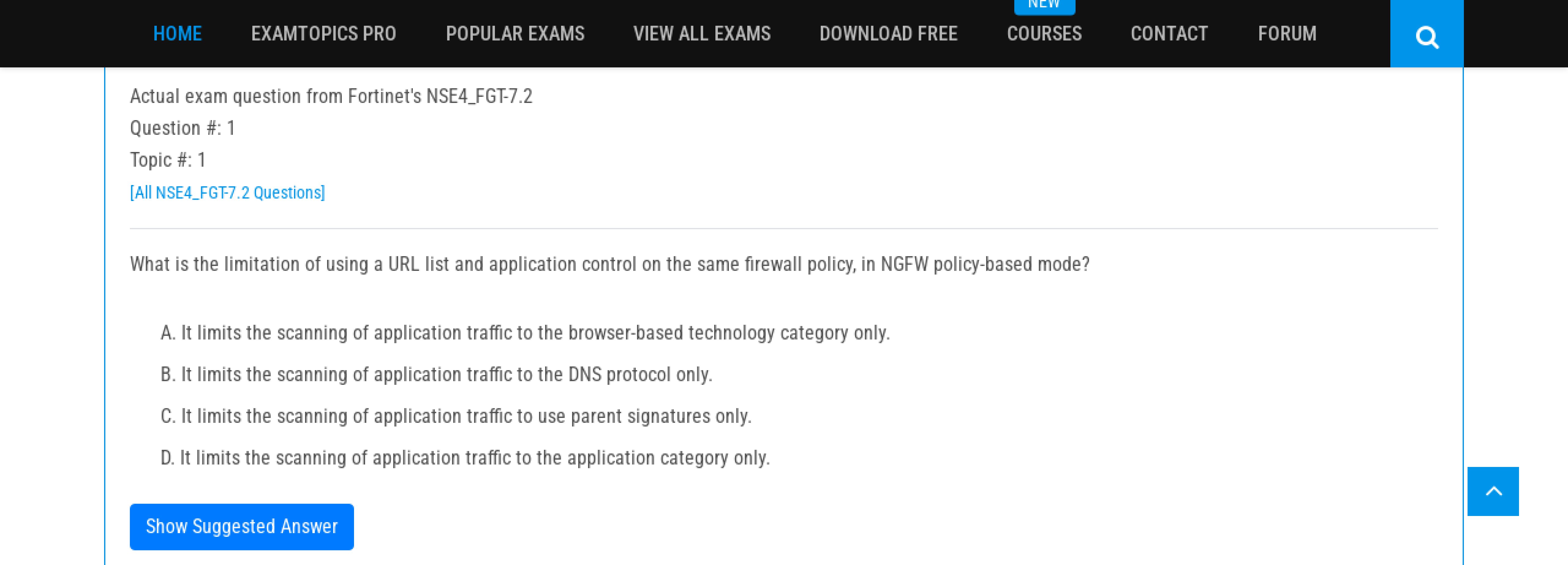


Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 1

Topic #: 1

[All NSE4_FGT-7.2 Questions]

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

A. It limits the scanning of application traffic to the browser-based technology category only.

B. It limits the scanning of application traffic to the DNS protocol only.

C. It limits the scanning of application traffic to use parent signatures only.

D. It limits the scanning of application traffic to the application category only.

Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 2
Topic #: 1
[All NSE4_FGT-7.2 Questions]

Refer to the exhibits.
The exhibits show the firewall policies and the objects used in the firewall policies.
The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.

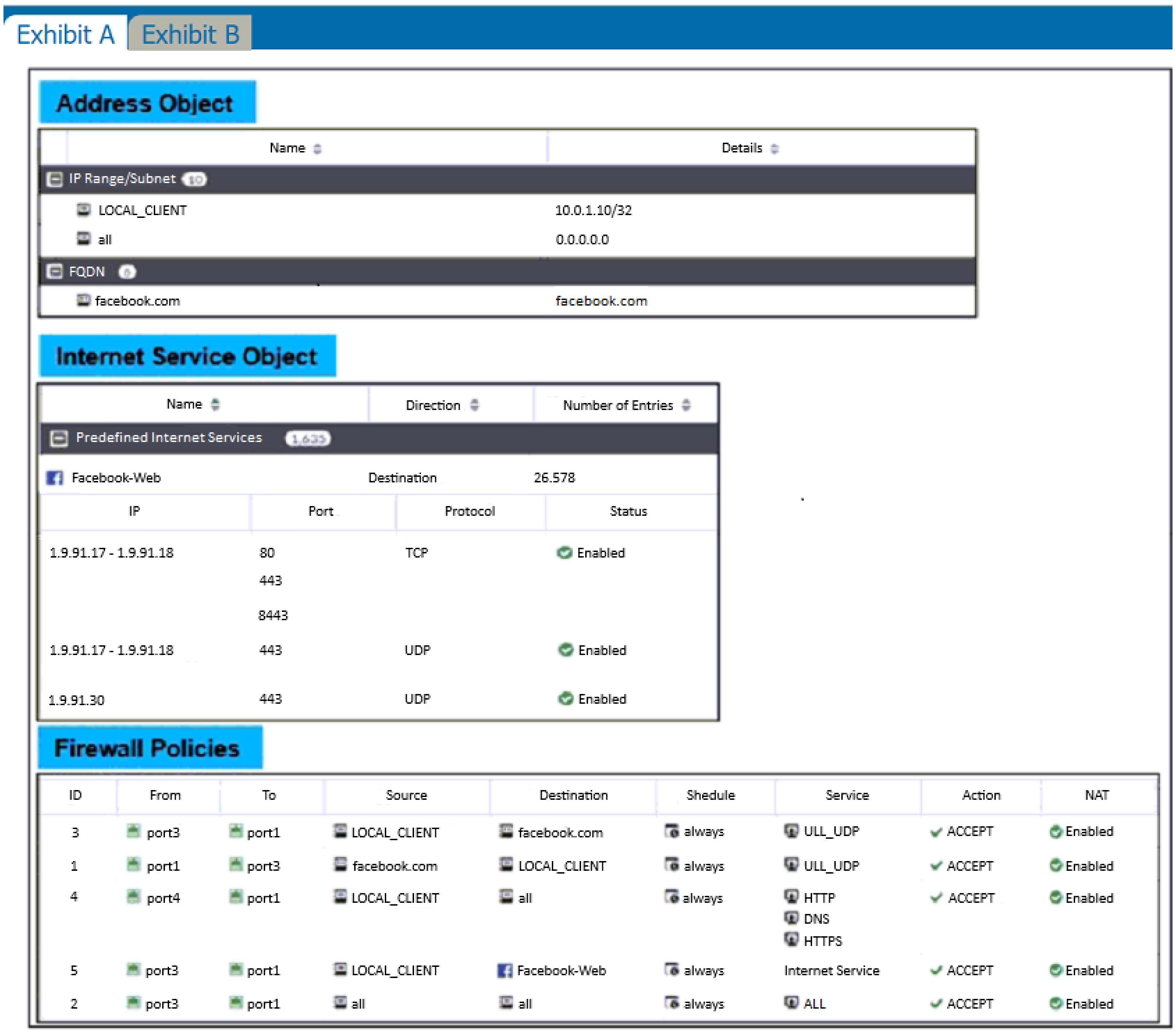


Exhibit A Exhibit B

Address Object

Name	Details
IP Range/Subnet 10	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN 6	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services 1,635		
Facebook-Web	Destination	26.578

IP	Port	Protocol	Status
1.9.91.17 - 1.9.91.18	80 443 8443	TCP	Enabled
1.9.91.17 - 1.9.91.18	443	UDP	Enabled
1.9.91.30	443	UDP	Enabled

Firewall Policies

ID	From	To	Source	Destination	Shedule	Service	Action	NAT
3	port3	port1	LOCAL_CLIENT	facebook.com	always	ULL_UDP	✓ ACCEPT	Enabled
1	port1	port3	facebook.com	LOCAL_CLIENT	always	ULL_UDP	✓ ACCEPT	Enabled
4	port4	port1	LOCAL_CLIENT	all	always	HTTP DNS HTTPS	✓ ACCEPT	Enabled
5	port3	port1	LOCAL_CLIENT	Facebook-Web	always	Internet Service	✓ ACCEPT	Enabled
2	port3	port1	all	all	always	ALL	✓ ACCEPT	Enabled

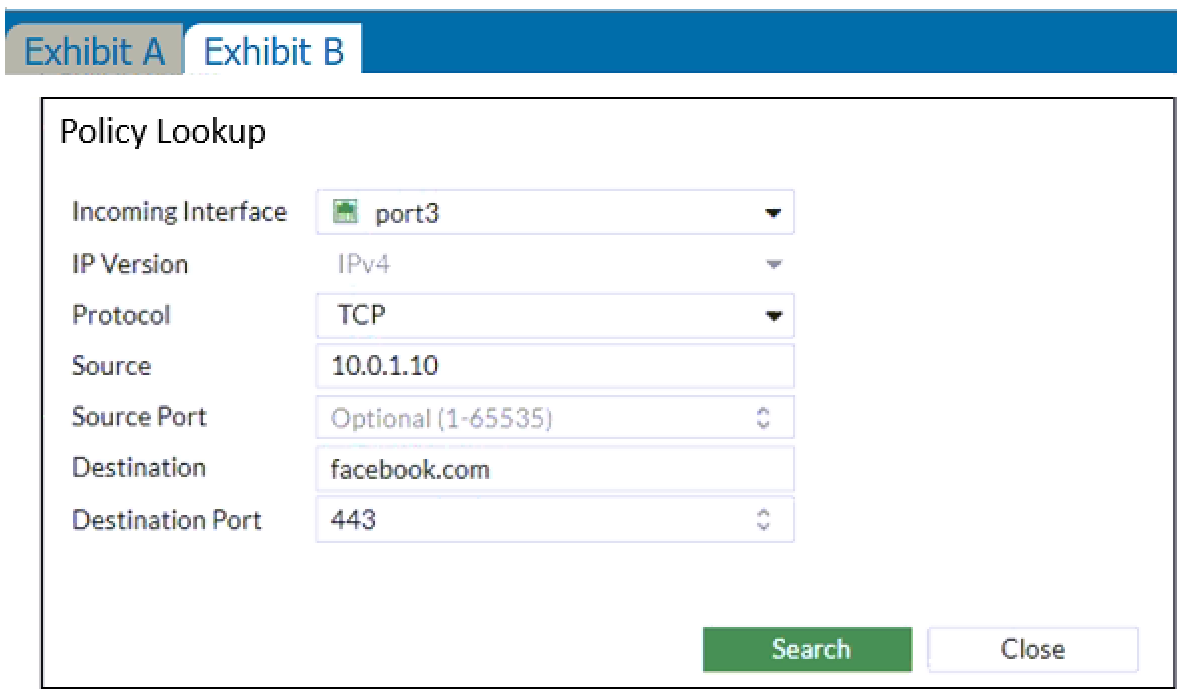


Exhibit A Exhibit B

Policy Lookup

Incoming Interface	port3
IP Version	IPv4
Protocol	TCP
Source	10.0.1.10
Source Port	Optional (1-65535)
Destination	facebook.com
Destination Port	443

Which policy will be highlighted, based on the input criteria?

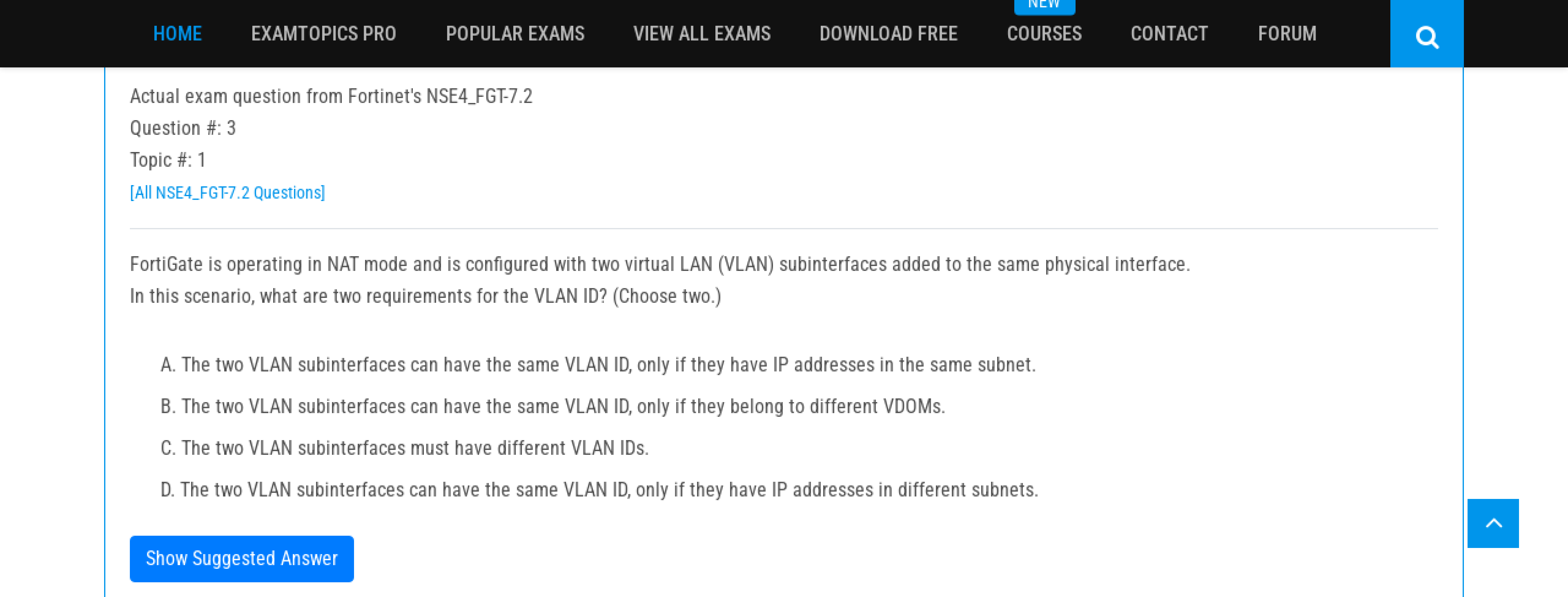
A. Policy with ID 4.

B. Policy with ID 5.

C. Policies with ID 2 and 3.

D. Policy with ID 4.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 3

Topic #: 1

[All NSE4_FGT-7.2 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, what are two requirements for the VLAN ID? (Choose two.)

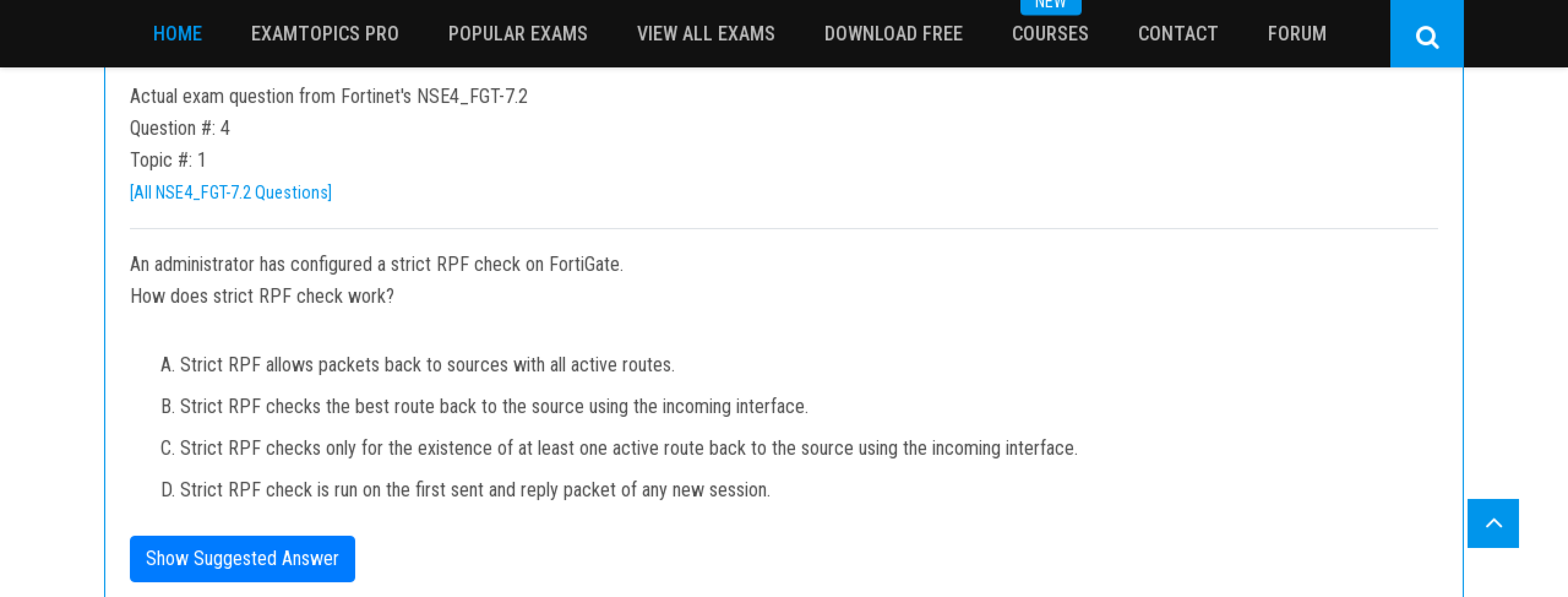
A. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.

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

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

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-7.2

Question #: 4

Topic #: 1

[All NSE4_FGT-7.2 Questions]

An administrator has configured a strict RPF check on FortiGate.

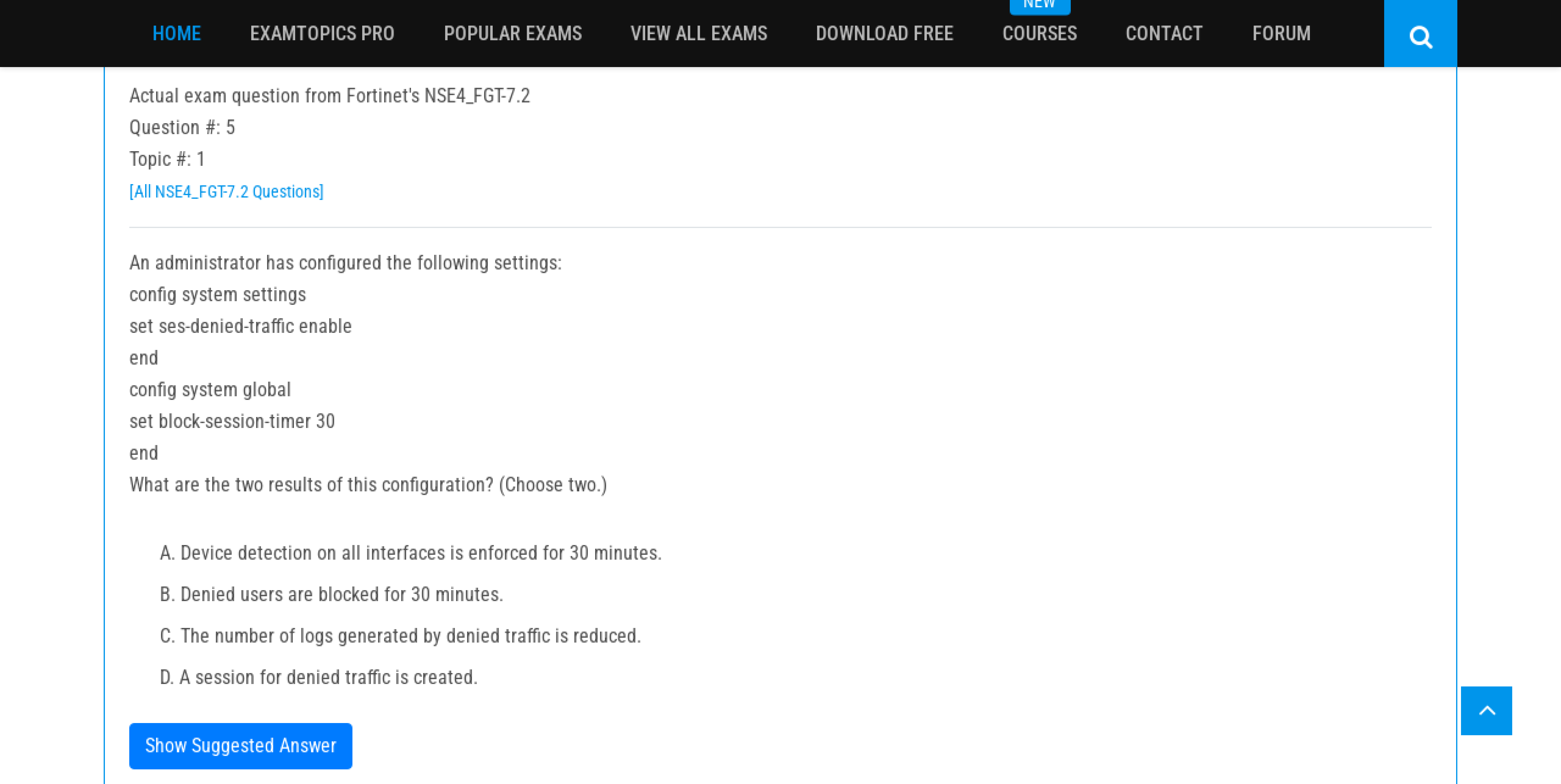
How does strict RPF check work?

