the same subnet.

D. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in different subnets.

Show Suggested Answer

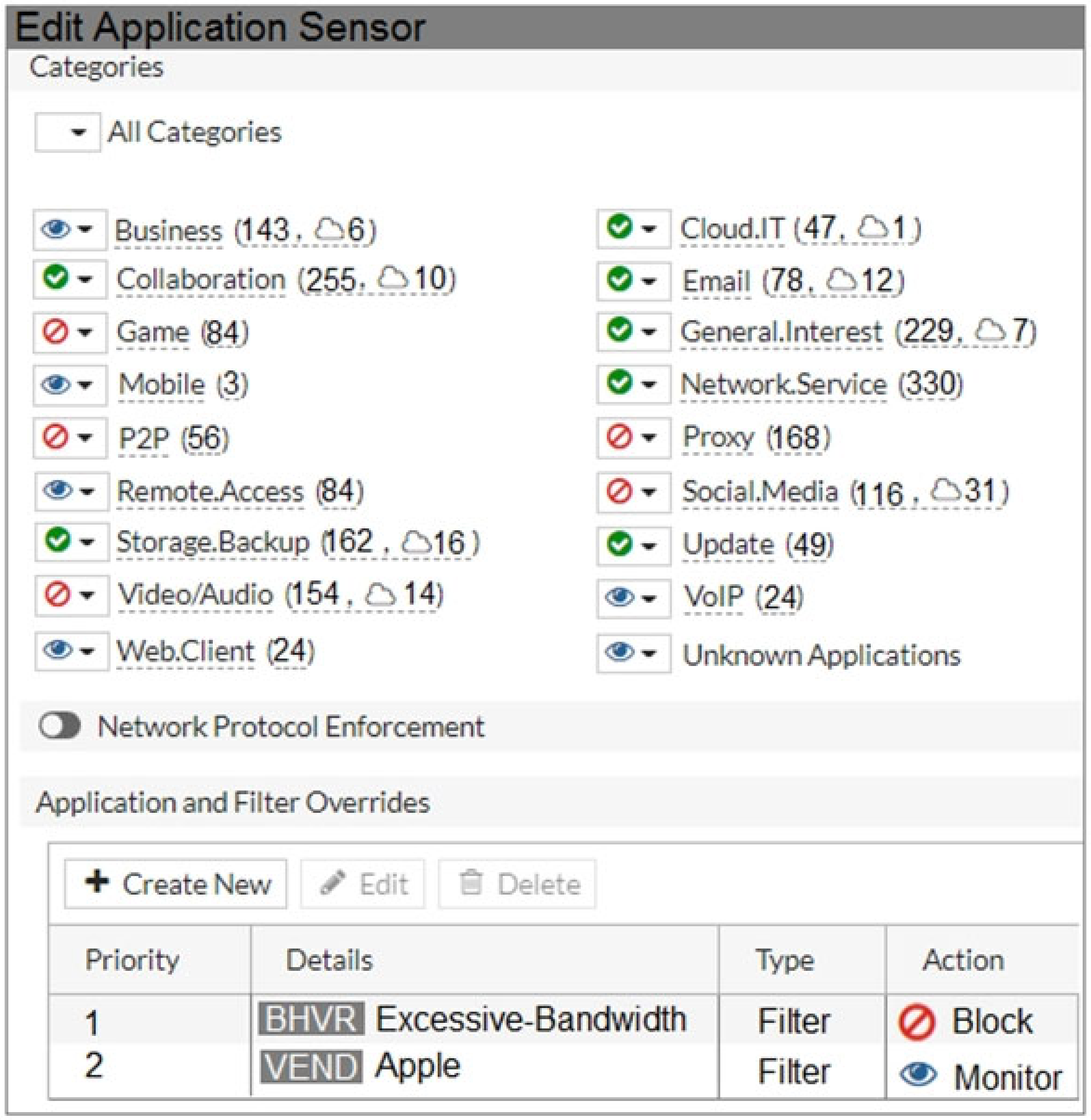
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 9

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit to view the application control profile.



Edit Application Sensor

Categories

▾ All Categories

👁 ▾ Business (143, ☁6)	✓ ▾ Cloud.IT (47, ☁1)
✓ ▾ Collaboration (255, ☁10)	✓ ▾ Email (78, ☁12)
⊘ ▾ Game (84)	✓ ▾ General.Interest (229, ☁7)
👁 ▾ Mobile (3)	✓ ▾ Network.Service (330)
⊘ ▾ P2P (56)	⊘ ▾ Proxy (168)
👁 ▾ Remote.Access (84)	⊘ ▾ Social.Media (116, ☁31)
✓ ▾ Storage.Backup (162, ☁16)	✓ ▾ Update (49)
⊘ ▾ Video/Audio (154, ☁14)	👁 ▾ VoIP (24)
👁 ▾ Web.Client (24)	👁 ▾ Unknown Applications

○ Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	⊘ Block
2	VEND Apple	Filter	👁 Monitor

Users who use Apple FaceTime video conferences are unable to set up meetings.

In this scenario, which statement is true?

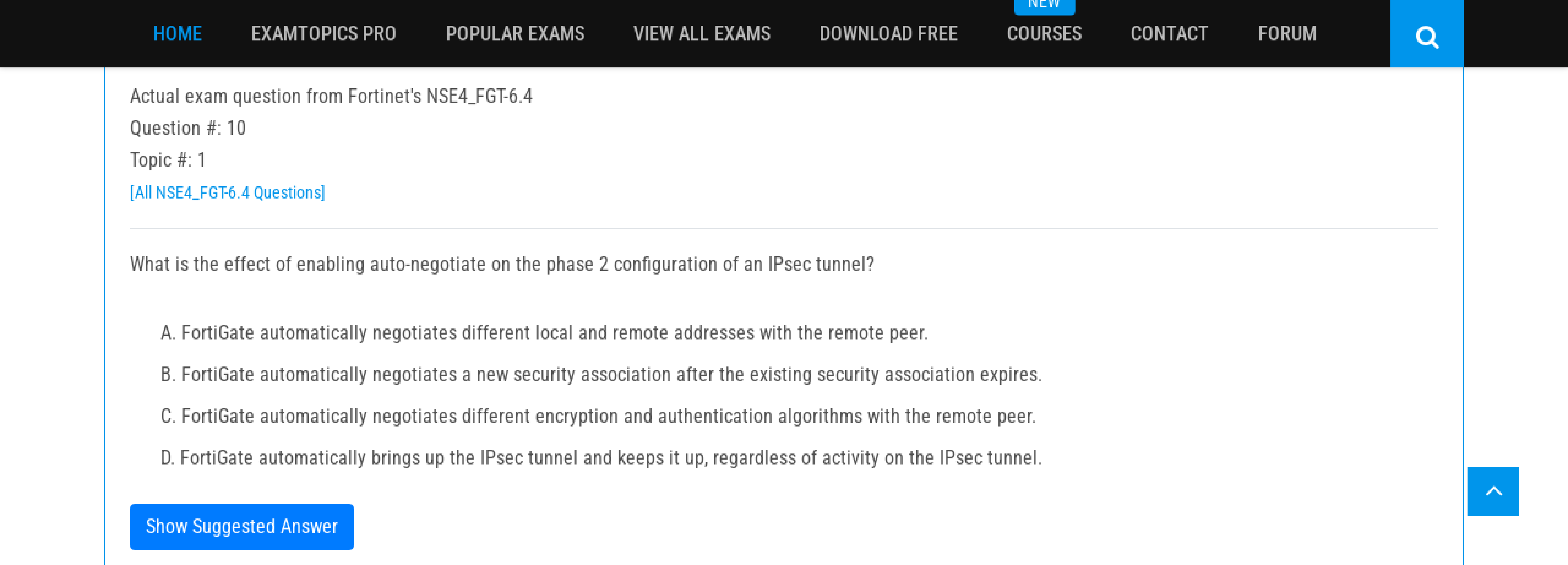
A. Apple FaceTime belongs to the custom monitored filter.

B. The category of Apple FaceTime is being monitored.

C. Apple FaceTime belongs to the custom blocked filter.

D. The category of Apple FaceTime is being blocked.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 10

Topic #: 1

[All NSE4_FGT-6.4 Questions]

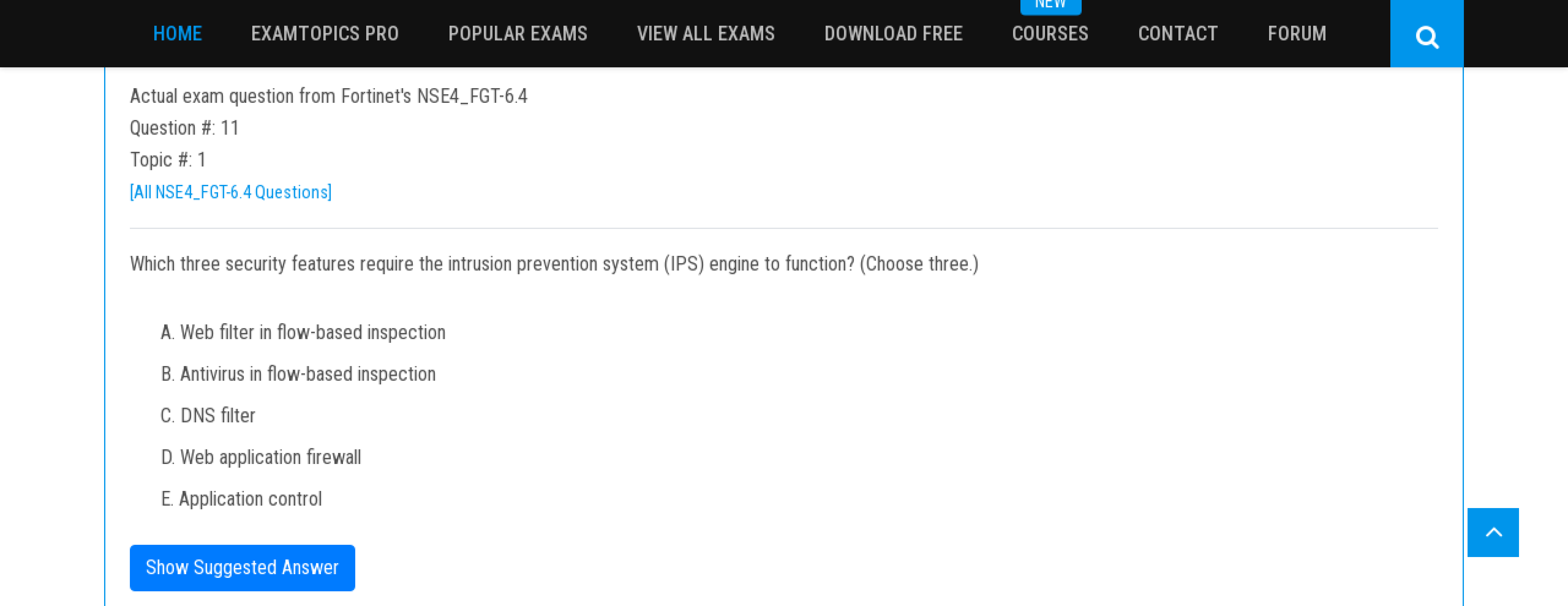
What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

A. FortiGate automatically negotiates different local and remote addresses with the remote peer.

B. FortiGate automatically negotiates a new security association after the existing security association expires.

C. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.

D. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 11

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

A. Web filter in flow-based inspection

B. Antivirus in flow-based inspection

C. DNS filter

D. Web application firewall

E. Application control

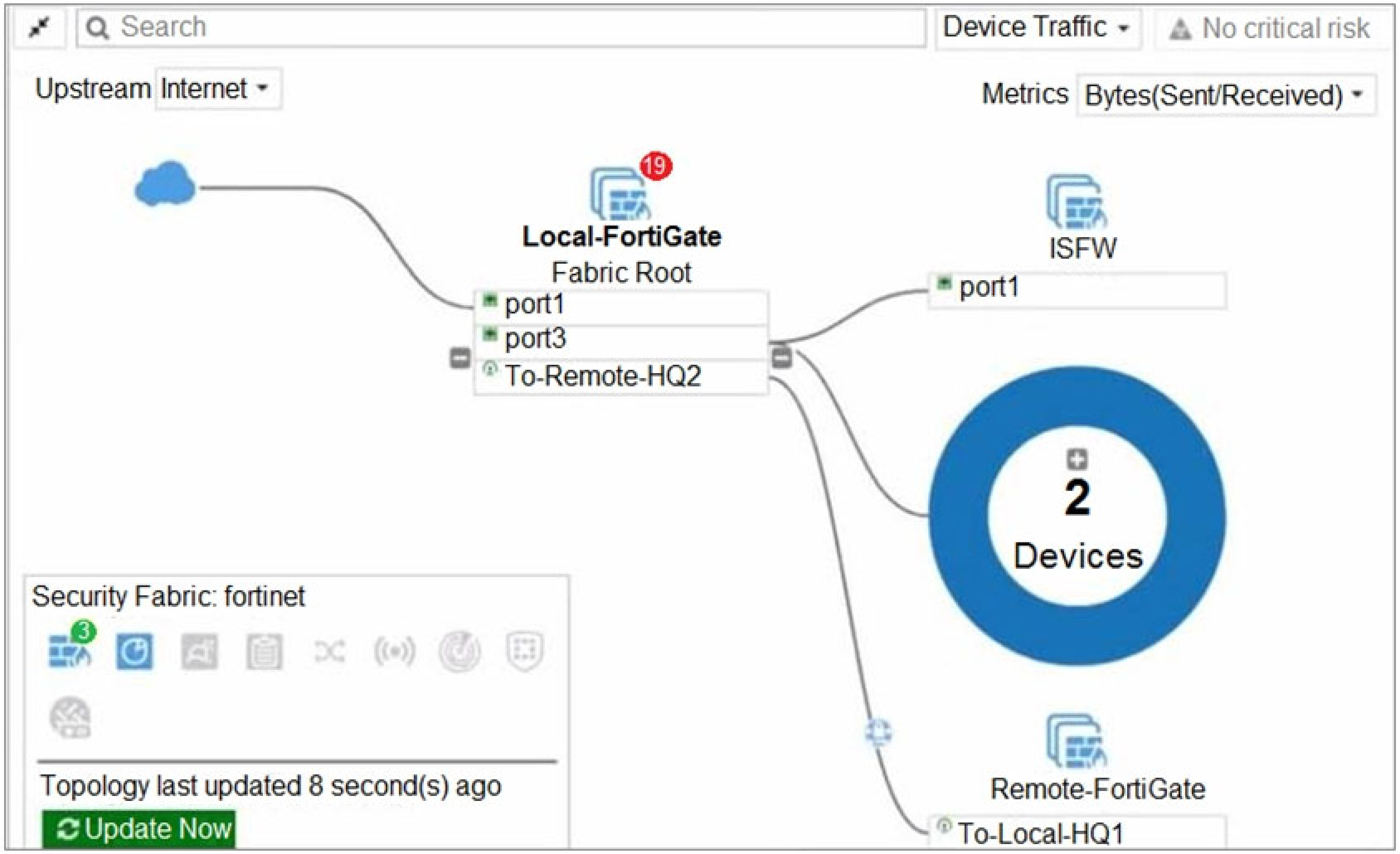
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 12

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

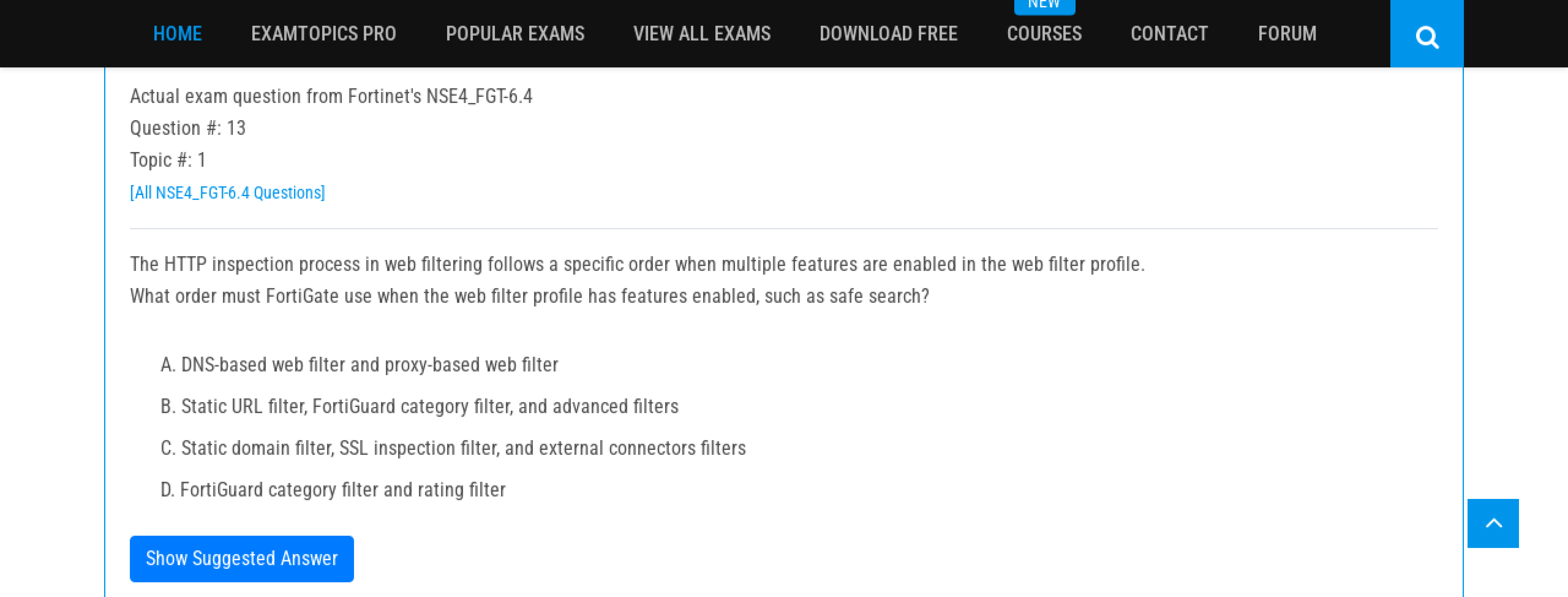
A. There are five devices that are part of the security fabric.

B. Device detection is disabled on all FortiGate devices.

C. This security fabric topology is a logical topology view.

D. There are 19 security recommendations for the security fabric.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 13

Topic #: 1

[All NSE4_FGT-6.4 Questions]

The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile.

What order must FortiGate use when the web filter profile has features enabled, such as safe search?

A. DNS-based web filter and proxy-based web filter

B. Static URL filter, FortiGuard category filter, and advanced filters

C. Static domain filter, SSL inspection filter, and external connectors filters

D. FortiGuard category filter and rating filter

Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 14

Topic #: 1

[All NSE4_FGT-6.4 Questions]

When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

A. Log ID

B. Universally Unique Identifier

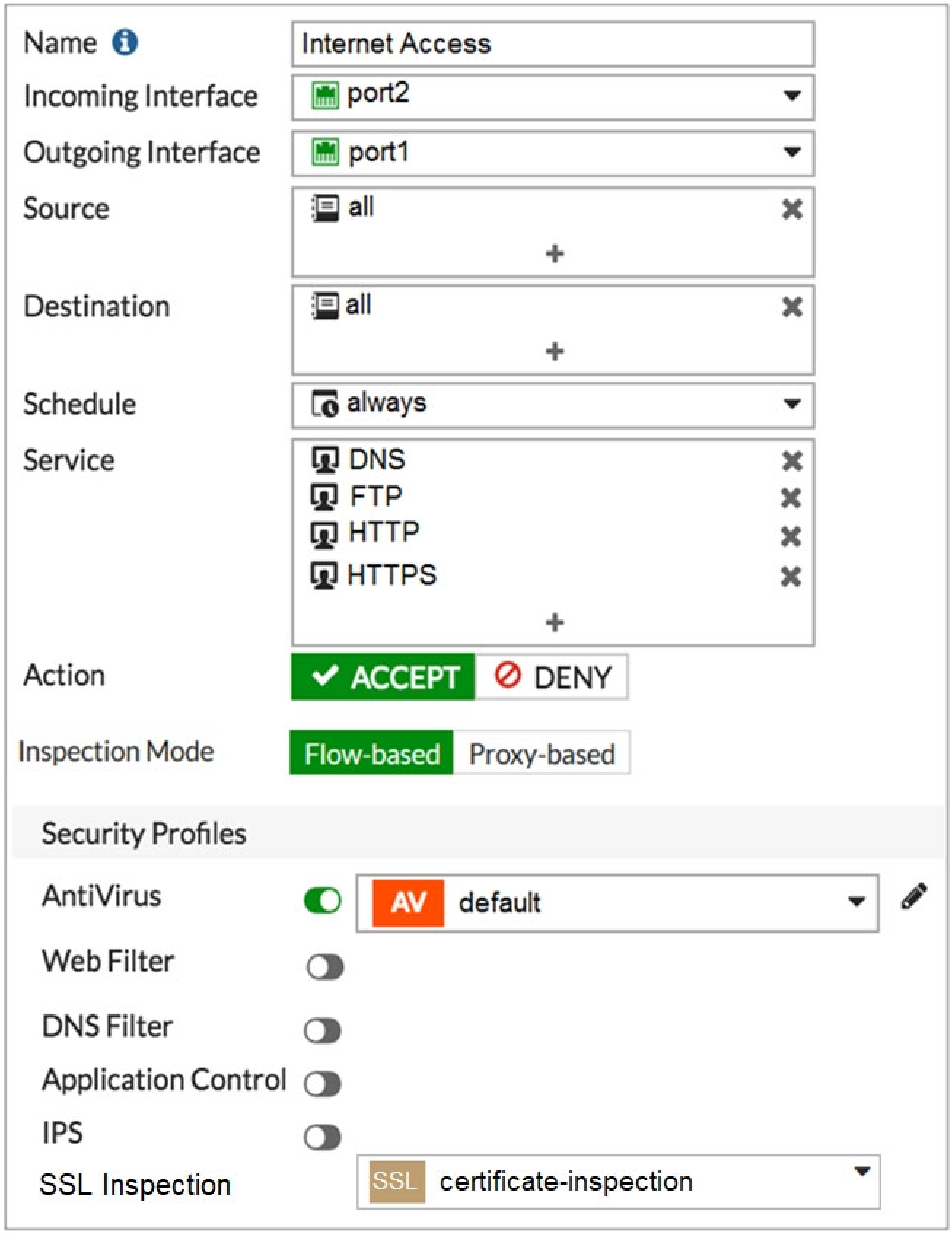
C. Policy ID

D. Sequence ID

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 15
Topic #: 1
[All NSE4_FGT-6.4 Questions]

Refer to the exhibit to view the firewall policy.



Name: Internet Access
Incoming Interface: port2
Outgoing Interface: port1
Source: all
Destination: all
Schedule: always
Service: DNS, FTP, HTTP, HTTPS
Action: ✓ ACCEPT | DENY
Inspection Mode: Flow-based | Proxy-based

Security Profiles

AntiVirus: ● AV default
Web Filter: ○
DNS Filter: ○
Application Control: ○
IPS: ○
SSL Inspection: SSL certificate-inspection

Which statement is correct if well-known viruses are not being blocked?

A. The firewall policy does not apply deep content inspection.

B. The firewall policy must be configured in proxy-based inspection mode.

C. The action on the firewall policy must be set to deny.

D. Web filter should be enabled on the firewall policy to complement the antivirus profile.

Show Suggested Answer

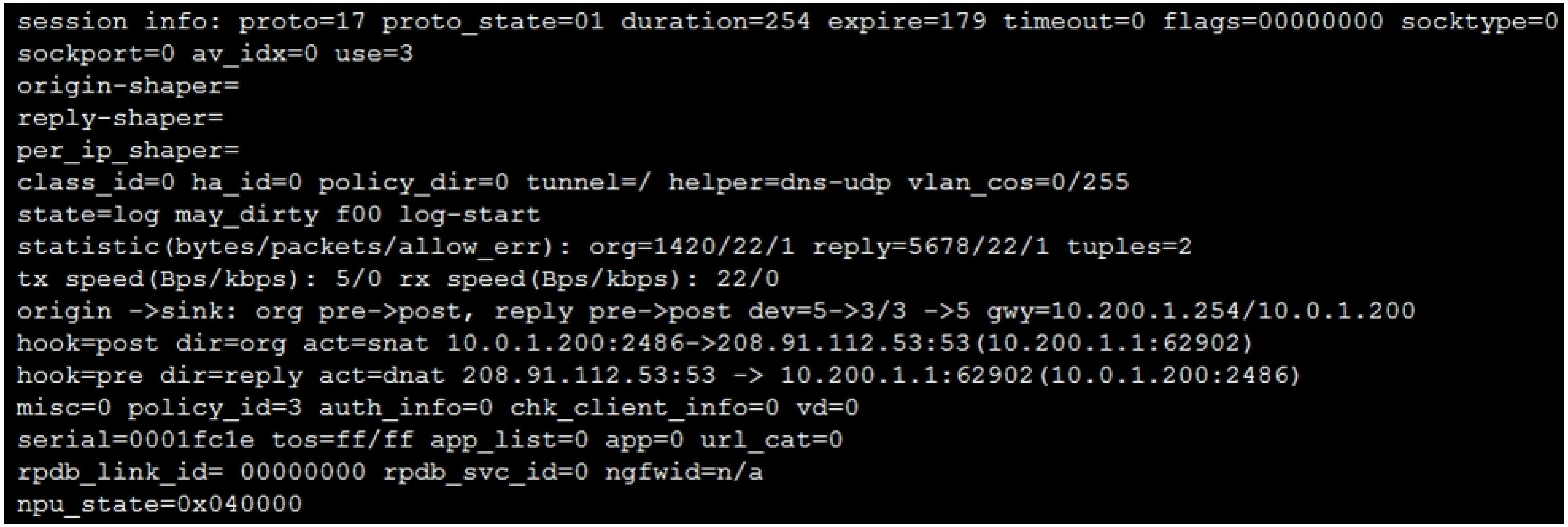
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 16

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit, which contains a session diagnostic output.



```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin ->sink: org pre->post, reply pre->post dev=5->3/3 ->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53 -> 10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

A. The session is a UDP unidirectional state.

B. The session is in TCP ESTABLISHED state.

C. The session is a bidirectional UDP connection.

D. The session is a bidirectional TCP connection.

Show Suggested Answer

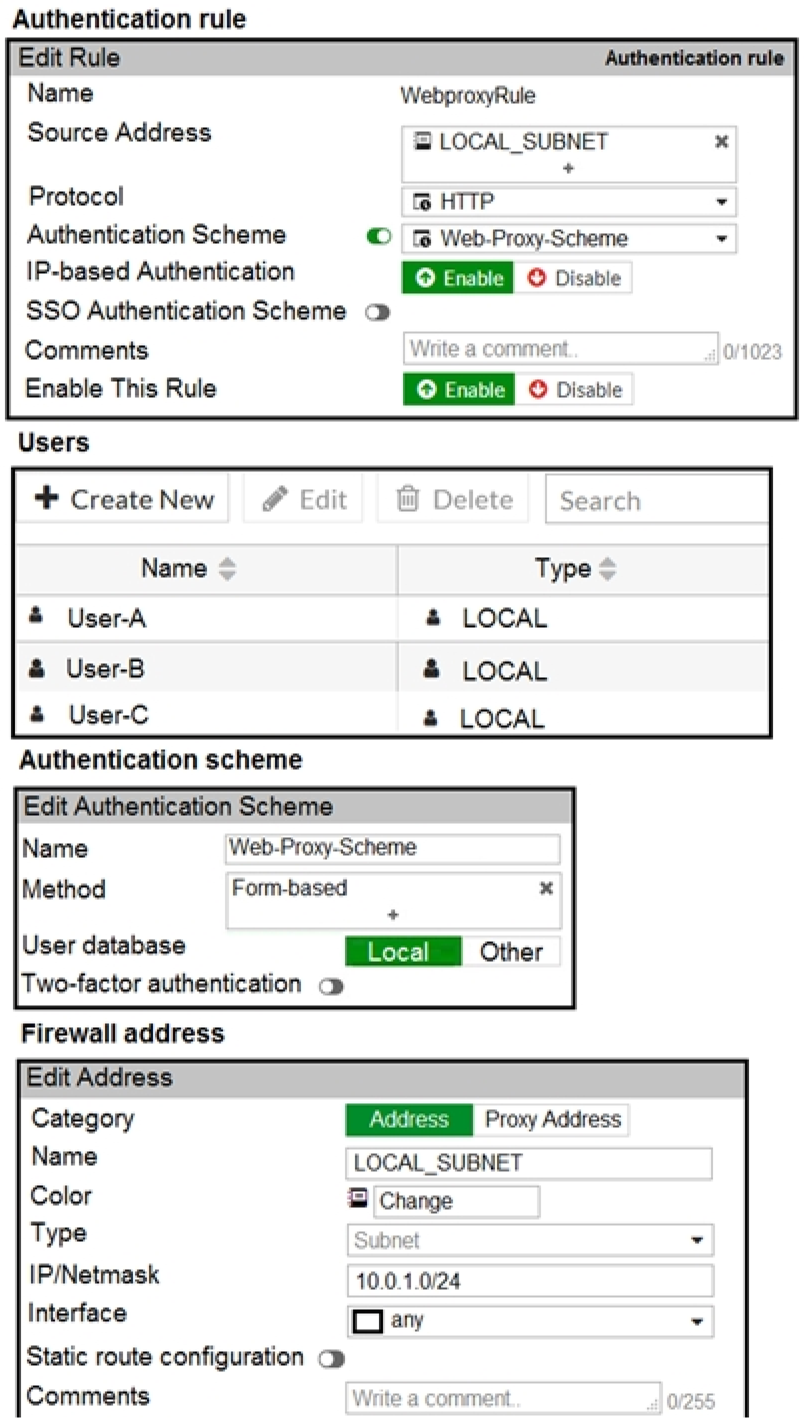
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 17

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



Authentication rule

Edit Rule — Authentication rule

Name	WebproxyRule
Source Address	LOCAL_SUBNET ✖ +
Protocol	HTTP
Authentication Scheme ●	Web-Proxy-Scheme
IP-based Authentication	[✓ Enable] Disable
SSO Authentication Scheme ○	
Comments	Write a comment.. 0/1023
Enable This Rule	[✓ Enable] Disable

Users

Create New Edit Delete Search

Name	Type
User-A	LOCAL
User-B	LOCAL
User-C	LOCAL

Authentication scheme

Edit Authentication Scheme

Name	Web-Proxy-Scheme
Method	Form-based ✖ +
User database	[✓ Local] Other
Two-factor authentication ○	

Firewall address

Edit Address

Category	[✓ Address] Proxy Address
Name	LOCAL_SUBNET
Color	Change
Type	Subnet
IP/Netmask	10.0.1.0/24
Interface	any
Static route configuration ○	
Comments	Write a comment.. 0/255

The exhibit shows proxy policies and proxy addresses, the authentication rule and authentication scheme, users, and firewall address.

An explicit web proxy is configured for subnet range 10.0.1.0/24 with three explicit web proxy policies.

The authentication rule is configured to authenticate HTTP requests for subnet range 10.0.1.0/24 with a form-based authentication scheme for the FortiGate local user database. Users will be prompted for authentication.

How will FortiGate process the traffic when the HTTP request comes from a machine with the source IP 10.0.1.10 to the destination http:// www.fortinet.com?

(Choose two.)

A. If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.

B. If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.

C. If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.

D. If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.

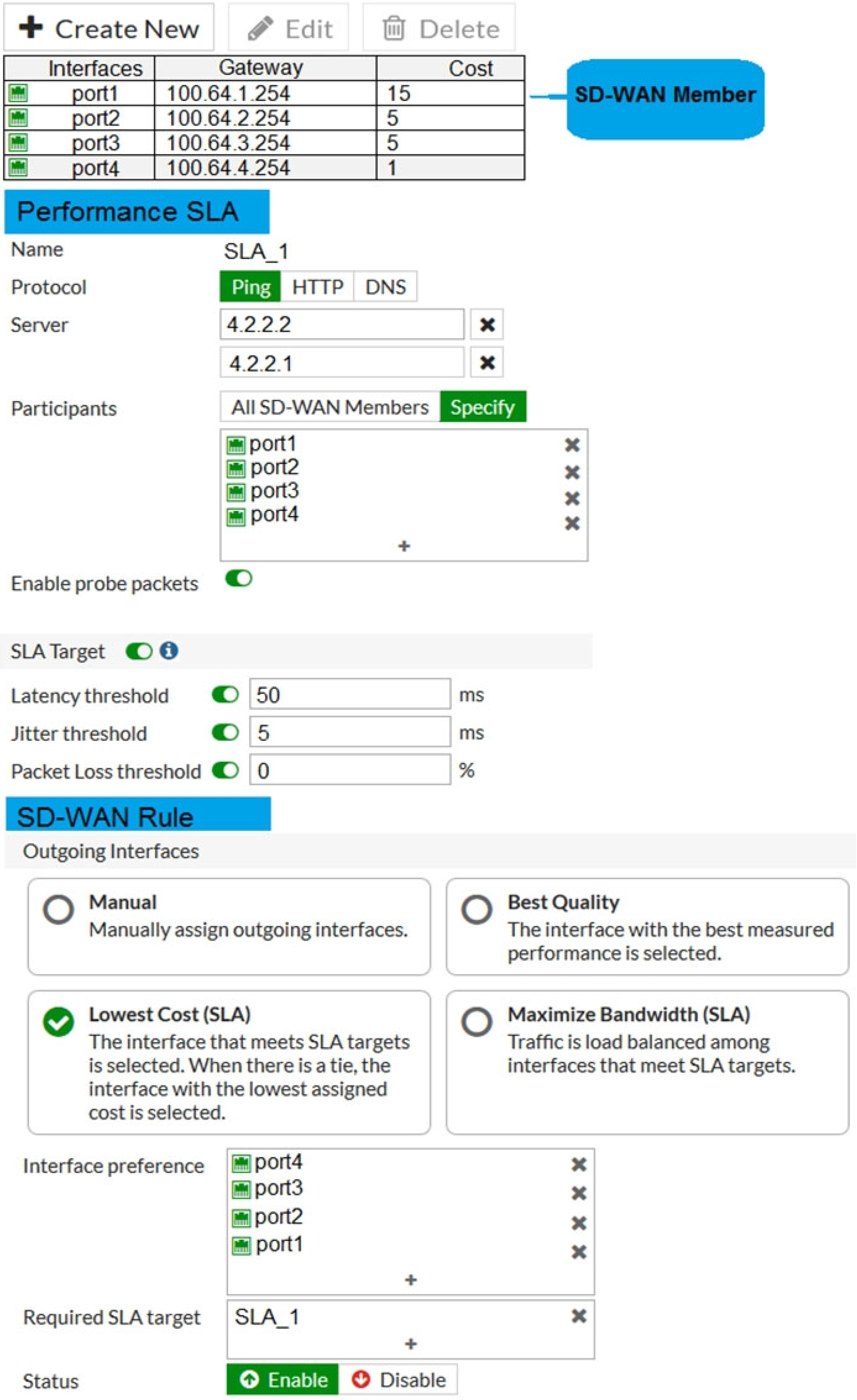
E. If a Mozilla Firefox browser is used with User-C credentials, the HTTP request will be denied.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 18
Topic #: 1
[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.

Exhibit A -



Interfaces	Gateway	Cost
port1	100.64.1.254	15
port2	100.64.2.254	5
port3	100.64.3.254	5
port4	100.64.4.254	1

Performance SLA

Name SLA_1
Protocol [✓ Ping] HTTP DNS
Server 4.2.2.2
4.2.2.1
Participants All SD-WAN Members [✓ Specify]
port1
port2
port3
port4
Enable probe packets ●

SLA Target ●
Latency threshold ● 50 ms
Jitter threshold ● 5 ms
Packet Loss threshold ● 0 %

SD-WAN Rule

Outgoing Interfaces

○ **Manual**
Manually assign outgoing interfaces.

○ **Best Quality**
The interface with the best measured performance is selected.

✓ **Lowest Cost (SLA)**
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.

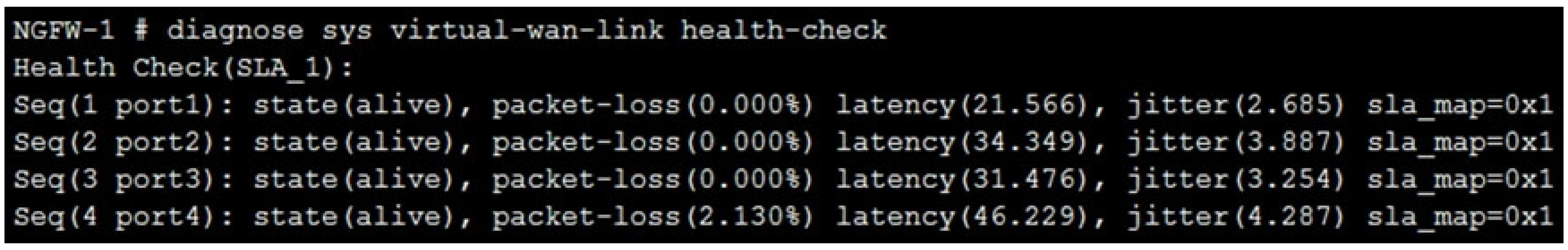
○ **Maximize Bandwidth (SLA)**
Traffic is load balanced among interfaces that meet SLA targets.

Interface preference port4
port3
port2
port1

Required SLA target SLA_1

Status [✓ Enable] Disable

Exhibit B -



```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(SLA_1):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x1
Seq(2 port2): state(alive), packet-loss(0.000%) latency(34.349), jitter(3.887) sla_map=0x1
Seq(3 port3): state(alive), packet-loss(0.000%) latency(31.476), jitter(3.254) sla_map=0x1
Seq(4 port4): state(alive), packet-loss(2.130%) latency(46.229), jitter(4.287) sla_map=0x1
```

The exhibit shows the configuration for the SD-WAN member, Performance SLA and SD-WAN Rule, as well as the output of diagnose sys virtual-wan- link health-check.
Which interface will be selected as an outgoing interface?

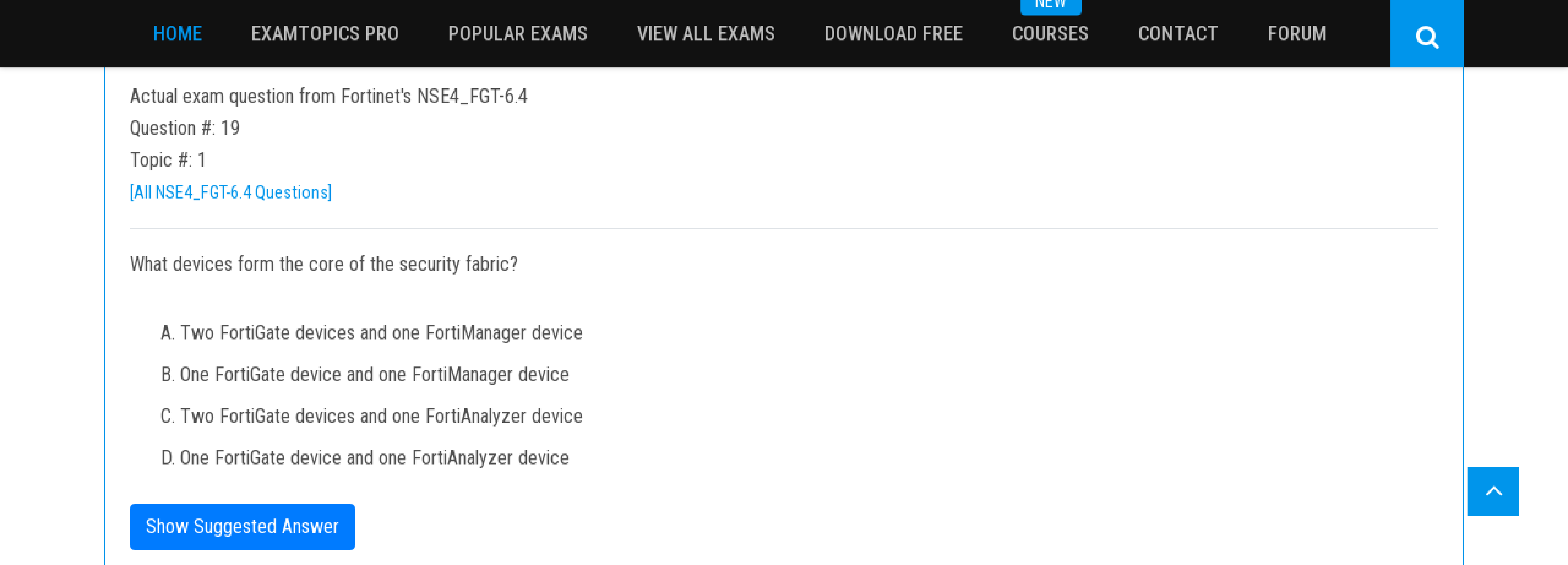
A. port4

B. port2

C. port1

D. port3

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 19

Topic #: 1

[All NSE4_FGT-6.4 Questions]

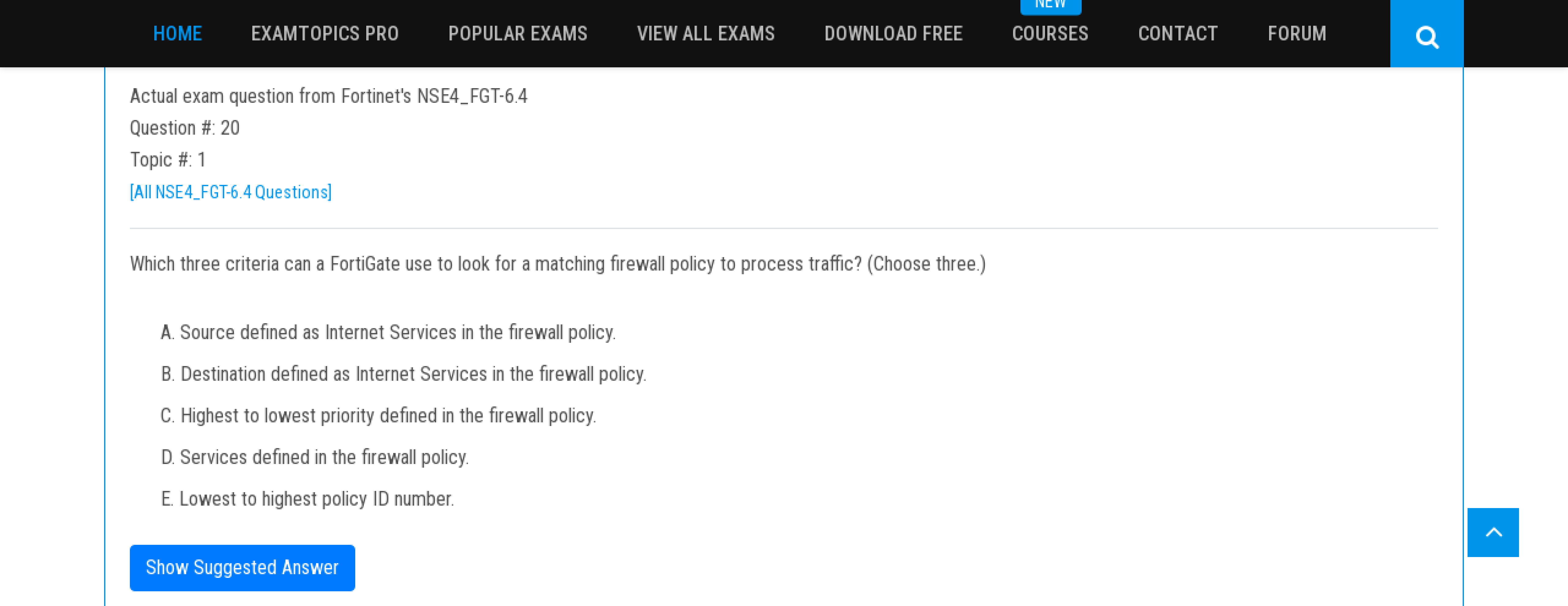
What devices form the core of the security fabric?

A. Two FortiGate devices and one FortiManager device

B. One FortiGate device and one FortiManager device

C. Two FortiGate devices and one FortiAnalyzer device

D. One FortiGate device and one FortiAnalyzer device



Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 20
Topic #: 1
[All NSE4_FGT-6.4 Questions]

Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

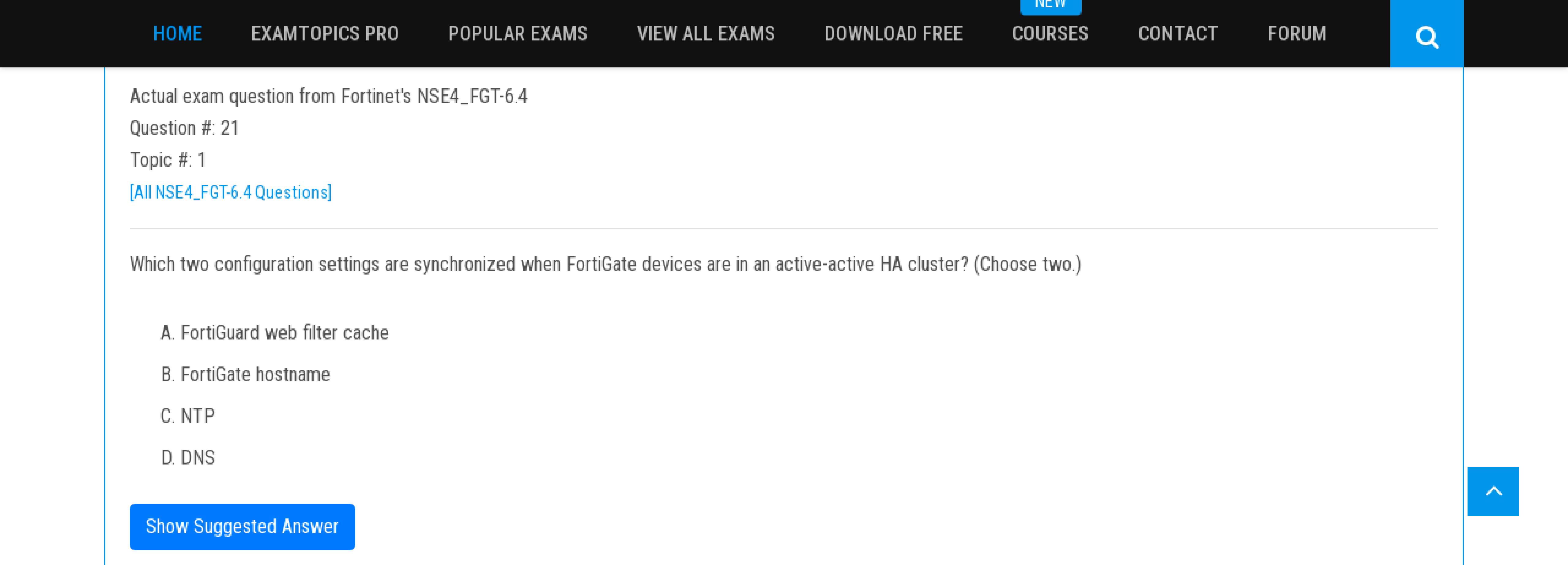
A. Source defined as Internet Services in the firewall policy.

B. Destination defined as Internet Services in the firewall policy.

C. Highest to lowest priority defined in the firewall policy.

D. Services defined in the firewall policy.

E. Lowest to highest policy ID number.



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 21

Topic #: 1

[All NSE4_FGT-6.4 Questions]

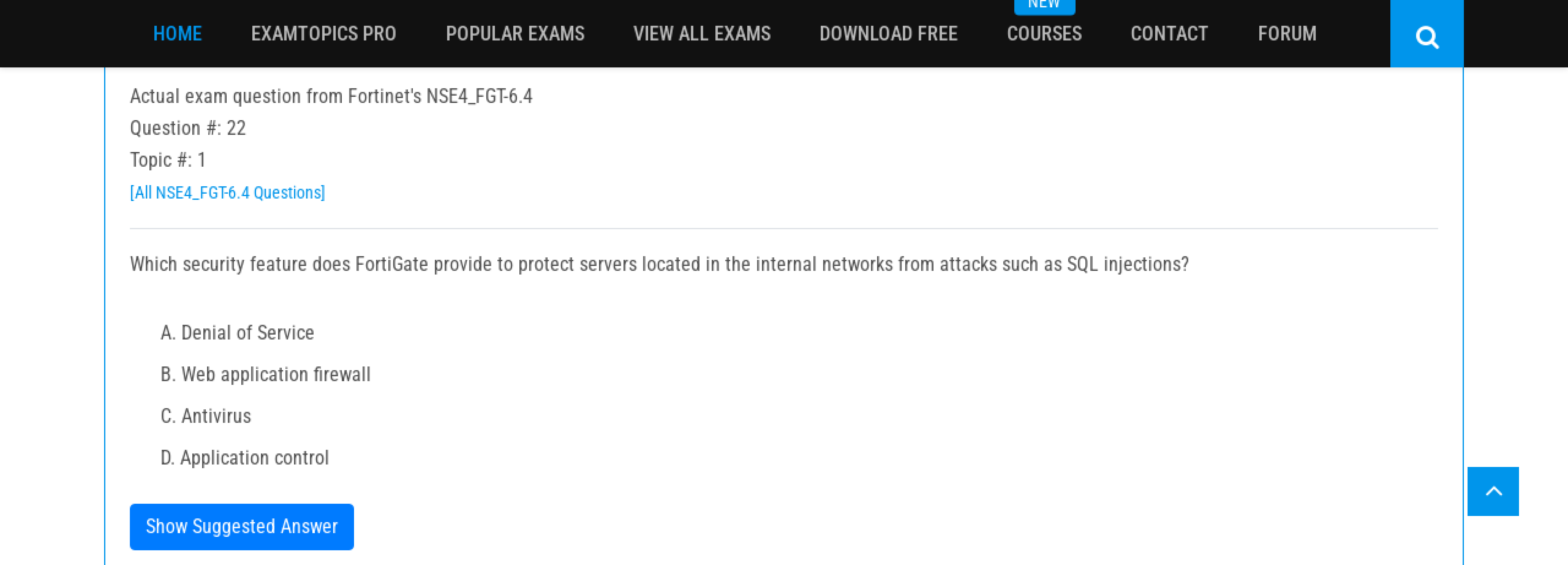
Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

A. FortiGuard web filter cache

B. FortiGate hostname

C. NTP

D. DNS



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 22

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which security feature does FortiGate provide to protect servers located in the internal networks from attacks such as SQL injections?

A. Denial of Service

B. Web application firewall

C. Antivirus

D. Application control

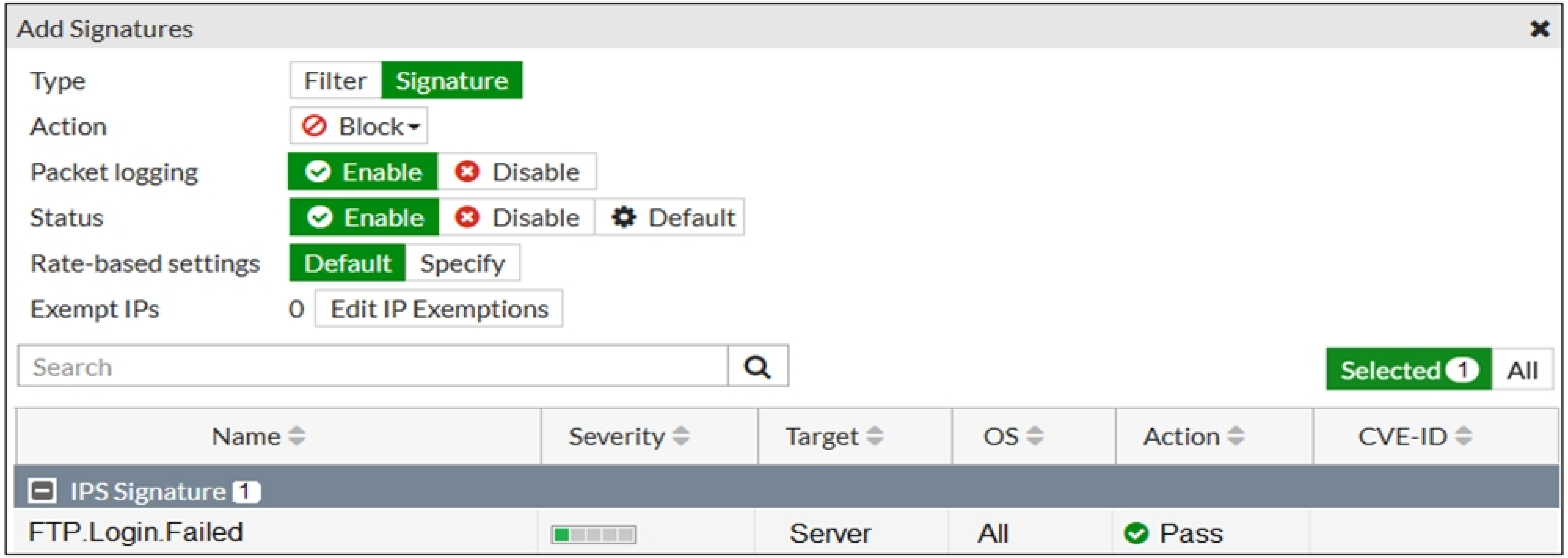
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 23

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



Add Signatures ✖

Type: Filter [✓ Signature]

Action: ⊘ Block ▾

Packet logging: [✓ Enable] ✖ Disable

Status: [✓ Enable] ✖ Disable ⚙ Default

Rate-based settings: [✓ Default] Specify

Exempt IPs: 0 Edit IP Exemptions

Search 🔍 [✓ Selected 1] All

Name	Severity	Target	OS	Action	CVE-ID
⊟ IPS Signature 1					
FTP.Login.Failed	▮▯▯▯▯	Server	All	✓ Pass	

Review the Intrusion Prevention System (IPS) profile signature settings.

Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

A. Traffic matching the signature will be silently dropped and logged.

B. The signature setting uses a custom rating threshold.

C. The signature setting includes a group of other signatures.

D. Traffic matching the signature will be allowed and logged.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 24

Topic #: 1

[All NSE4_FGT-6.4 Questions]

How does FortiGate act when using SSL VPN in web mode?

A. FortiGate acts as an FDS server.

B. FortiGate acts as an HTTP reverse proxy.

C. FortiGate acts as DNS server.

D. FortiGate acts as router.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-6.4

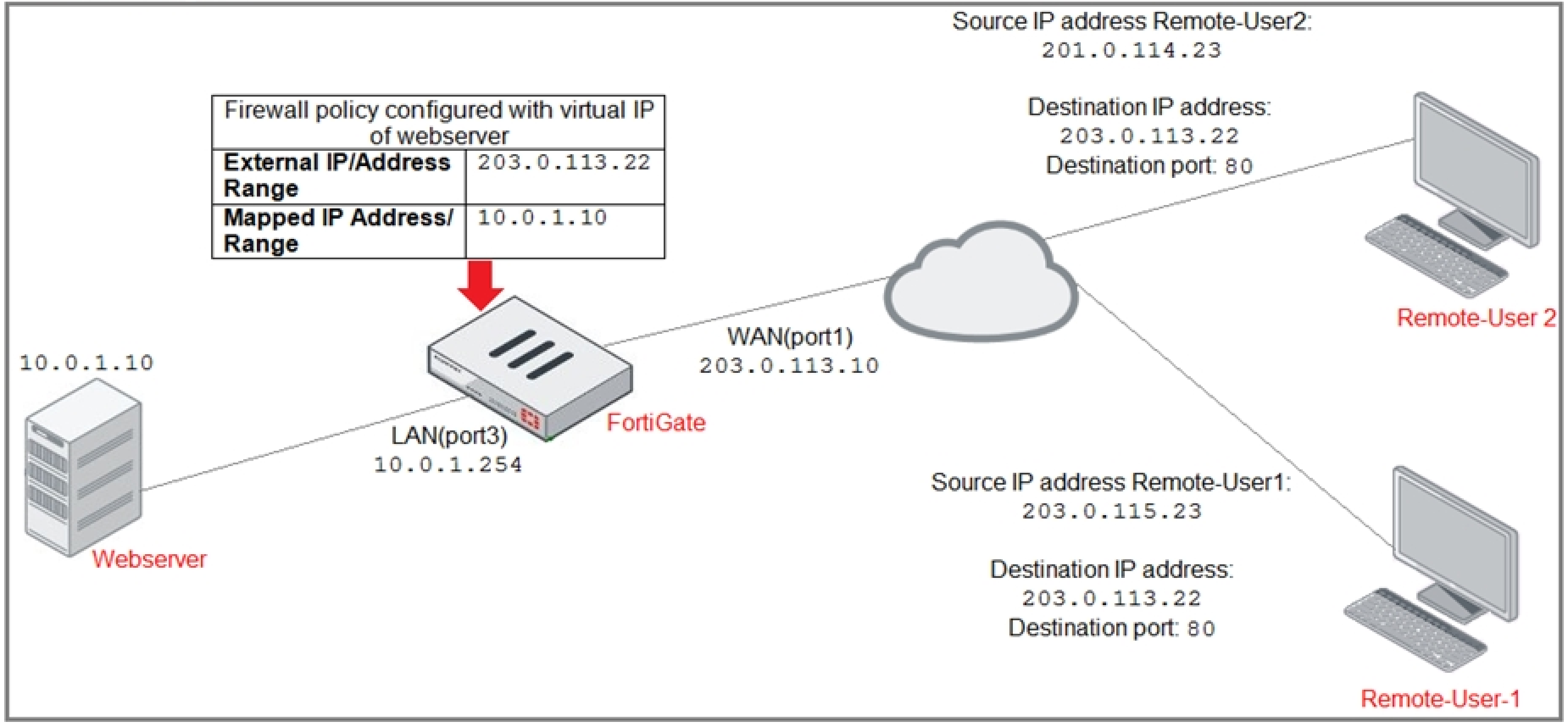
Question #: 25

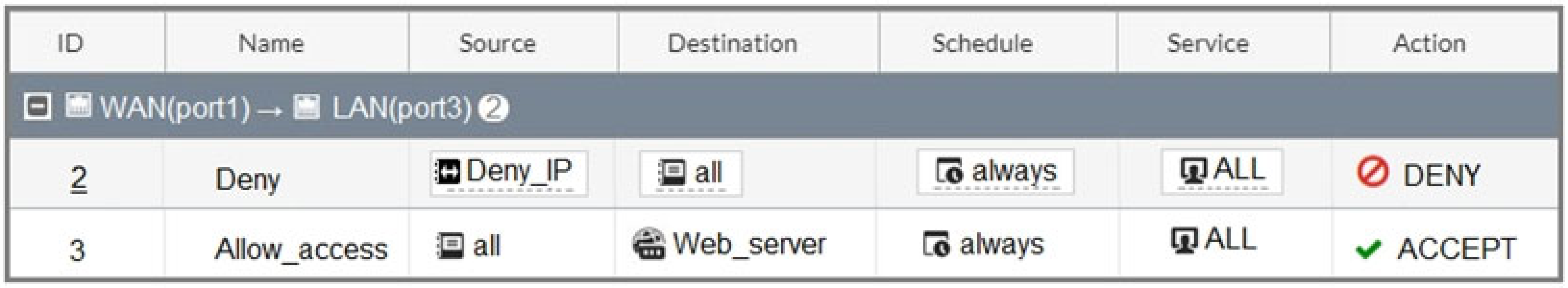
Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.

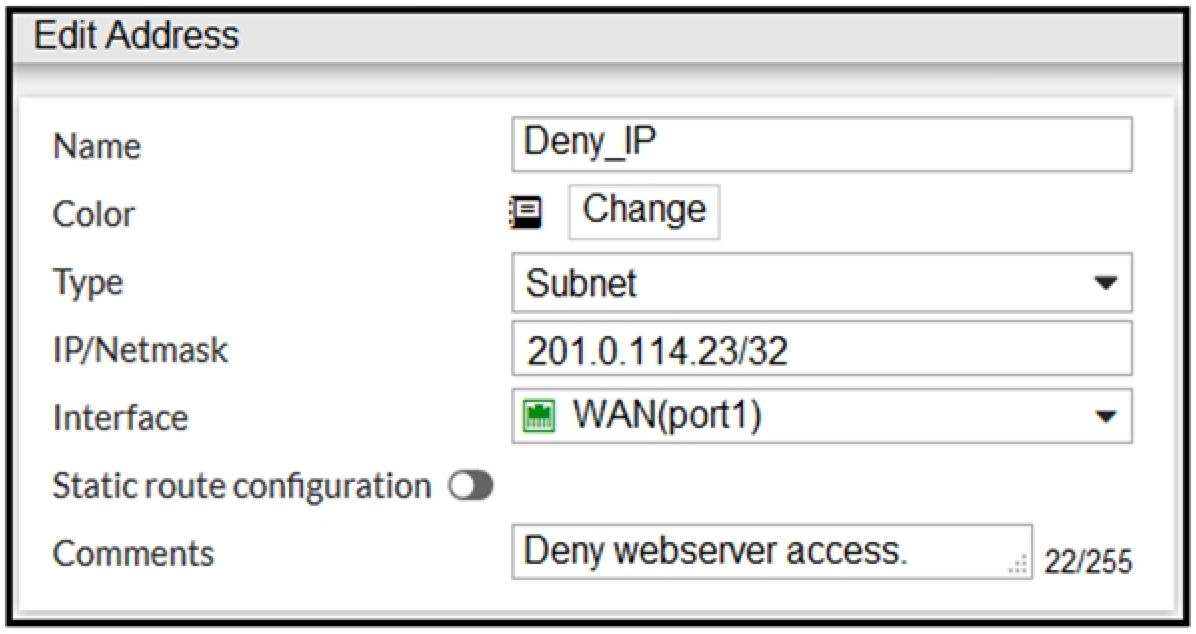
Network diagram





ID	Name	Source	Destination	Schedule	Service	Action
⊟ WAN(port1) → LAN(port3) 2						
2	Deny	Deny_IP	all	always	ALL	⊘ DENY
3	Allow_access	all	Web_server	always	ALL	✓ ACCEPT

Firewall address object



Edit Address

Name	Deny_IP
Color	Change
Type	Subnet
IP/Netmask	201.0.114.23/32
Interface	WAN(port1)
Static route configuration	○
Comments	Deny webserver access. 22/255

The exhibit contains a network diagram, firewall policies, and a firewall address object configuration.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-user2. Remote-user2 is still able to access Webserver.

Which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

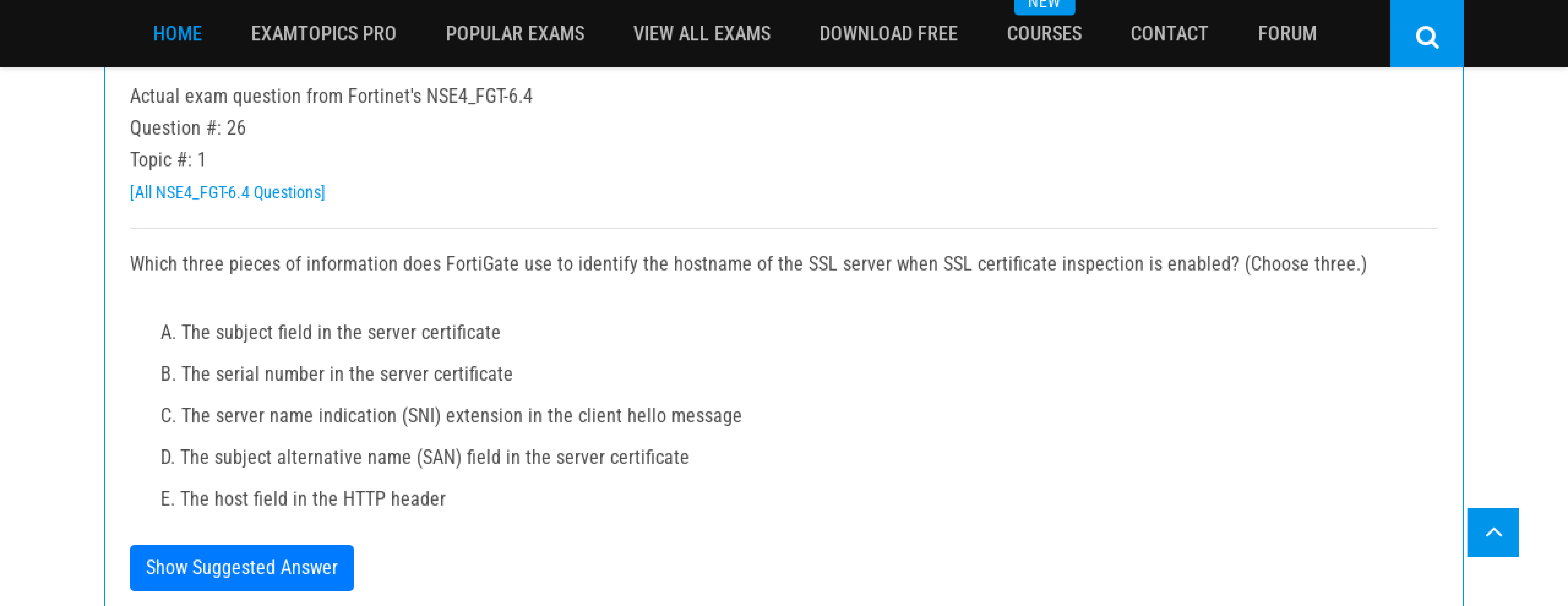
A. Disable match-vip in the Deny policy.

B. Set the Destination address as Deny_IP in the Allow-access policy.

C. Enable match-vip in the Deny policy.

D. Set the Destination address as Web_server in the Deny policy.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 26

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

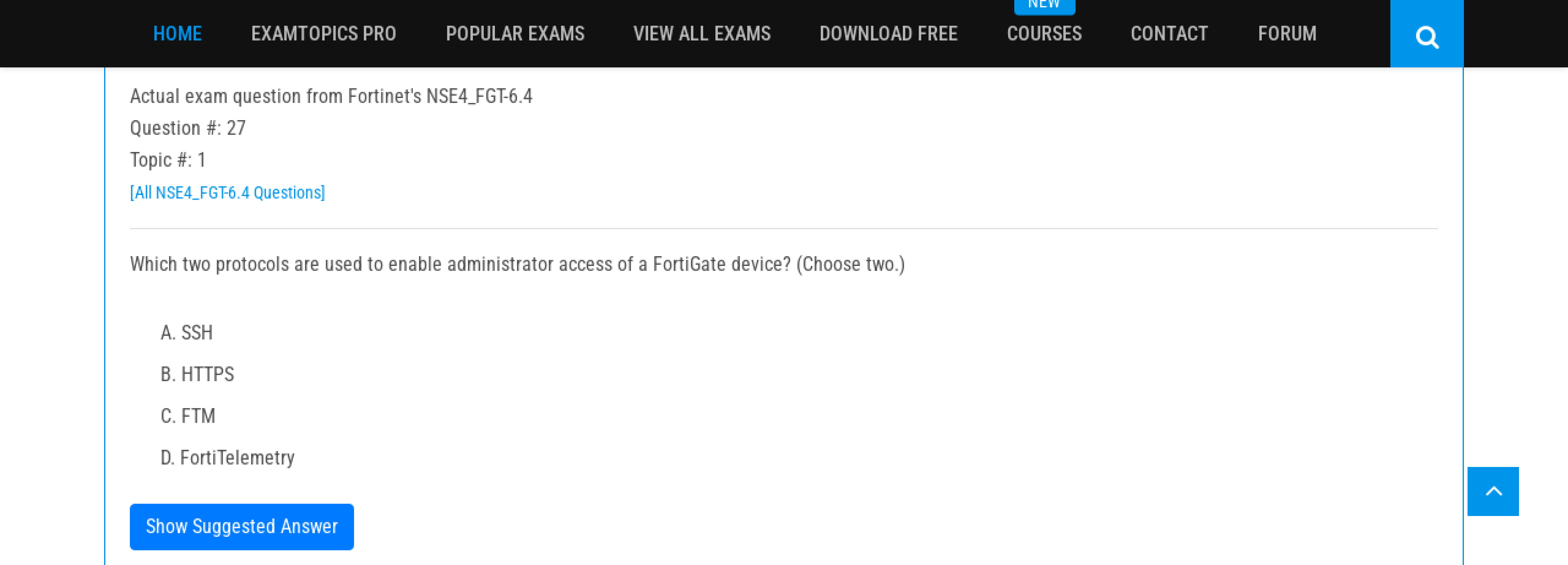
A. The subject field in the server certificate

B. The serial number in the server certificate

C. The server name indication (SNI) extension in the client hello message

D. The subject alternative name (SAN) field in the server certificate

E. The host field in the HTTP header



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 27

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

A. SSH

B. HTTPS

C. FTM

D. FortiTelemetry

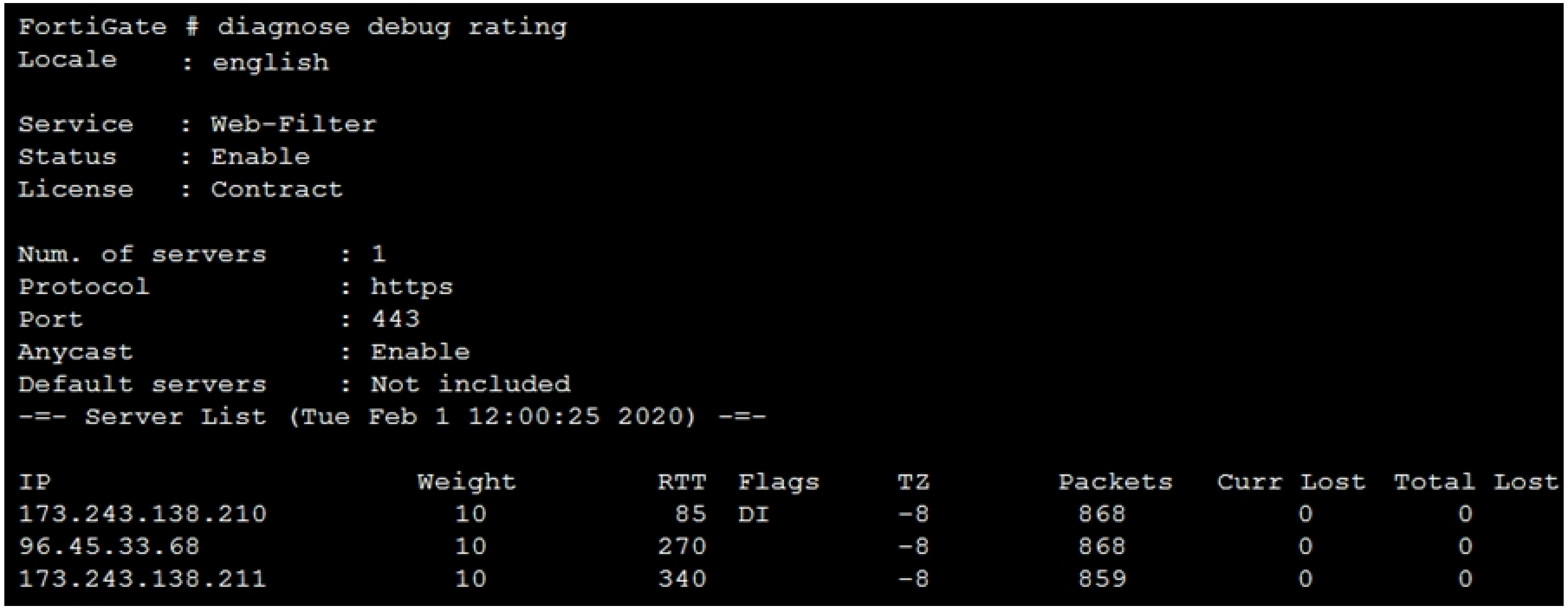
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 28

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the FortiGuard connection debug output.