A. Strict RPF allows packets back to sources with all active routes.

B. Strict RPF checks the best route back to the source using the incoming interface.

C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.

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



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 5

Topic #: 1

[All NSE4_FGT-7.2 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.

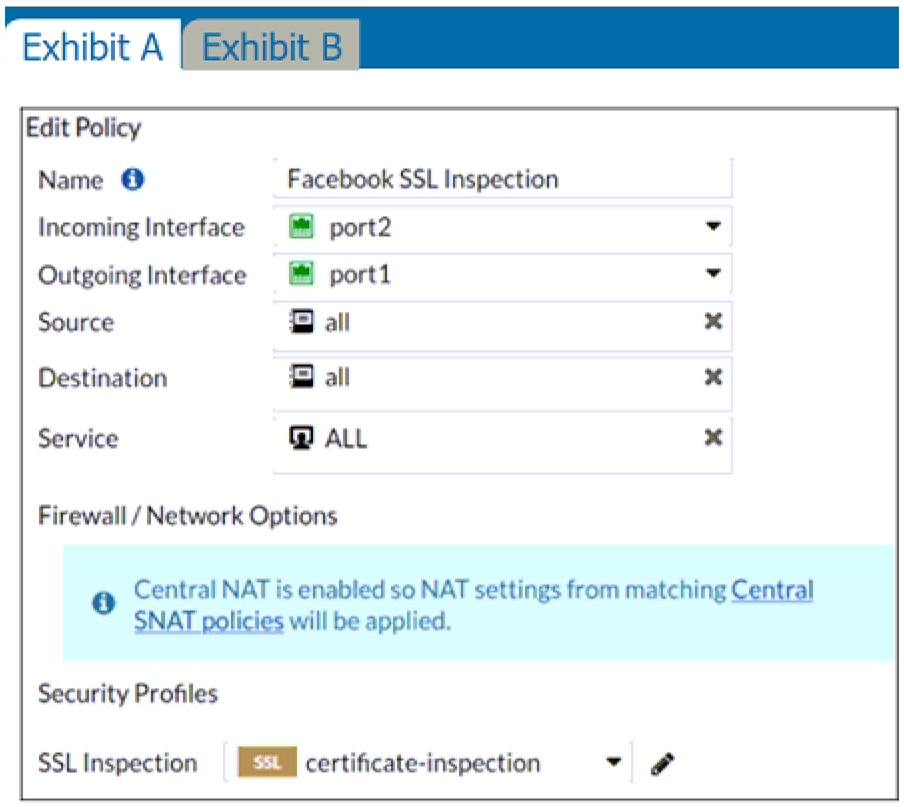
C. The number of logs generated by denied traffic is reduced.

D. A session for denied traffic is created.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 6
Topic #: 1
[All NSE4_FGT-7.2 Questions]

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



Edit Policy

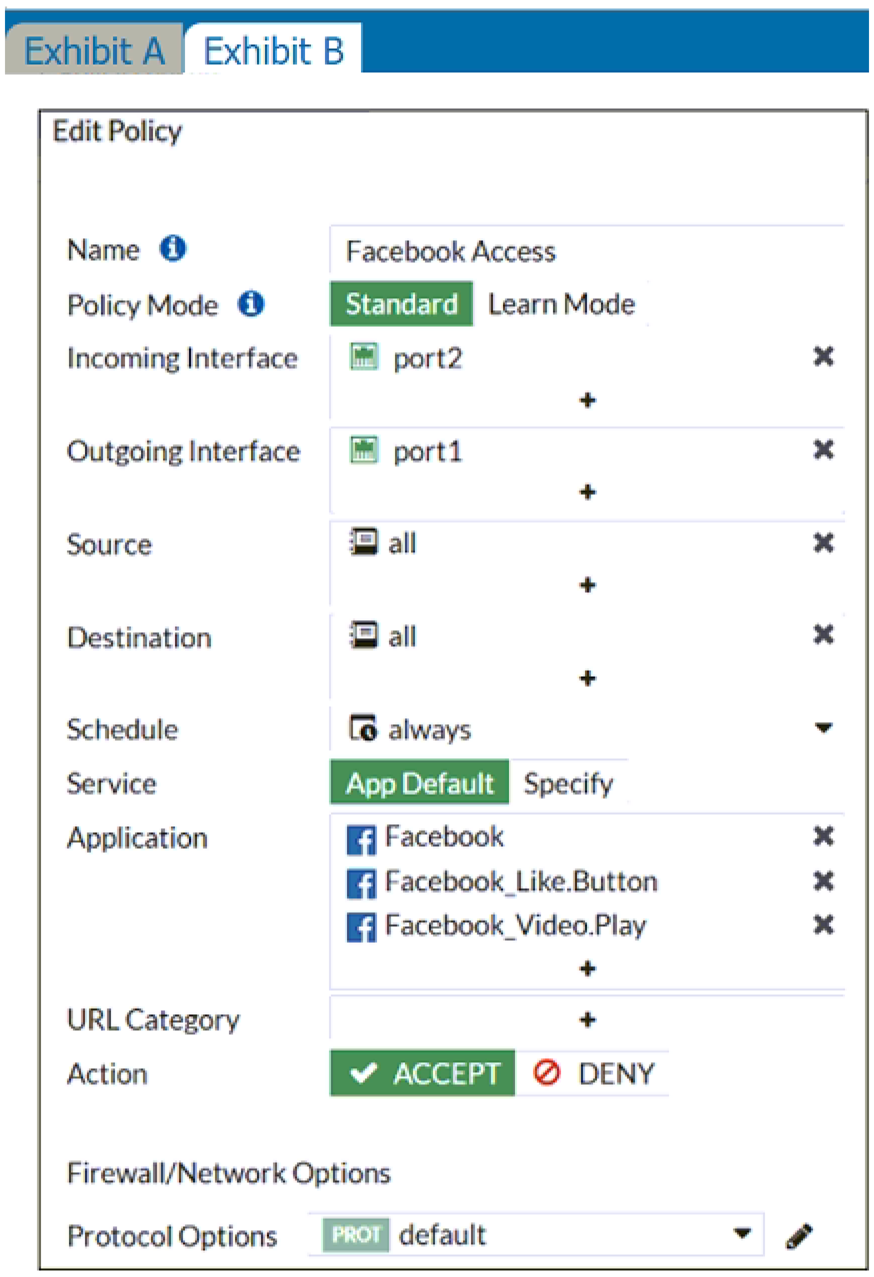
Name: Facebook SSL Inspection
Incoming Interface: port2
Outgoing Interface: port1
Source: all
Destination: all
Service: ALL

Firewall / Network Options

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

Security Profiles

SSL Inspection: SSL certificate-inspection



Edit Policy

Name: Facebook Access
Policy Mode: Standard | Learn Mode
Incoming Interface: port2
Outgoing Interface: port1
Source: all
Destination: all
Schedule: always
Service: App Default | Specify
Application: Facebook
Facebook_Like.Button
Facebook_Video.Play
URL Category:
Action: ✓ ACCEPT | ⊘ DENY

Firewall/Network Options

Protocol Options: PROT default

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

A. Force access to Facebook using the HTTP service.

B. Make the SSL inspection a deep content inspection.

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

D. Get the additional application signatures required to add to the security policy.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

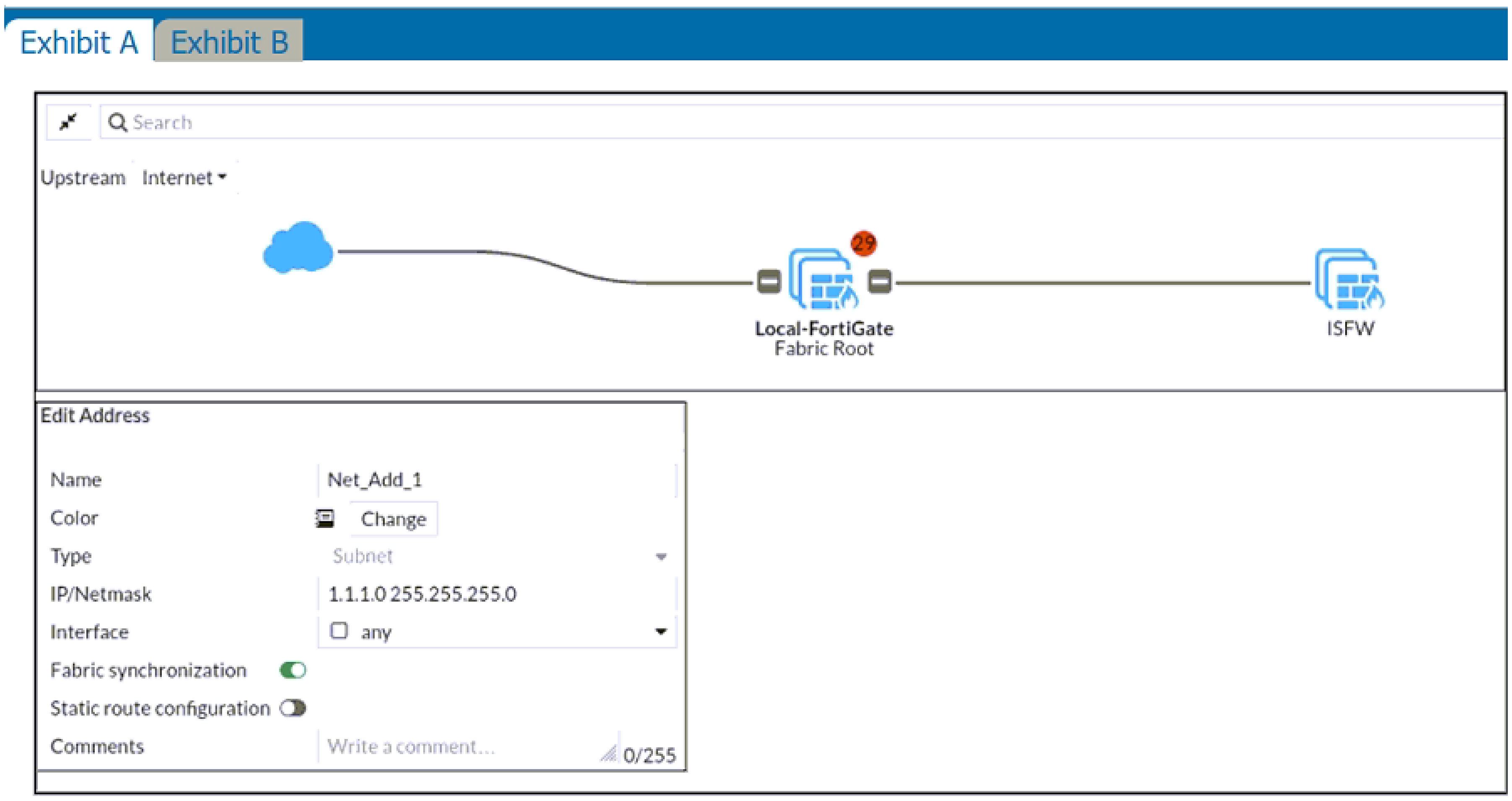
Question #: 7

Topic #: 1

[All NSE4_FGT-7.2 Questions]

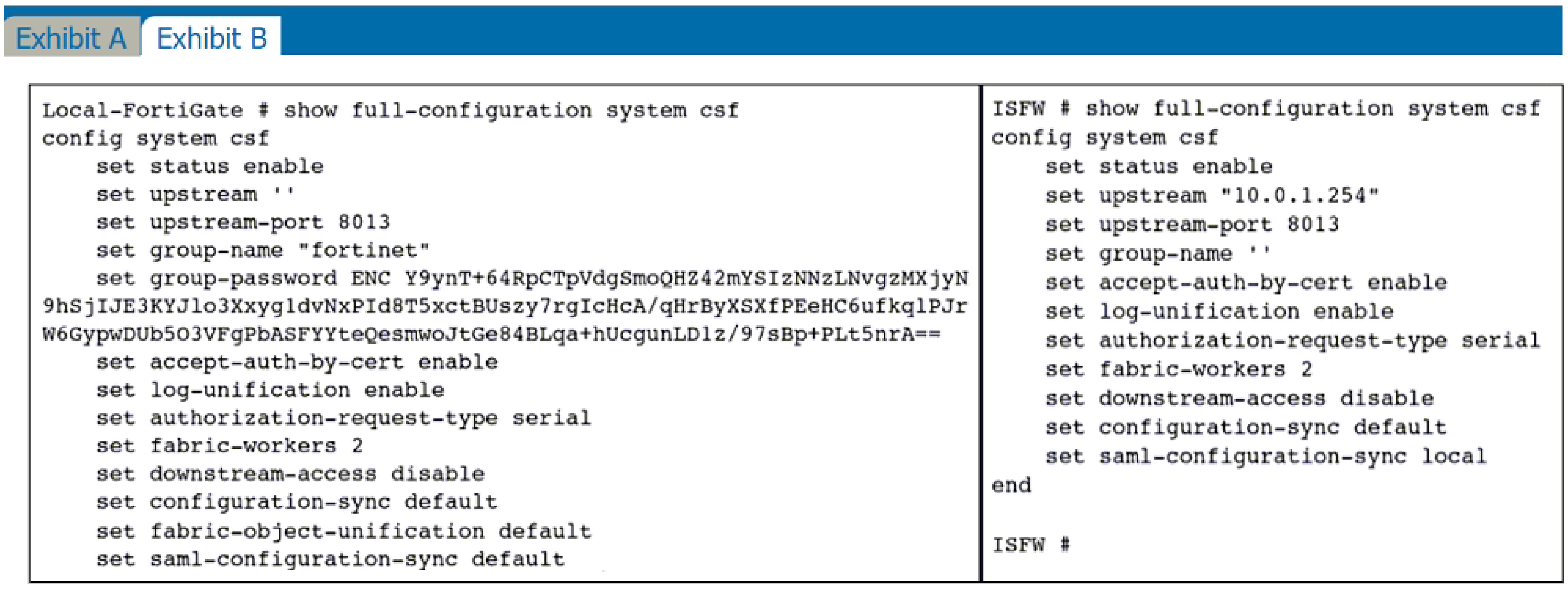
Refer to the exhibits.

An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric. After synchronization, this object is not available on the downstream FortiGate (ISFW).



Edit Address

Name	Net_Add_1
Color	Change
Type	Subnet
IP/Netmask	1.1.1.0 255.255.255.0
Interface	□ any
Fabric synchronization	●
Static route configuration	○
Comments	Write a comment... 0/255



```
Local-FortiGate # show full-configuration system csf
config system csf
    set status enable
    set upstream ''
    set upstream-port 8013
    set group-name "fortinet"
    set group-password ENC Y9ynT+64RpCTpVdgSmoQHZ42mYSIzNNzLNvgzMXjyN
9hSjIJE3KYJlo3XxygldvNxPId8T5xctBUszy7rgIcHcA/qHrByXSXfPEeHC6ufkqlPJr
W6GypwDUb5O3VFgPbASFYYteQesmwoJtGe84BLqa+hUcgunLDlz/97sBp+PLt5nrA==
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set fabric-object-unification default
    set saml-configuration-sync default
```

```
ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream "10.0.1.254"
    set upstream-port 8013
    set group-name ''
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set saml-configuration-sync local
end

ISFW #
```

What must the administrator do to synchronize the address object?

A. Change the csf setting on ISFW (downstream) to set configuration-sync local.

B. Change the csf setting on ISFW (downstream) to set authorization-request-type certificate.

C. Change the csf setting on both devices to set downstream-access enable.

D. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

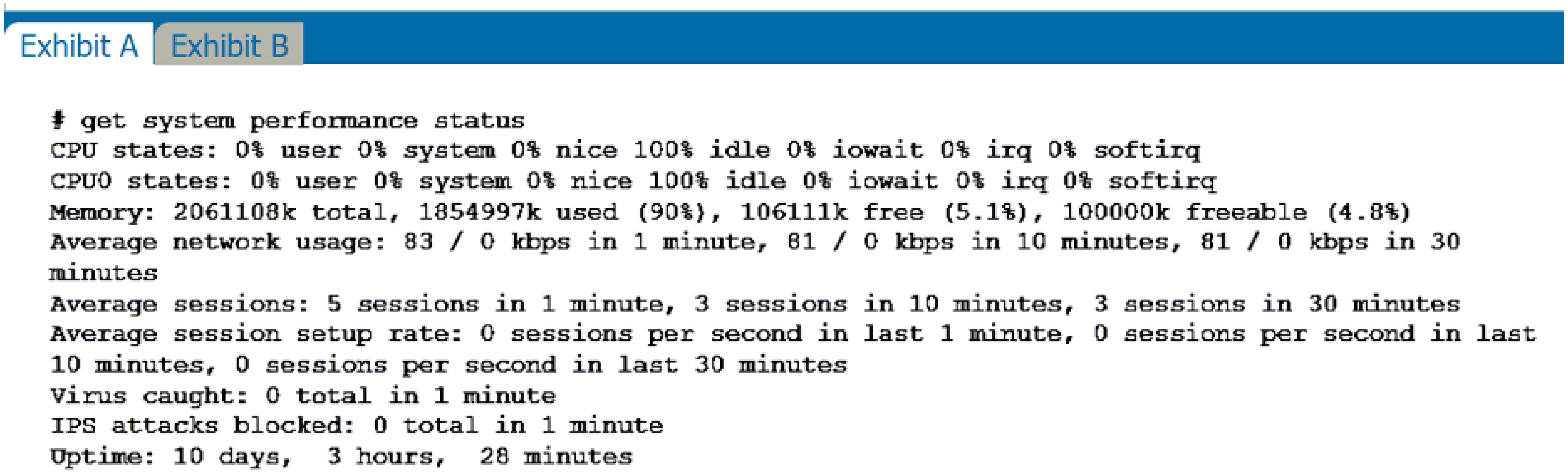
Question #: 8

Topic #: 1

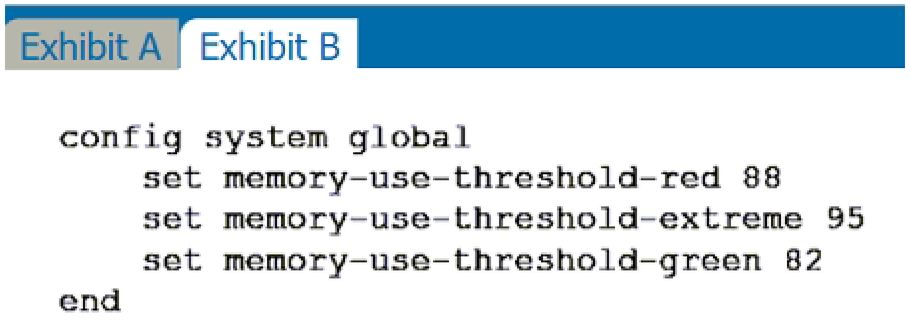
[All NSE4_FGT-7.2 Questions]

Refer to the exhibits.

Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds.



```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```



```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Based on the system performance output, which two results are correct? (Choose two.)

A. FortiGate will start sending all files to FortiSandbox for inspection.

B. FortiGate has entered conserve mode.

C. Administrators cannot change the configuration.

D. Administrators can access FortiGate only through the console port.

Show Suggested Answer

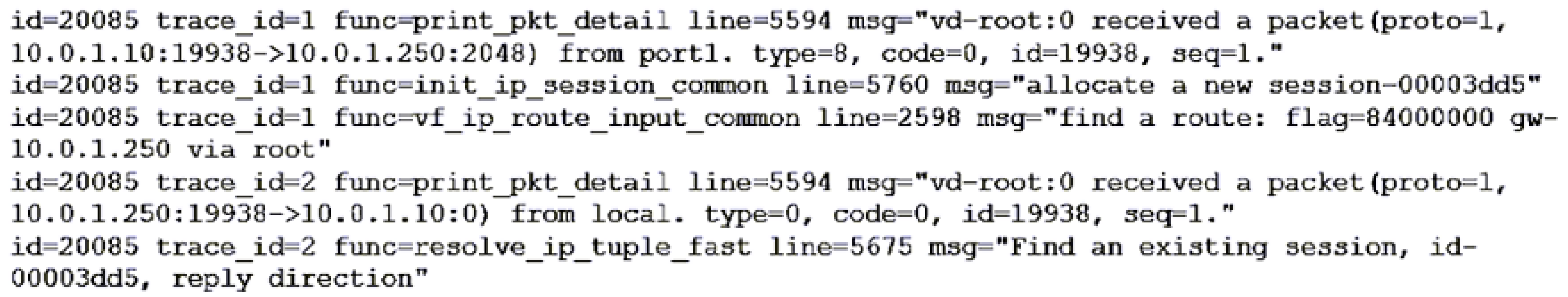
Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 9