```
FortiGate # diagnose debug rating
Locale     : english

Service    : Web-Filter
Status     : Enable
License    : Contract

Num. of servers     : 1
Protocol            : https
Port                : 443
Anycast             : Enable
Default servers     : Not included
-=- Server List (Tue Feb 1 12:00:25 2020) -=-

IP                      Weight        RTT  Flags     TZ        Packets   Curr Lost  Total Lost
173.243.138.210           10           85  DI        -8         868           0          0
96.45.33.68               10          270            -8         868           0          0
173.243.138.211           10          340            -8         859           0          0
```

Based on the output shown in the exhibit, which two statements are correct? (Choose two.)

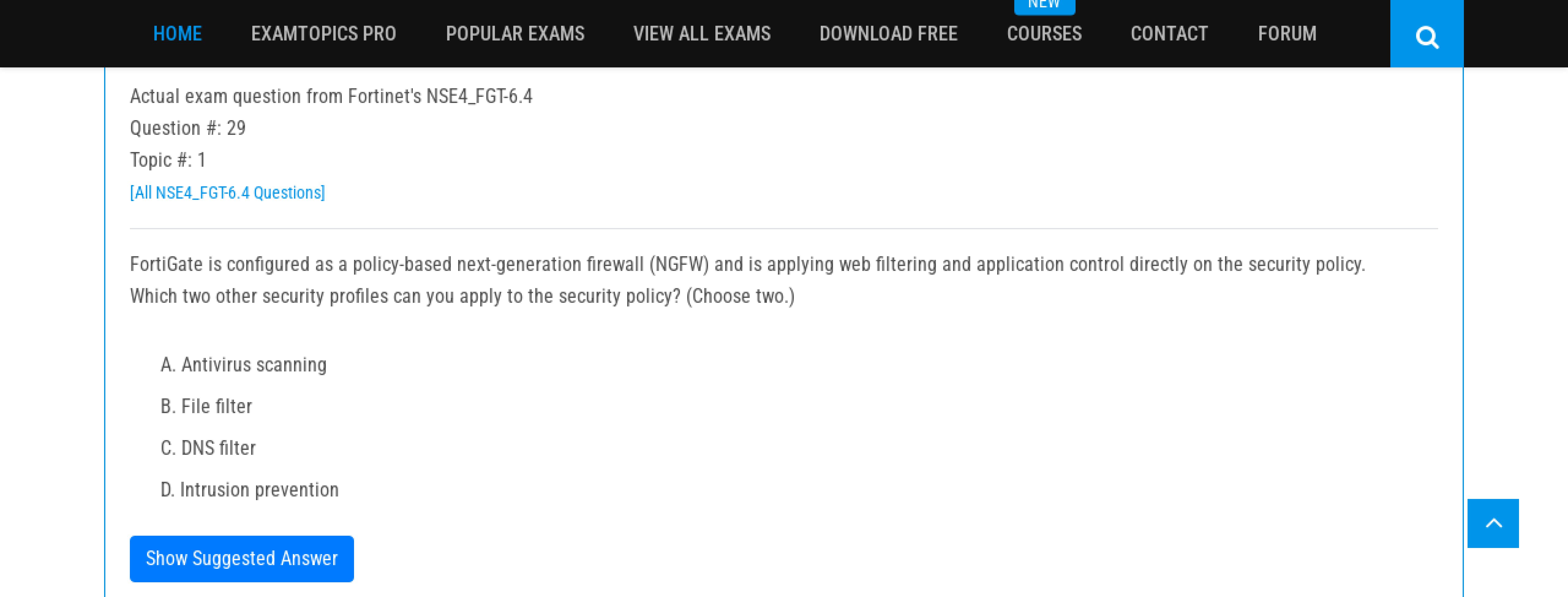
A. A local FortiManager is one of the servers FortiGate communicates with.

B. One server was contacted to retrieve the contract information.

C. There is at least one server that lost packets consecutively.

D. FortiGate is using default FortiGuard communication settings.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 29

Topic #: 1

[All NSE4_FGT-6.4 Questions]

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.

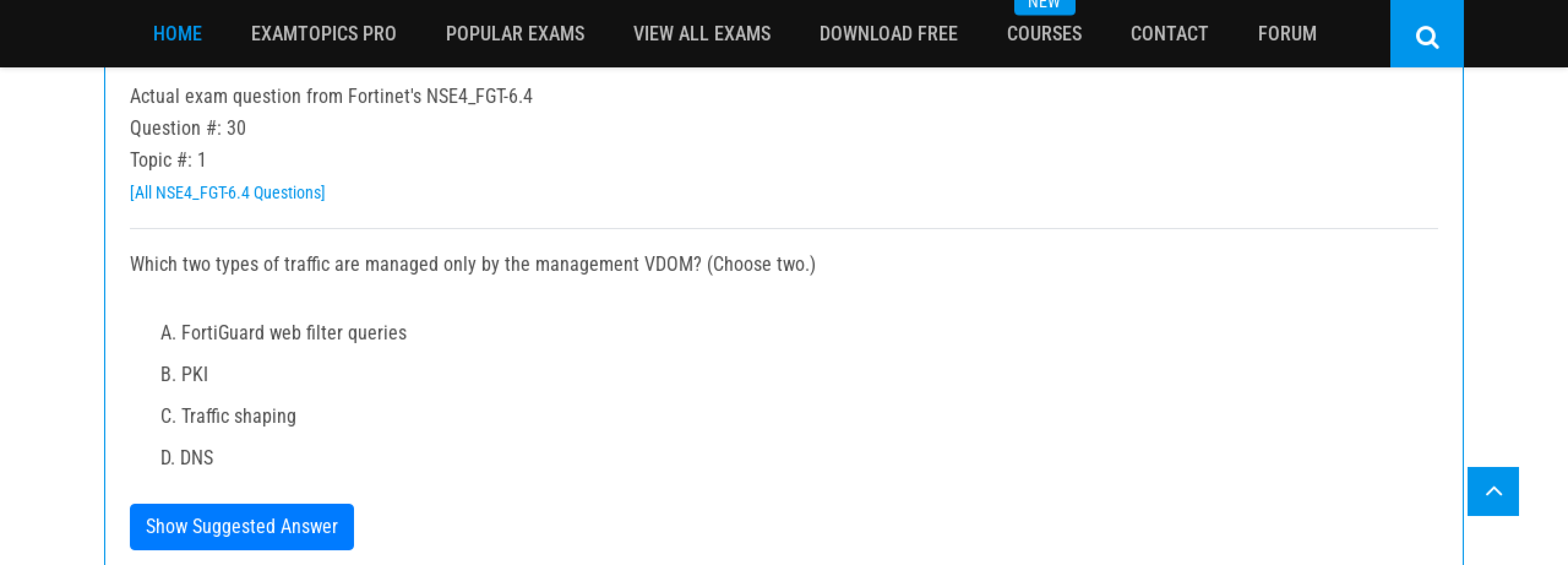
Which two other security profiles can you apply to the security policy? (Choose two.)

A. Antivirus scanning

B. File filter

C. DNS filter

D. Intrusion prevention



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 30

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which two types of traffic are managed only by the management VDOM? (Choose two.)

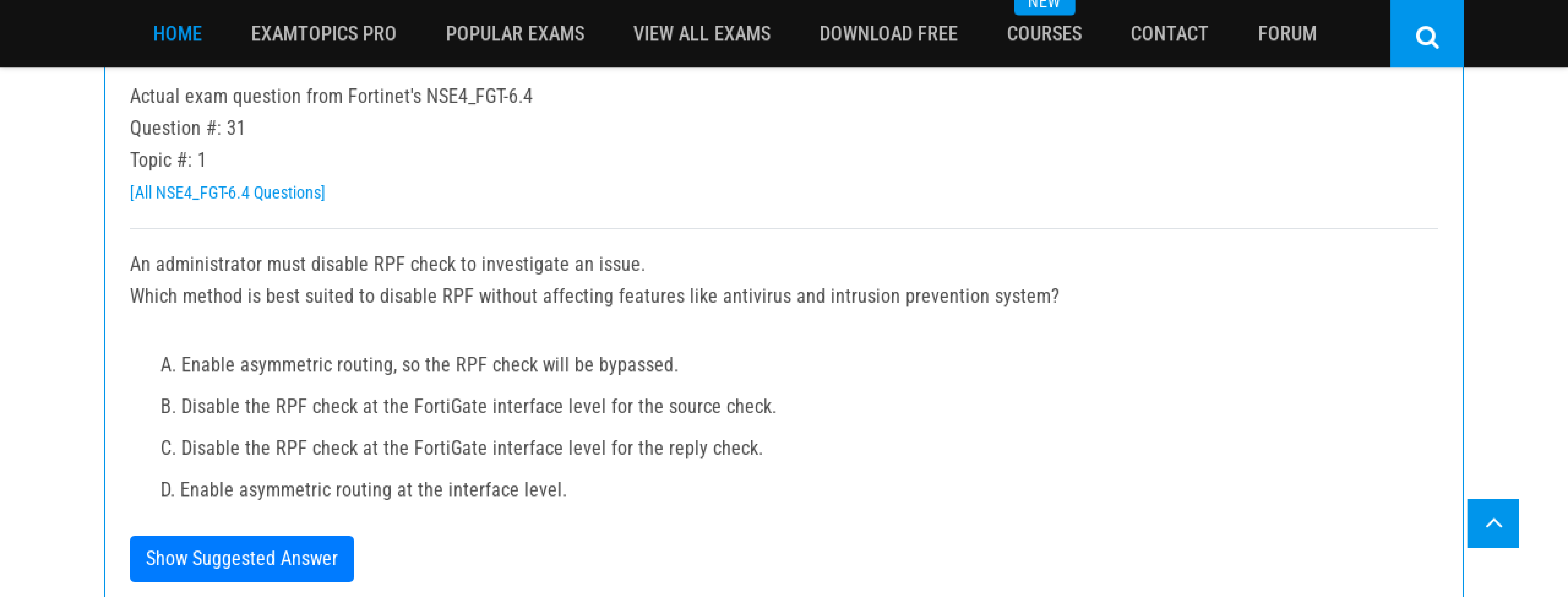
A. FortiGuard web filter queries

B. PKI

C. Traffic shaping

D. DNS

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 31

Topic #: 1

[All NSE4_FGT-6.4 Questions]

An administrator must disable RPF check to investigate an issue.

Which method is best suited to disable RPF without affecting features like antivirus and intrusion prevention system?

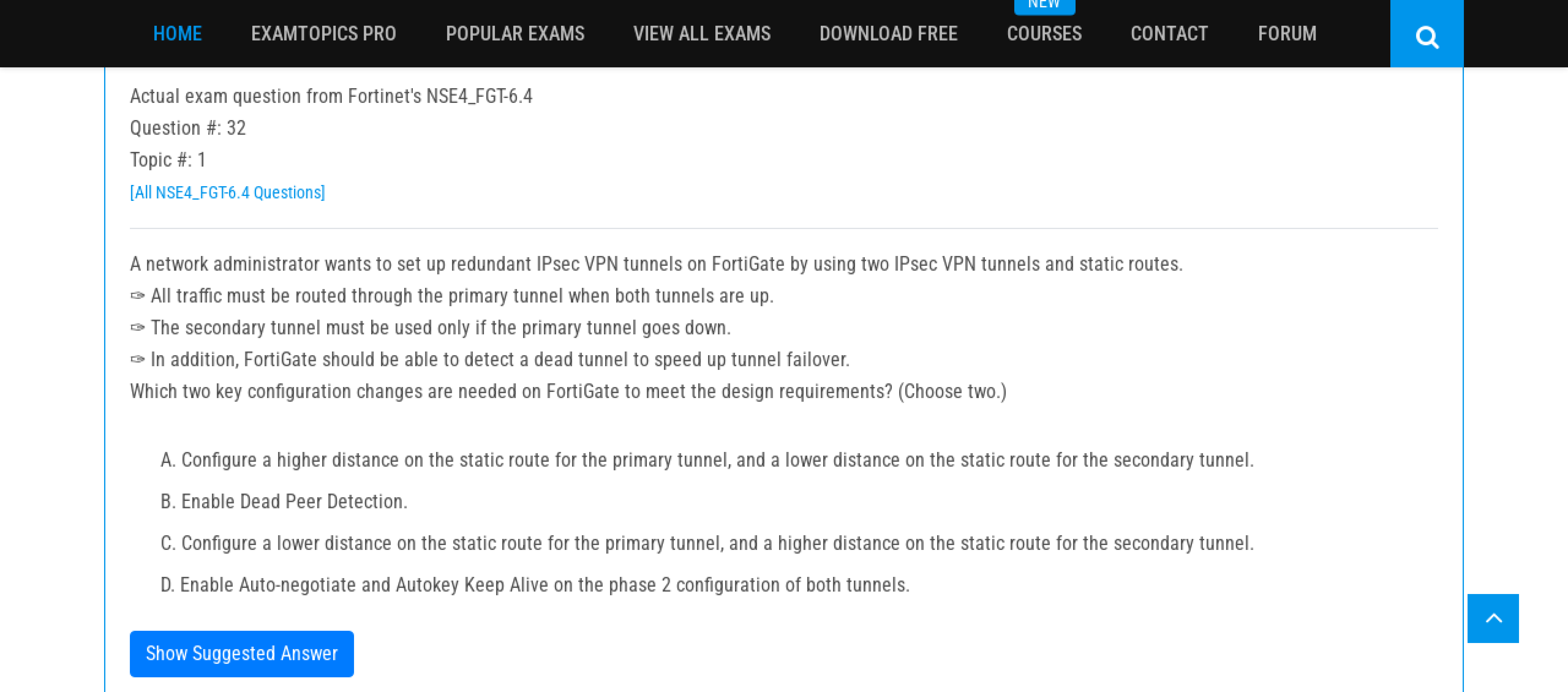
A. Enable asymmetric routing, so the RPF check will be bypassed.

B. Disable the RPF check at the FortiGate interface level for the source check.

C. Disable the RPF check at the FortiGate interface level for the reply check.

D. Enable asymmetric routing at the interface level.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 32

Topic #: 1

[All NSE4_FGT-6.4 Questions]

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

✑ All traffic must be routed through the primary tunnel when both tunnels are up.

✑ The secondary tunnel must be used only if the primary tunnel goes down.

✑ In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover.

Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two.)

A. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

B. Enable Dead Peer Detection.

C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.

D. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

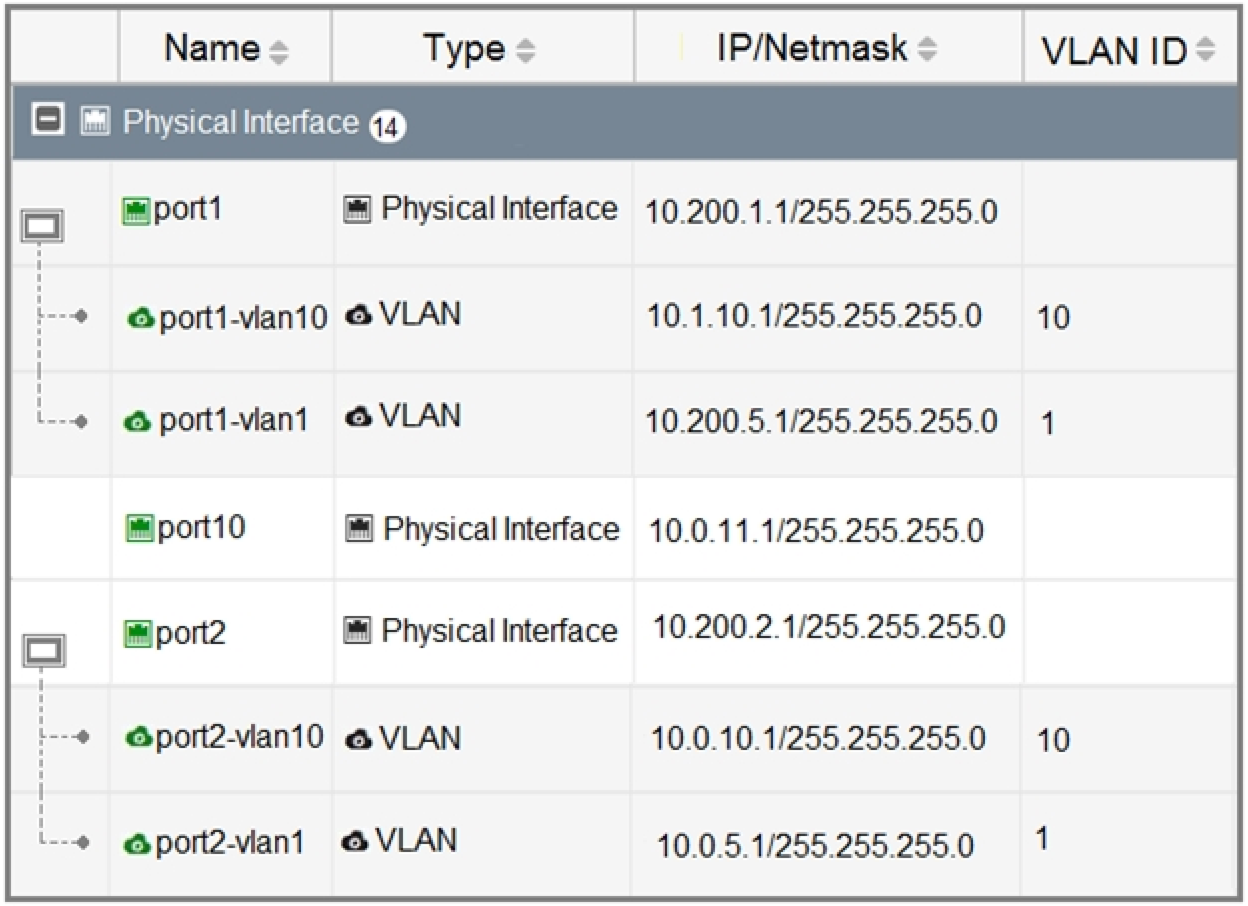
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 33

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



Name	Type	IP/Netmask	VLAN ID
Physical Interface 14			
port1	Physical Interface	10.200.1.1/255.255.255.0	
port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
port10	Physical Interface	10.0.11.1/255.255.255.0	
port2	Physical Interface	10.200.2.1/255.255.255.0	
port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit, which two statements are true? (Choose two.)

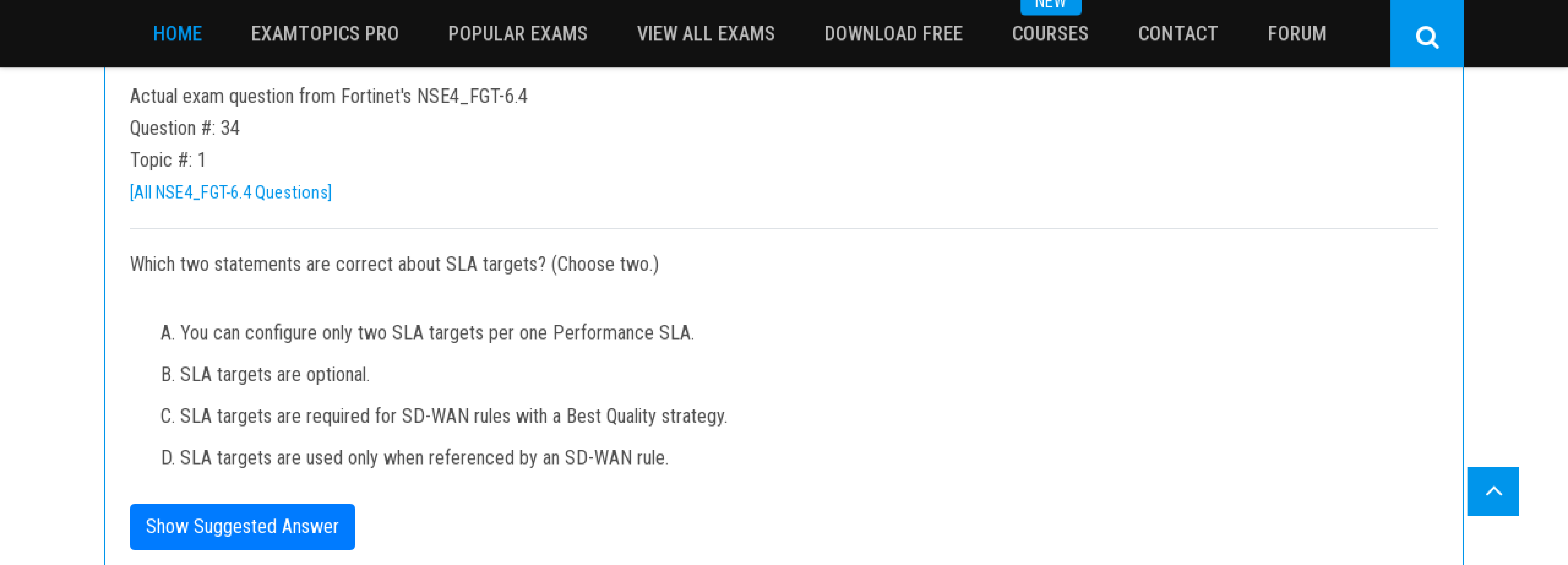
A. Traffic between port2 and port2-vlan1 is allowed by default.

B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.

C. port1 is a native VLAN.

D. port1-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 34

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which two statements are correct about SLA targets? (Choose two.)

A. You can configure only two SLA targets per one Performance SLA.

B. SLA targets are optional.

C. SLA targets are required for SD-WAN rules with a Best Quality strategy.

D. SLA targets are used only when referenced by an SD-WAN rule.

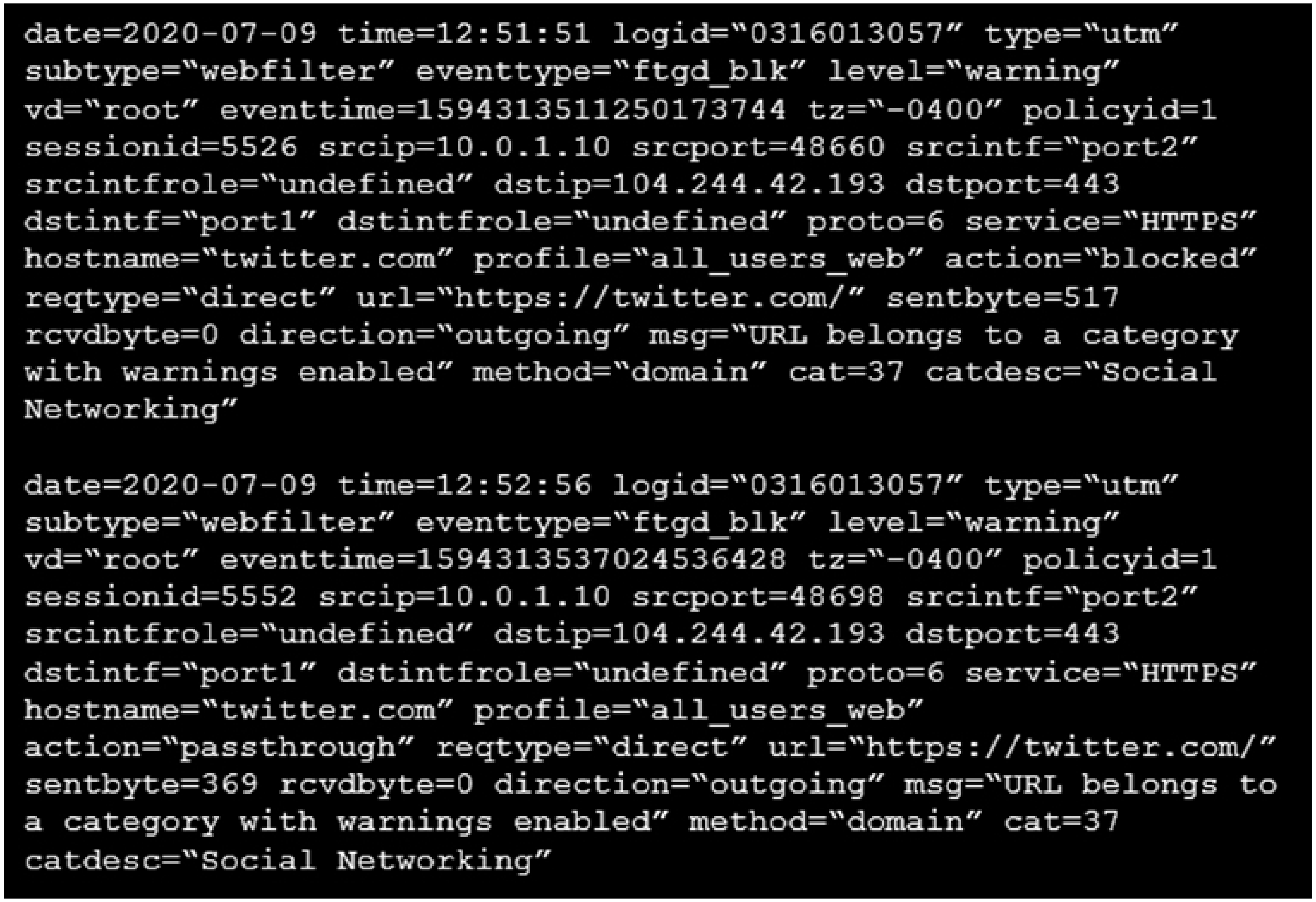
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 35

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the web filter raw logs.