Topic #: 1

[All NSE4_FGT-7.2 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"
```

What two conclusions can you make from the debug flow output? (Choose two.)

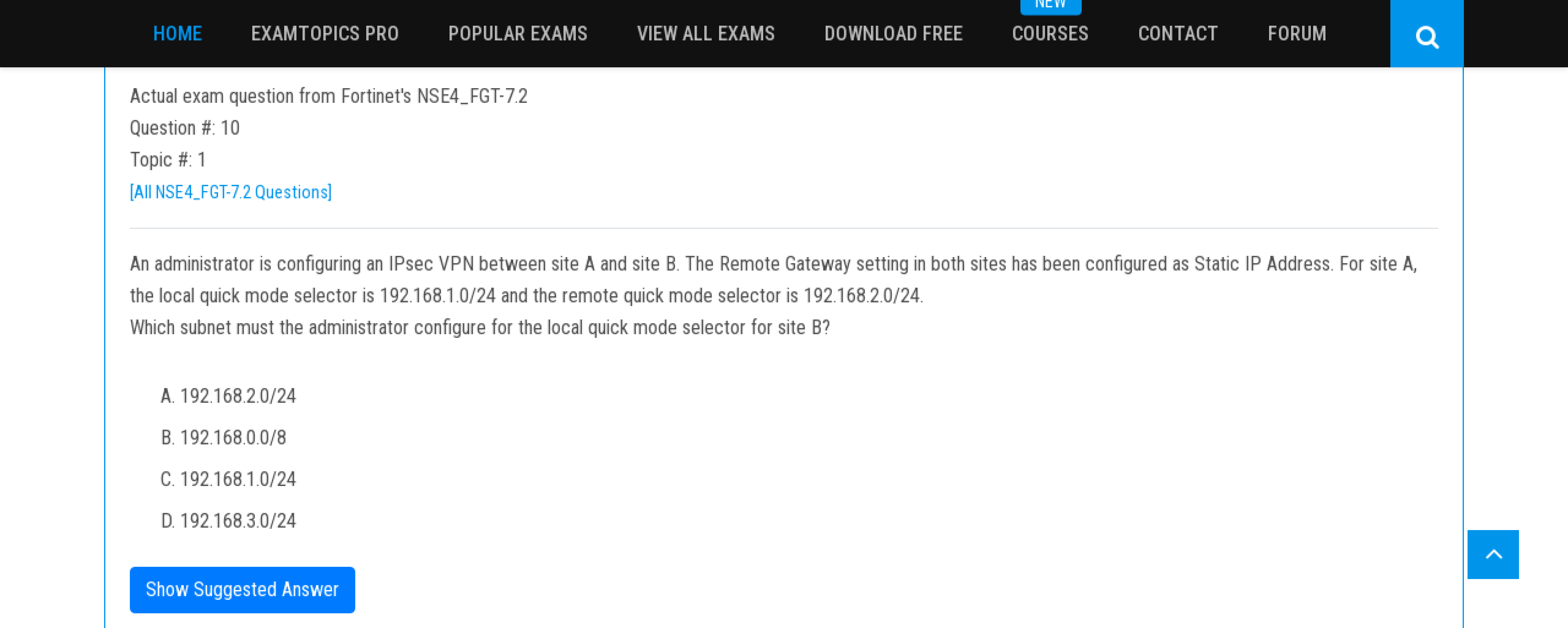
A. The debug flow is for ICMP traffic.

B. The default route is required to receive a reply.

C. Anew traffic session was created.

D. A firewall policy allowed the connection.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 10
Topic #: 1
[All NSE4_FGT-7.2 Questions]

An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.168.1.0/24 and the remote quick mode selector is 192.168.2.0/24.
Which subnet must the administrator configure for the local quick mode selector for site B?

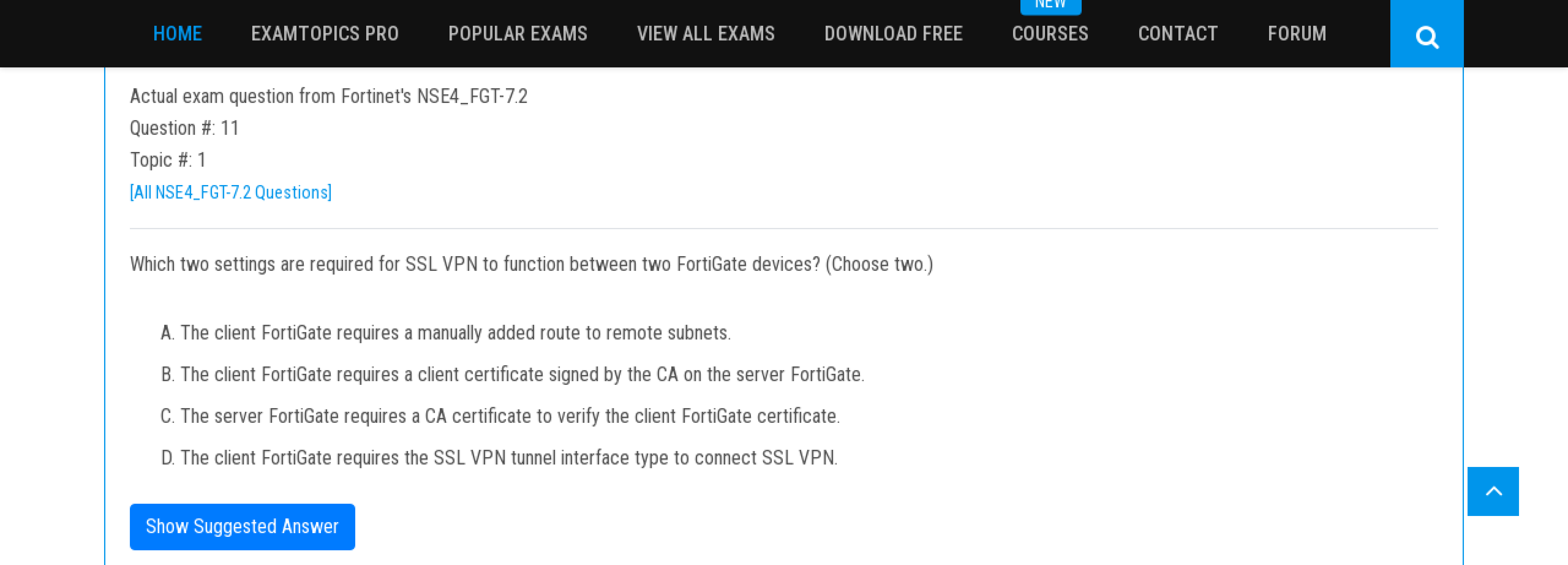
A. 192.168.2.0/24

B. 192.168.0.0/8

C. 192.168.1.0/24

D. 192.168.3.0/24

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 11

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

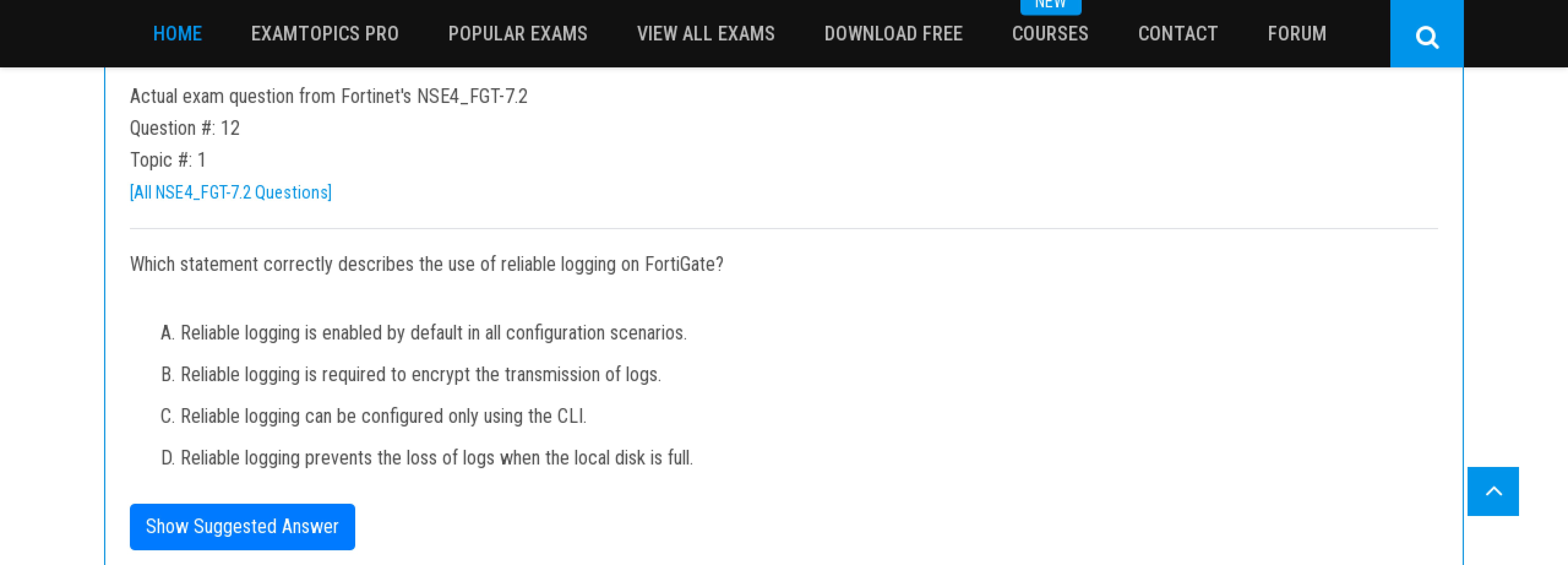
A. The client FortiGate requires a manually added route to remote subnets.

B. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.

C. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.

D. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 12

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Which statement correctly describes the use of reliable logging on FortiGate?

A. Reliable logging is enabled by default in all configuration scenarios.

B. Reliable logging is required to encrypt the transmission of logs.

C. Reliable logging can be configured only using the CLI.

D. Reliable logging prevents the loss of logs when the local disk is full.

Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 13

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibits.

The exhibits contain a network diagram, and virtual IP, IP pool, and firewall policies configuration information.

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.

The first firewall policy has NAT enabled using IP pool.

The second firewall policy is configured with a VIP as the destination address.

Exhibit A Exhibit B

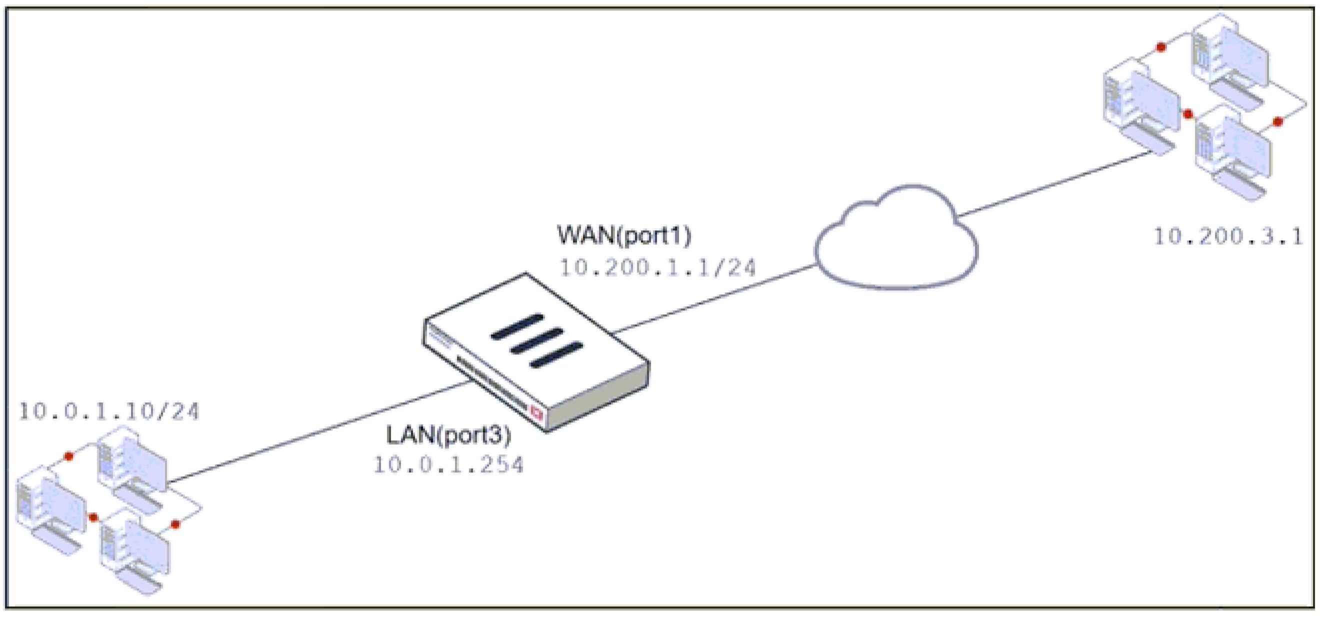
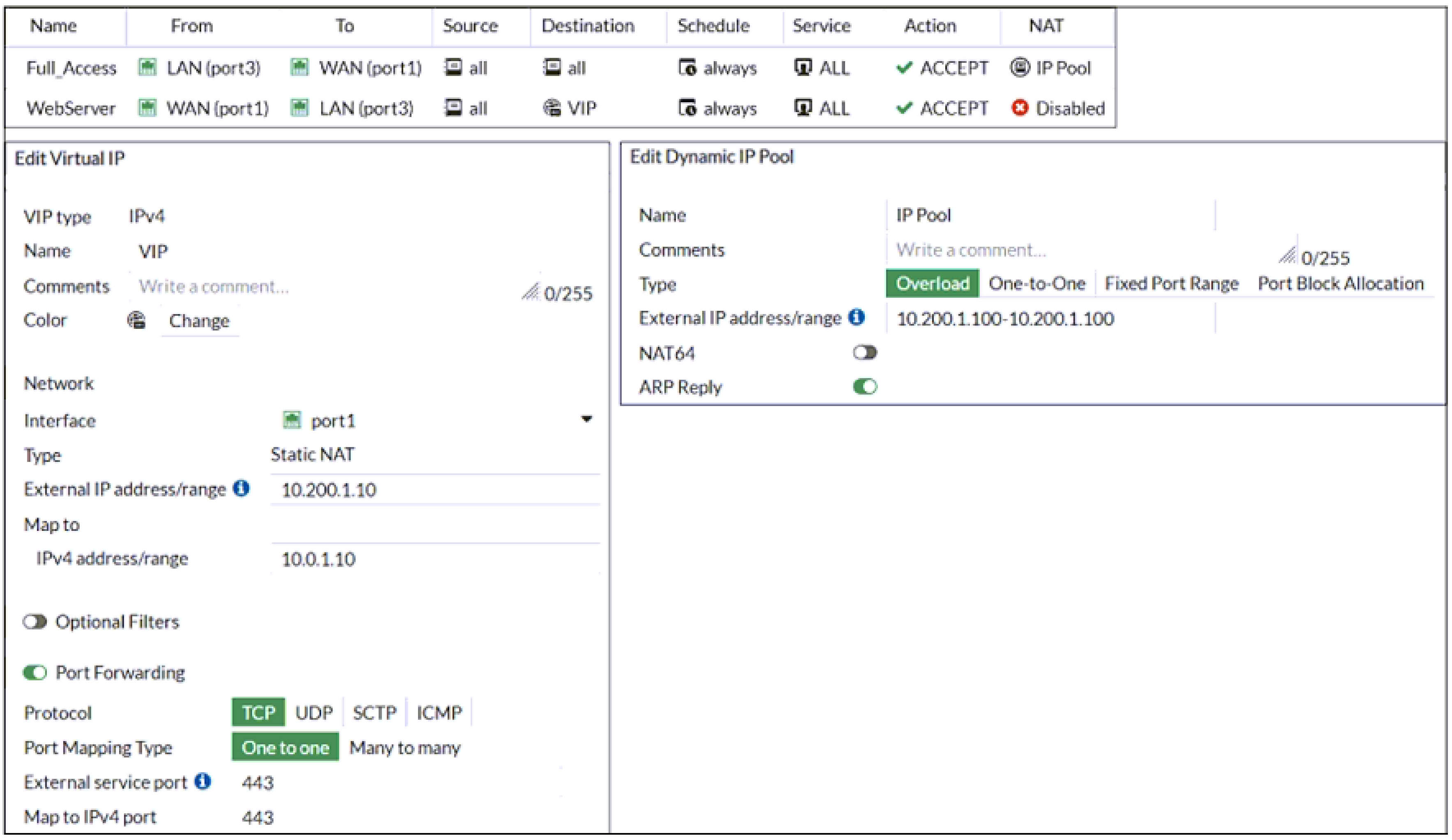


Exhibit A Exhibit B



Name	From	To	Source	Destination	Schedule	Service	Action	NAT
Full_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	✓ ACCEPT	IP Pool
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	✓ ACCEPT	Disabled

Edit Virtual IP

VIP type IPv4

Name VIP

Comments Write a comment... 0/255

Color Change

Network

Interface port1

Type Static NAT

External IP address/range 10.200.1.10

Map to

IPv4 address/range 10.0.1.10

Optional Filters

Port Forwarding

Protocol TCP UDP SCTP ICMP

Port Mapping Type One to one Many to many

External service port 443

Map to IPv4 port 443

Edit Dynamic IP Pool

Name IP Pool

Comments Write a comment... 0/255

Type Overload One-to-One Fixed Port Range Port Block Allocation

External IP address/range 10.200.1.100-10.200.1.100

NAT64

ARP Reply

Which IP address will be used to source NAT (SNAT) the internet traffic coming from a workstation with the IP address 10.0.1.10?

A. 10.200.1.1

B. 10.0.1.254

C. 10.200.1.10

D. 10.200.1.100

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 14

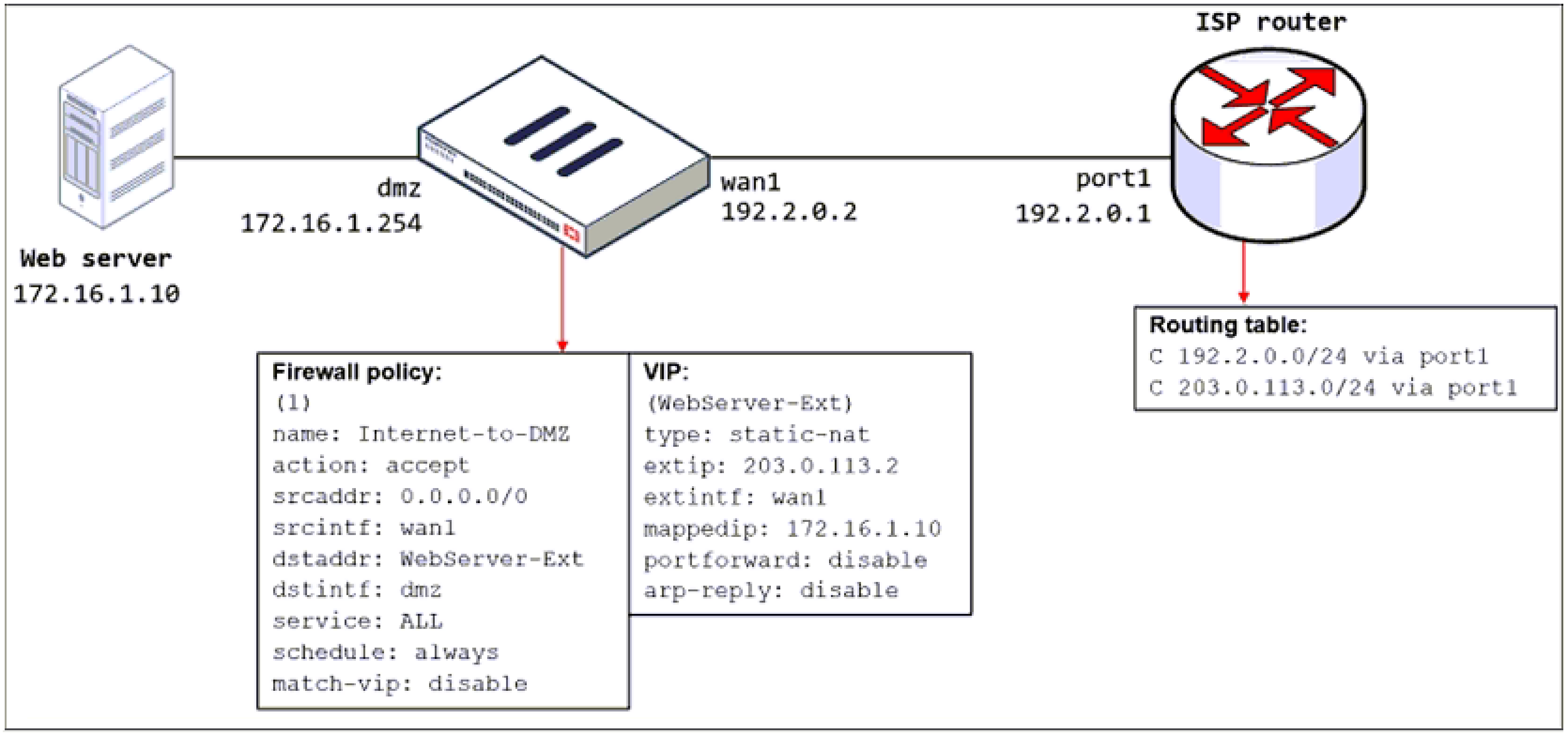
Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibit.

The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.

When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.



Routing table:
```
C 192.2.0.0/24 via port1
C 203.0.113.0/24 via port1
```

Firewall policy:
```
(1)
name: Internet-to-DMZ
action: accept
srcaddr: 0.0.0.0/0
srcintf: wan1
dstaddr: WebServer-Ext
dstintf: dmz
service: ALL
schedule: always
match-vip: disable
```

VIP:
```
(WebServer-Ext)
type: static-nat
extip: 203.0.113.2
extintf: wan1
mappedip: 172.16.1.10
portforward: disable
arp-reply: disable
```

Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

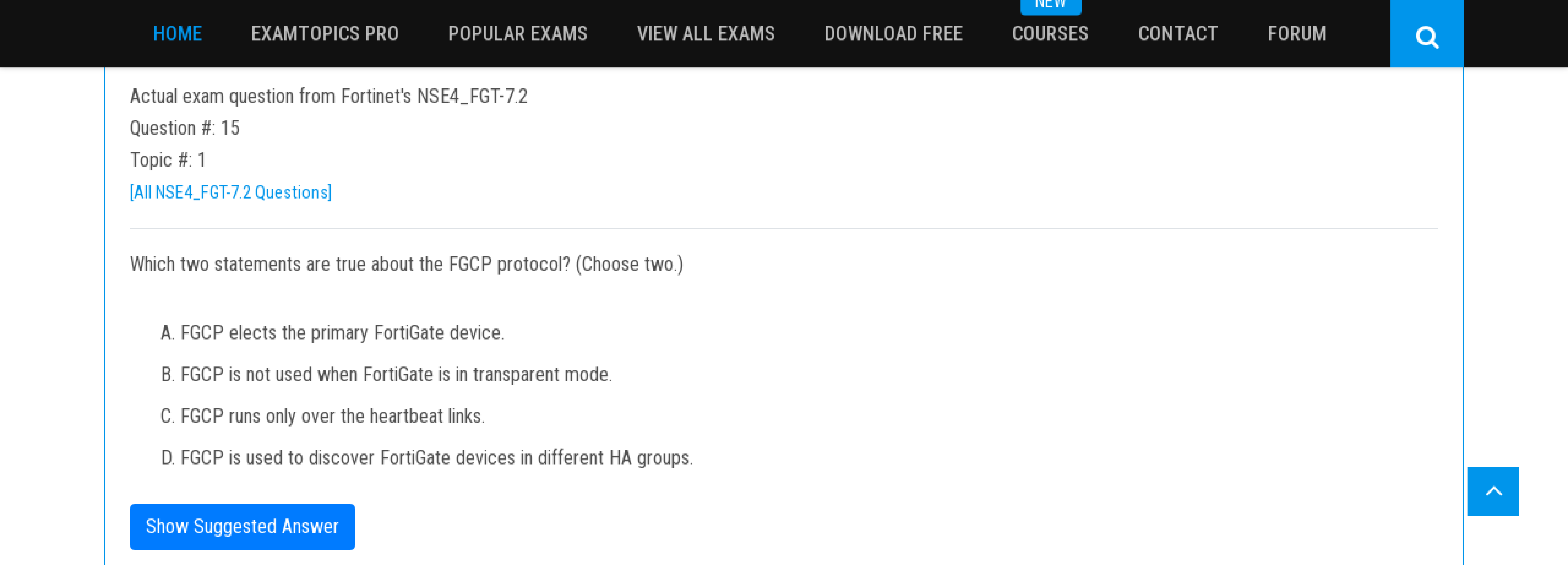
A. Configure a loopback interface with address 203.0.113.2/32.

B. In the VIP configuration, enable arp-reply.

C. Enable port forwarding on the server to map the external service port to the internal service port.

D. In the firewall policy configuration, enable match-vip.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 15

Topic #: 1

[All NSE4_FGT-7.2 Questions]

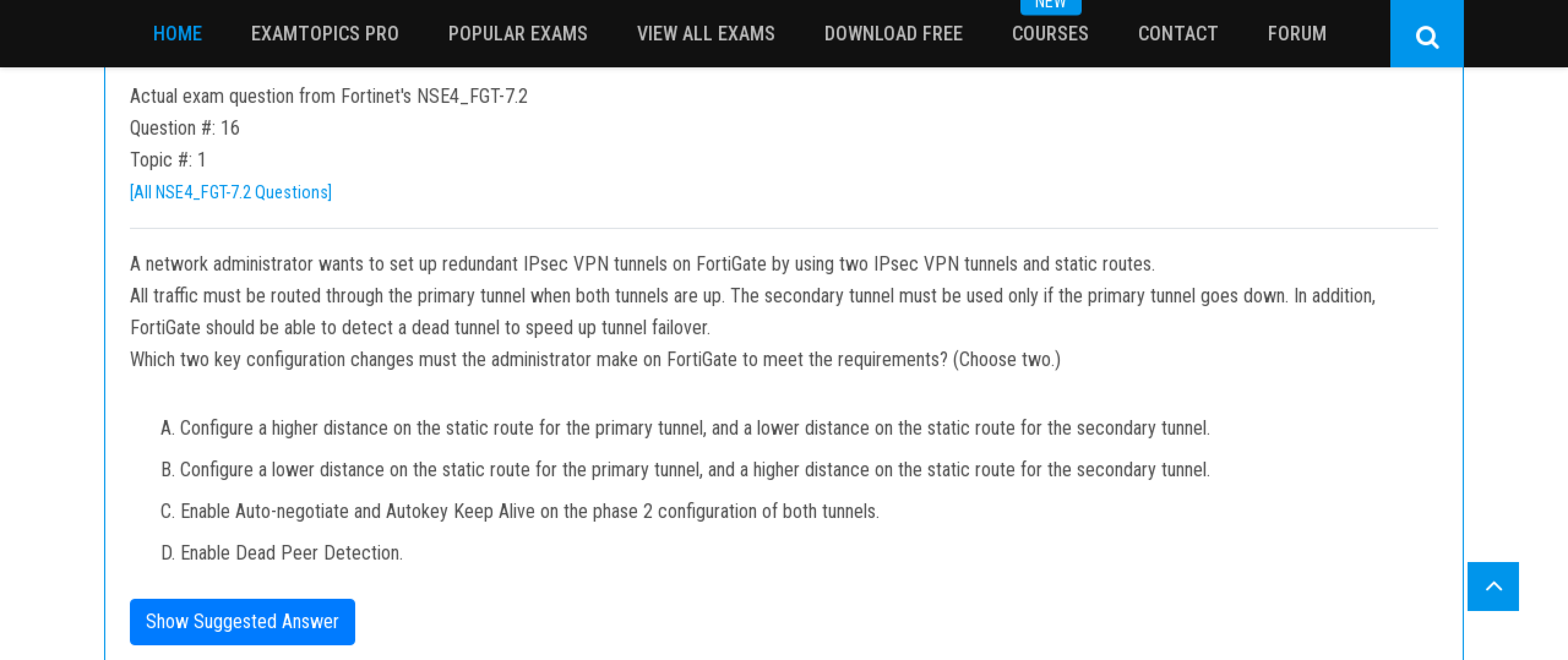
Which two statements are true about the FGCP protocol? (Choose two.)

A. FGCP elects the primary FortiGate device.

B. FGCP is not used when FortiGate is in transparent mode.

C. FGCP runs only over the heartbeat links.

D. FGCP is used to discover FortiGate devices in different HA groups.



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 16

Topic #: 1

[All NSE4_FGT-7.2 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.

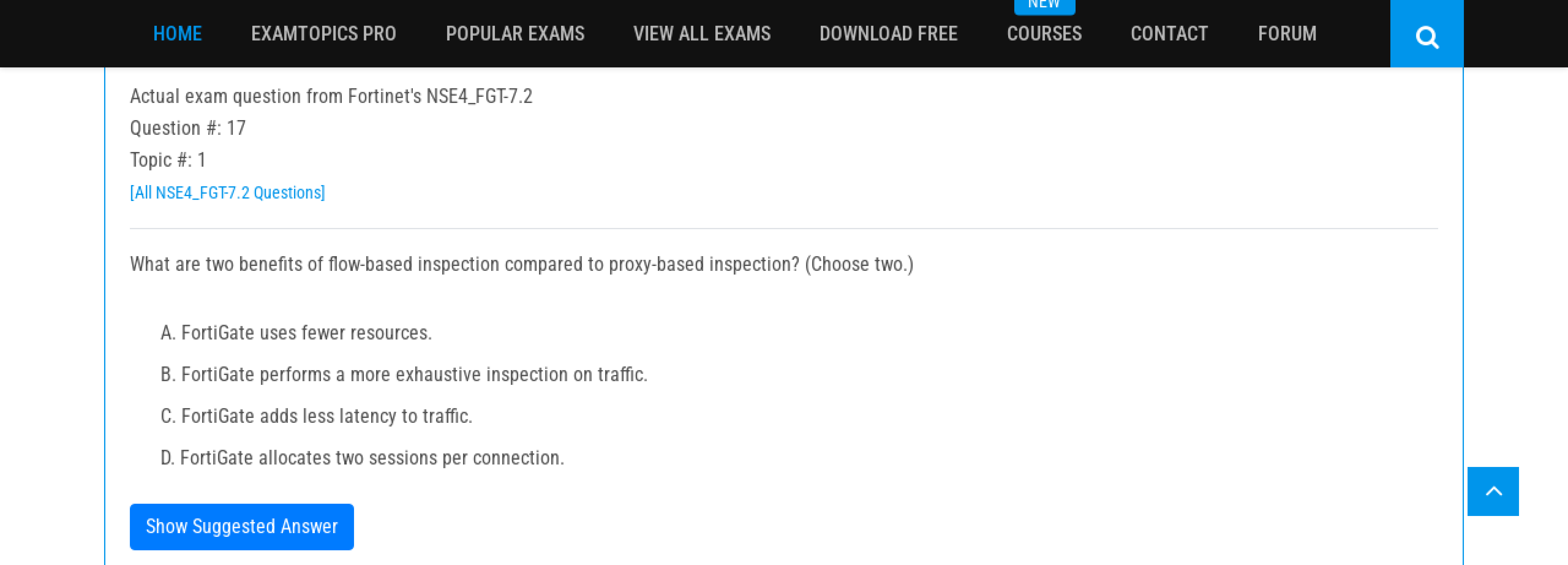
Which two key configuration changes must the administrator make on FortiGate to meet the requirements? (Choose two.)

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

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

D. Enable Dead Peer Detection.



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 17

Topic #: 1

[All NSE4_FGT-7.2 Questions]

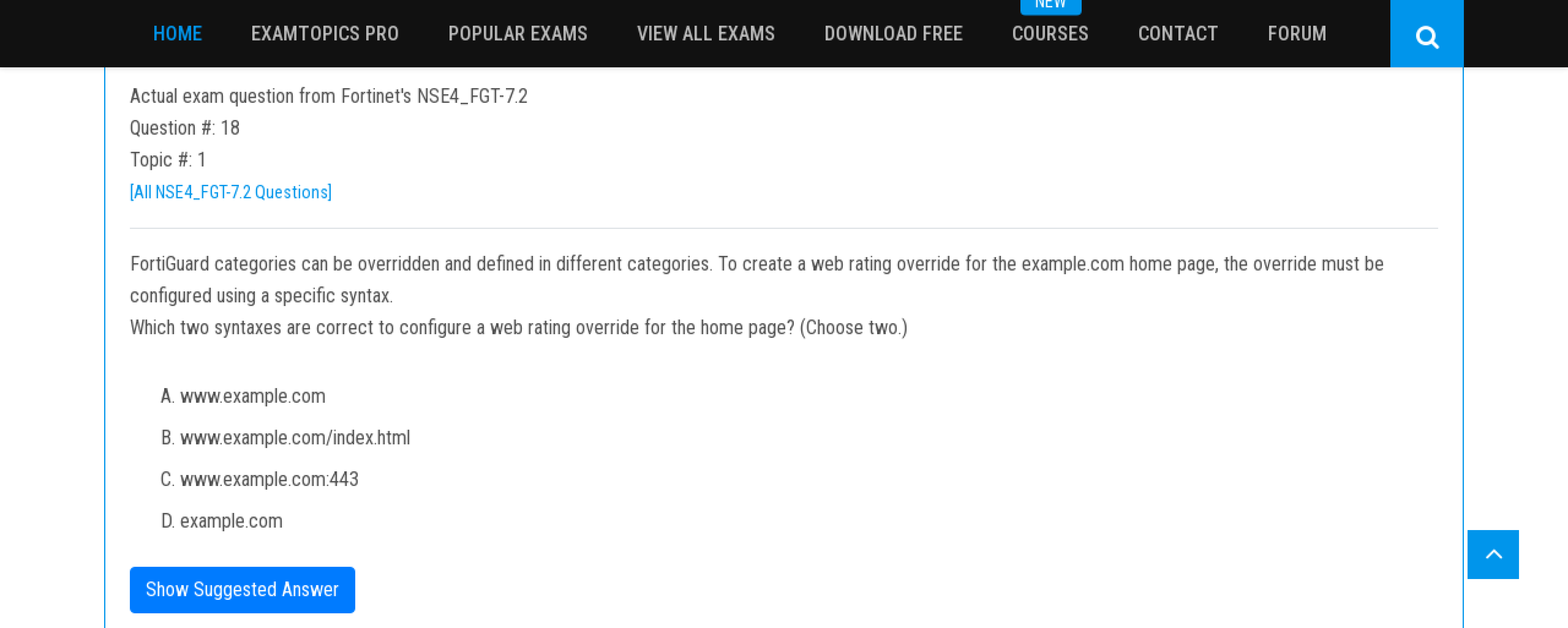
What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)

A. FortiGate uses fewer resources.

B. FortiGate performs a more exhaustive inspection on traffic.

C. FortiGate adds less latency to traffic.

D. FortiGate allocates two sessions per connection.



Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 18
Topic #: 1
[All NSE4_FGT-7.2 Questions]

FortiGuard categories can be overridden and defined in different categories. To create a web rating override for the example.com home page, the override must be configured using a specific syntax.

Which two syntaxes are correct to configure a web rating override for the home page? (Choose two.)

A. www.example.com

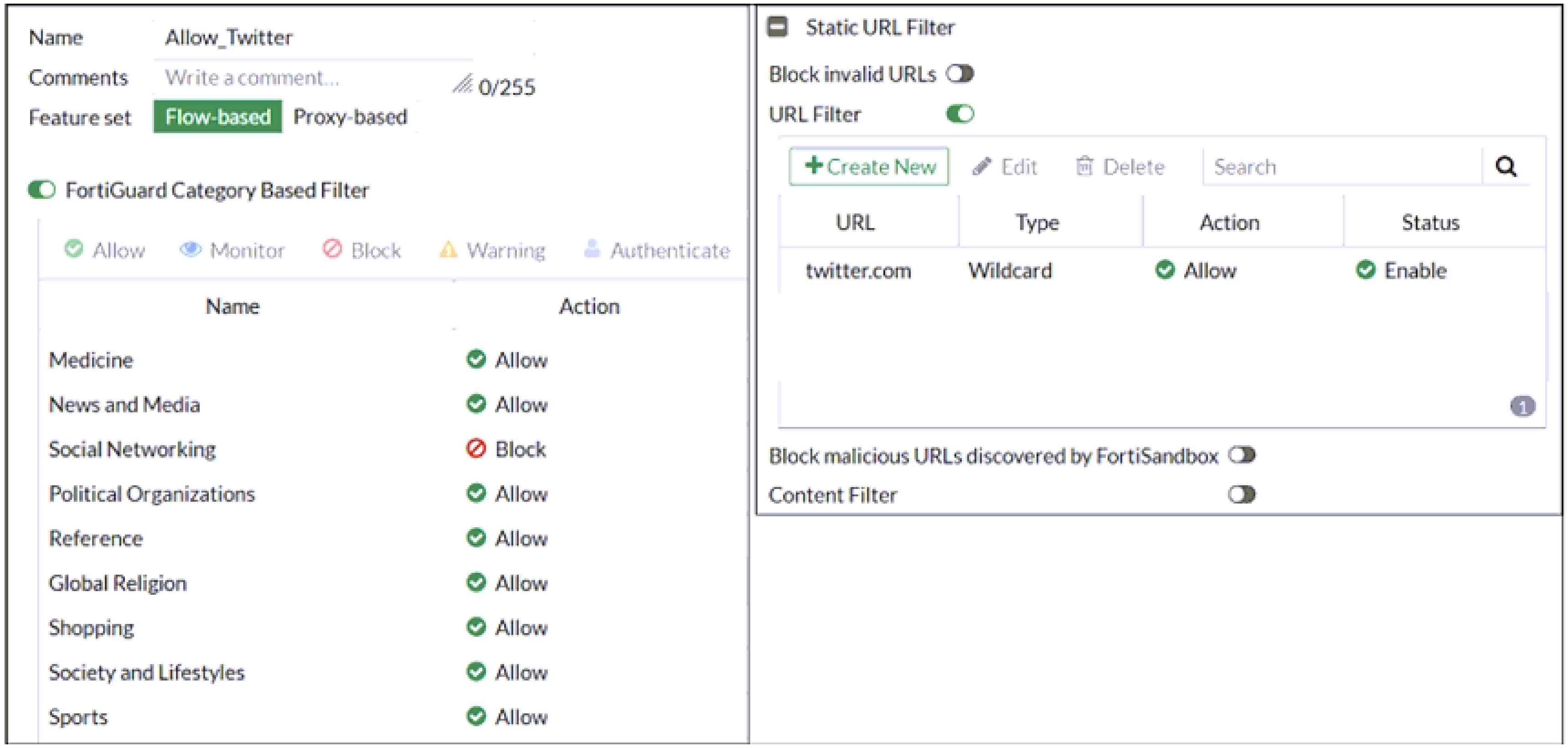
B. www.example.com/index.html

C. www.example.com:443

D. example.com

Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 19
Topic #: 1
[All NSE4_FGT-7.2 Questions]

Refer to exhibit.
An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.



Name: Allow_Twitter
Comments: Write a comment... 0/255
Feature set: Flow-based | Proxy-based

FortiGuard Category Based Filter

Name	Action
Medicine	✓ Allow
News and Media	✓ Allow
Social Networking	⊘ Block
Political Organizations	✓ Allow
Reference	✓ Allow
Global Religion	✓ Allow
Shopping	✓ Allow
Society and Lifestyles	✓ Allow
Sports	✓ Allow

Static URL Filter
Block invalid URLs ○
URL Filter ●

URL	Type	Action	Status
twitter.com	Wildcard	✓ Allow	✓ Enable

Block malicious URLs discovered by FortiSandbox ○
Content Filter ○

Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

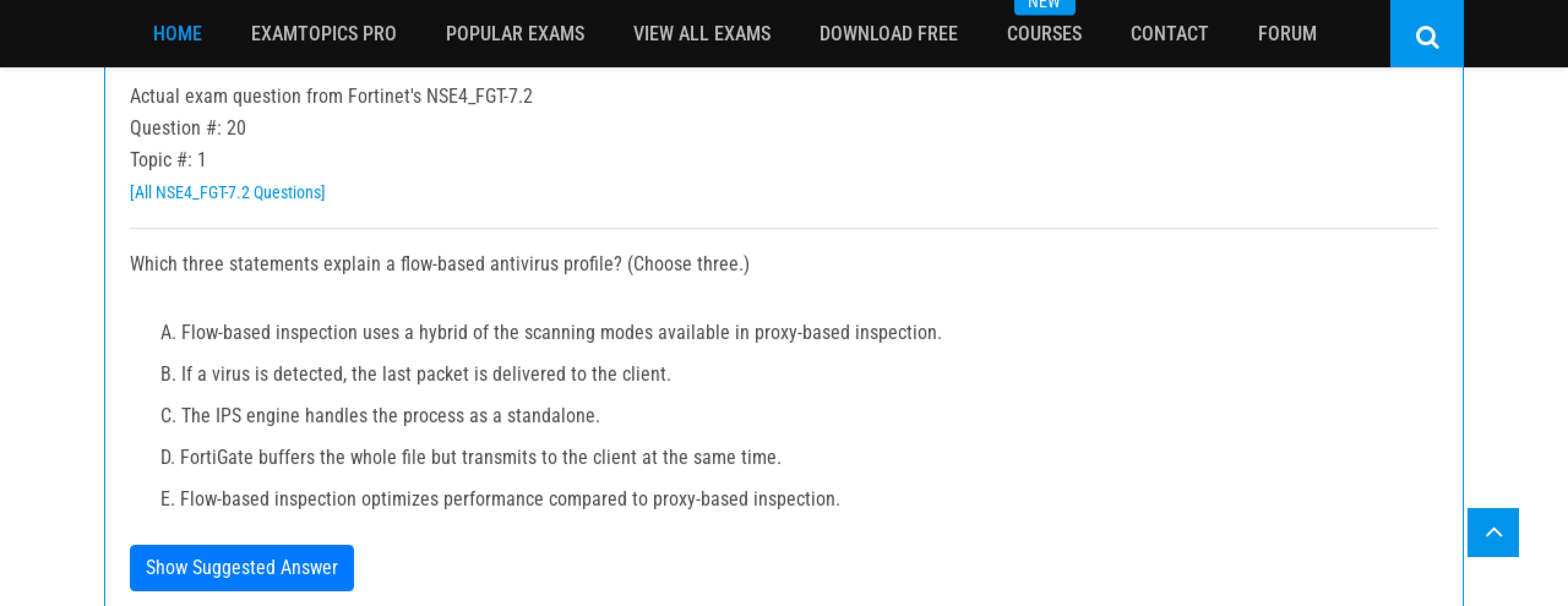
A. On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking.

B. On the Static URL Filter configuration, set Type to Simple.

C. On the Static URL Filter configuration, set Action to Exempt.

D. On the Static URL Filter configuration, set Action to Monitor.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 20

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Which three statements explain a flow-based antivirus profile? (Choose three.)

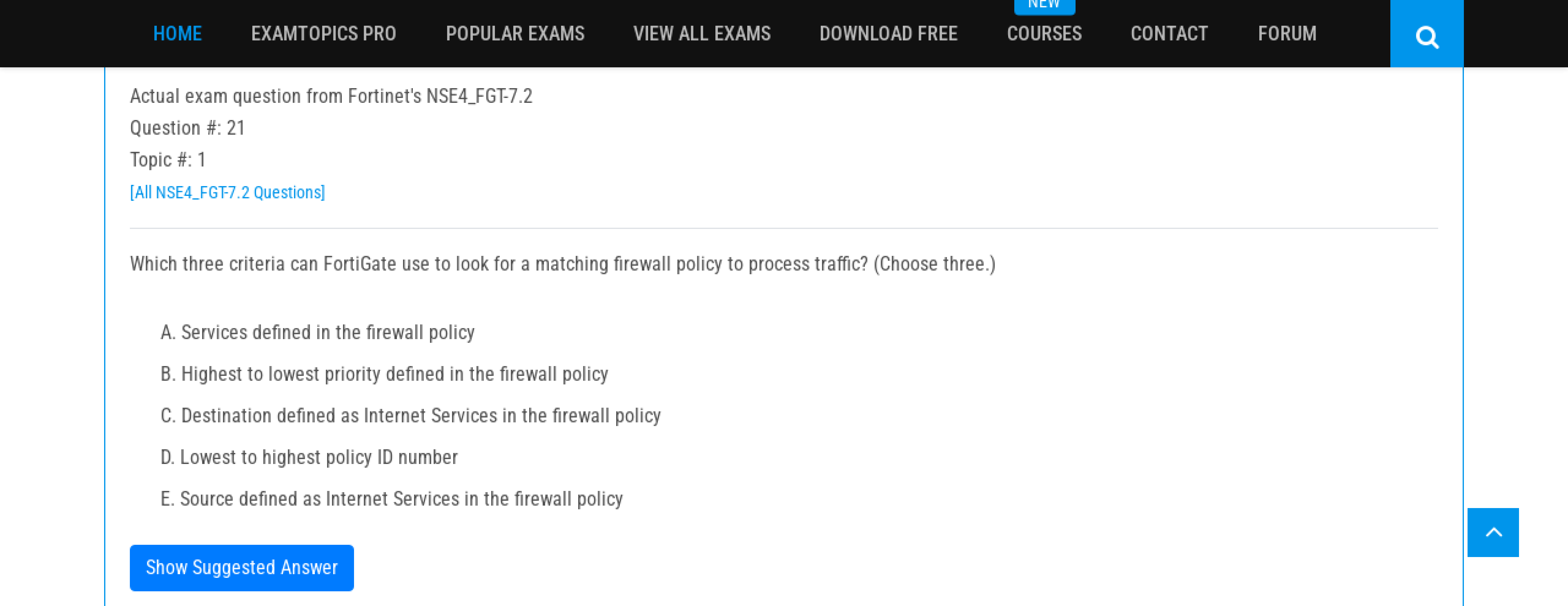
A. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.

B. If a virus is detected, the last packet is delivered to the client.

C. The IPS engine handles the process as a standalone.

D. FortiGate buffers the whole file but transmits to the client at the same time.

E. Flow-based inspection optimizes performance compared to proxy-based inspection.



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 21

Topic #: 1

[All NSE4_FGT-7.2 Questions]

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

A. Services defined in the firewall policy

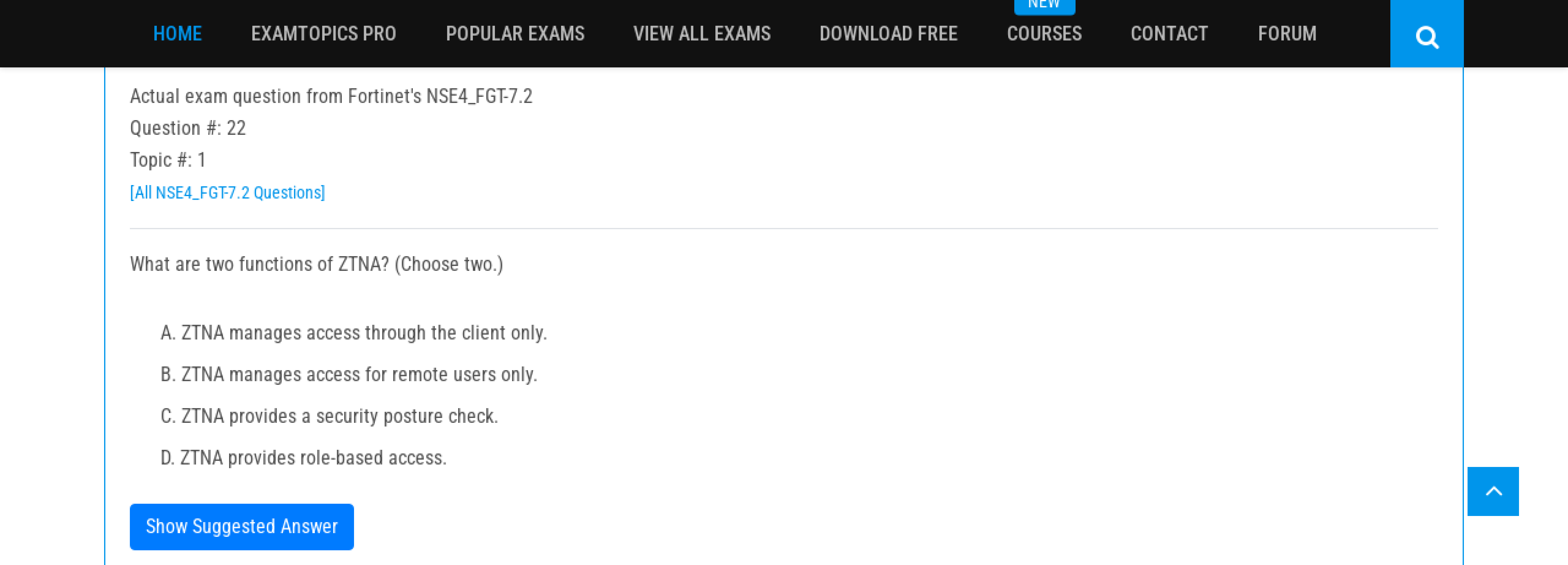
B. Highest to lowest priority defined in the firewall policy

C. Destination defined as Internet Services in the firewall policy

D. Lowest to highest policy ID number

E. Source defined as Internet Services in the firewall policy

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 22

Topic #: 1

[All NSE4_FGT-7.2 Questions]

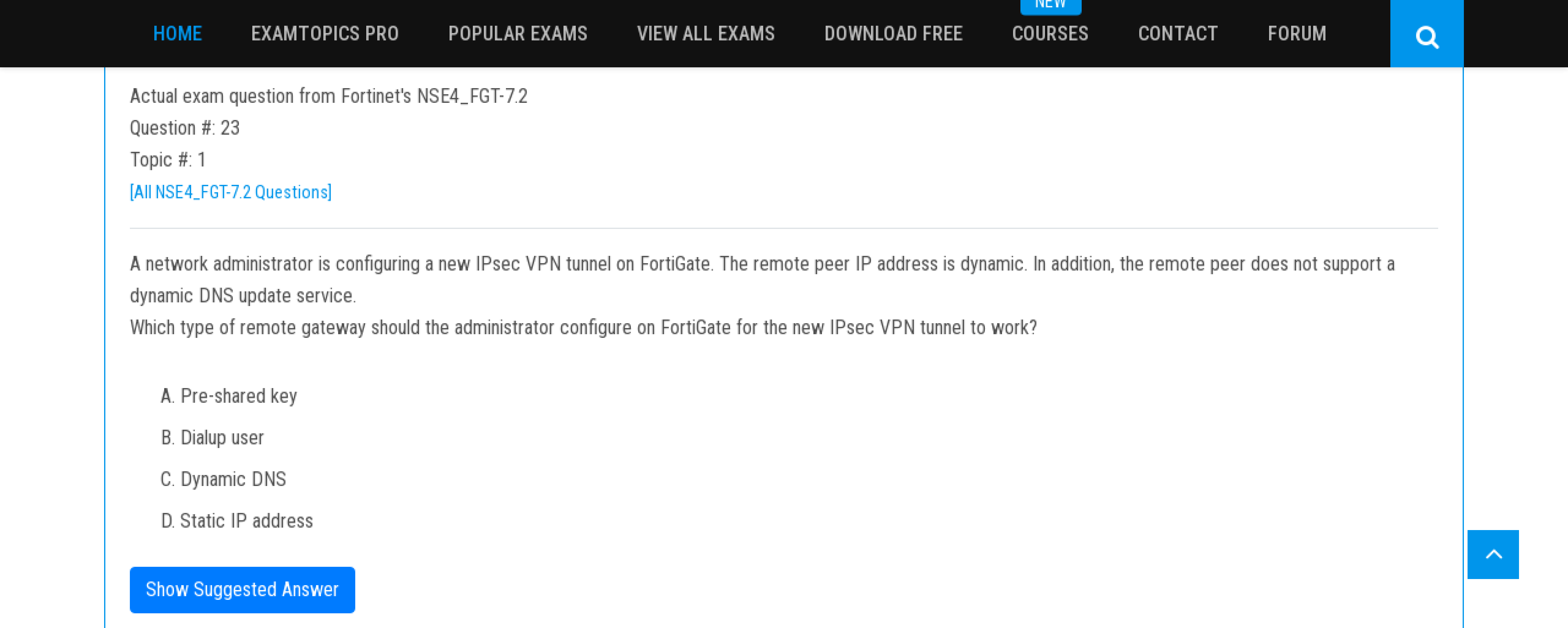
What are two functions of ZTNA? (Choose two.)

A. ZTNA manages access through the client only.

B. ZTNA manages access for remote users only.

C. ZTNA provides a security posture check.

D. ZTNA provides role-based access.



Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 23
Topic #: 1

[All NSE4_FGT-7.2 Questions]

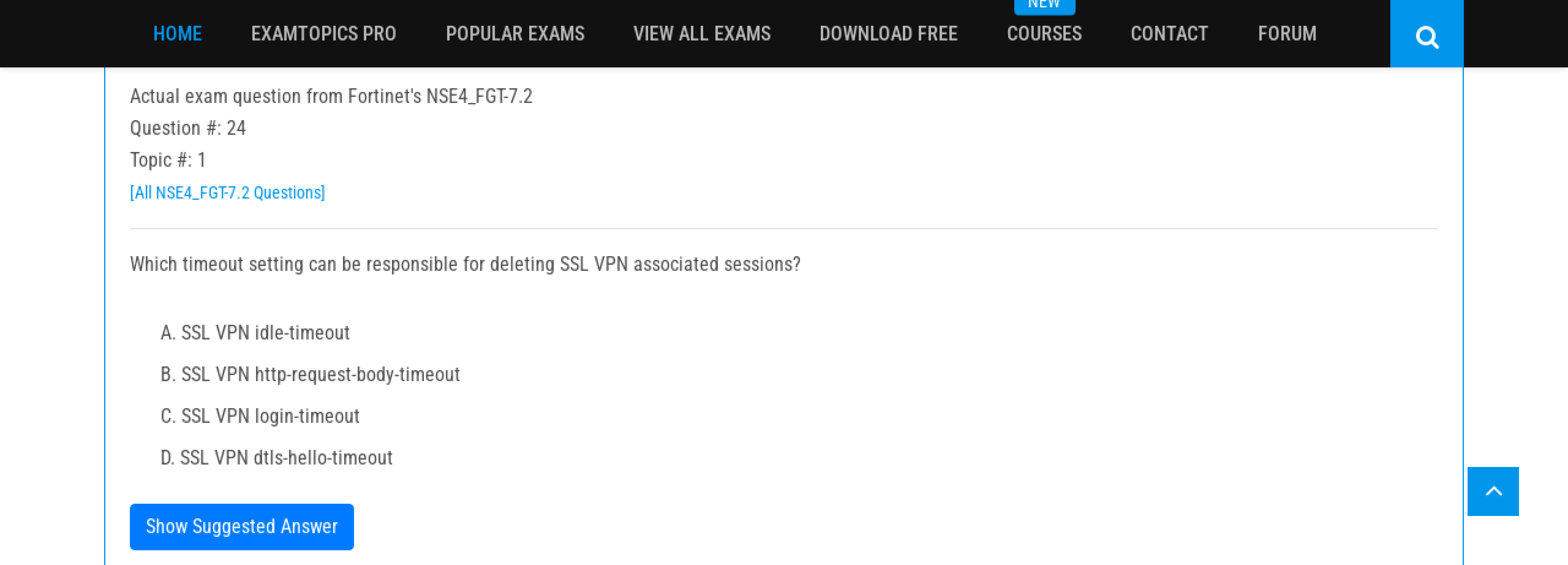
A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.
Which type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

A. Pre-shared key

B. Dialup user

C. Dynamic DNS

D. Static IP address



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 24

Topic #: 1

[All NSE4_FGT-7.2 Questions]

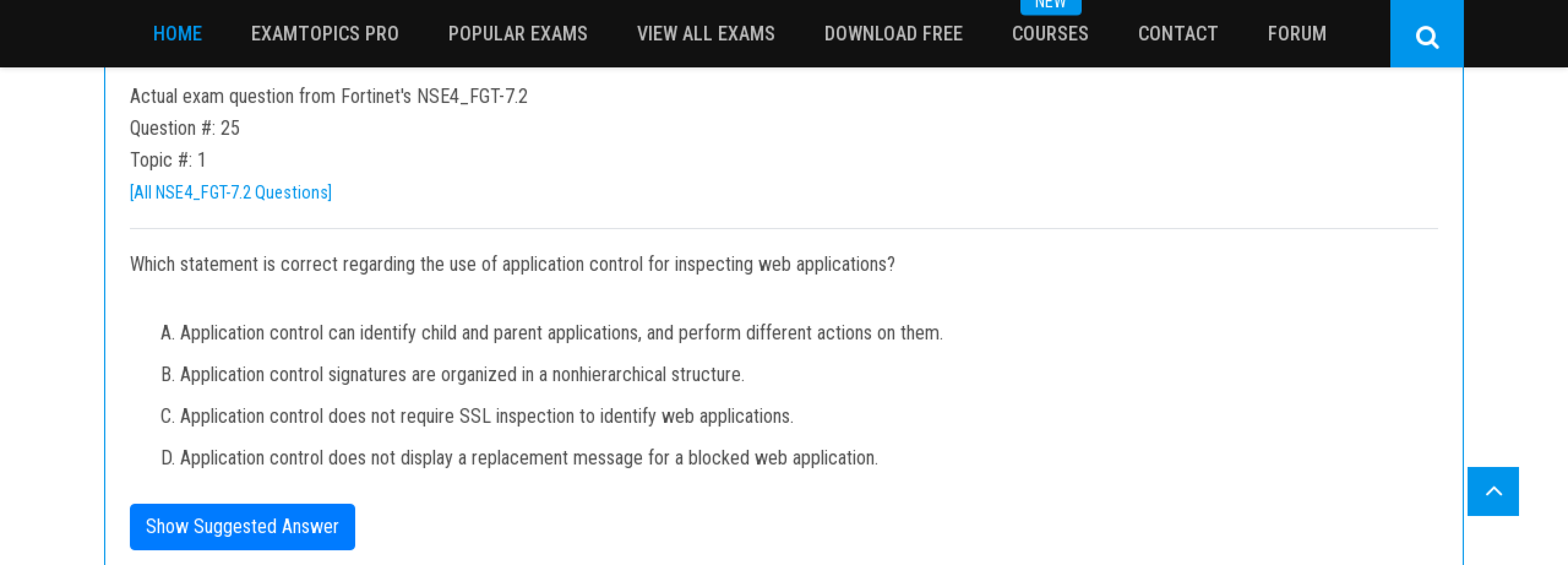
Which timeout setting can be responsible for deleting SSL VPN associated sessions?

A. SSL VPN idle-timeout

B. SSL VPN http-request-body-timeout

C. SSL VPN login-timeout

D. SSL VPN dtls-hello-timeout



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 25

Topic #: 1

[All NSE4_FGT-7.2 Questions]

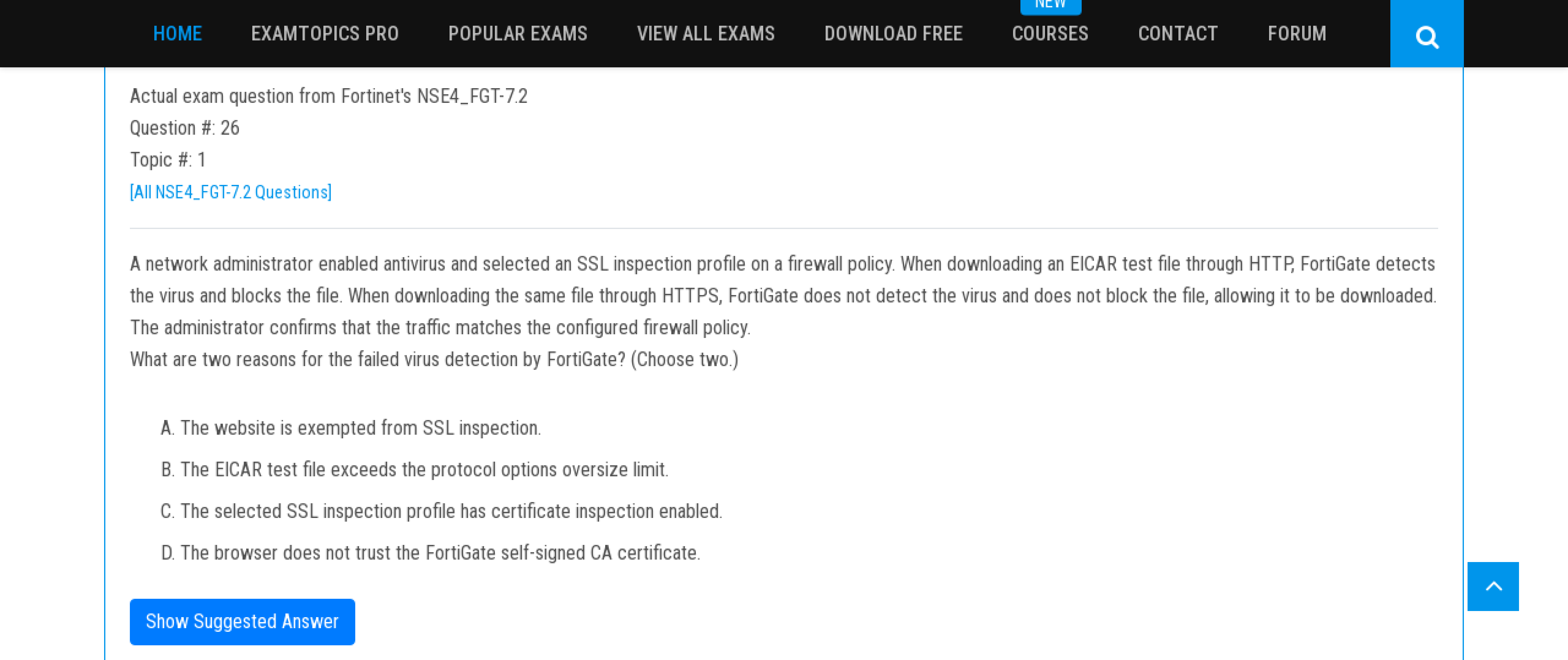
Which statement is correct regarding the use of application control for inspecting web applications?

A. Application control can identify child and parent applications, and perform different actions on them.

B. Application control signatures are organized in a nonhierarchical structure.

C. Application control does not require SSL inspection to identify web applications.

D. Application control does not display a replacement message for a blocked web application.



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 26

Topic #: 1

[All NSE4_FGT-7.2 Questions]

A network administrator enabled antivirus and selected an SSL inspection profile on a firewall policy. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and does not block the file, allowing it to be downloaded.

The administrator confirms that the traffic matches the configured firewall policy.

What are two reasons for the failed virus detection by FortiGate? (Choose two.)

A. The website is exempted from SSL inspection.

B. The EICAR test file exceeds the protocol options oversize limit.

C. The selected SSL inspection profile has certificate inspection enabled.

D. The browser does not trust the FortiGate self-signed CA certificate.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

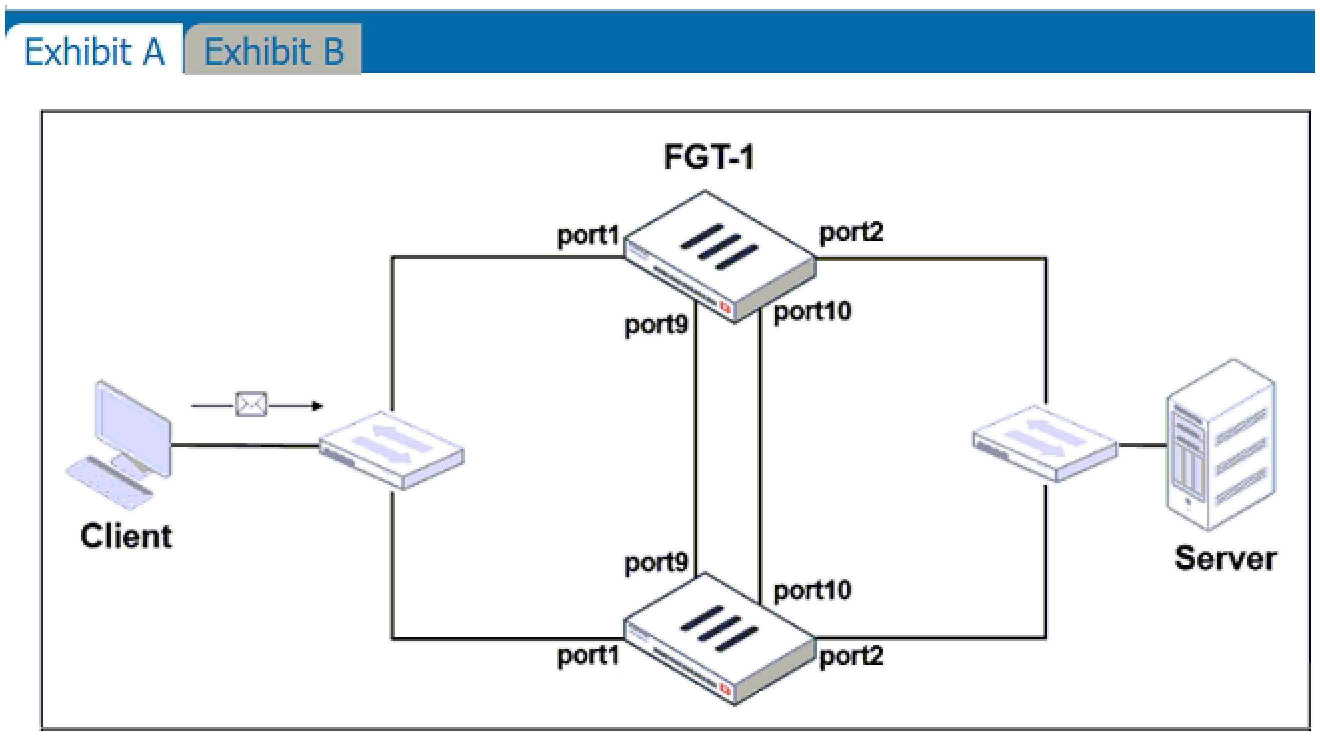
Question #: 27

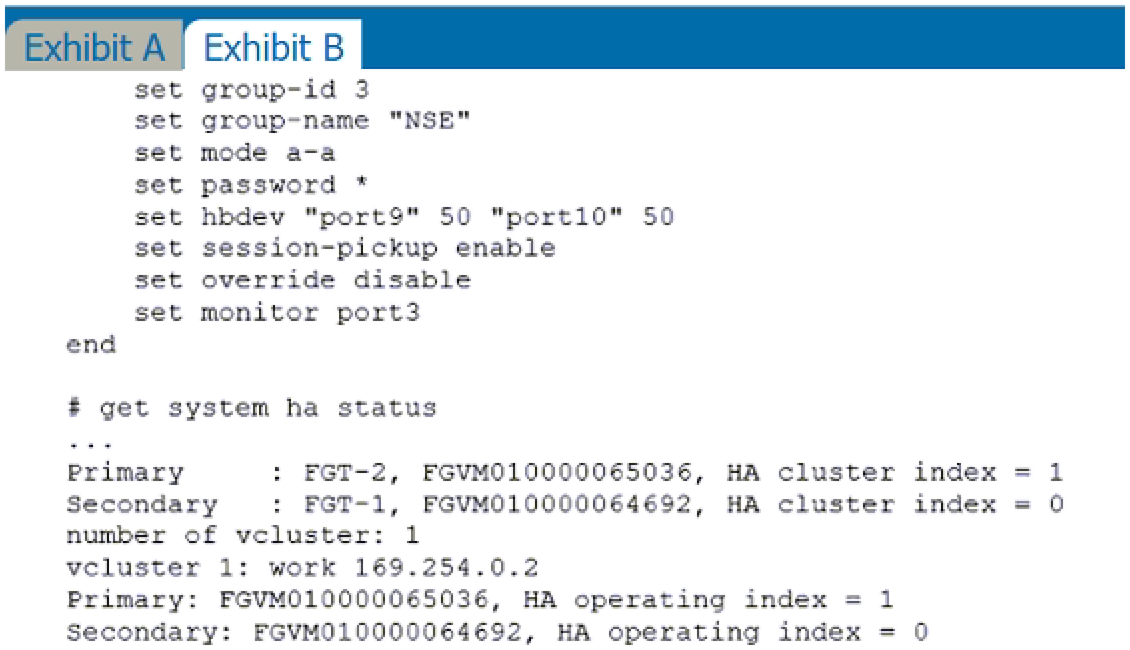
Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibits.

Exhibit A shows a topology for a FortiGate HA cluster that performs proxy-based inspection on traffic. Exhibit B shows the HA configuration and the partial output of the get system ha status command.