```
date=2020-07-09 time=12:51:51 logid=“0316013057” type=“utm”
subtype=“webfilter” eventtype=“ftgd_blk” level=“warning”
vd=“root” eventtime=1594313511250173744 tz=“-0400” policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf=“port2”
srcintfrole=“undefined” dstip=104.244.42.193 dstport=443
dstintf=“port1” dstintfrole=“undefined” proto=6 service=“HTTPS”
hostname=“twitter.com” profile=“all_users_web” action=“blocked”
reqtype=“direct” url=“https://twitter.com/” sentbyte=517
rcvdbyte=0 direction=“outgoing” msg=“URL belongs to a category
with warnings enabled” method=“domain” cat=37 catdesc=“Social
Networking”

date=2020-07-09 time=12:52:56 logid=“0316013057” type=“utm”
subtype=“webfilter” eventtype=“ftgd_blk” level=“warning”
vd=“root” eventtime=1594313537024536428 tz=“-0400” policyid=1
sessionid=5552 srcip=10.0.1.10 srcport=48698 srcintf=“port2”
srcintfrole=“undefined” dstip=104.244.42.193 dstport=443
dstintf=“port1” dstintfrole=“undefined” proto=6 service=“HTTPS”
hostname=“twitter.com” profile=“all_users_web”
action=“passthrough” reqtype=“direct” url=“https://twitter.com/”
sentbyte=369 rcvdbyte=0 direction=“outgoing” msg=“URL belongs to
a category with warnings enabled” method=“domain” cat=37
catdesc=“Social Networking”
```

Based on the raw logs shown in the exhibit, which statement is correct?

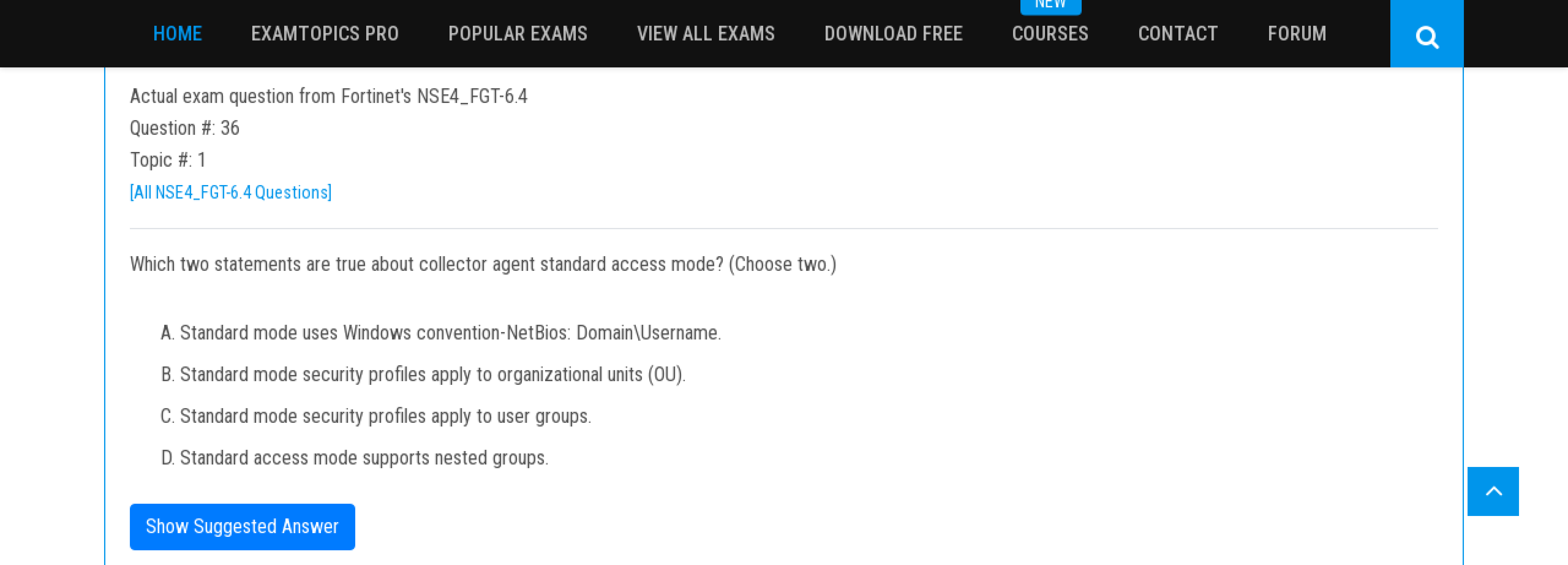
A. Access to the social networking web filter category was explicitly blocked to all users.

B. The action on firewall policy ID 1 is set to warning.

C. Social networking web filter category is configured with the action set to authenticate.

D. The name of the firewall policy is all_users_web.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 36

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which two statements are true about collector agent standard access mode? (Choose two.)

A. Standard mode uses Windows convention-NetBios: Domain\Username.

B. Standard mode security profiles apply to organizational units (OU).

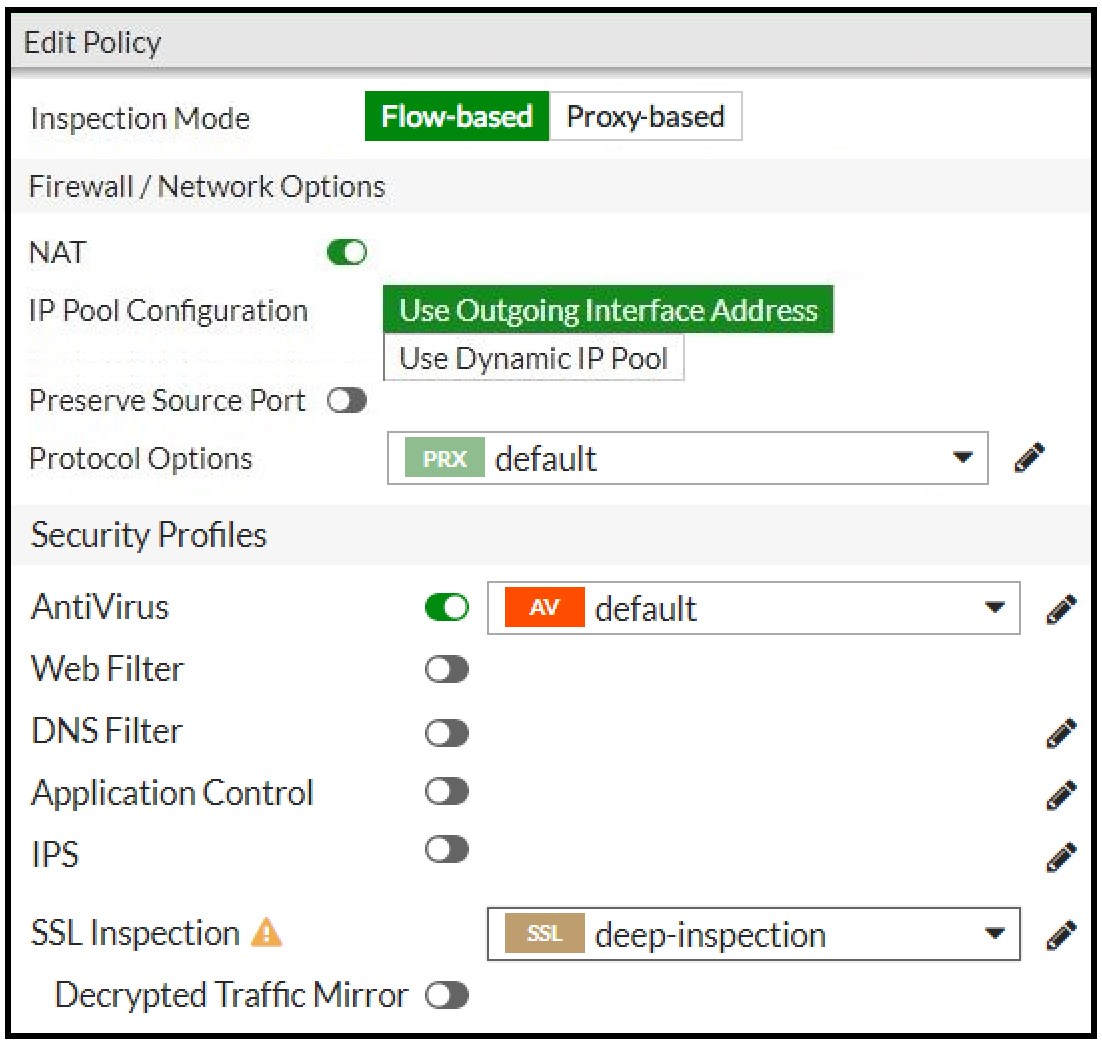
C. Standard mode security profiles apply to user groups.

D. Standard access mode supports nested groups.

Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 37
Topic #: 1
[All NSE4_FGT-6.4 Questions]

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Exhibit A -



Edit Policy

Inspection Mode: Flow-based (selected) | Proxy-based

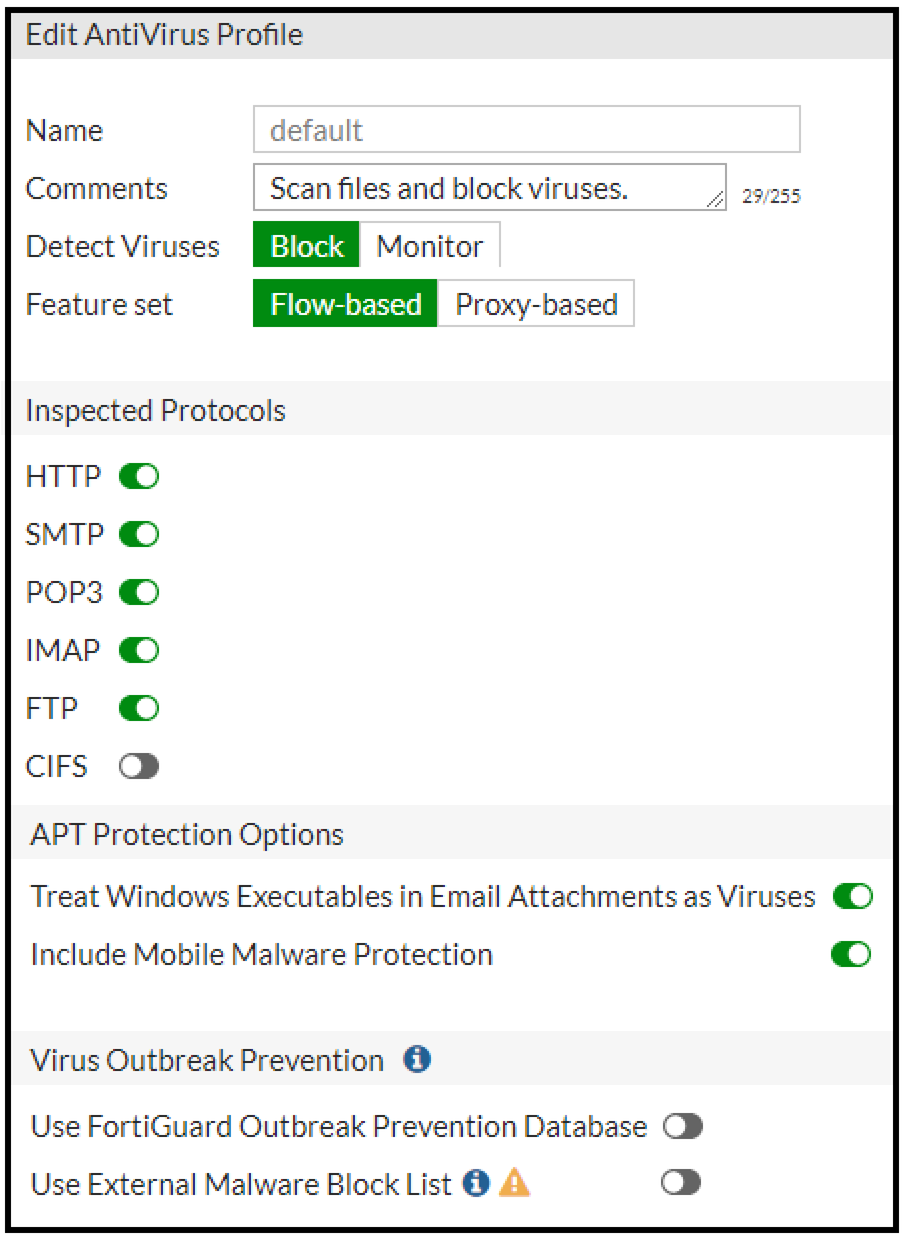
Firewall / Network Options

NAT: ●
IP Pool Configuration: Use Outgoing Interface Address (selected) | Use Dynamic IP Pool
Preserve Source Port: ○
Protocol Options: PRX default

Security Profiles

AntiVirus: ● AV default
Web Filter: ○
DNS Filter: ○
Application Control: ○
IPS: ○
SSL Inspection ⚠: SSL deep-inspection
Decrypted Traffic Mirror: ○

Exhibit B -



Edit AntiVirus Profile

Name: default
Comments: Scan files and block viruses. 29/255
Detect Viruses: Block (selected) | Monitor
Feature set: Flow-based (selected) | Proxy-based

Inspected Protocols

HTTP ●
SMTP ●
POP3 ●
IMAP ●
FTP ●
CIFS ○

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ●
Include Mobile Malware Protection ●

Virus Outbreak Prevention ℹ

Use FortiGuard Outbreak Prevention Database ○
Use External Malware Block List ℹ ⚠ ○

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

A. The volume of traffic being inspected is too high for this model of FortiGate.

B. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

C. The firewall policy performs the full content inspection on the file.

D. The flow-based inspection is used, which resets the last packet to the user.

Show Suggested Answer

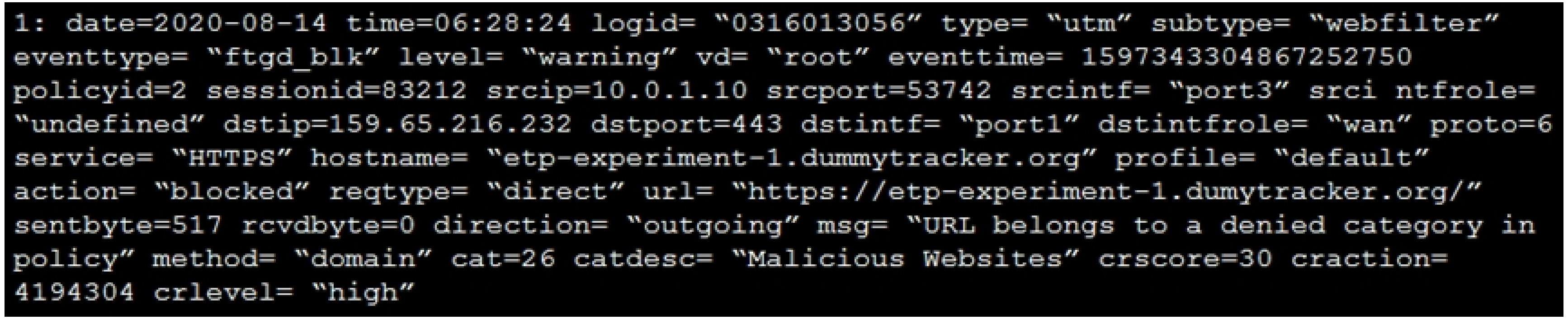
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 38

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



```
1: date=2020-08-14 time=06:28:24 logid= “0316013056” type= “utm” subtype= “webfilter”
eventtype= “ftgd_blk” level= “warning” vd= “root” eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= “port3” srci ntfrole=
“undefined” dstip=159.65.216.232 dstport=443 dstintf= “port1” dstintfrole= “wan” proto=6
service= “HTTPS” hostname= “etp-experiment-1.dummytracker.org” profile= “default”
action= “blocked” reqtype= “direct” url= “https://etp-experiment-1.dumytracker.org/”
sentbyte=517 rcvdbyte=0 direction= “outgoing” msg= “URL belongs to a denied category in
policy” method= “domain” cat=26 catdesc= “Malicious Websites” crscore=30 craction=
4194304 crlevel= “high”
```

Based on the raw log, which two statements are correct? (Choose two.)

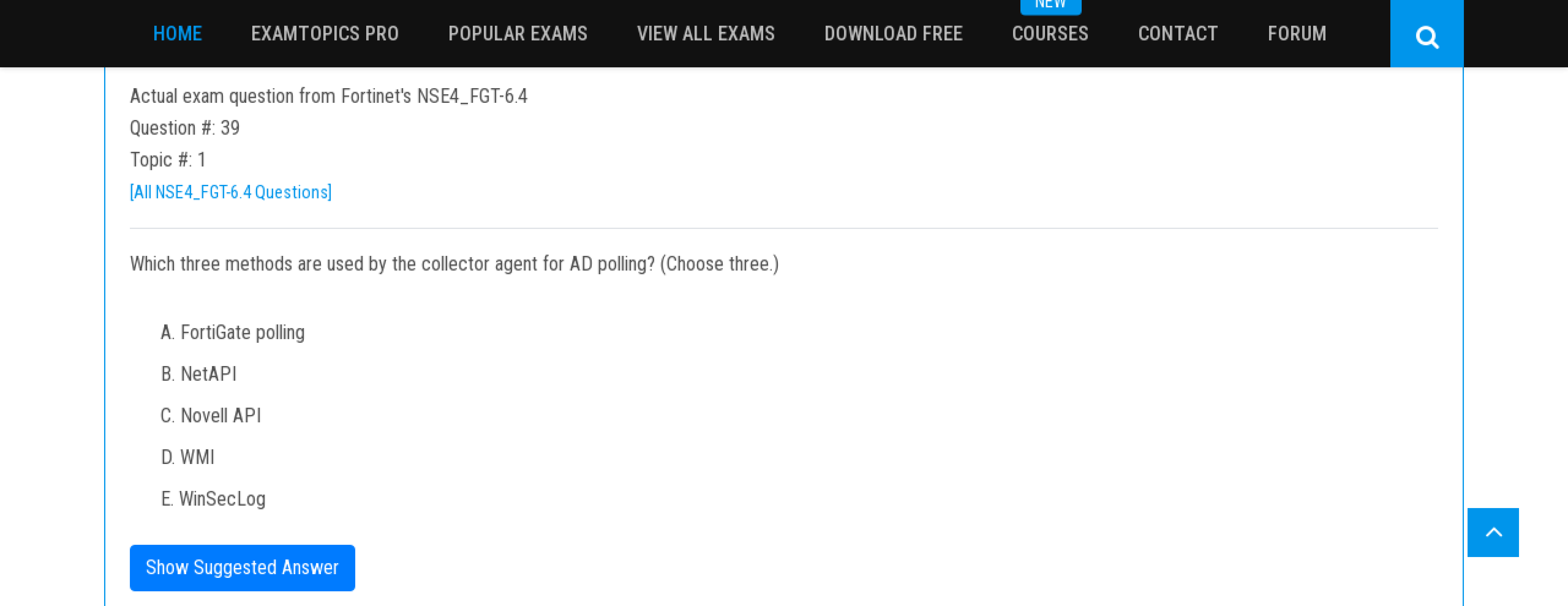
A. Traffic is blocked because Action is set to DENY in the firewall policy.

B. Traffic belongs to the root VDOM.

C. This is a security log.

D. Log severity is set to error on FortiGate.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 39

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which three methods are used by the collector agent for AD polling? (Choose three.)

A. FortiGate polling

B. NetAPI

C. Novell API

D. WMI

E. WinSecLog

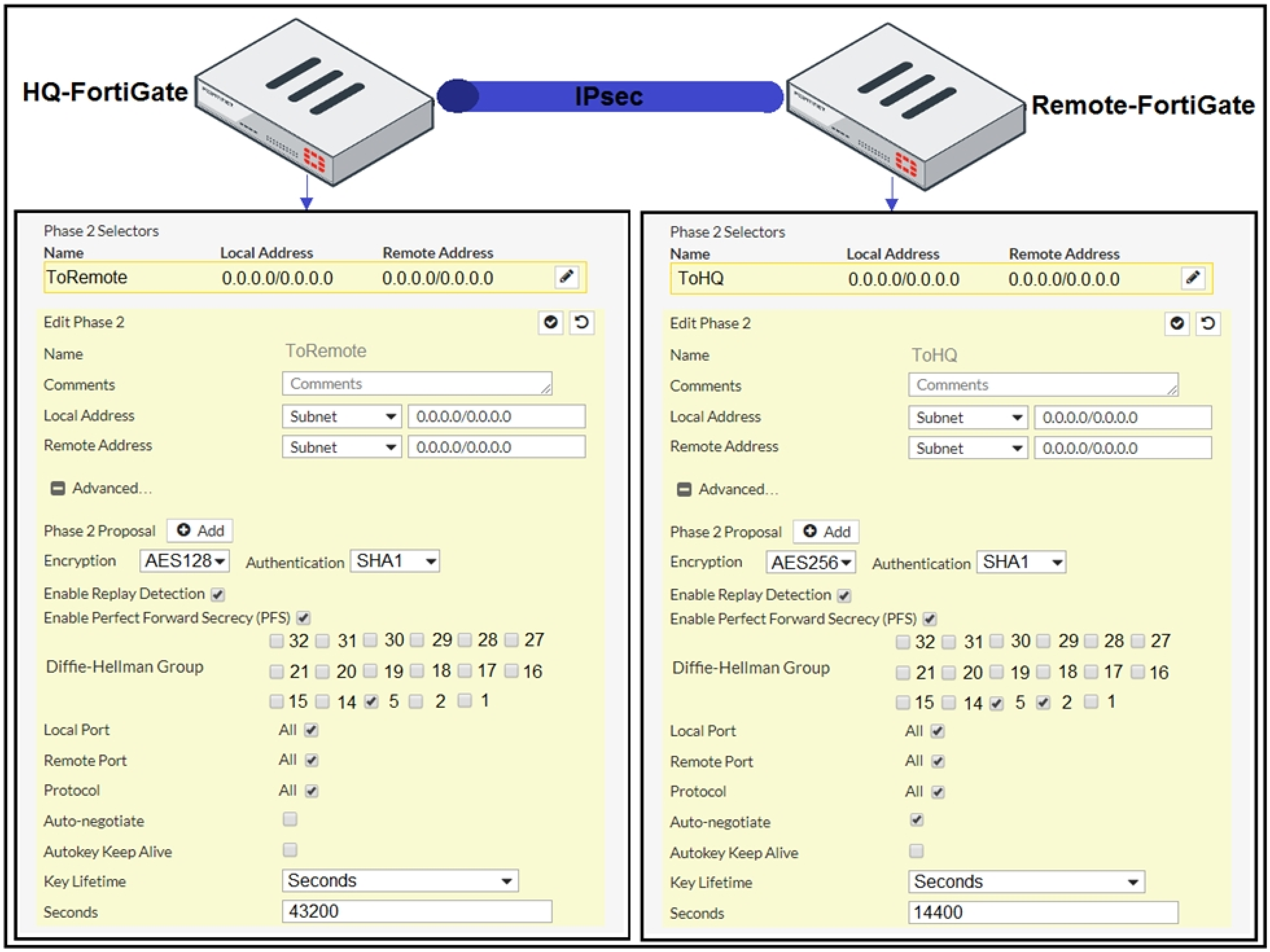
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 40

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



HQ-FortiGate

Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: ToRemote

Comments: Comments

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal: Add

Encryption: AES128 Authentication: SHA1

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) ☑

Diffie-Hellman Group: ☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☐ 14 ☑ 5 ☐ 2 ☐ 1

Local Port: All ☑

Remote Port: All ☑

Protocol: All ☑

Auto-negotiate ☐

Autokey Keep Alive ☐

Key Lifetime: Seconds

Seconds: 43200

Remote-FortiGate

Phase 2 Selectors

Name	Local Address	Remote Address
ToHQ	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: ToHQ

Comments: Comments

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal: Add

Encryption: AES256 Authentication: SHA1

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) ☑

Diffie-Hellman Group: ☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☐ 14 ☑ 5 ☑ 2 ☐ 1

Local Port: All ☑

Remote Port: All ☑

Protocol: All ☑

Auto-negotiate ☑

Autokey Keep Alive ☐

Key Lifetime: Seconds

Seconds: 14400

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, what configuration change will bring phase 2 up?

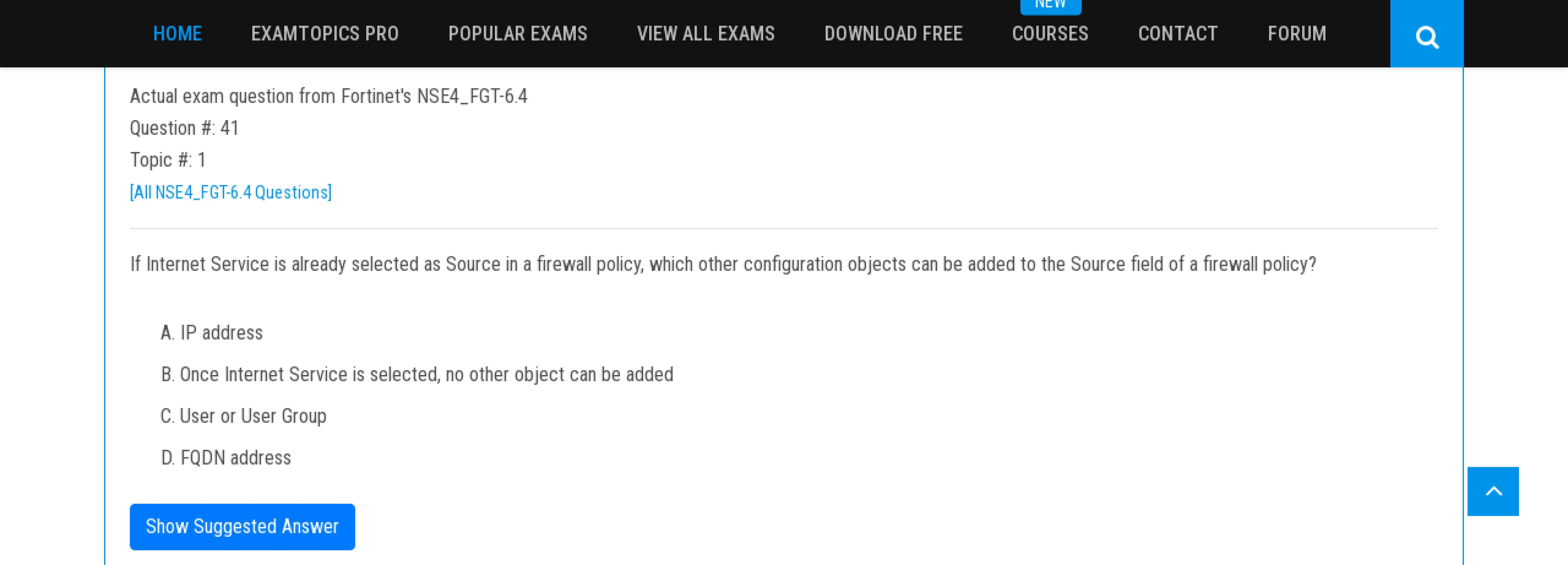
A. On HQ-FortiGate, enable Diffie-Hellman Group 2.

B. On HQ-FortiGate, enable Auto-negotiate.

C. On Remote-FortiGate, set Seconds to 43200.

D. On HQ-FortiGate, set Encryption to AES256.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 41

Topic #: 1

[All NSE4_FGT-6.4 Questions]

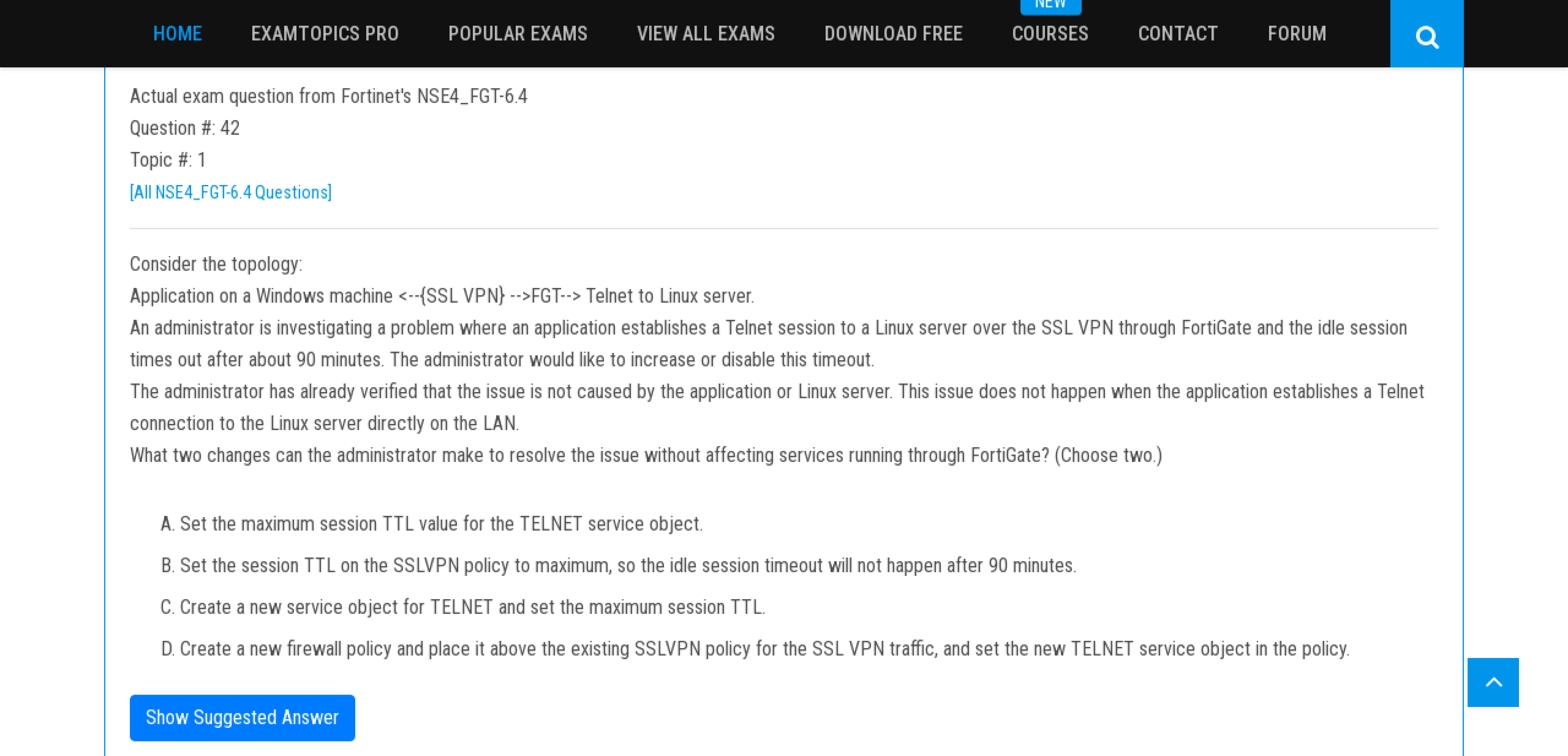
If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source field of a firewall policy?

A. IP address

B. Once Internet Service is selected, no other object can be added

C. User or User Group

D. FQDN address



Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 42
Topic #: 1
[All NSE4_FGT-6.4 Questions]

Consider the topology:
Application on a Windows machine <--{SSL VPN} -->FGT--> Telnet to Linux server.
An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.
The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.
What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

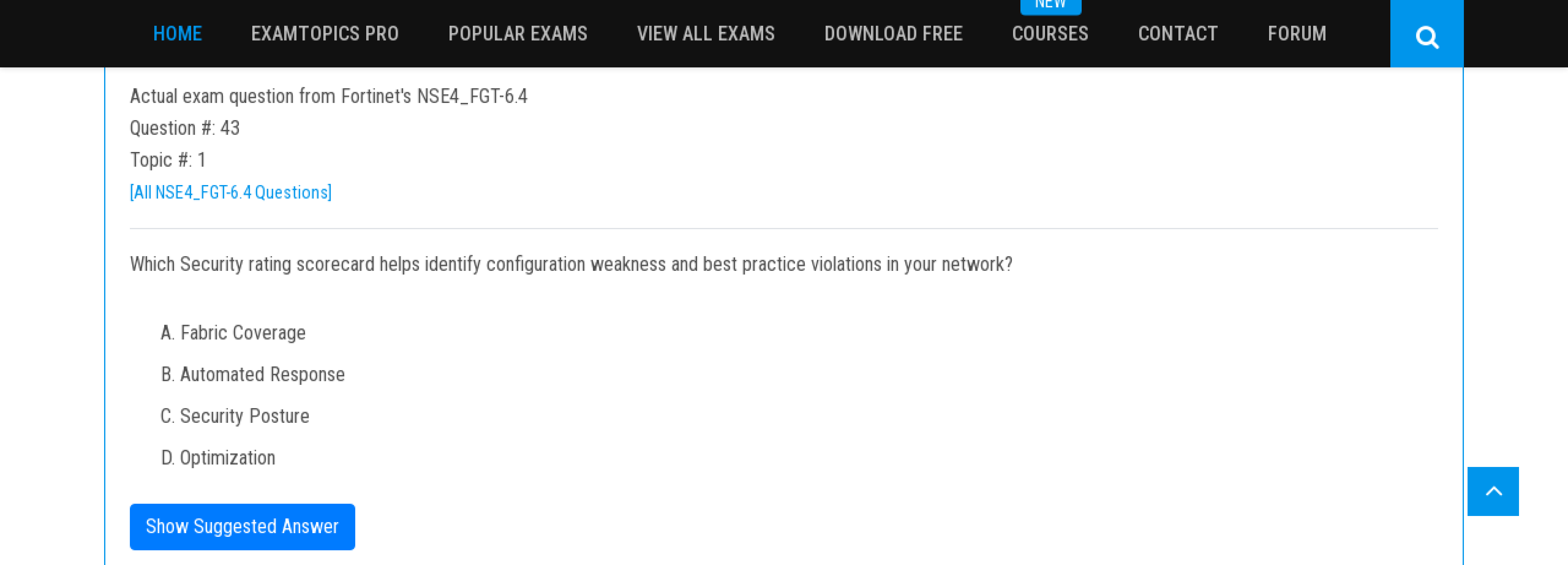
A. Set the maximum session TTL value for the TELNET service object.

B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.

C. Create a new service object for TELNET and set the maximum session TTL.

D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 43

Topic #: 1

[All NSE4_FGT-6.4 Questions]

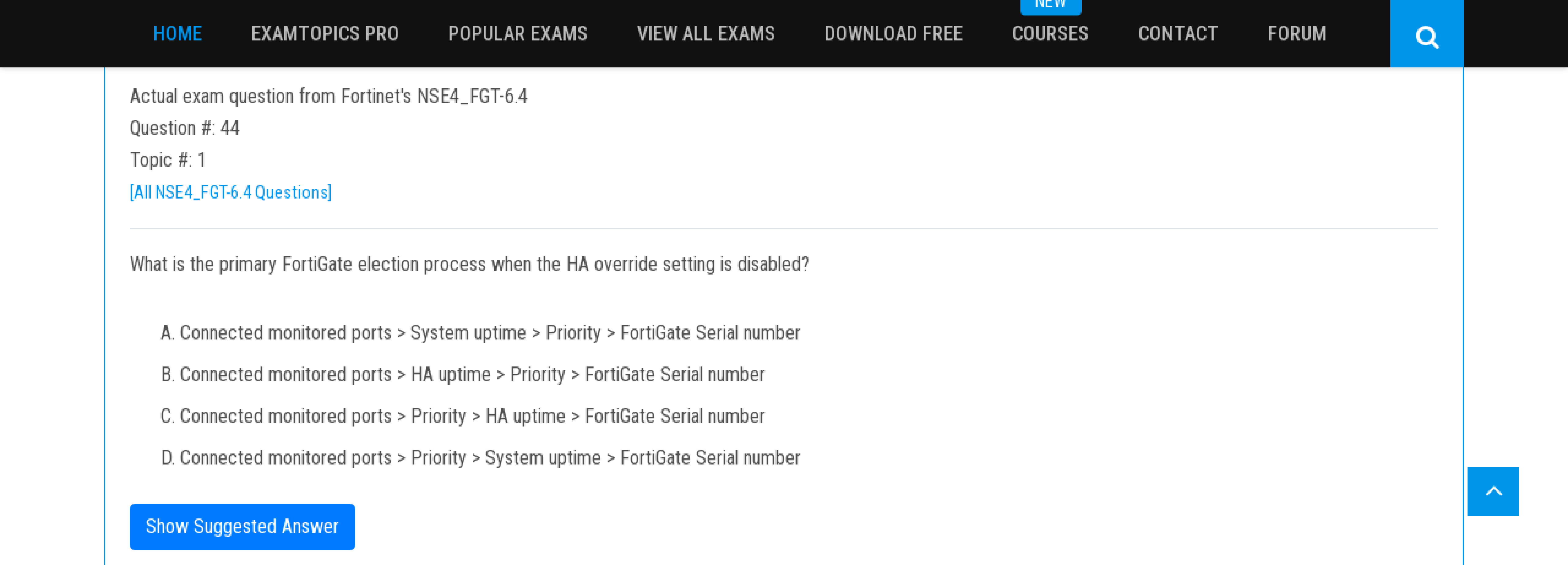
Which Security rating scorecard helps identify configuration weakness and best practice violations in your network?

A. Fabric Coverage

B. Automated Response

C. Security Posture

D. Optimization



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 44

Topic #: 1

[All NSE4_FGT-6.4 Questions]

What is the primary FortiGate election process when the HA override setting is disabled?

A. Connected monitored ports > System uptime > Priority > FortiGate Serial number

B. Connected monitored ports > HA uptime > Priority > FortiGate Serial number

C. Connected monitored ports > Priority > HA uptime > FortiGate Serial number

D. Connected monitored ports > Priority > System uptime > FortiGate Serial number

Actual exam question from Fortinet's NSE4_FGT-6.4

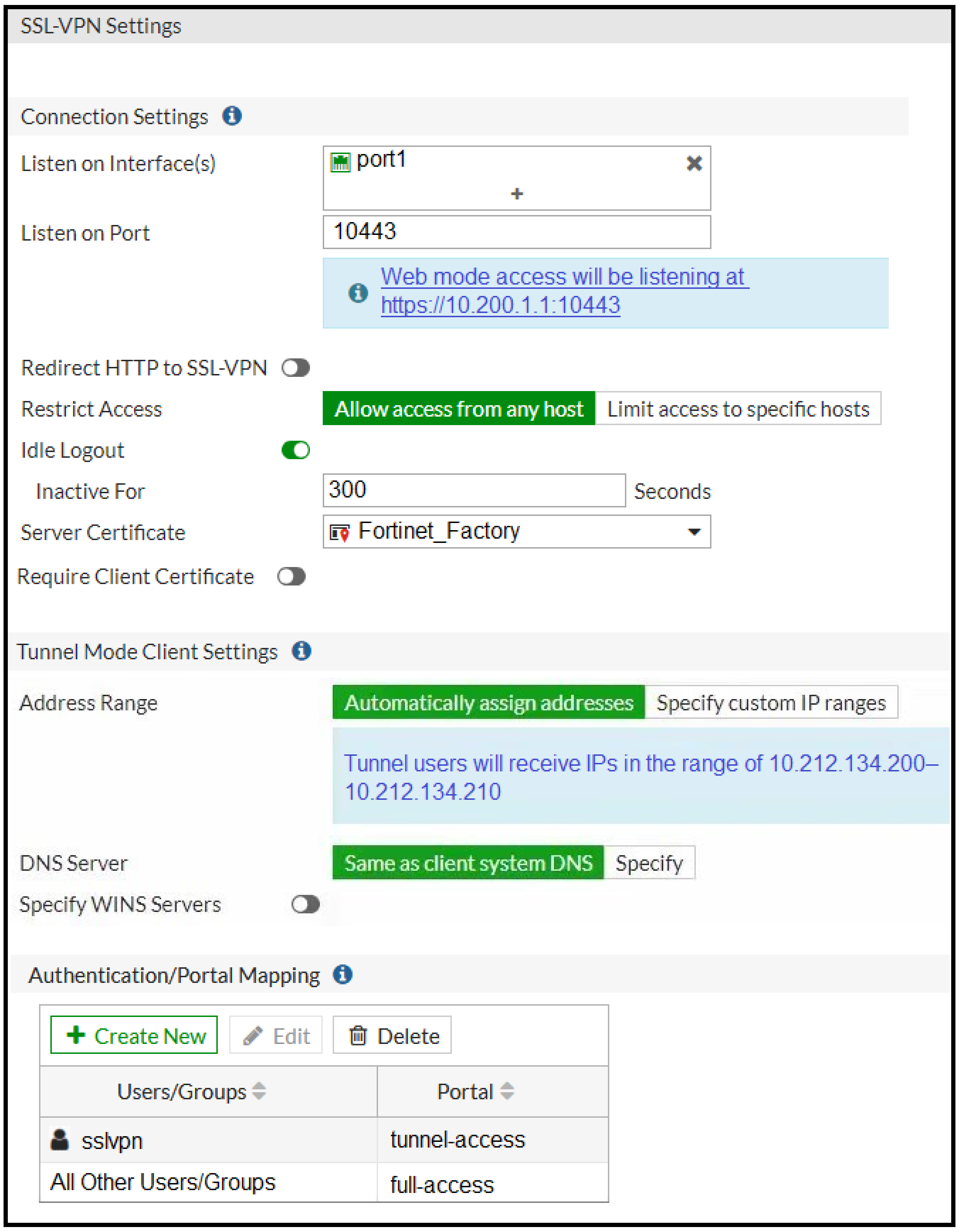
Question #: 45

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.

Exhibit A -



SSL-VPN Settings

Connection Settings

Listen on Interface(s): port1

Listen on Port: 10443

Web mode access will be listening at https://10.200.1.1:10443

Redirect HTTP to SSL-VPN: ○

Restrict Access: **Allow access from any host** | Limit access to specific hosts

Idle Logout: ●

Inactive For: 300 Seconds

Server Certificate: Fortinet_Factory

Require Client Certificate: ○

Tunnel Mode Client Settings

Address Range: **Automatically assign addresses** | Specify custom IP ranges

Tunnel users will receive IPs in the range of 10.212.134.200–10.212.134.210

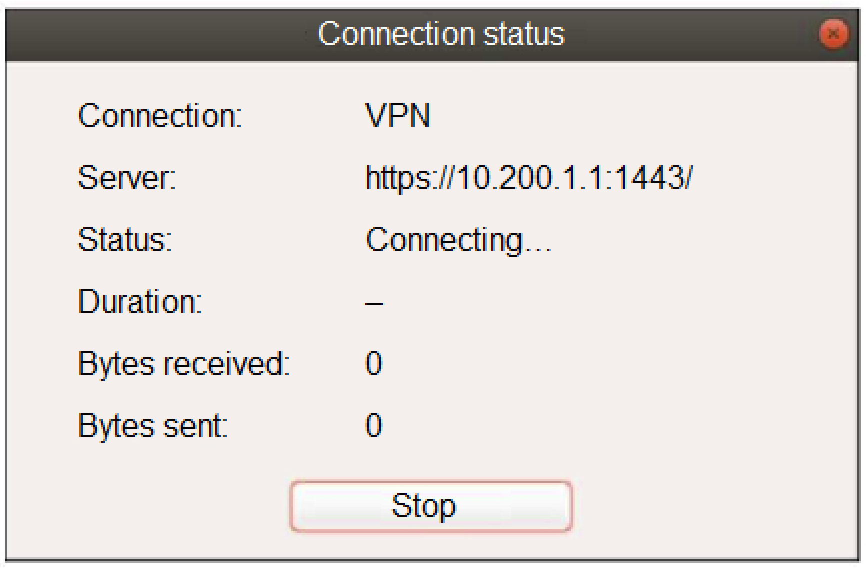
DNS Server: **Same as client system DNS** | Specify

Specify WINS Servers: ○

Authentication/Portal Mapping

Users/Groups	Portal
sslvpn	tunnel-access
All Other Users/Groups	full-access

Exhibit B -



Connection status

Connection:	VPN
Server:	https://10.200.1.1:1443/
Status:	Connecting...
Duration:	–
Bytes received:	0
Bytes sent:	0

The SSL VPN connection fails when a user attempts to connect to it.

What should the user do to successfully connect to SSL VPN?

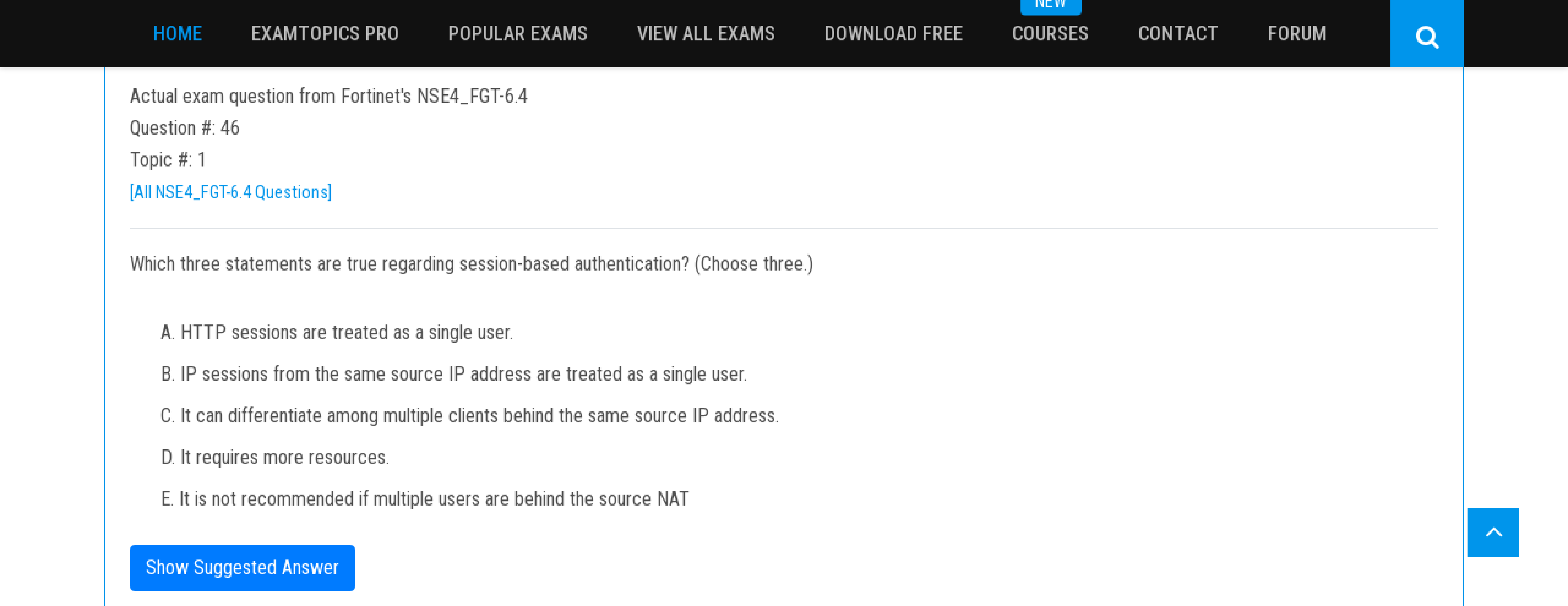
A. Change the SSL VPN port on the client.

B. Change the Server IP address.

C. Change the idle-timeout.

D. Change the SSL VPN portal to the tunnel.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 46
Topic #: 1
[All NSE4_FGT-6.4 Questions]

Which three statements are true regarding session-based authentication? (Choose three.)

A. HTTP sessions are treated as a single user.

B. IP sessions from the same source IP address are treated as a single user.

C. It can differentiate among multiple clients behind the same source IP address.

D. It requires more resources.

E. It is not recommended if multiple users are behind the source NAT

Show Suggested Answer

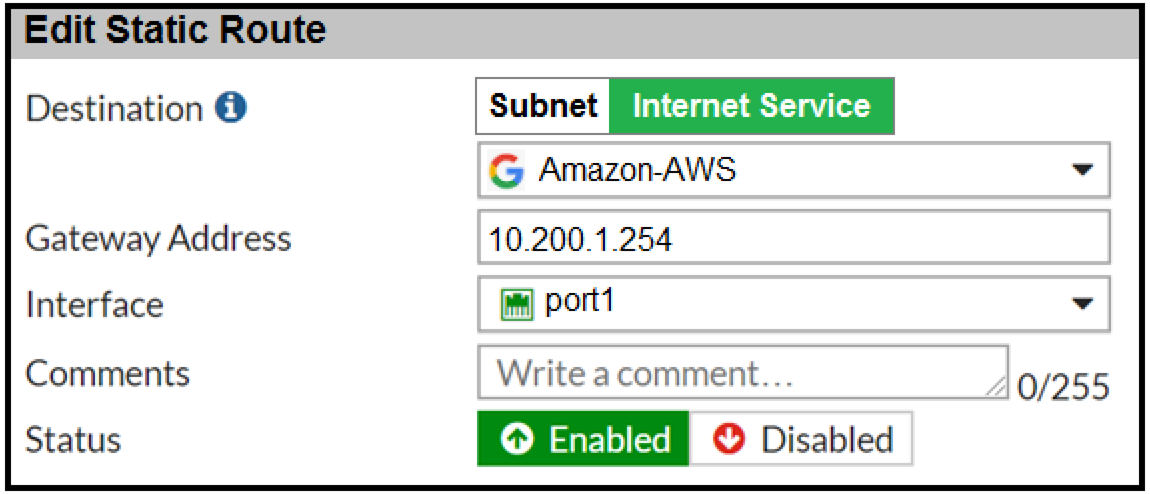
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 47

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit, which contains a static route configuration.



Edit Static Route

Destination: Subnet | Internet Service

Amazon-AWS

Gateway Address: 10.200.1.254

Interface: port1

Comments: Write a comment... 0/255

Status: Enabled | Disabled

An administrator created a static route for Amazon Web Services.

What CLI command must the administrator use to view the route?

A. get router info routing-table all

B. get internet service route list

C. get router info routing-table database

D. diagnose firewall proute list

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 48

Topic #: 1

[All NSE4_FGT-6.4 Questions]

An administrator needs to increase network bandwidth and provide redundancy.

What interface type must the administrator select to bind multiple FortiGate interfaces?

A. VLAN interface

B. Software Switch interface

C. Aggregate interface

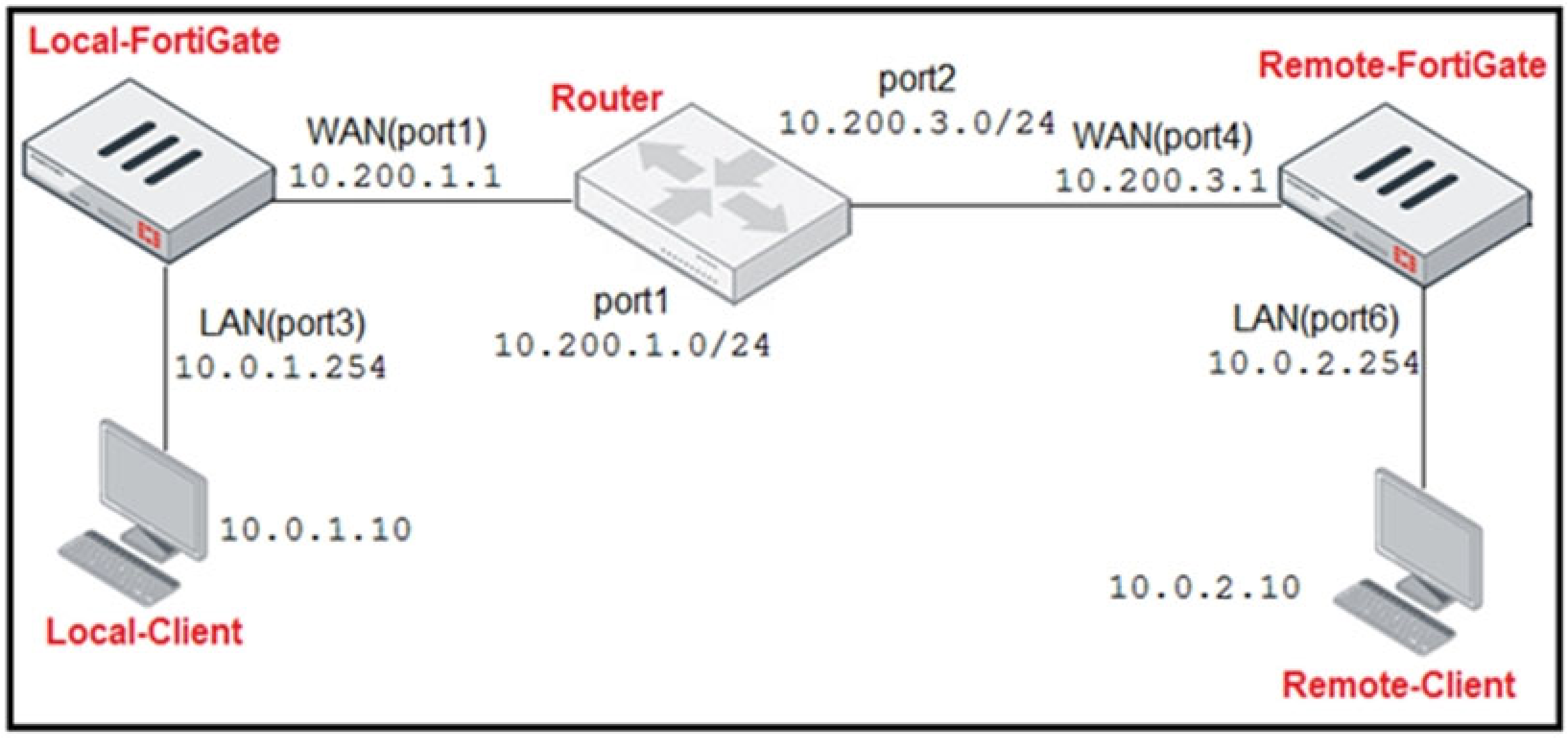
D. Redundant interface

Show Suggested Answer

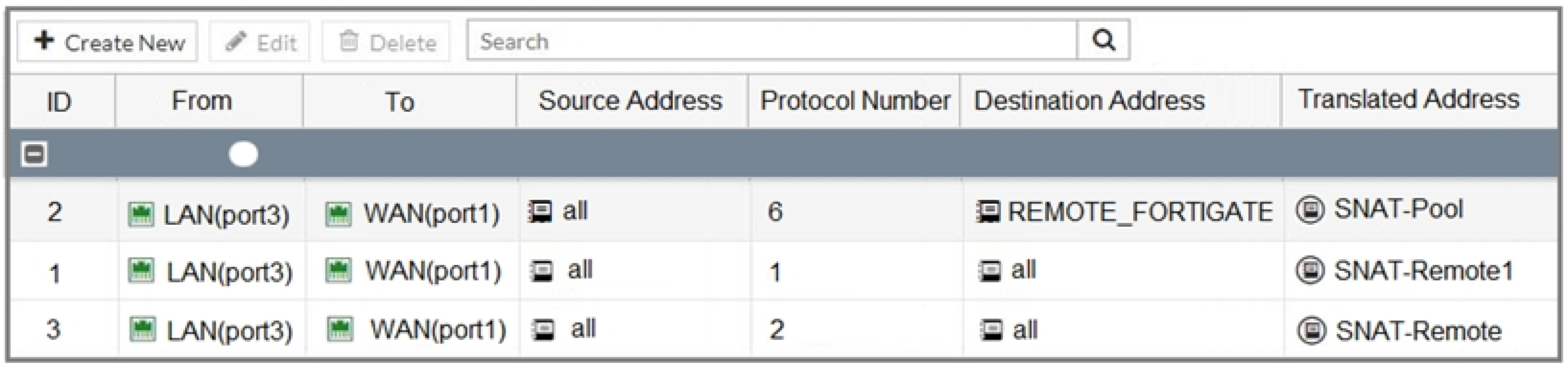
Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 49
Topic #: 1
[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.

Network Diagram

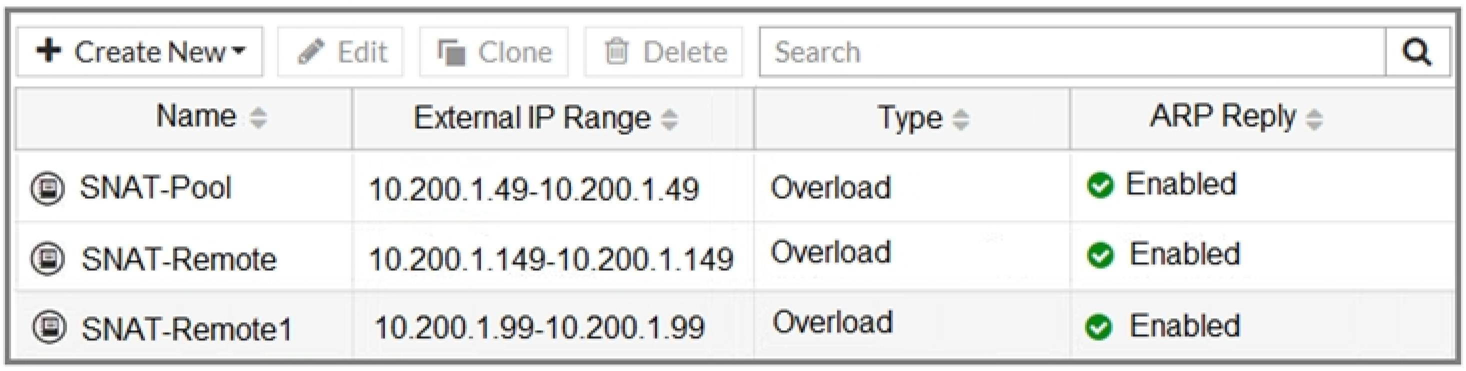


Central SNAT Policies Local-FortiGate



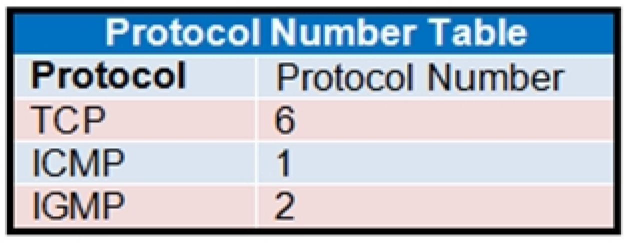
ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

IP Pool Local-FortiGate



Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	✓ Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	✓ Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	✓ Enabled

Protocol Number Table



Protocol Number Table

Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration.
The WAN (port1) interface has the IP address 10.200.1.1/24.
The LAN (port3) interface has the IP address 10.0.1.254/24.
A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1).
Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied.
Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

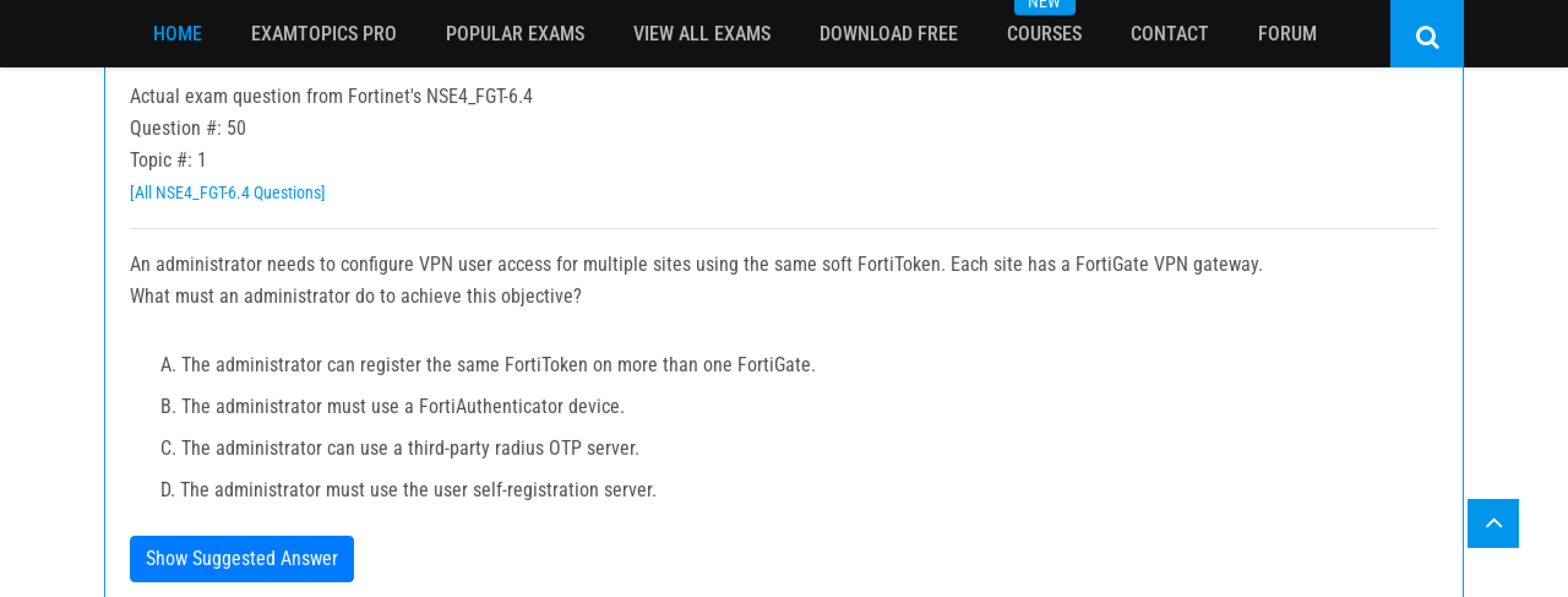
A. 10.200.1.149

B. 10.200.1.1

C. 10.200.1.49

D. 10.200.1.99

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 50
Topic #: 1

[All NSE4_FGT-6.4 Questions]

An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway.
What must an administrator do to achieve this objective?

A. The administrator can register the same FortiToken on more than one FortiGate.

B. The administrator must use a FortiAuthenticator device.

C. The administrator can use a third-party radius OTP server.

D. The administrator must use the user self-registration server.

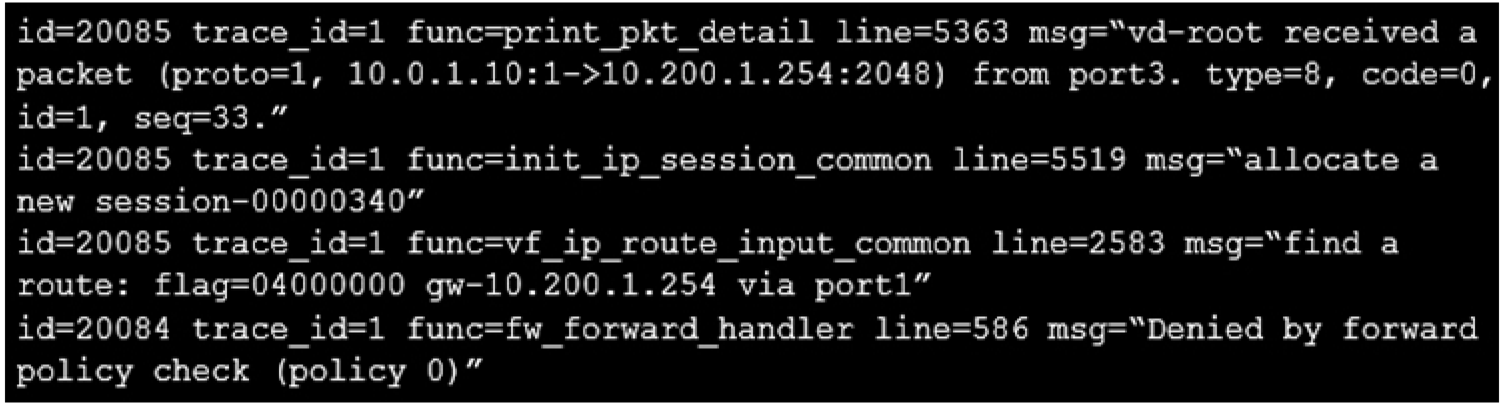
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 51

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a
packet (proto=1, 10.0.1.10:1->10.200.1.254:2048) from port3. type=8, code=0,
id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a
new session-00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a
route: flag=04000000 gw-10.200.1.254 via port1"
id=20084 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward
policy check (policy 0)"
```