```
        set group-id 3
        set group-name "NSE"
        set mode a-a
        set password *
        set hbdev "port9" 50 "port10" 50
        set session-pickup enable
        set override disable
        set monitor port3
    end

    # get system ha status
    ...
    Primary     : FGT-2, FGVM010000065036, HA cluster index = 1
    Secondary   : FGT-1, FGVM010000064692, HA cluster index = 0
    number of vcluster: 1
    vcluster 1: work 169.254.0.2
    Primary: FGVM010000065036, HA operating index = 1
    Secondary: FGVM010000064692, HA operating index = 0
```

Based on the exhibits, which two statements about the traffic passing through the cluster are true? (Choose two.)

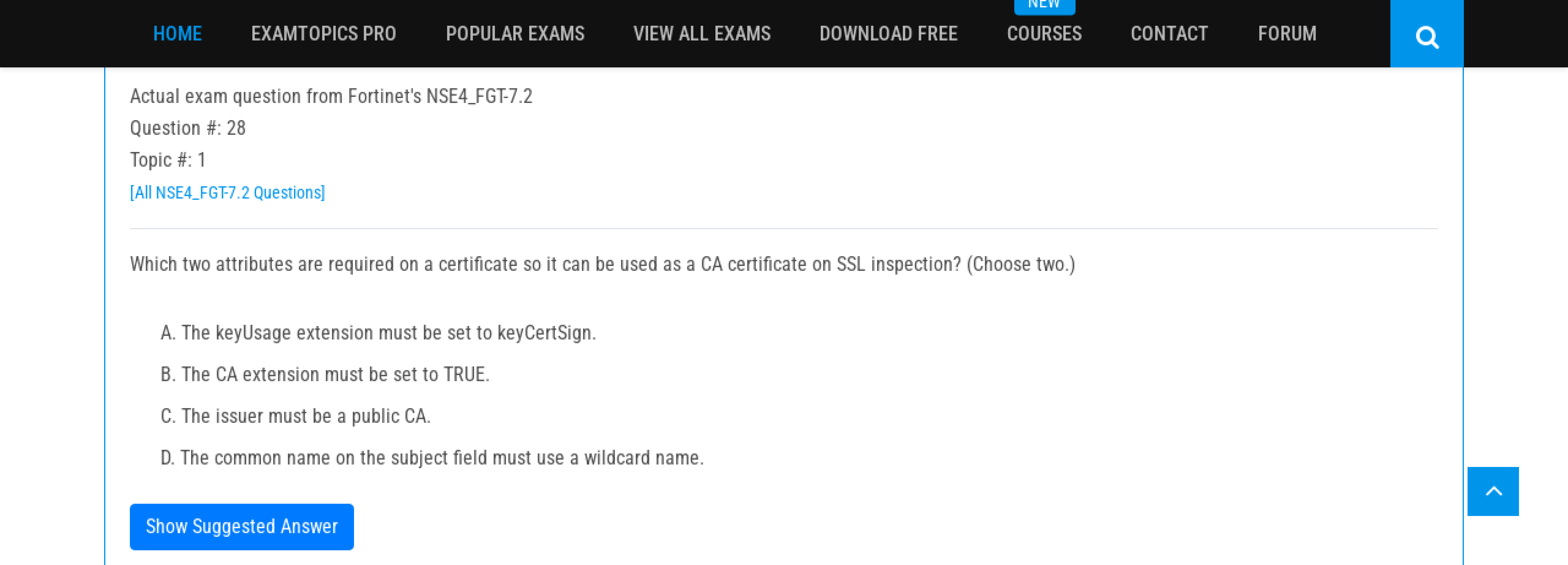
A. For non-load balanced connections, packets forwarded by the cluster to the server contain the virtual MAC address of port2 as source.

B. The traffic sourced from the client and destined to the server is sent to FGT-1.

C. The cluster can load balance ICMP connections to the secondary.

D. For load balanced connections, the primary encapsulates TCP SYN packets before forwarding them to the secondary.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 28

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Which two attributes are required on a certificate so it can be used as a CA certificate on SSL inspection? (Choose two.)

A. The keyUsage extension must be set to keyCertSign.

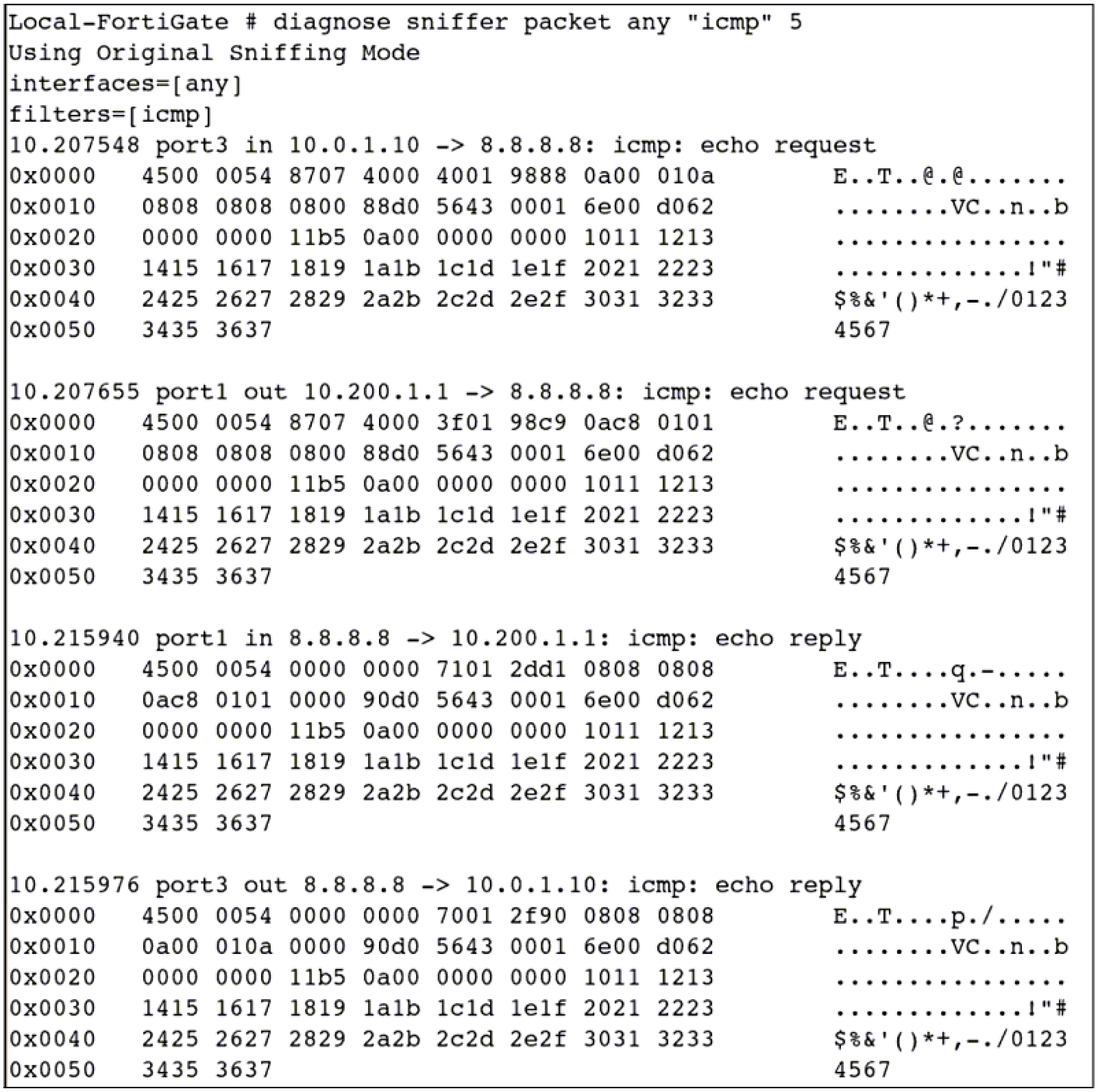
B. The CA extension must be set to TRUE.

C. The issuer must be a public CA.

D. The common name on the subject field must use a wildcard name.

Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 29
Topic #: 1
[All NSE4_FGT-7.2 Questions]

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



```
Local-FortiGate # diagnose sniffer packet any "icmp" 5
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
10.207548 port3 in 10.0.1.10 -> 8.8.8.8: icmp: echo request
0x0000   4500 0054 8707 4000 4001 9888 0a00 010a        E..T..@.@.......
0x0010   0808 0808 0800 88d0 5643 0001 6e00 d062        ........VC..n..b
0x0020   0000 0000 11b5 0a00 0000 0000 1011 1213        ................
0x0030   1415 1617 1819 1a1b 1c1d 1e1f 2021 2223        .............!"#
0x0040   2425 2627 2829 2a2b 2c2d 2e2f 3031 3233        $%&'()*+,-./0123
0x0050   3435 3637                                      4567

10.207655 port1 out 10.200.1.1 -> 8.8.8.8: icmp: echo request
0x0000   4500 0054 8707 4000 3f01 98c9 0ac8 0101        E..T..@.?.......
0x0010   0808 0808 0800 88d0 5643 0001 6e00 d062        ........VC..n..b
0x0020   0000 0000 11b5 0a00 0000 0000 1011 1213        ................
0x0030   1415 1617 1819 1a1b 1c1d 1e1f 2021 2223        .............!"#
0x0040   2425 2627 2829 2a2b 2c2d 2e2f 3031 3233        $%&'()*+,-./0123
0x0050   3435 3637                                      4567