Why did FortiGate drop the packet?

A. It matched an explicitly configured firewall policy with the action DENY.

B. The next-hop IP address is unreachable.

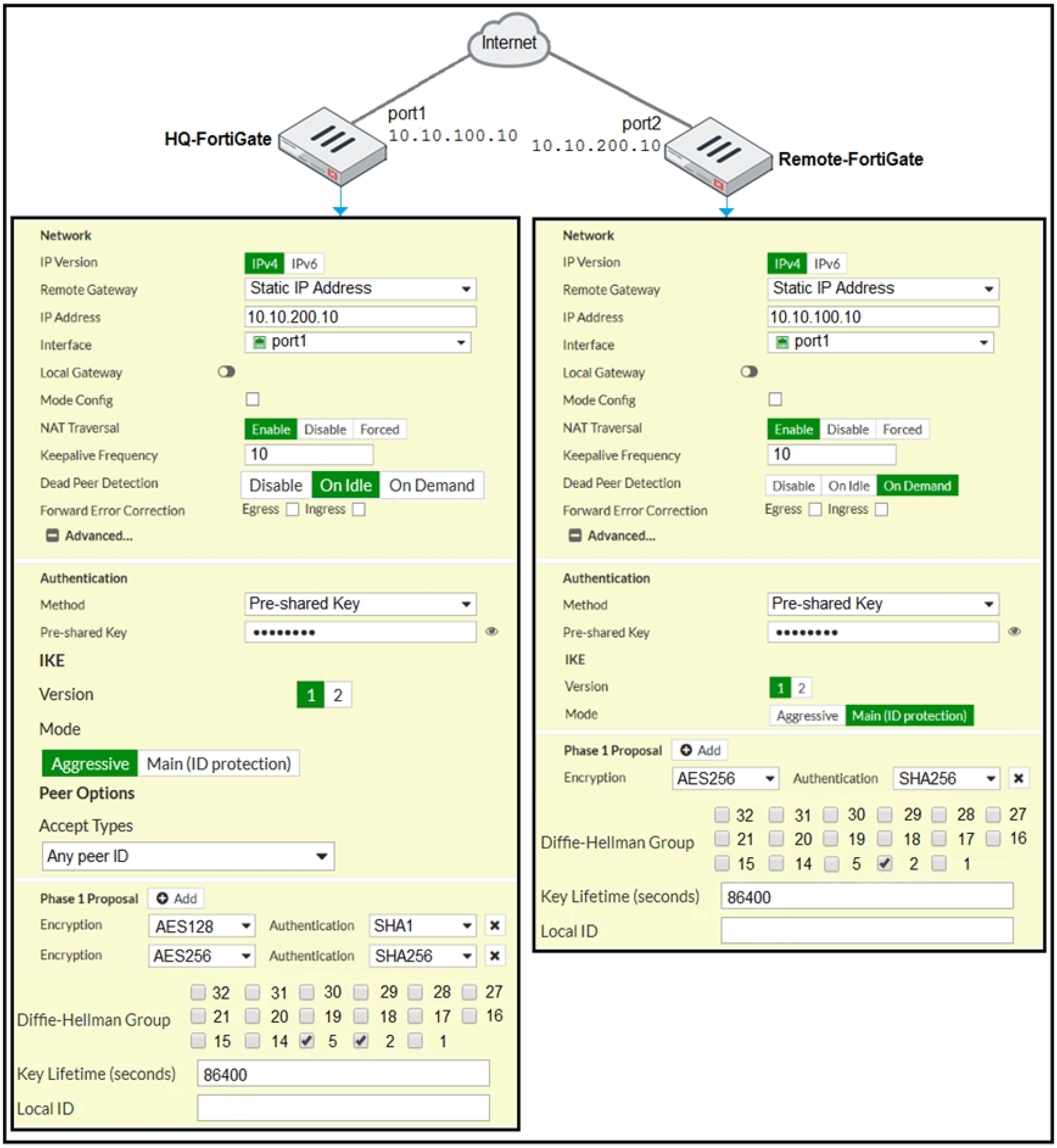
C. It failed the RPF check.

D. It matched the default implicit firewall policy.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 52
Topic #: 1
[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



HQ-FortiGate

Network
IP Version [✓ IPv4] IPv6
Remote Gateway Static IP Address
IP Address 10.10.200.10
Interface port1
Local Gateway ○
Mode Config ☐
NAT Traversal [✓ Enable] Disable Forced
Keepalive Frequency 10
Dead Peer Detection Disable [✓ On Idle] On Demand
Forward Error Correction Egress ☐ Ingress ☐
Advanced...

Authentication
Method Pre-shared Key
Pre-shared Key ••••••••
IKE
Version [✓ 1] 2
Mode [✓ Aggressive] Main (ID protection)
Peer Options
Accept Types Any peer ID

Phase 1 Proposal Add
Encryption AES128 Authentication SHA1
Encryption AES256 Authentication SHA256
Diffie-Hellman Group ☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27
☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16
☐ 15 ☐ 14 ☑ 5 ☑ 2 ☐ 1
Key Lifetime (seconds) 86400
Local ID

Remote-FortiGate

Network
IP Version [✓ IPv4] IPv6
Remote Gateway Static IP Address
IP Address 10.10.100.10
Interface port1
Local Gateway ○
Mode Config ☐
NAT Traversal [✓ Enable] Disable Forced
Keepalive Frequency 10
Dead Peer Detection Disable On Idle [✓ On Demand]
Forward Error Correction Egress ☐ Ingress ☐
Advanced...

Authentication
Method Pre-shared Key
Pre-shared Key ••••••••
IKE
Version [✓ 1] 2
Mode Aggressive [✓ Main (ID protection)]

Phase 1 Proposal Add
Encryption AES256 Authentication SHA256
Diffie-Hellman Group ☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27
☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16
☐ 15 ☐ 14 ☐ 5 ☑ 2 ☐ 1
Key Lifetime (seconds) 86400
Local ID

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.
Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

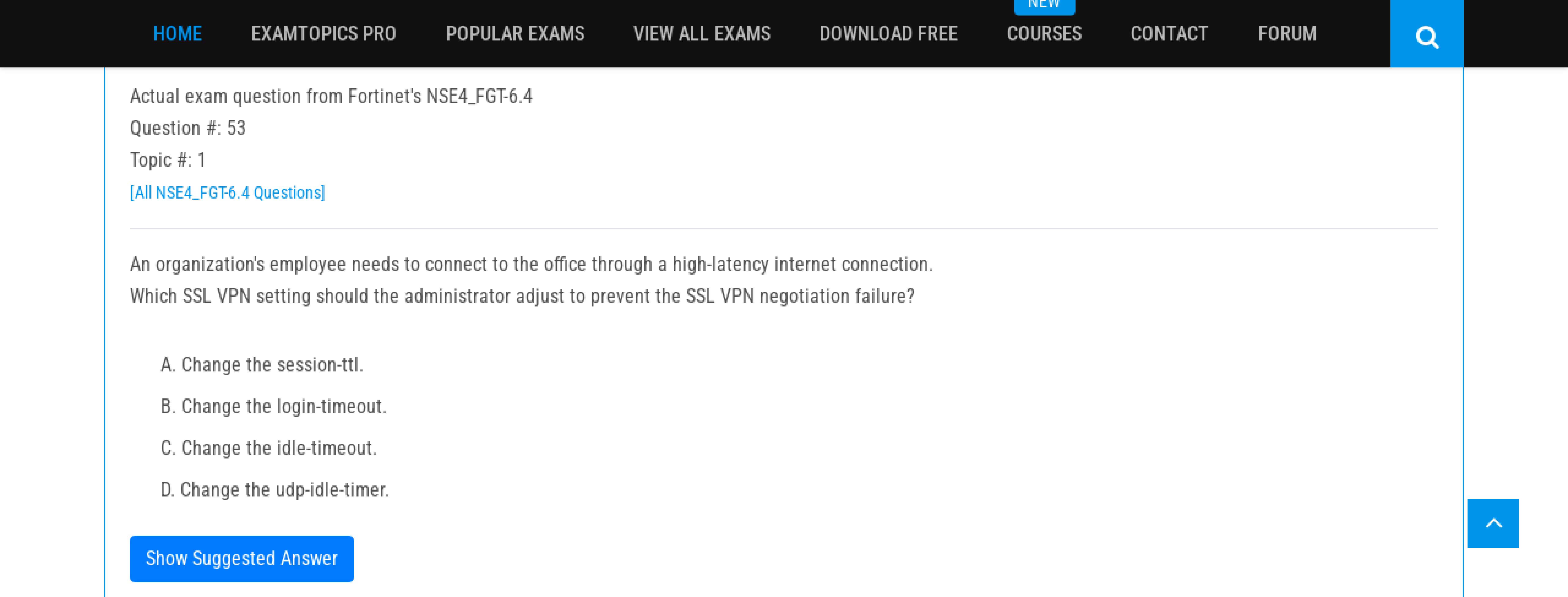
A. On HQ-FortiGate, set IKE mode to Main (ID protection).

B. On both FortiGate devices, set Dead Peer Detection to On Demand.

C. On HQ-FortiGate, disable Diffie-Helman group 2.

D. On Remote-FortiGate, set port2 as Interface.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 53
Topic #: 1
[All NSE4_FGT-6.4 Questions]

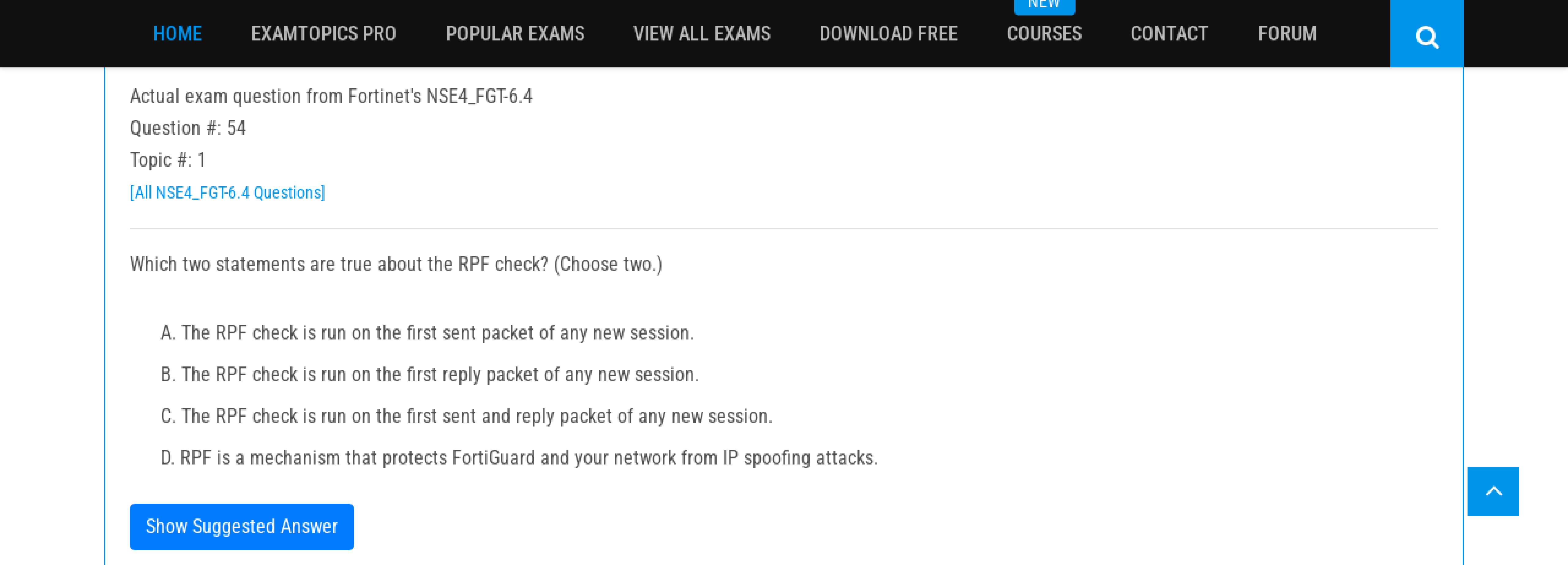
An organization's employee needs to connect to the office through a high-latency internet connection.
Which SSL VPN setting should the administrator adjust to prevent the SSL VPN negotiation failure?

A. Change the session-ttl.

B. Change the login-timeout.

C. Change the idle-timeout.

D. Change the udp-idle-timer.



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 54

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which two statements are true about the RPF check? (Choose two.)

A. The RPF check is run on the first sent packet of any new session.

B. The RPF check is run on the first reply packet of any new session.

C. The RPF check is run on the first sent and reply packet of any new session.

D. RPF is a mechanism that protects FortiGuard and your network from IP spoofing attacks.

Show Suggested Answer

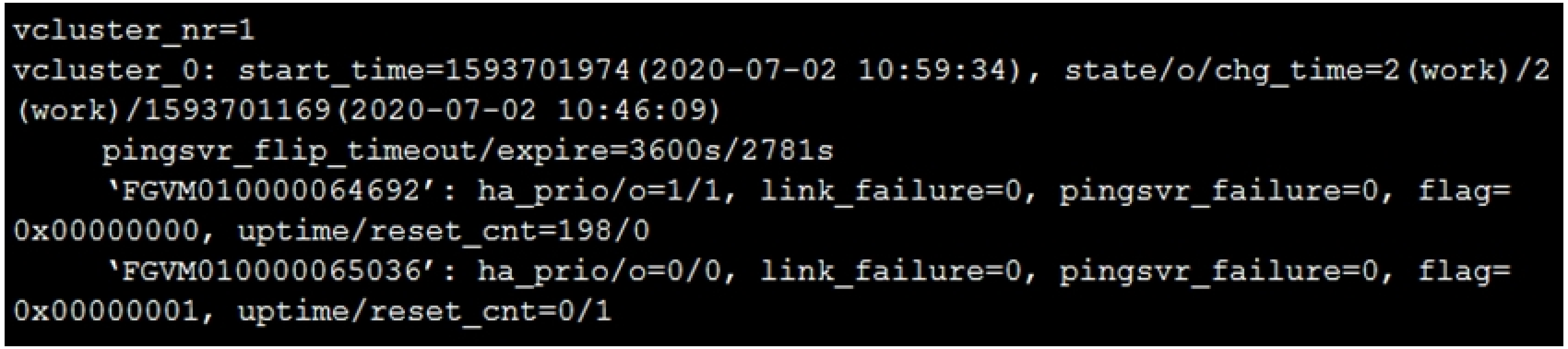
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 55

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
    pingsvr_flip_timeout/expire=3600s/2781s
    ‘FGVM010000064692’: ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
    ‘FGVM010000065036’: ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster.

Which two statements are true? (Choose two.)

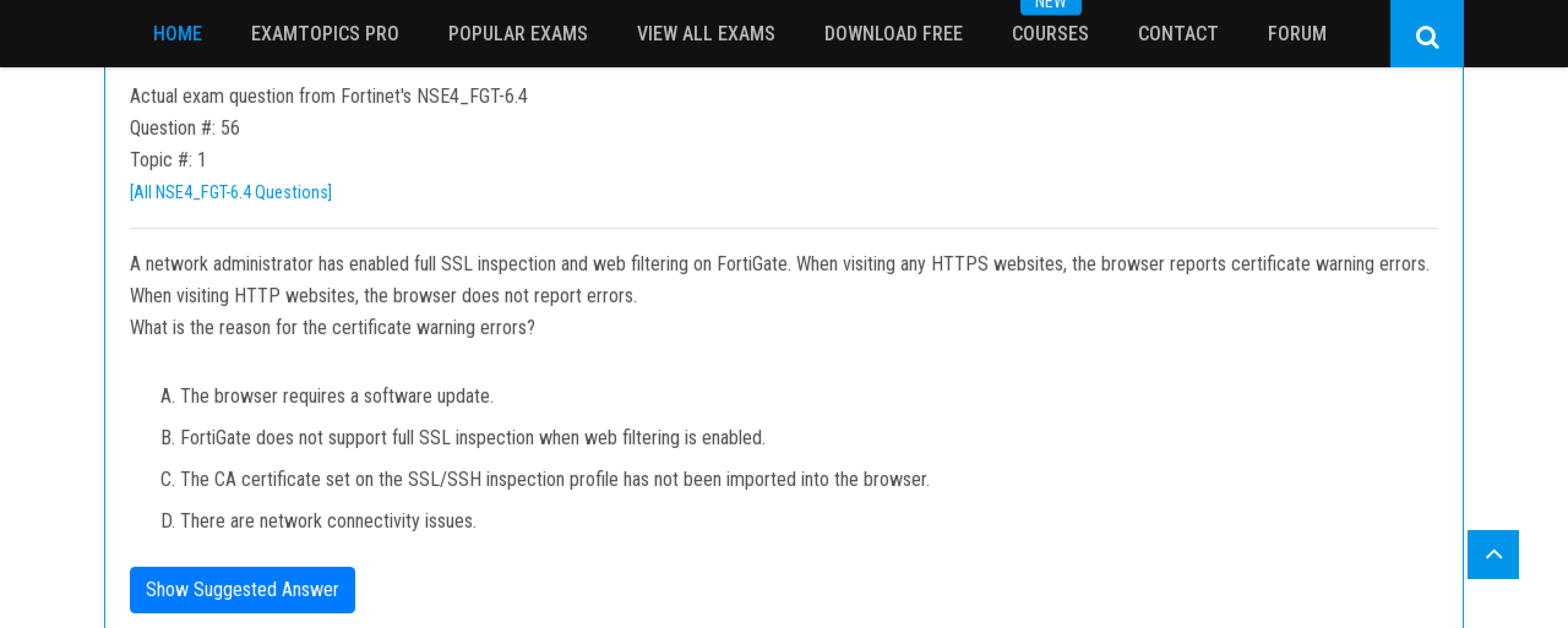
A. FortiGate SN FGVM010000065036 HA uptime has been reset.

B. FortiGate devices are not in sync because one device is down.

C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.

D. FortiGate SN FGVM010000064692 has the higher HA priority.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 56
Topic #: 1
[All NSE4_FGT-6.4 Questions]

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?

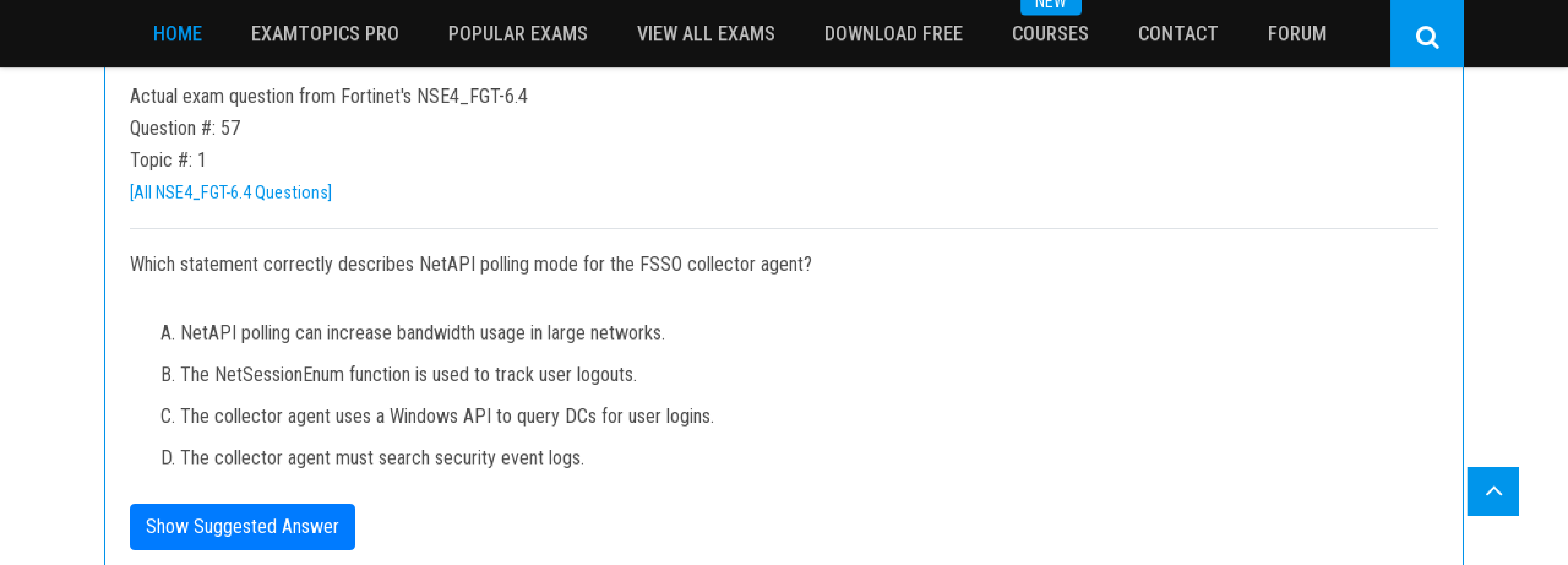
A. The browser requires a software update.

B. FortiGate does not support full SSL inspection when web filtering is enabled.

C. The CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.

D. There are network connectivity issues.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 57

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. NetAPI polling can increase bandwidth usage in large networks.

B. The NetSessionEnum function is used to track user logouts.

C. The collector agent uses a Windows API to query DCs for user logins.

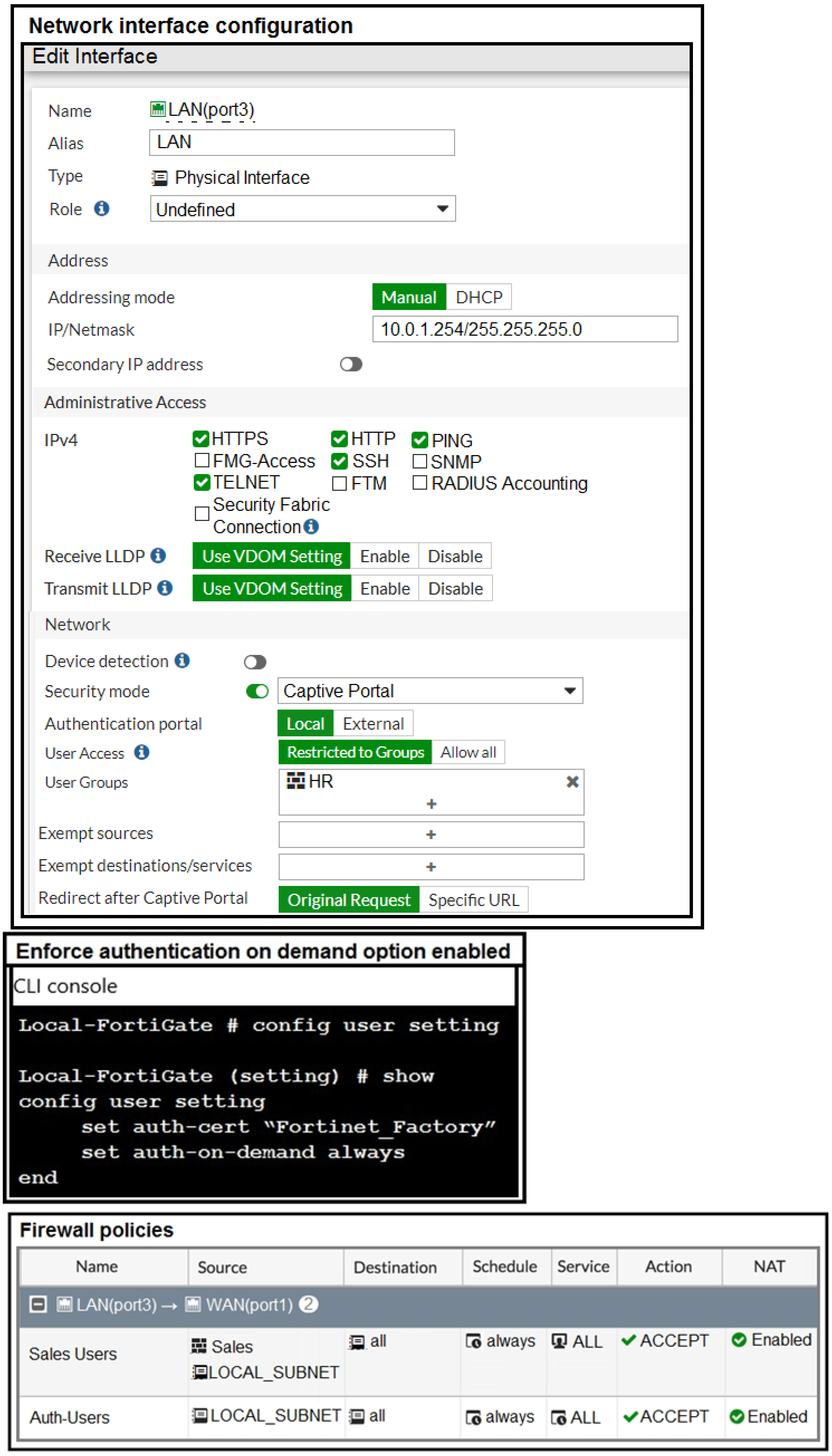
D. The collector agent must search security event logs.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-6.4
Question #: 58
Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



Network interface configuration

Edit Interface

Name LAN(port3)
Alias LAN
Type Physical Interface
Role Undefined

Address

Addressing mode [✓ Manual] DHCP
IP/Netmask 10.0.1.254/255.255.255.0
Secondary IP address ○

Administrative Access

IPv4 ☑ HTTPS ☑ HTTP ☑ PING
☐ FMG-Access ☑ SSH ☐ SNMP
☑ TELNET ☐ FTM ☐ RADIUS Accounting
☐ Security Fabric Connection

Receive LLDP [✓ Use VDOM Setting] Enable Disable
Transmit LLDP [✓ Use VDOM Setting] Enable Disable

Network

Device detection ○
Security mode ● Captive Portal
Authentication portal [✓ Local] External
User Access [✓ Restricted to Groups] Allow all
User Groups HR
Exempt sources +
Exempt destinations/services +
Redirect after Captive Portal [✓ Original Request] Specific URL

Enforce authentication on demand option enabled

CLI console

```
Local-FortiGate # config user setting

Local-FortiGate (setting) # show
config user setting
    set auth-cert "Fortinet_Factory"
    set auth-on-demand always
end
```

Firewall policies

Name	Source	Destination	Schedule	Service	Action	NAT
LAN(port3) → WAN(port1) 2						
Sales Users	Sales LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	✓ Enabled
Auth-Users	LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	✓ Enabled

The exhibit contains a network interface configuration, firewall policies, and a CLI console configuration.

How will FortiGate handle user authentication for traffic that arrives on the LAN interface?

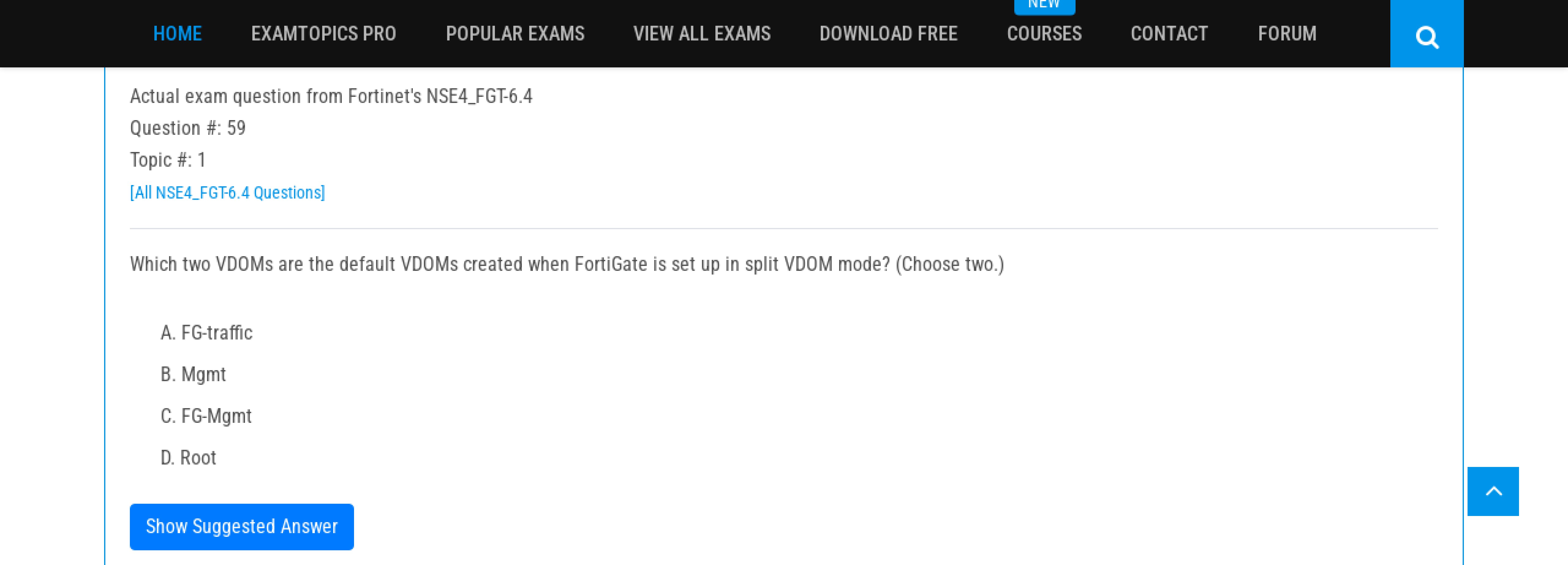
A. If there is a fall-through policy in place, users will not be prompted for authentication.

B. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.

C. Authentication is enforced at a policy level; all users will be prompted for authentication.

D. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 59

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which two VDOMs are the default VDOMs created when FortiGate is set up in split VDOM mode? (Choose two.)

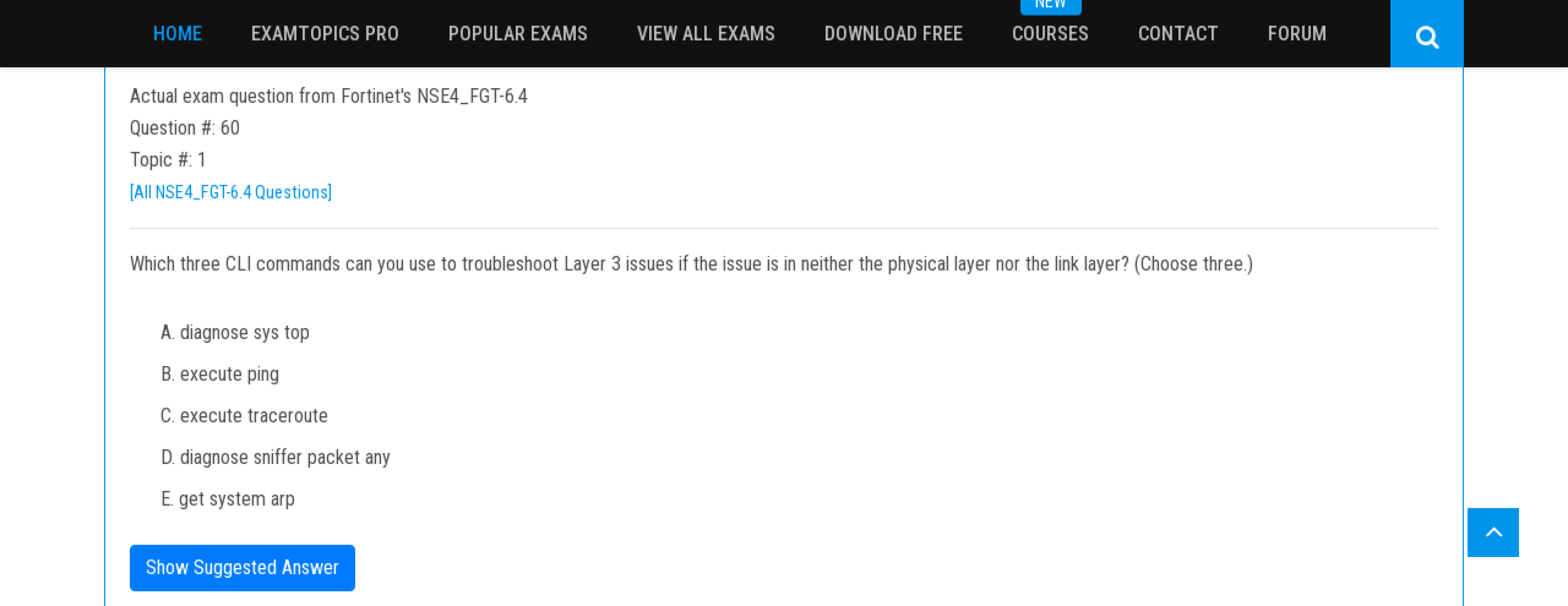
A. FG-traffic

B. Mgmt

C. FG-Mgmt

D. Root

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 60

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

A. diagnose sys top

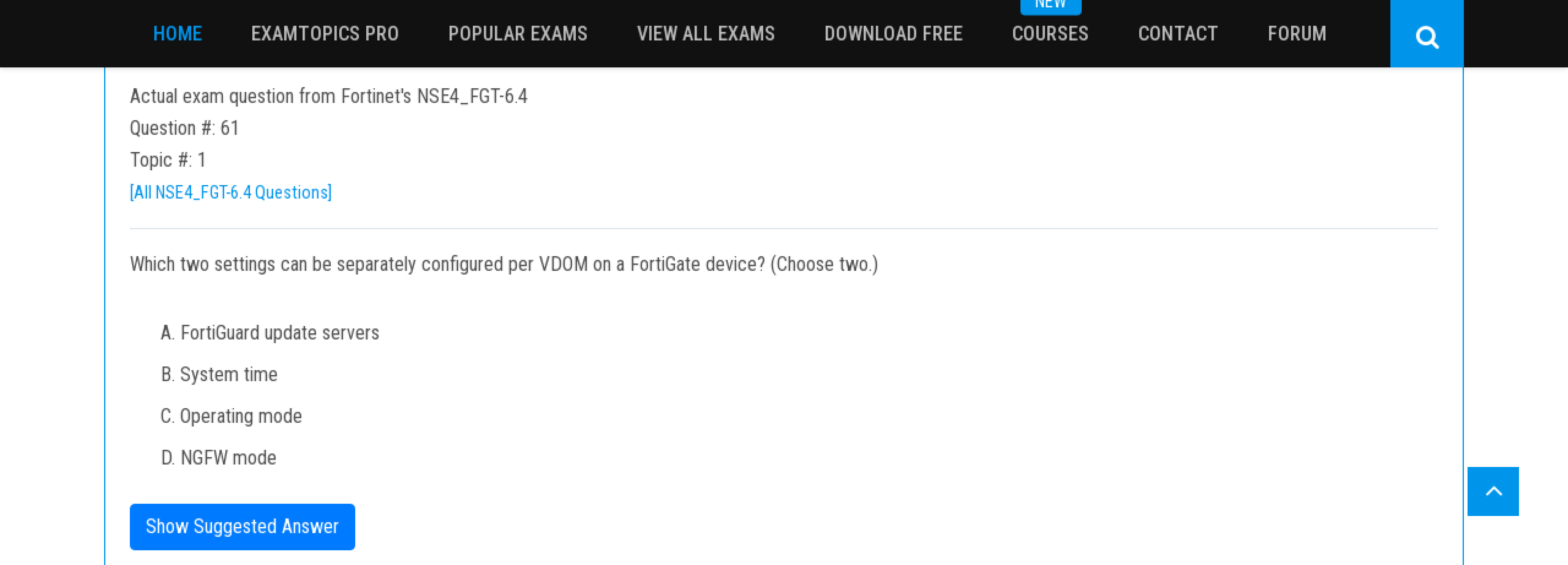
B. execute ping

C. execute traceroute

D. diagnose sniffer packet any

E. get system arp

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 61

Topic #: 1

[All NSE4_FGT-6.4 Questions]

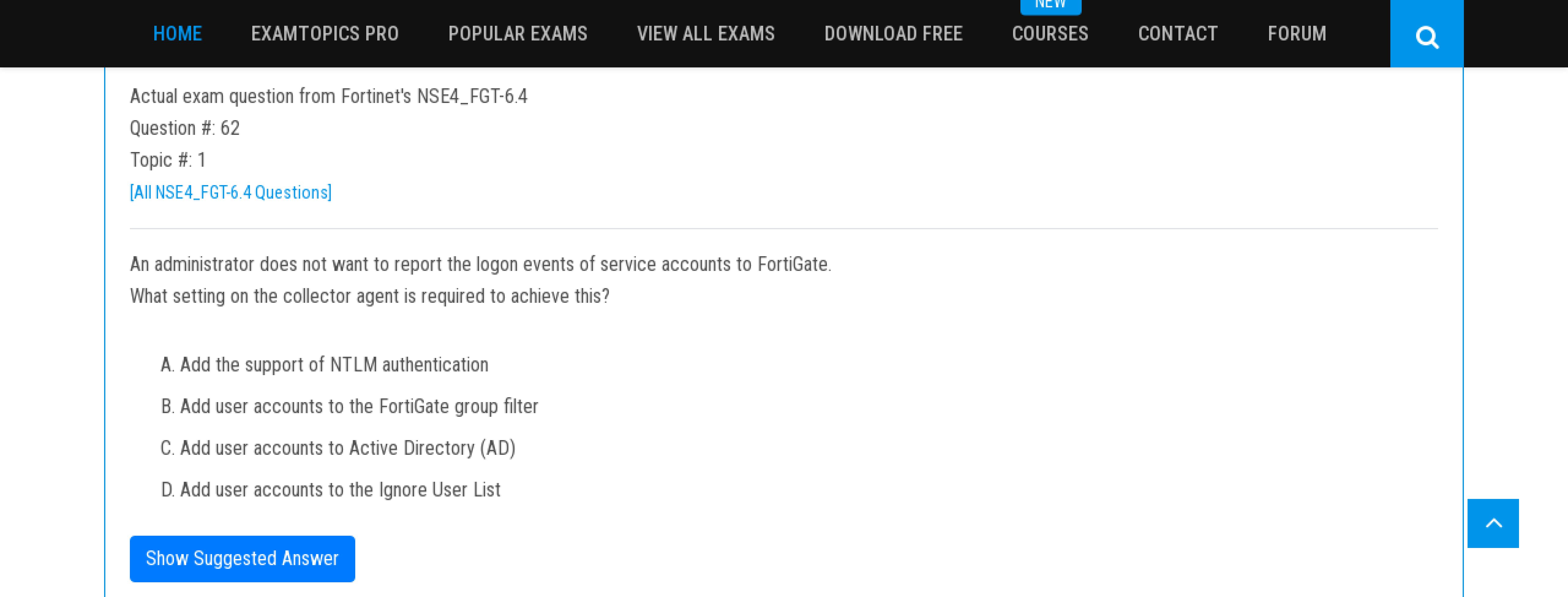
Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

A. FortiGuard update servers

B. System time

C. Operating mode

D. NGFW mode



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 62

Topic #: 1

[All NSE4_FGT-6.4 Questions]

An administrator does not want to report the logon events of service accounts to FortiGate.

What setting on the collector agent is required to achieve this?

A. Add the support of NTLM authentication

B. Add user accounts to the FortiGate group filter

C. Add user accounts to Active Directory (AD)

D. Add user accounts to the Ignore User List

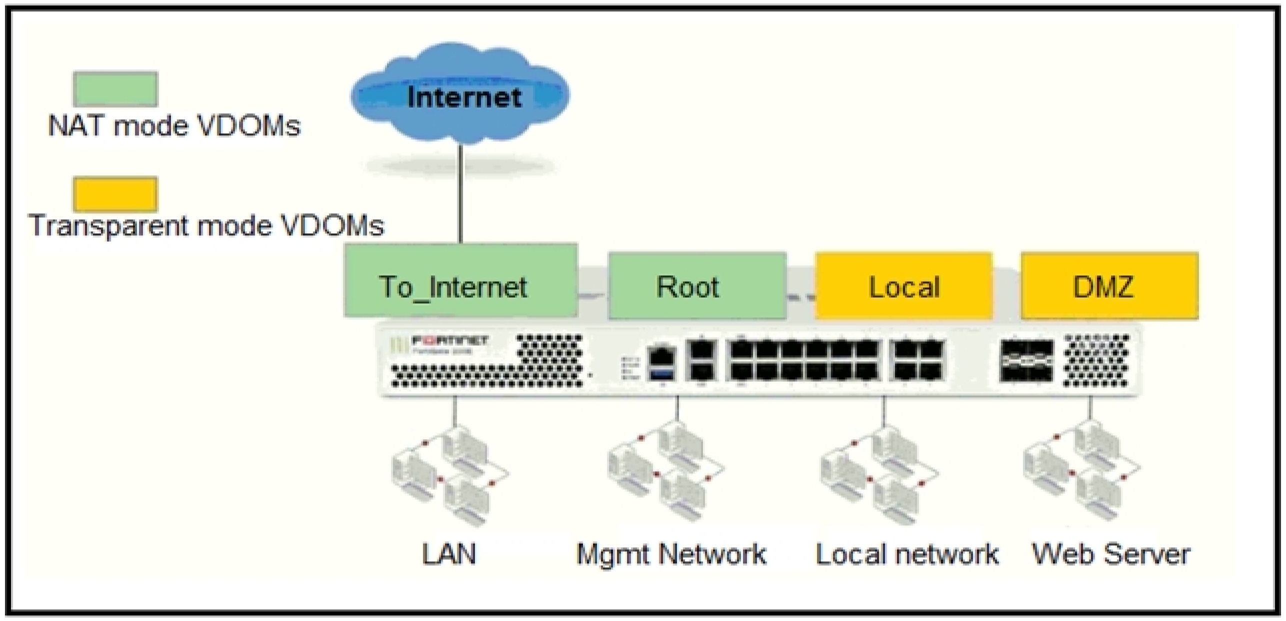
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 63

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.

The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the Internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem.

Which two statements are true? (Choose two.)

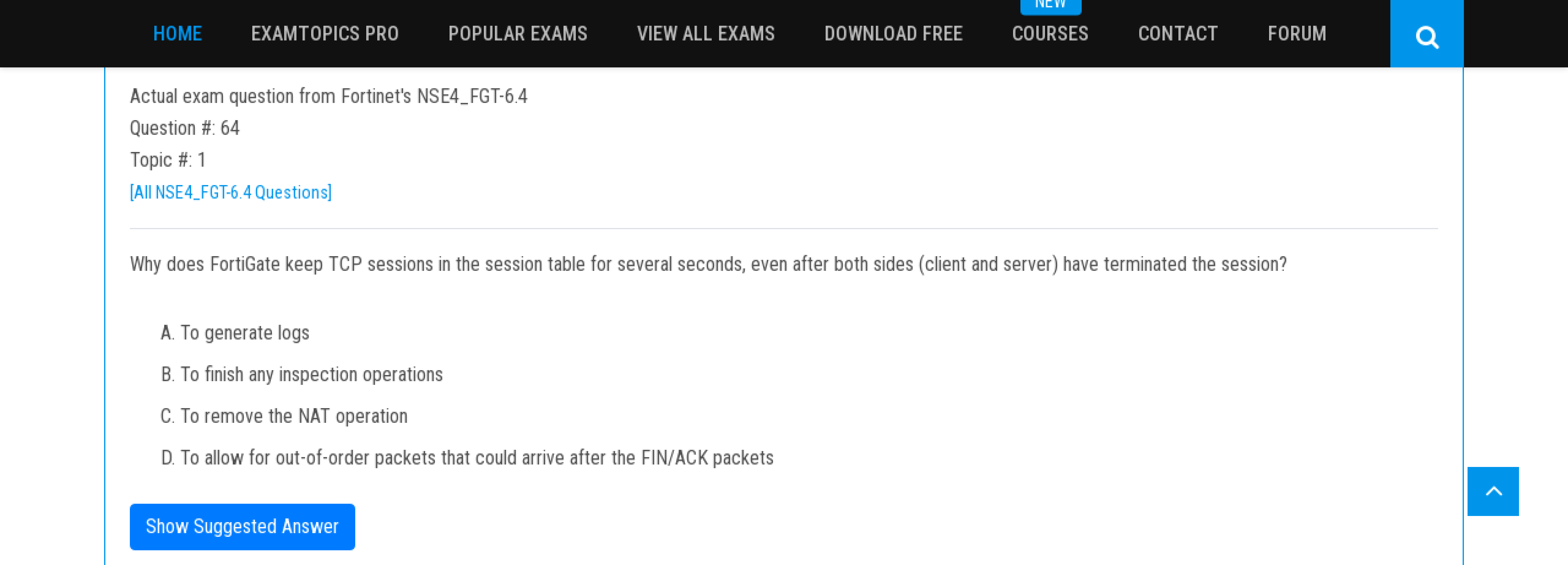
A. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.

B. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.

C. A static route is required on the To-Internet VDOM to allow LAN users to access the Internet.

D. Inter-VDOM links are not required between the Root and To-Internet VDOMs because the Root VDOM is used only as a management VDOM.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 64

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Why does FortiGate keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

A. To generate logs

B. To finish any inspection operations

C. To remove the NAT operation

D. To allow for out-of-order packets that could arrive after the FIN/ACK packets

Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 65

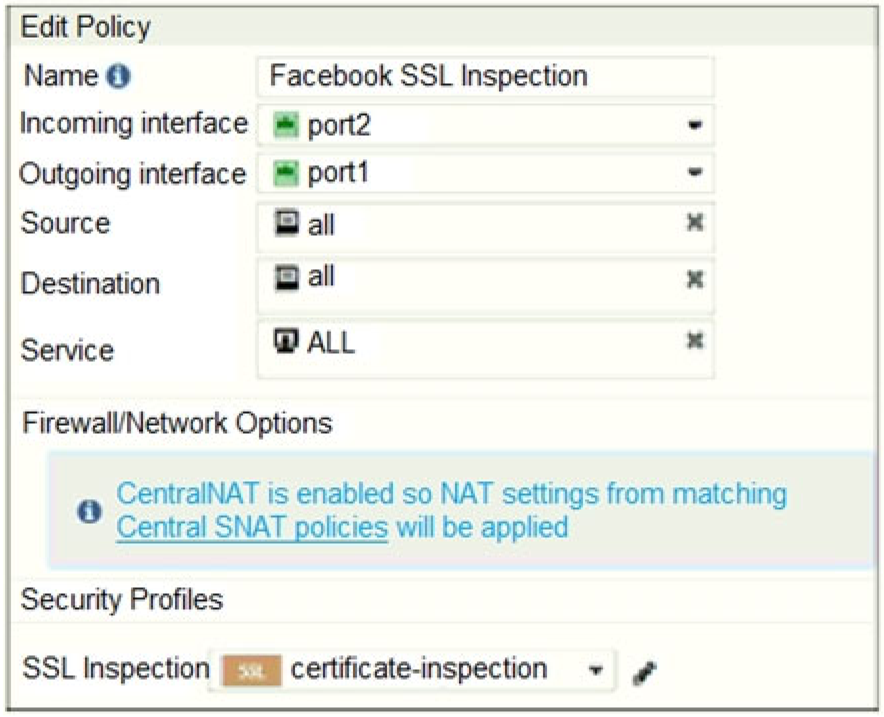
Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibits.

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook.

Exhibit A.



Edit Policy

Name: Facebook SSL Inspection

Incoming interface: port2

Outgoing interface: port1

Source: all

Destination: all

Service: ALL

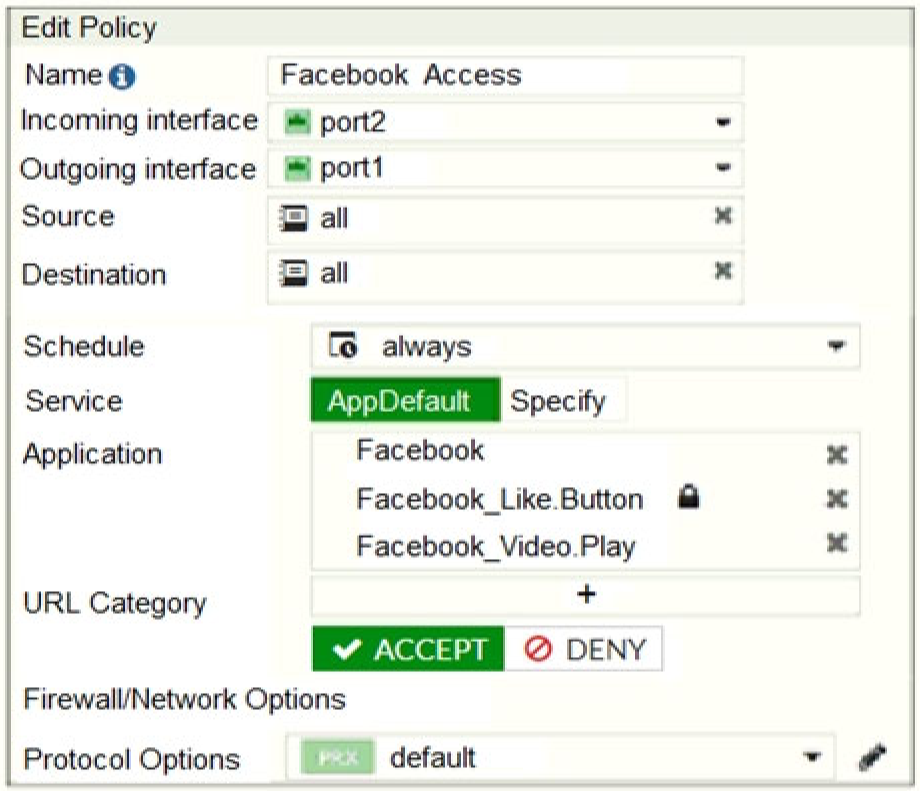
Firewall/Network Options

CentralNAT is enabled so NAT settings from matching Central SNAT policies will be applied

Security Profiles

SSL Inspection: certificate-inspection

Exhibit B.



Edit Policy

Name: Facebook Access

Incoming interface: port2

Outgoing interface: port1

Source: all

Destination: all

Schedule: always

Service: AppDefault Specify

Application: Facebook
Facebook_Like.Button
Facebook_Video.Play

URL Category: +

✓ ACCEPT ⊘ DENY

Firewall/Network Options

Protocol Options: default

Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.

Which part of the policy configuration must you change to resolve the issue?

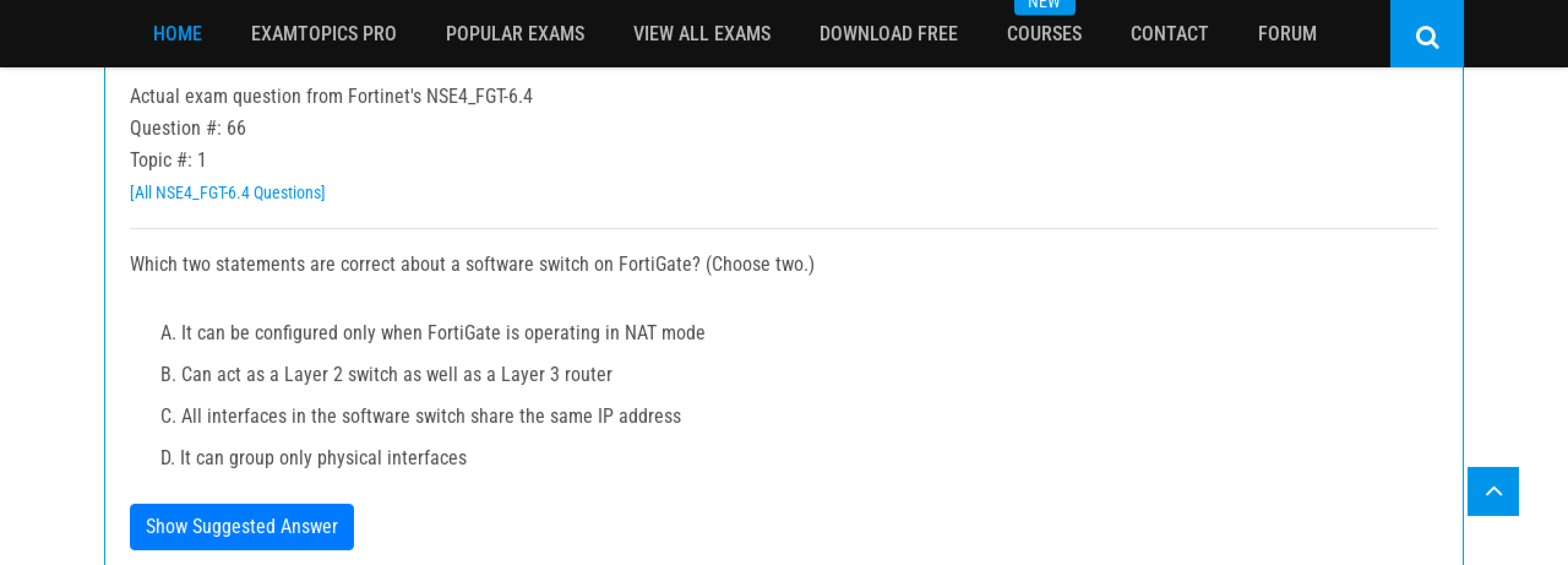
A. Add Facebook in the URL category in the security policy

B. Force access to Facebook using the HTTP service

C. Additional application signatures are required to add to the security policy

D. The SSL inspection needs to be a deep content inspection

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 66

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which two statements are correct about a software switch on FortiGate? (Choose two.)

A. It can be configured only when FortiGate is operating in NAT mode

B. Can act as a Layer 2 switch as well as a Layer 3 router

C. All interfaces in the software switch share the same IP address

D. It can group only physical interfaces

Show Suggested Answer

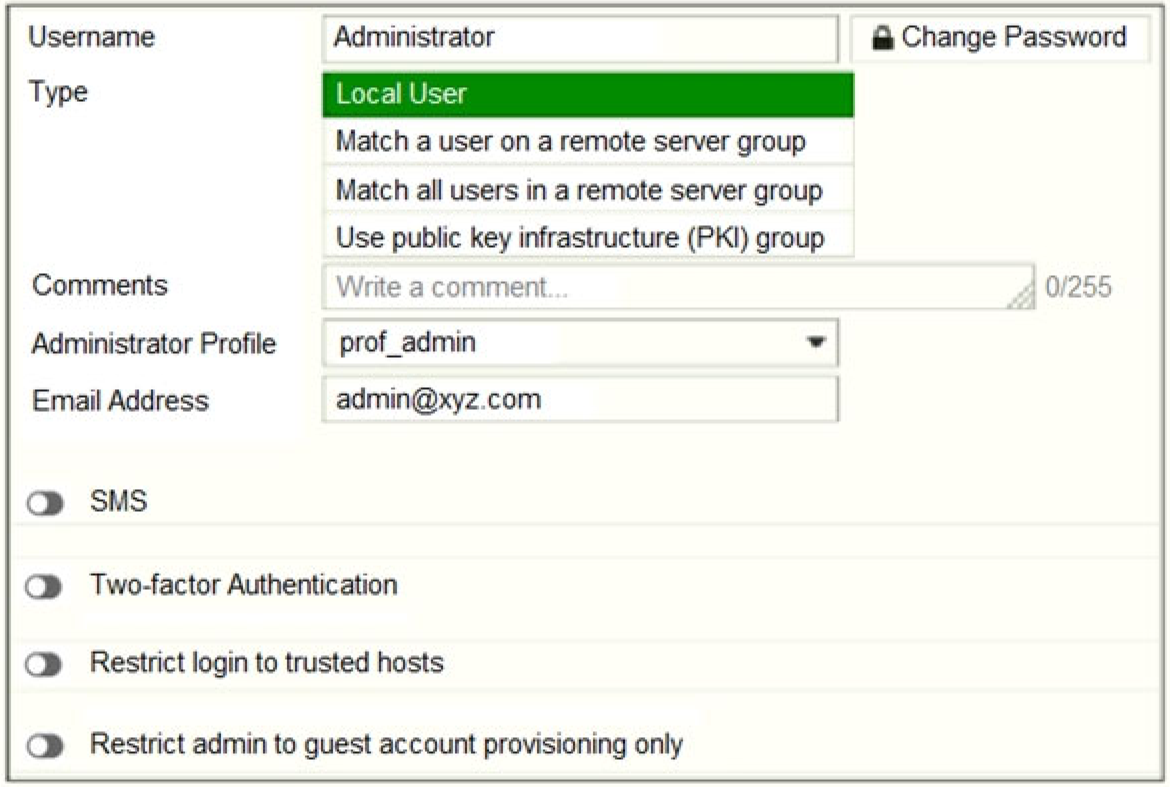
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 67

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



Username	Administrator	🔒 Change Password
Type	Local User Match a user on a remote server group Match all users in a remote server group Use public key infrastructure (PKI) group	
Comments	Write a comment...	0/255
Administrator Profile	prof_admin	
Email Address	admin@xyz.com	

○ SMS

○ Two-factor Authentication

○ Restrict login to trusted hosts

○ Restrict admin to guest account provisioning only

The global settings on a FortiGate device must be changed to align with company security policies.
What does the Administrator account need to access the FortiGate global settings?

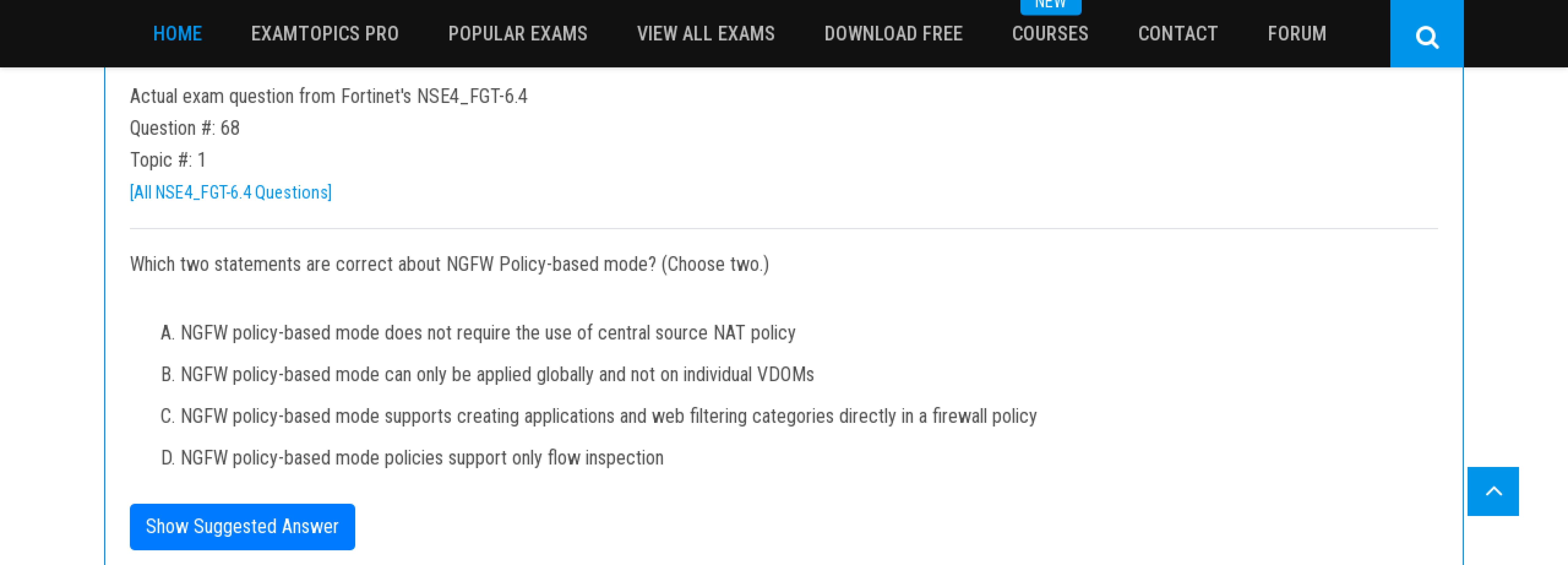
A. Enable restrict access to trusted hosts

B. Change password

C. Enable two-factor authentication

D. Change Administrator profile

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 68

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which two statements are correct about NGFW Policy-based mode? (Choose two.)

A. NGFW policy-based mode does not require the use of central source NAT policy

B. NGFW policy-based mode can only be applied globally and not on individual VDOMs

C. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy

D. NGFW policy-based mode policies support only flow inspection

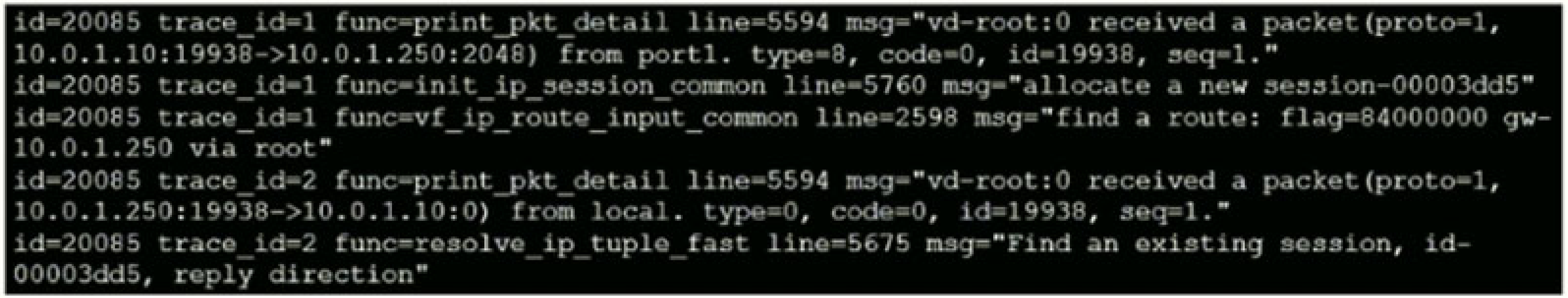
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 69

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit showing a debug flow output.



```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

Which two statements about the debug flow output are correct? (Choose two.)

A. The debug flow is of ICMP traffic

B. The default route is required to receive a reply

C. A firewall policy allowed the connection

D. A new traffic session is created

Show Suggested Answer

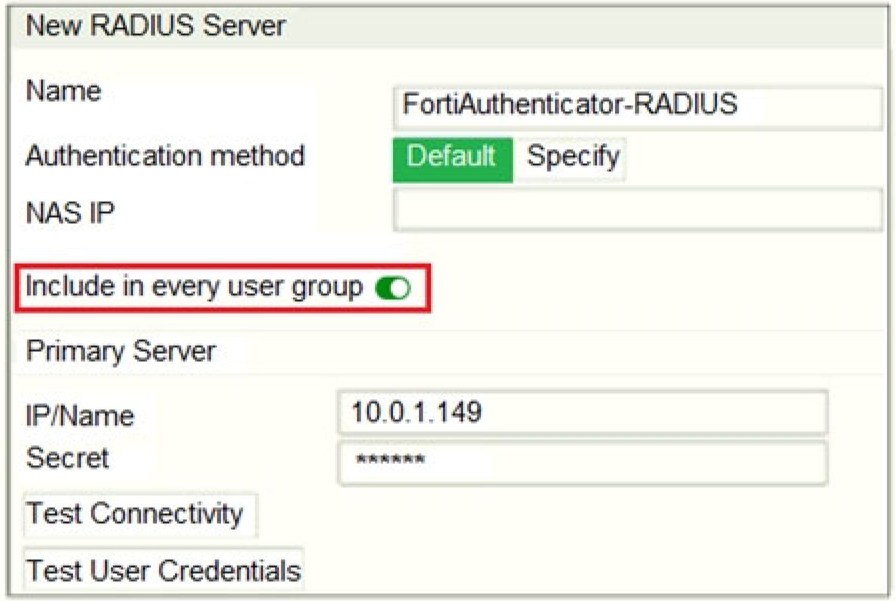
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 70

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit, which contains a radius server configuration.



New RADIUS Server

Name: FortiAuthenticator-RADIUS

Authentication method: Default Specify

NAS IP:

Include in every user group ●

Primary Server

IP/Name: 10.0.1.149

Secret: ******

An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option.

What will be the impact of using Include in every user group option in a RADIUS configuration?

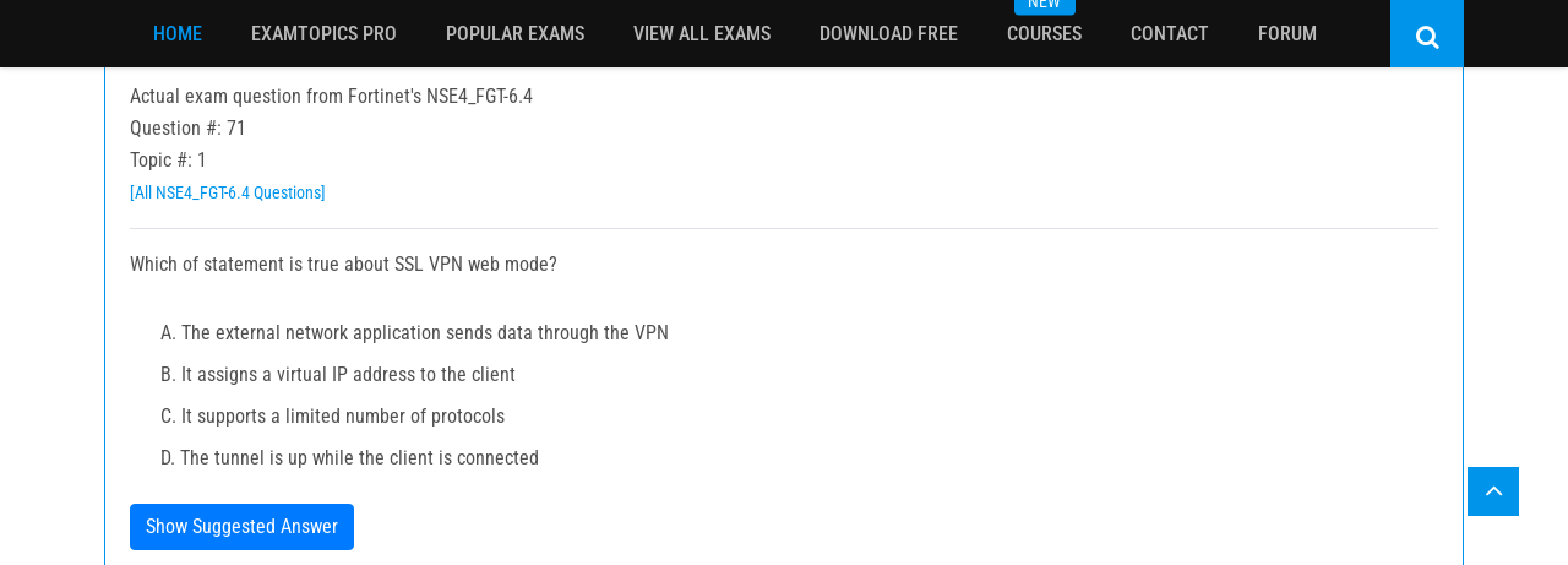
A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.

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 all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.

D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 71

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which of statement is true about SSL VPN web mode?

A. The external network application sends data through the VPN

B. It assigns a virtual IP address to the client

C. It supports a limited number of protocols

D. The tunnel is up while the client is connected

Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 72

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

A. Antivirus engine

B. Intrusion prevention system engine

C. Flow engine

D. Detection engine

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 73

Topic #: 1

[All NSE4_FGT-6.4 Questions]

An administrator has configured the following settings:

```
config system settings
      set ses-denied-traffic enable
end
config system global
      set block-session-timer 30
end
```

What are the two results of this configuration? (Choose two.)

A. Device detection on all interfaces is enforced for 30 minutes

B. Denied users are blocked for 30 minutes

C. A session for denied traffic is created

D. The number of logs generated by denied traffic is reduced

Show Suggested Answer

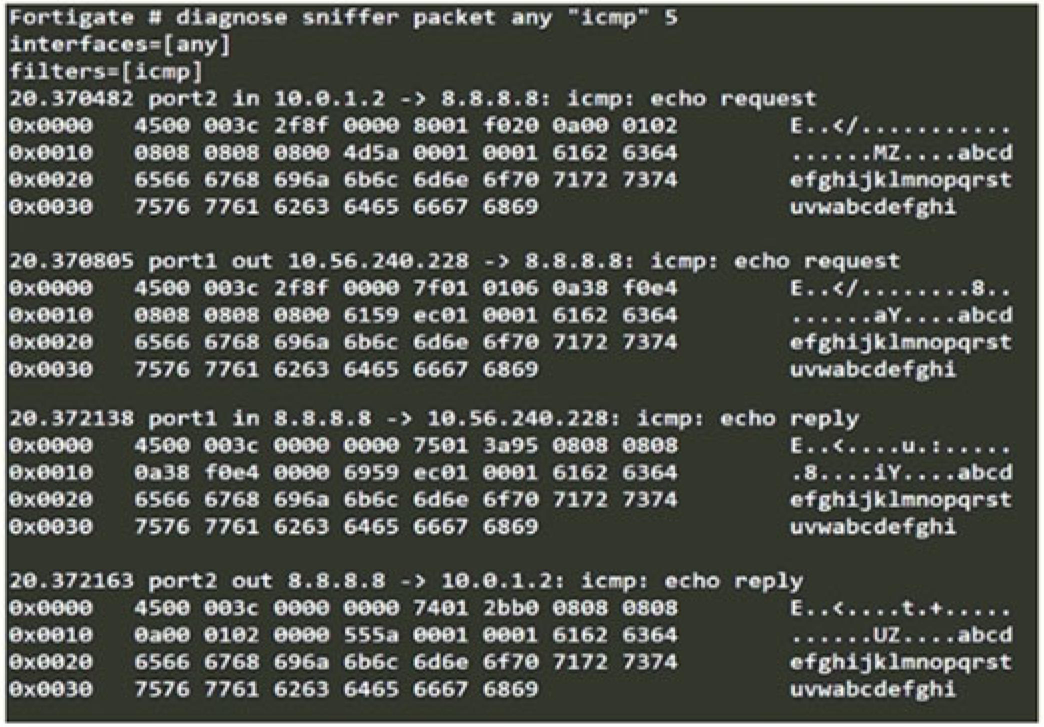
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 74

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit.



```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000   4500 003c 2f8f 0000 8001 f020 0a00 0102        E..</..........
0x0010   0808 0808 0800 4d5a 0001 0001 6162 6364        ......MZ....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000   4500 003c 2f8f 0000 7f01 0106 0a38 f0e4        E..</........8..
0x0010   0808 0808 0800 6159 ec01 0001 6162 6364        ......aY....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000   4500 003c 0000 0000 7501 3a95 0808 0808        E..<....u.:.....
0x0010   0a38 f0e4 0000 6959 ec01 0001 6162 6364        .8....iY....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000   4500 003c 0000 0000 7401 2bb0 0808 0808        E..<....t.+.....
0x0010   0a00 0102 0000 555a 0001 0001 6162 6364        ......UZ....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.

Which three pieces of information are included in the sniffer output? (Choose three.)

A. Interface name

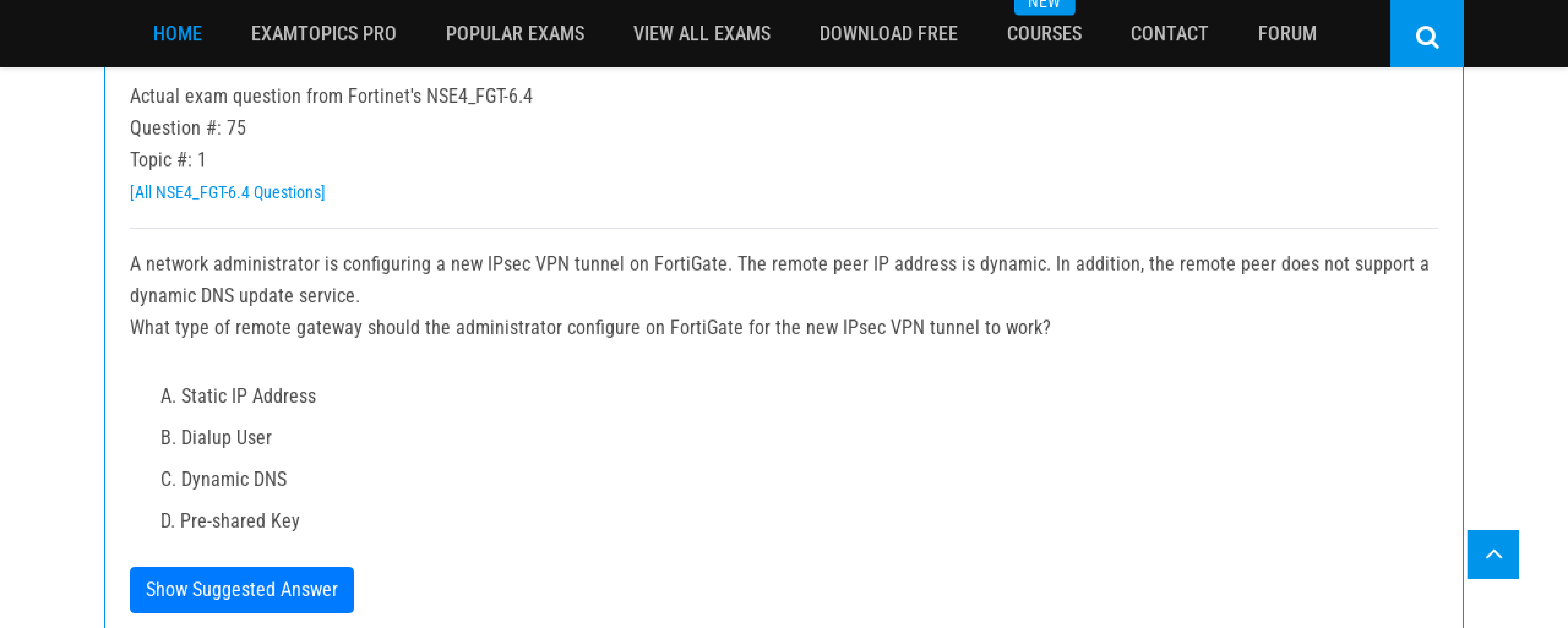
B. Ethernet header

C. IP header

D. Application header

E. Packet payload

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 75

Topic #: 1

[All NSE4_FGT-6.4 Questions]

A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.

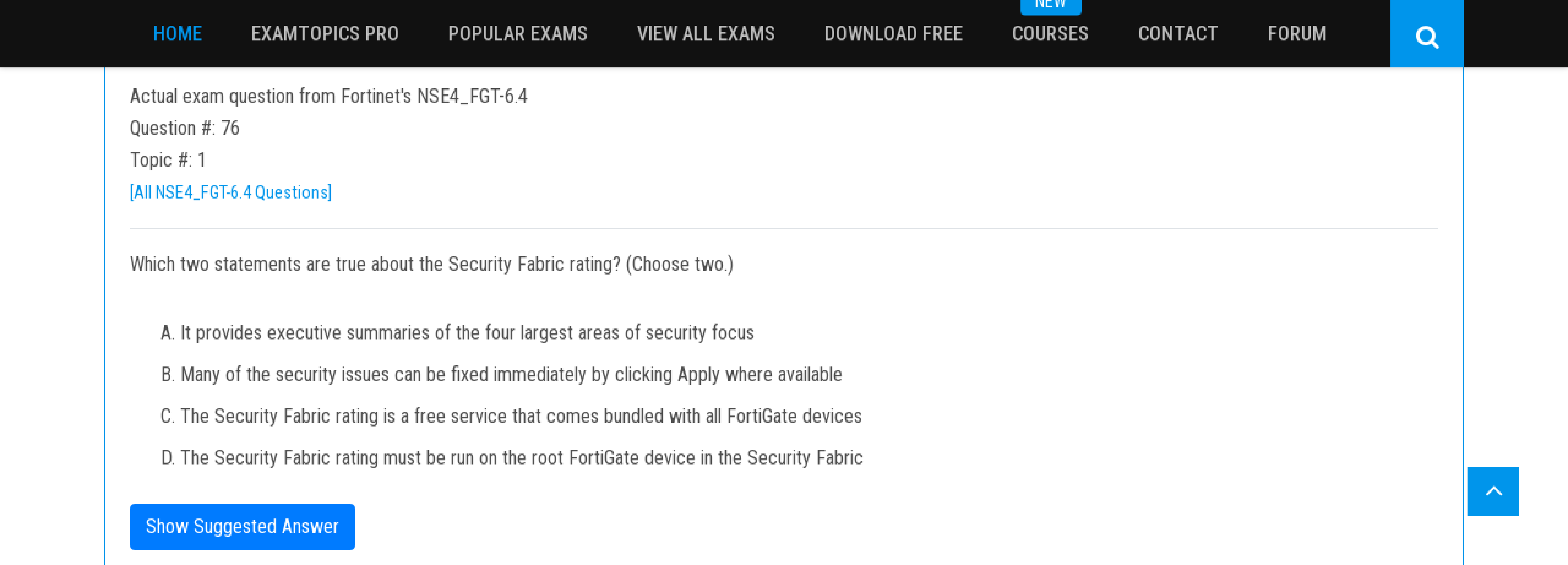
What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

A. Static IP Address

B. Dialup User

C. Dynamic DNS

D. Pre-shared Key



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 76

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which two statements are true about the Security Fabric rating? (Choose two.)

A. It provides executive summaries of the four largest areas of security focus

B. Many of the security issues can be fixed immediately by clicking Apply where available

C. The Security Fabric rating is a free service that comes bundled with all FortiGate devices

D. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric

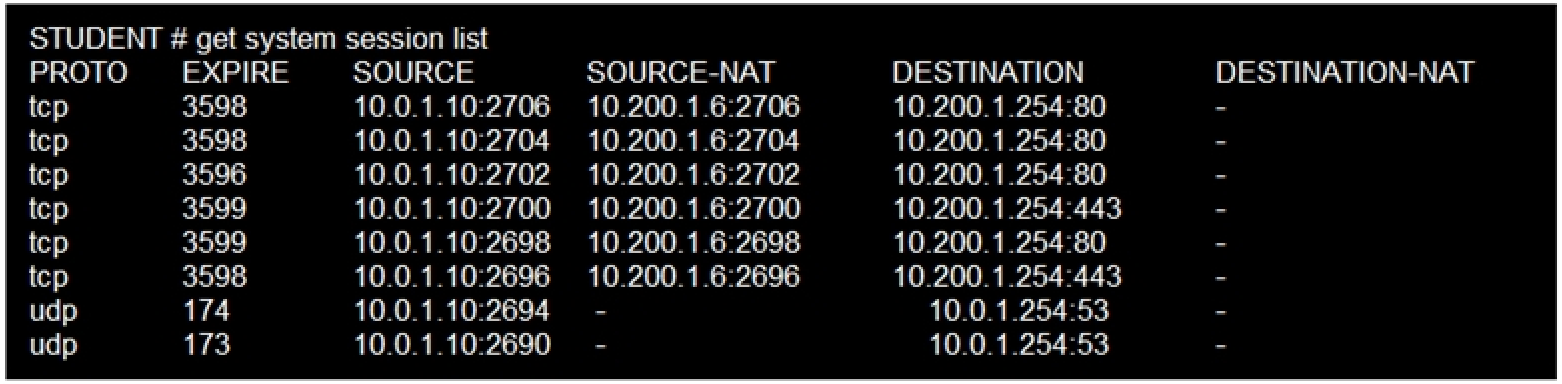
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 77

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit, which contains a session list output.



```
STUDENT # get system session list
PROTO    EXPIRE    SOURCE           SOURCE-NAT        DESTINATION         DESTINATION-NAT
tcp      3598      10.0.1.10:2706   10.200.1.6:2706   10.200.1.254:80     -
tcp      3598      10.0.1.10:2704   10.200.1.6:2704   10.200.1.254:80     -
tcp      3596      10.0.1.10:2702   10.200.1.6:2702   10.200.1.254:80     -
tcp      3599      10.0.1.10:2700   10.200.1.6:2700   10.200.1.254:443    -
tcp      3599      10.0.1.10:2698   10.200.1.6:2698   10.200.1.254:80     -
tcp      3598      10.0.1.10:2696   10.200.1.6:2696   10.200.1.254:443    -
udp      174       10.0.1.10:2694    -                  10.0.1.254:53     -
udp      173       10.0.1.10:2690    -                  10.0.1.254:53     -
```

Based on the information shown in the exhibit, which statement is true?

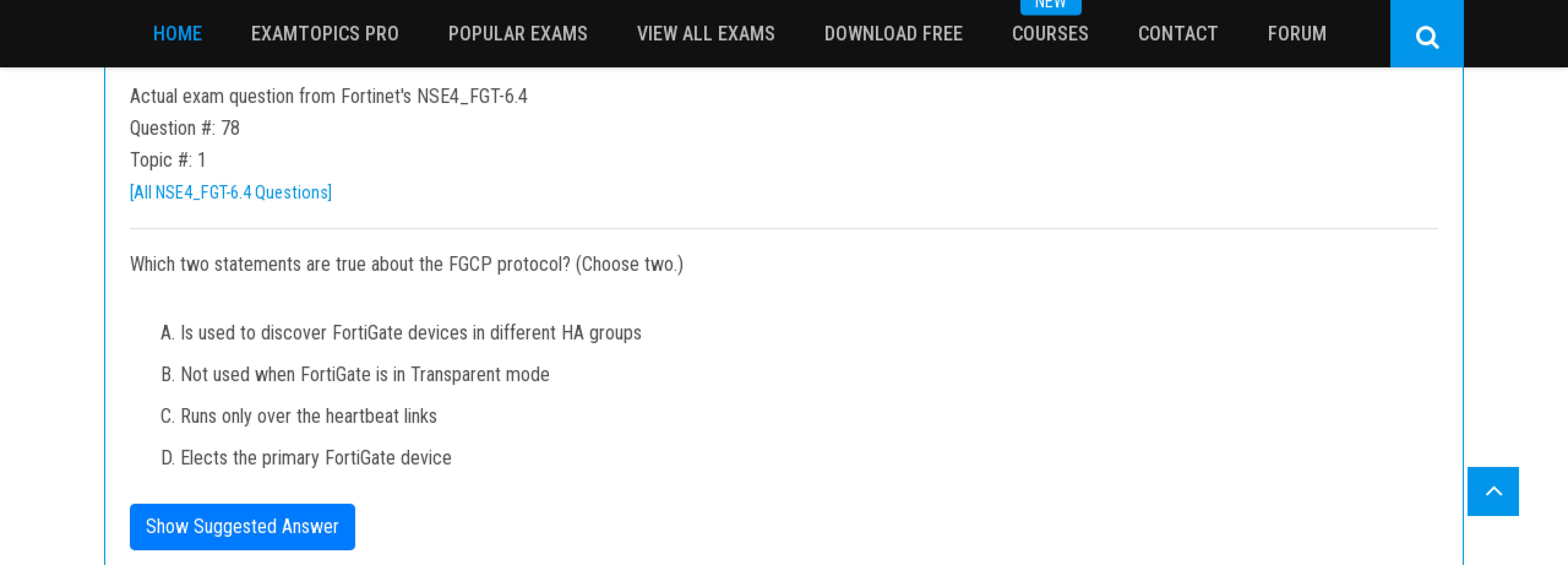
A. Port block allocation IP pool is used in the firewall policy

B. Destination NAT is disabled in the firewall policy

C. Overload NAT IP pool is used in the firewall policy

D. One-to-one NAT IP pool is used in the firewall policy

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 78

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Which two statements are true about the FGCP protocol? (Choose two.)

A. Is used to discover FortiGate devices in different HA groups

B. Not used when FortiGate is in Transparent mode

C. Runs only over the heartbeat links

D. Elects the primary FortiGate device

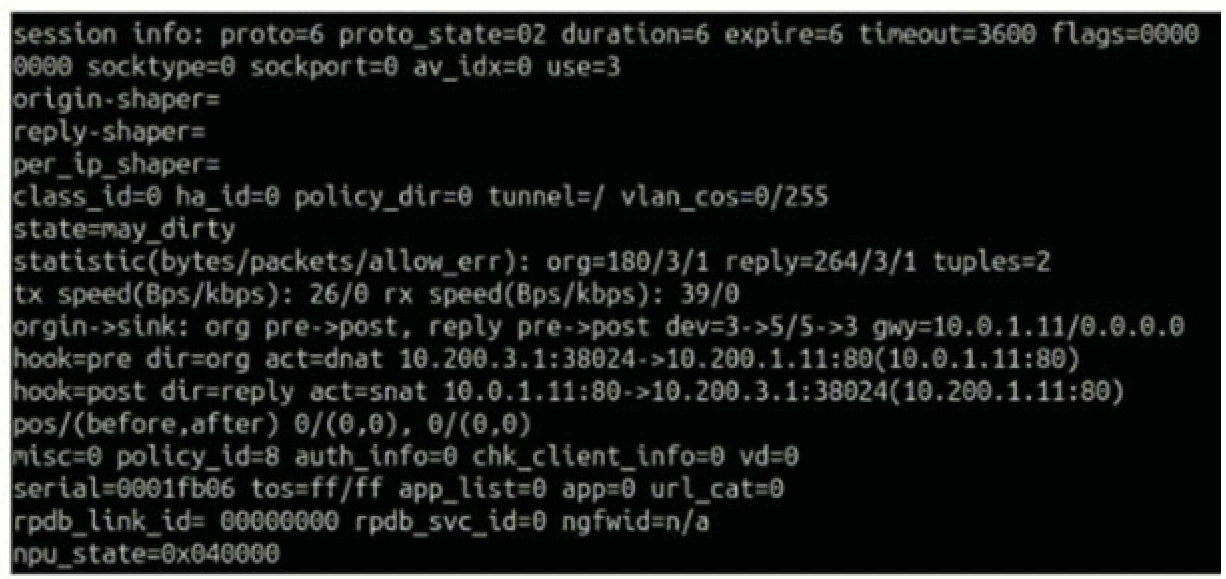
Actual exam question from Fortinet's NSE4_FGT-6.4

Question #: 79

Topic #: 1

[All NSE4_FGT-6.4 Questions]

Refer to the exhibit, which contains a session diagnostic output.



```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 39/0
orgin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80(10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024(10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

A. The session is in ESTABLISHED state

B. The session is in SYN_SENT state

C. The session is in FIN_ACK state

D. The session is in FIN_WAIT state

Show Suggested Answer