10.215940 port1 in 8.8.8.8 -> 10.200.1.1: icmp: echo reply
0x0000   4500 0054 0000 0000 7101 2dd1 0808 0808        E..T....q.-.....
0x0010   0ac8 0101 0000 90d0 5643 0001 6e00 d062        ........VC..n..b
0x0020   0000 0000 11b5 0a00 0000 0000 1011 1213        ................
0x0030   1415 1617 1819 1a1b 1c1d 1e1f 2021 2223        .............!"#
0x0040   2425 2627 2829 2a2b 2c2d 2e2f 3031 3233        $%&'()*+,-./0123
0x0050   3435 3637                                      4567

10.215976 port3 out 8.8.8.8 -> 10.0.1.10: icmp: echo reply
0x0000   4500 0054 0000 0000 7001 2f90 0808 0808        E..T....p./.....
0x0010   0a00 010a 0000 90d0 5643 0001 6e00 d062        ........VC..n..b
0x0020   0000 0000 11b5 0a00 0000 0000 1011 1213        ................
0x0030   1415 1617 1819 1a1b 1c1d 1e1f 2021 2223        .............!"#
0x0040   2425 2627 2829 2a2b 2c2d 2e2f 3031 3233        $%&'()*+,-./0123
0x0050   3435 3637                                      4567
```

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

A. Packet payload

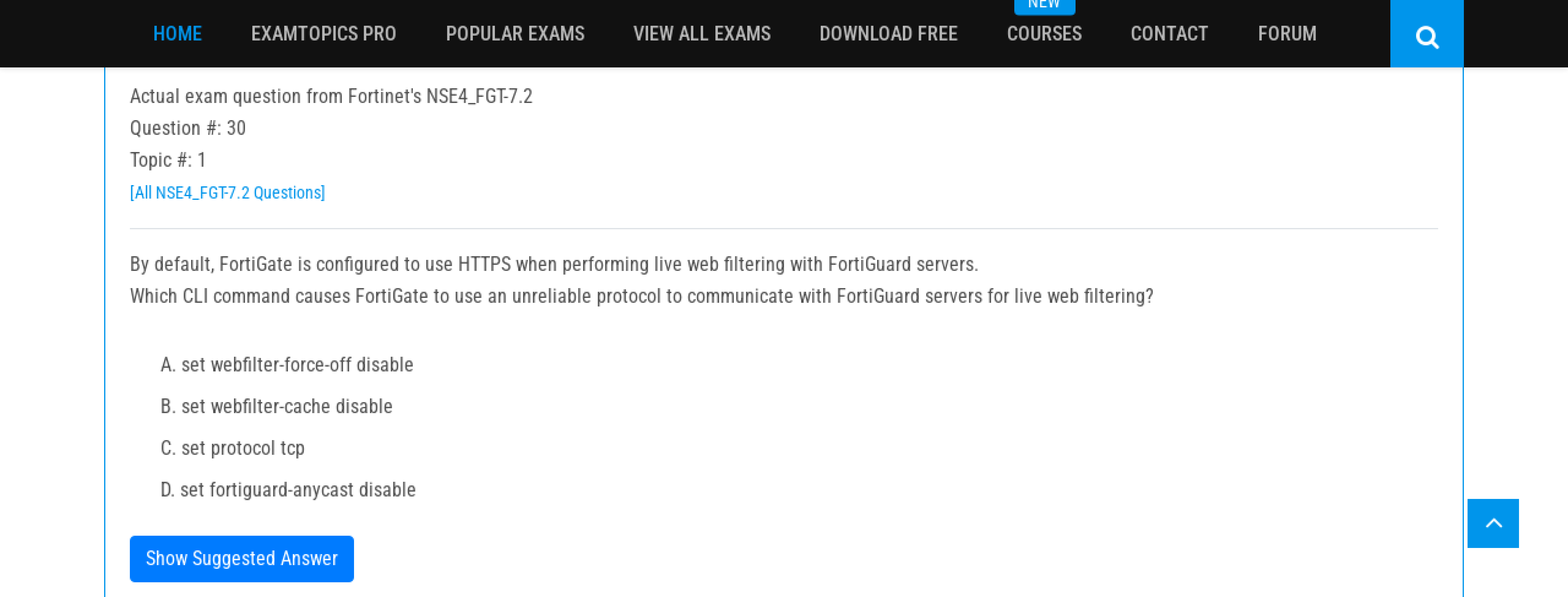
B. Application header

C. IP header

D. Ethernet header

E. Interface name

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 30

Topic #: 1

[All NSE4_FGT-7.2 Questions]

By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers.

Which CLI command causes FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering?

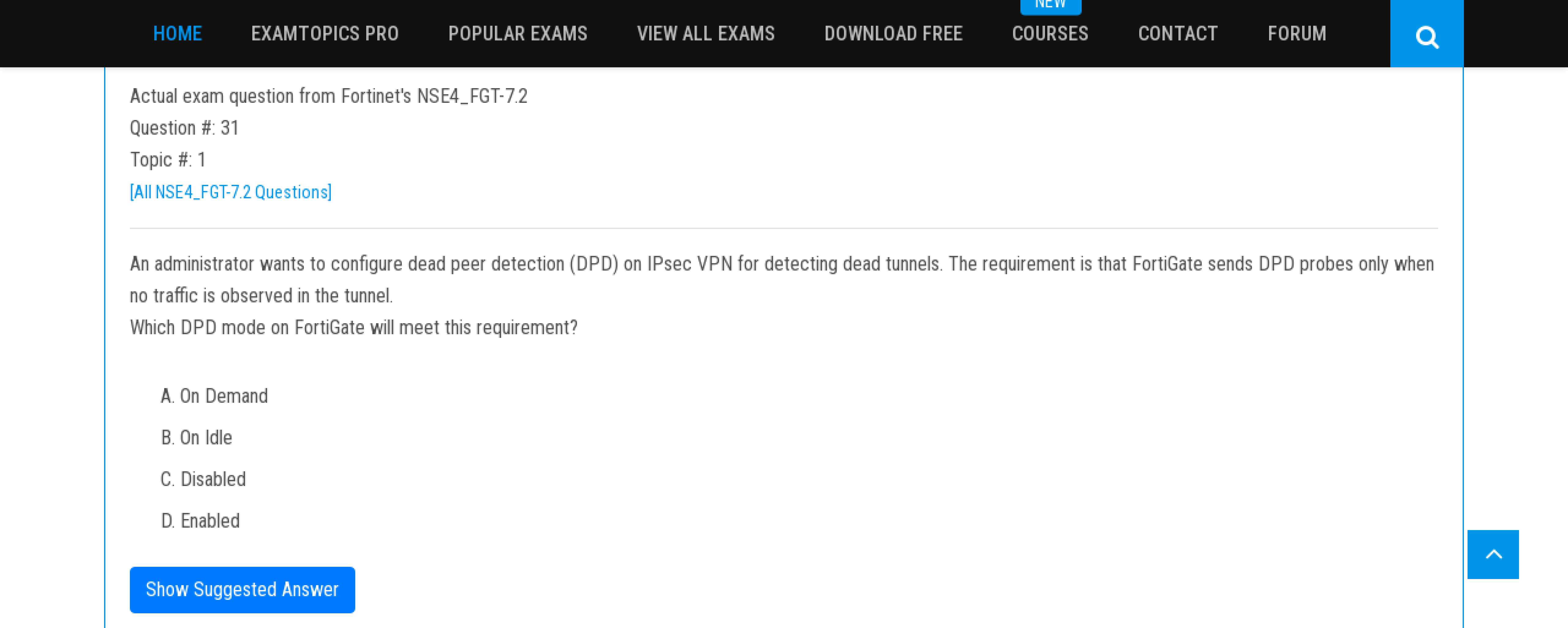
A. set webfilter-force-off disable

B. set webfilter-cache disable

C. set protocol tcp

D. set fortiguard-anycast disable

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 31
Topic #: 1
[All NSE4_FGT-7.2 Questions]

An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.
Which DPD mode on FortiGate will meet this requirement?

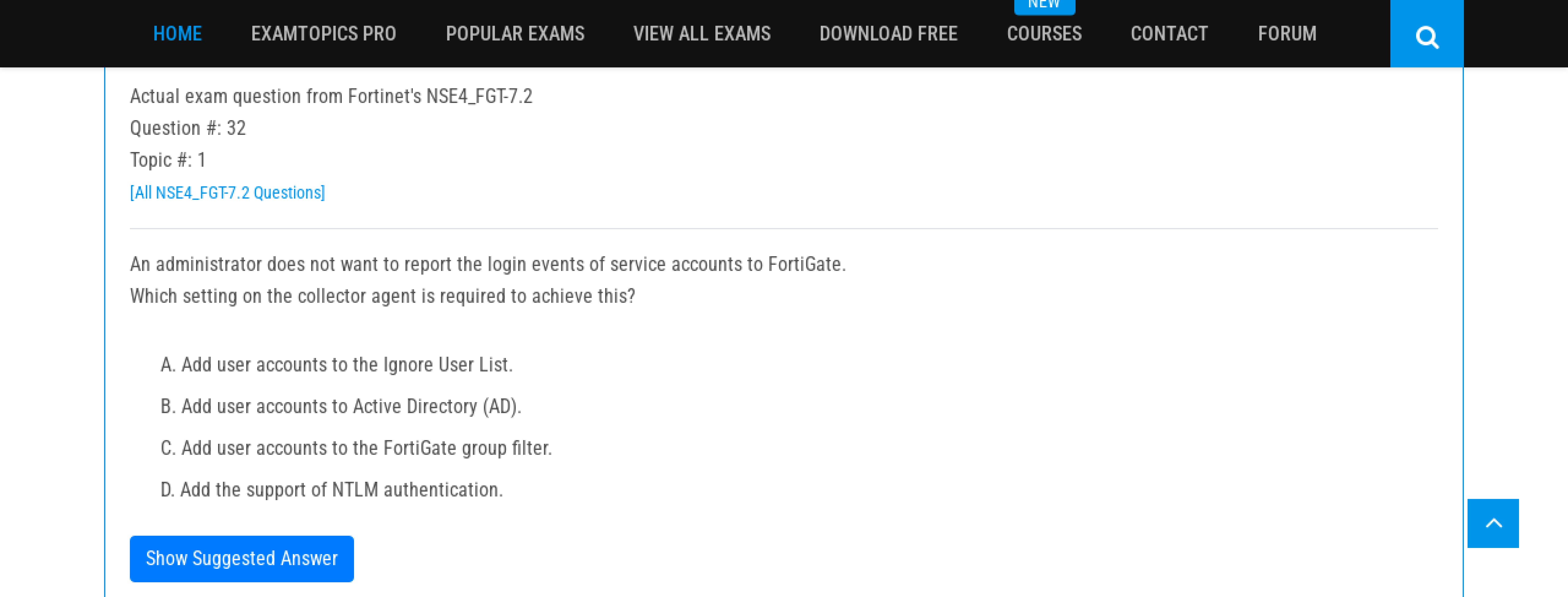
A. On Demand

B. On Idle

C. Disabled

D. Enabled

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 32
Topic #: 1
[All NSE4_FGT-7.2 Questions]

An administrator does not want to report the login events of service accounts to FortiGate.
Which setting on the collector agent is required to achieve this?

A. Add user accounts to the Ignore User List.

B. Add user accounts to Active Directory (AD).

C. Add user accounts to the FortiGate group filter.

D. Add the support of NTLM authentication.

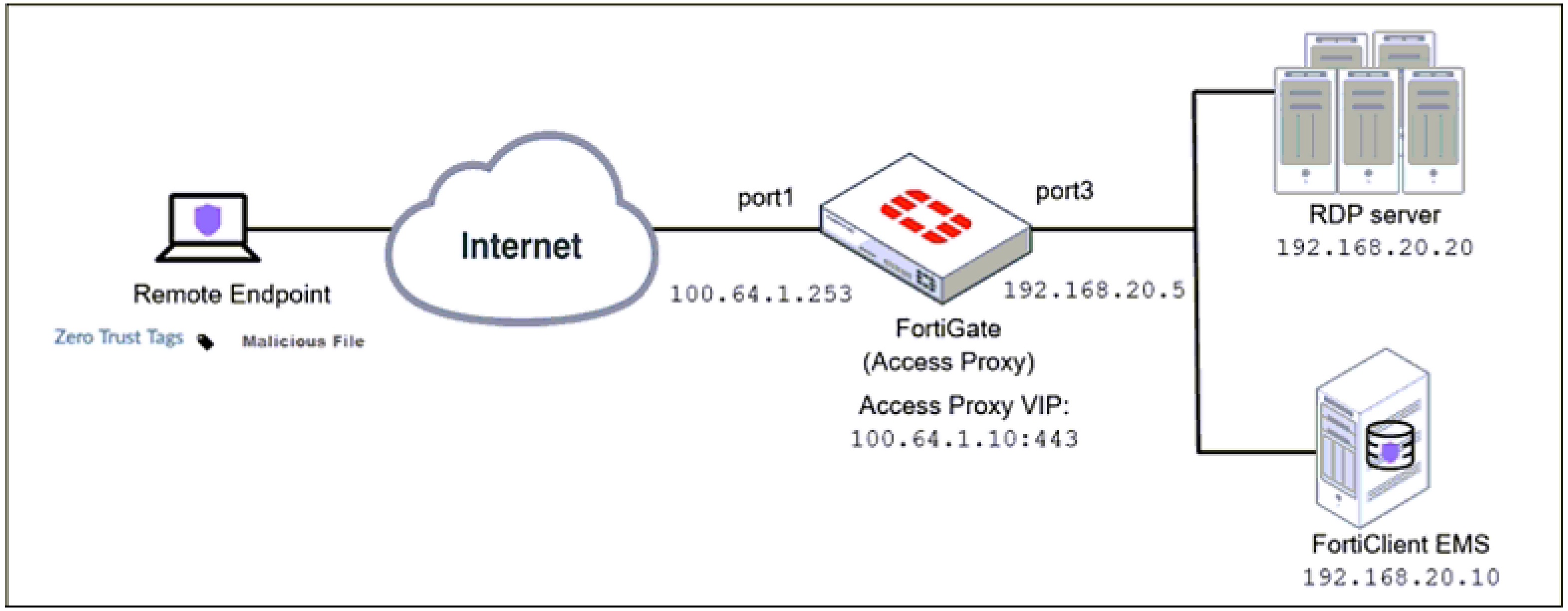
Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 33

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibit.



Based on the ZTNA tag, the security posture of the remote endpoint has changed.

What will happen to endpoint active ZTNA sessions?

A. They will be re-evaluated to match the endpoint policy.

B. They will be re-evaluated to match the firewall policy.

C. They will be re-evaluated to match the ZTNA policy.

D. They will be re-evaluated to match the security policy.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

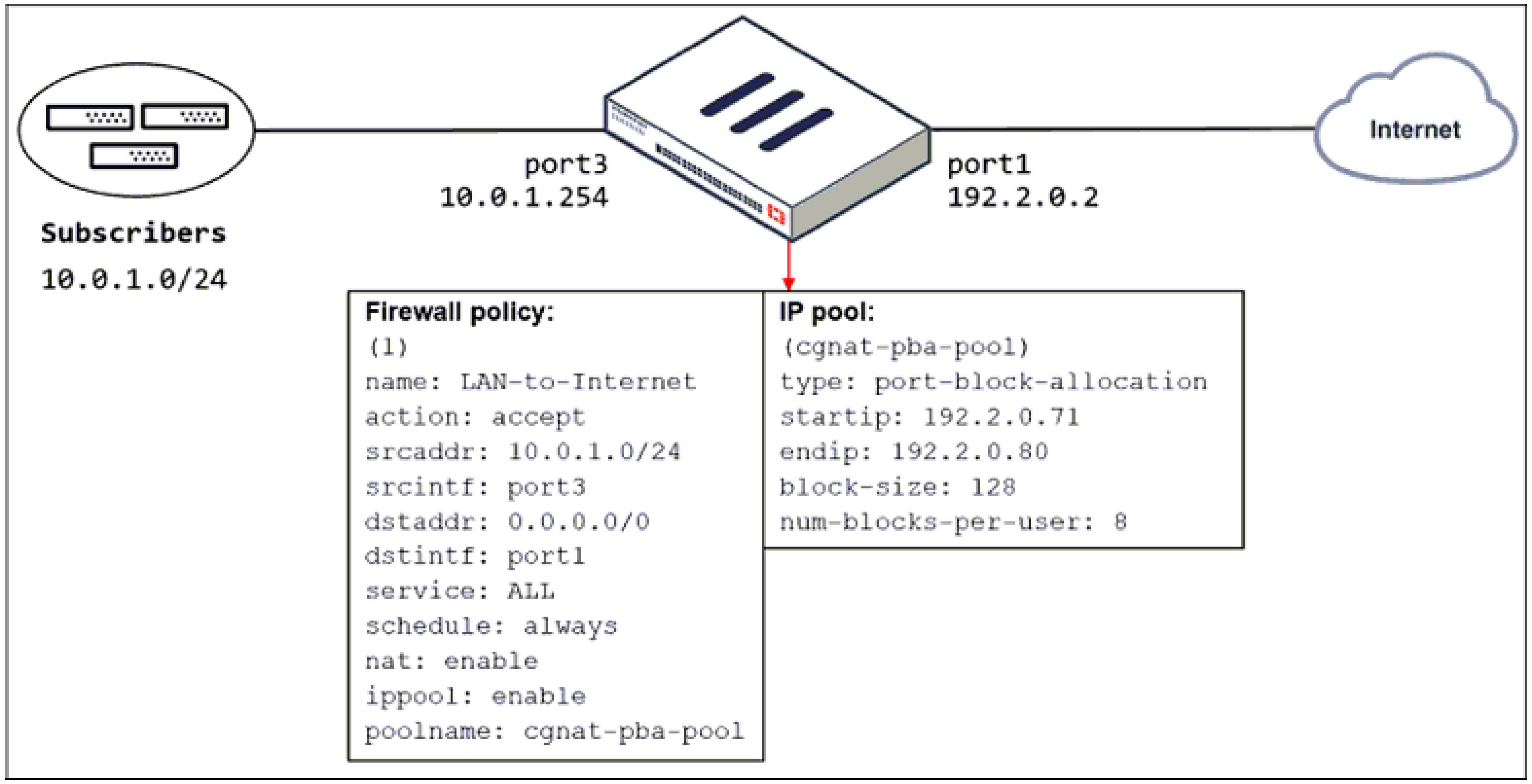
Question #: 34

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibit.

The exhibit shows a diagram of a FortiGate device connected to the network and the firewall policy and IP pool configuration on the FortiGate device.



Firewall policy:

```
(1)
name: LAN-to-Internet
action: accept
srcaddr: 10.0.1.0/24
srcintf: port3
dstaddr: 0.0.0.0/0
dstintf: port1
service: ALL
schedule: always
nat: enable
ippool: enable
poolname: cgnat-pba-pool
```

IP pool:

```
(cgnat-pba-pool)
type: port-block-allocation
startip: 192.2.0.71
endip: 192.2.0.80
block-size: 128
num-blocks-per-user: 8
```

Which two actions does FortiGate take on internet traffic sourced from the subscribers? (Choose two.)

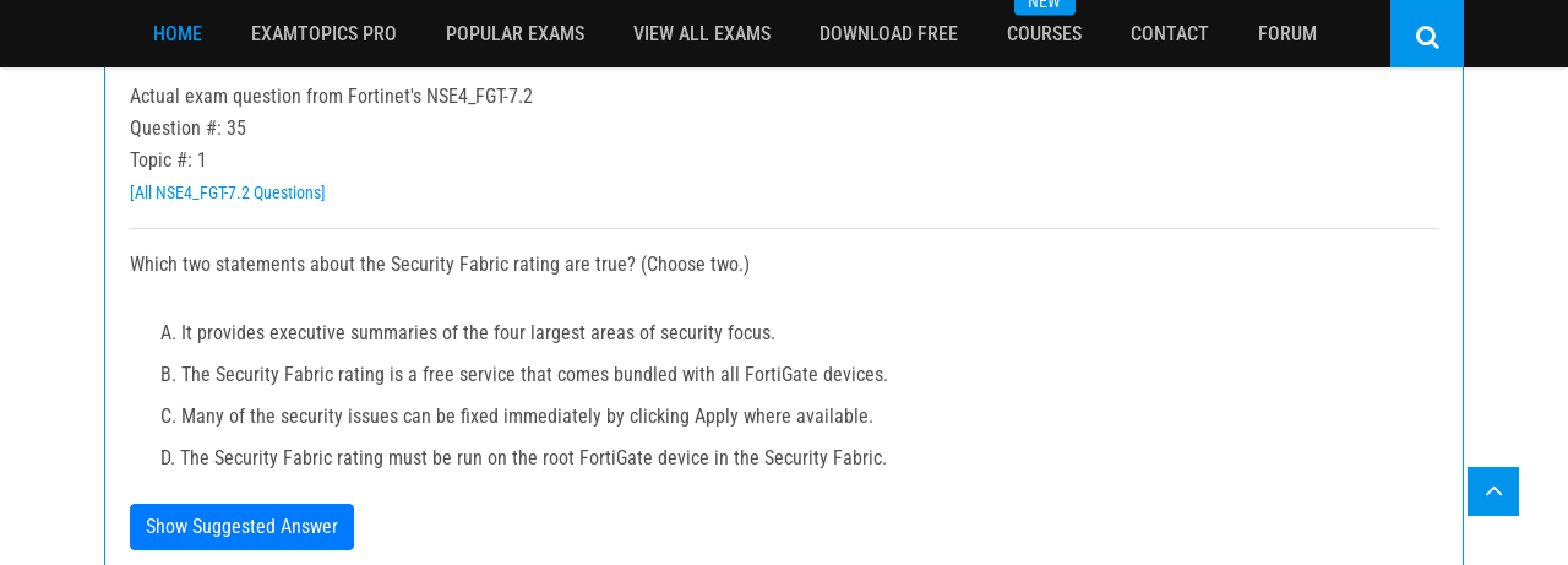
A. FortiGate allocates port blocks per user, based on the configured range of internal IP addresses.

B. FortiGate allocates port blocks on a first-come, first-served basis.

C. FortiGate generates a system event log for every port block allocation made per user.

D. FortiGate allocates 128 port blocks per user.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 35

Topic #: 1

[All NSE4_FGT-7.2 Questions]

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

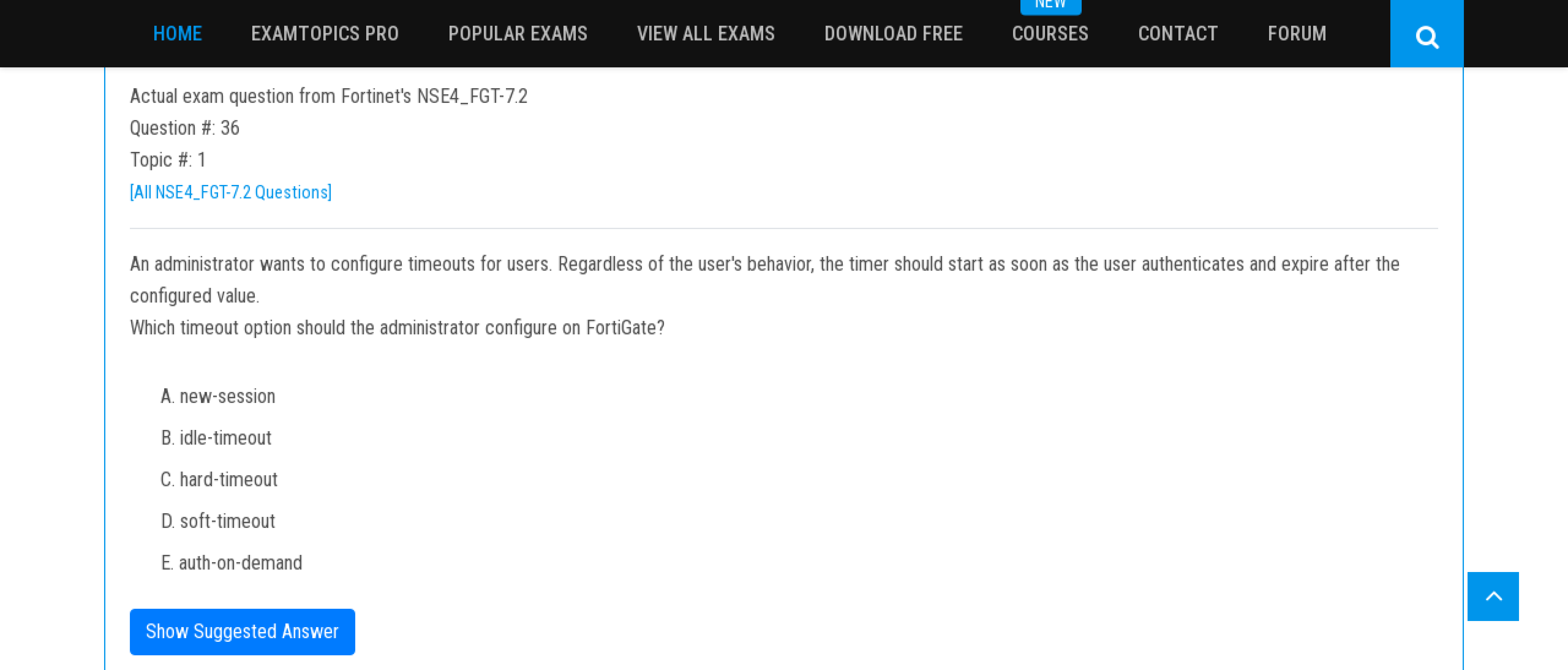
A. It provides executive summaries of the four largest areas of security focus.

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

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

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

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 36
Topic #: 1
[All NSE4_FGT-7.2 Questions]

An administrator wants to configure timeouts for users. Regardless of the user's behavior, the timer should start as soon as the user authenticates and expire after the configured value.
Which timeout option should the administrator configure on FortiGate?

A. new-session

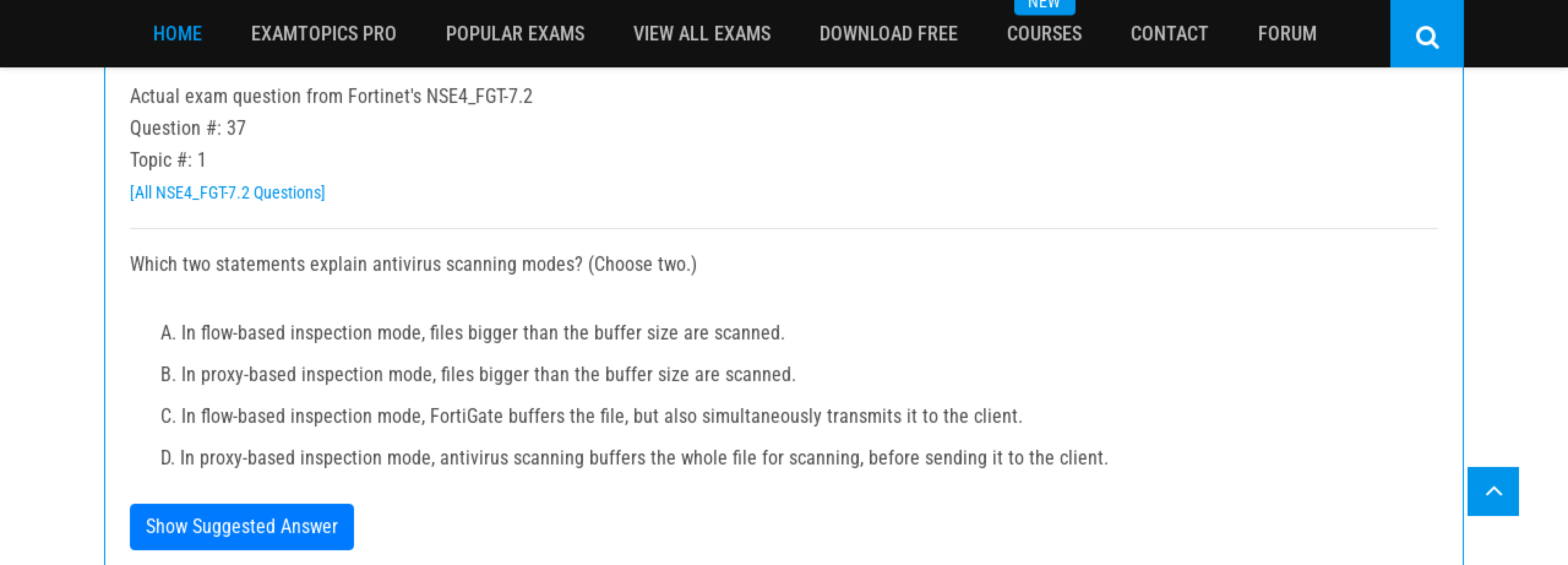
B. idle-timeout

C. hard-timeout

D. soft-timeout

E. auth-on-demand

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 37

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Which two statements explain antivirus scanning modes? (Choose two.)

A. In flow-based inspection mode, files bigger than the buffer size are scanned.

B. In proxy-based inspection mode, files bigger than the buffer size are scanned.

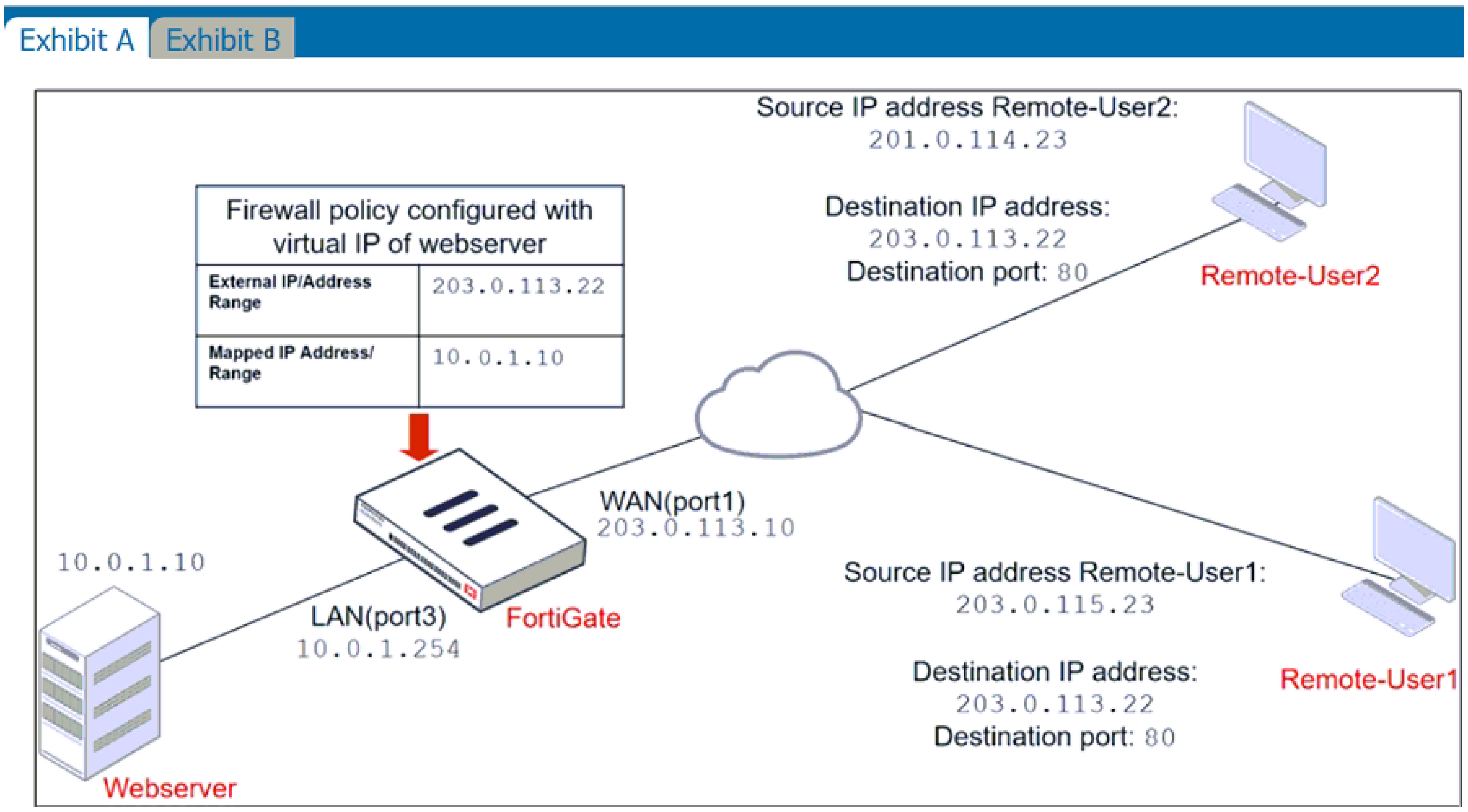
C. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.

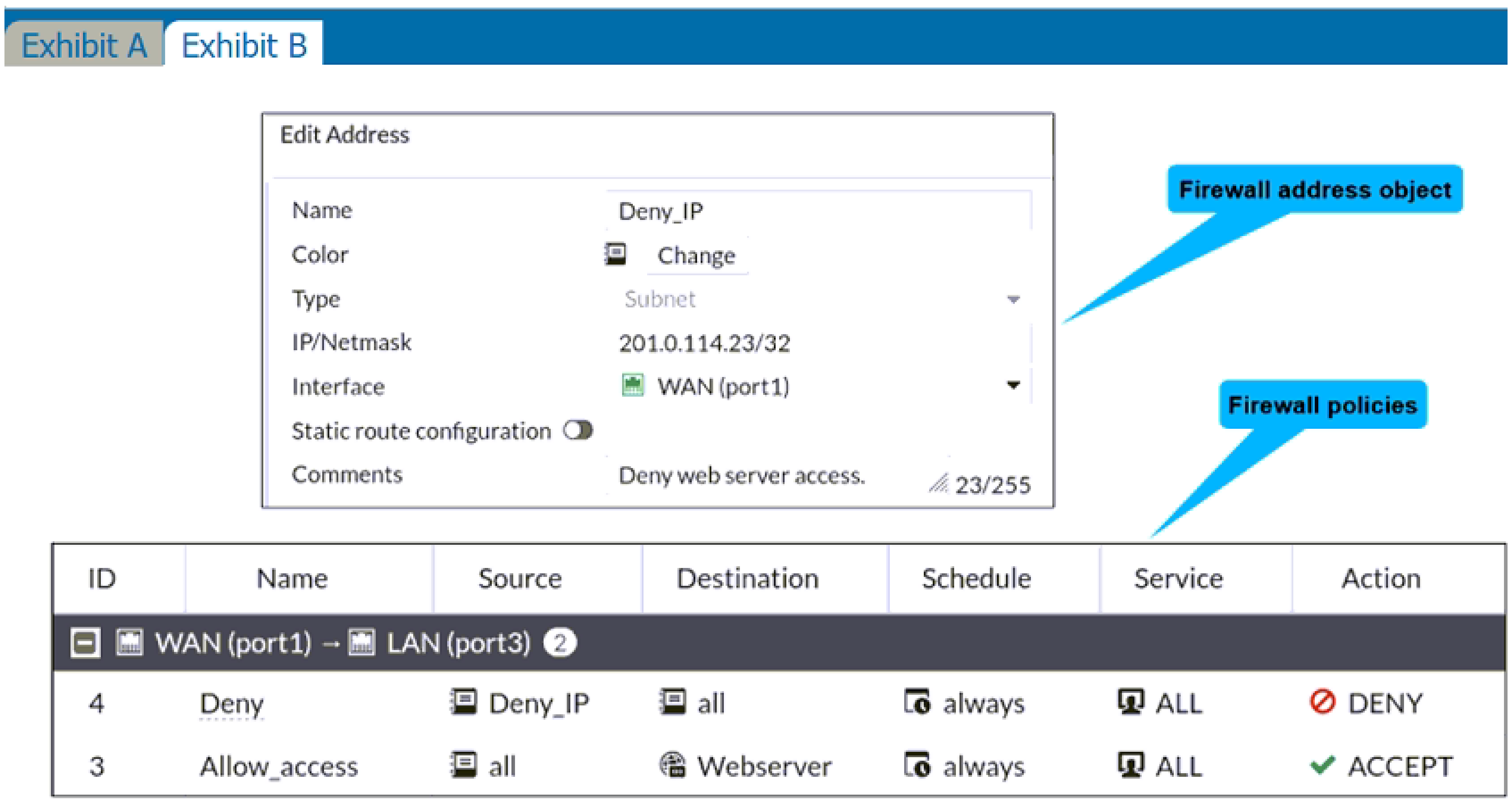
D. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 38
Topic #: 1
[All NSE4_FGT-7.2 Questions]

Refer to the exhibits.
The exhibits show a network diagram and firewall configurations.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver. Remote-User2 must not be able to access the Webserver.





Edit Address

Name	Deny_IP
Color	Change
Type	Subnet
IP/Netmask	201.0.114.23/32
Interface	WAN (port1)
Static route configuration	○
Comments	Deny web server access. 23/255

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

In this scenario, 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 Webserver in the Deny policy.

C. Enable match-vip in the Deny policy.

D. Set the Destination address as Deny_IP in the Allow_access policy.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

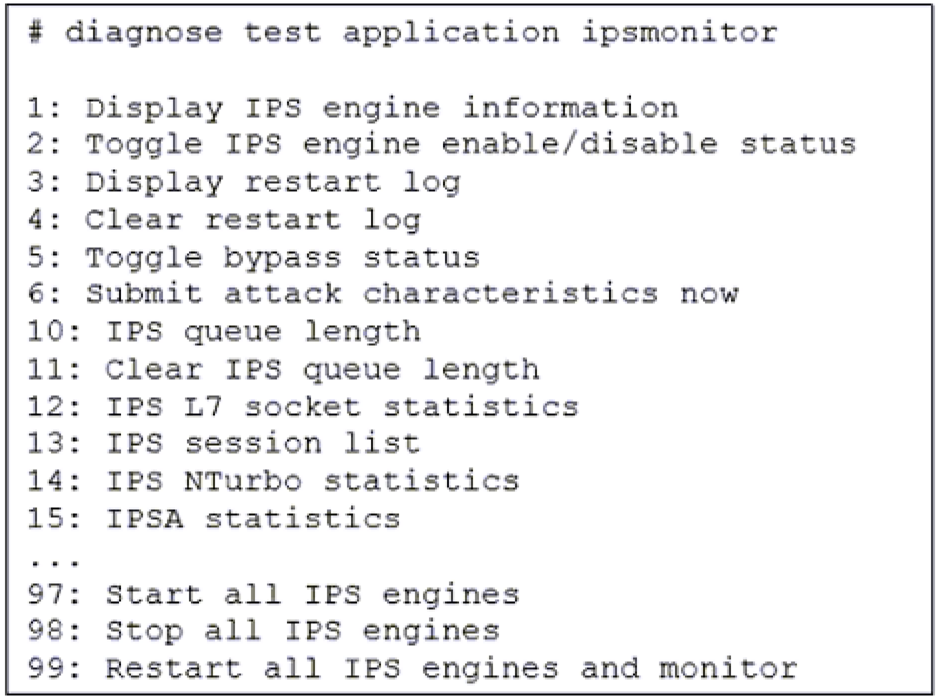
Question #: 39

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibit.

Examine the intrusion prevention system (IPS) diagnostic command shown in the exhibit.



```
# diagnose test application ipsmonitor

1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
6: Submit attack characteristics now
10: IPS queue length
11: Clear IPS queue length
12: IPS L7 socket statistics
13: IPS session list
14: IPS NTurbo statistics
15: IPSA statistics
...
97: Start all IPS engines
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

If option 5 is used with the IPS diagnostic command and the outcome is a decrease in the CPU usage, what is the correct conclusion?

A. The IPS engine is unable to prevent an intrusion attack.

B. The IPS engine is inspecting a high volume of traffic.

C. The IPS engine will continue to run in a normal state.

D. The IPS engine is blocking all traffic.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 40

Topic #: 1

[All NSE4_FGT-7.2 Questions]

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

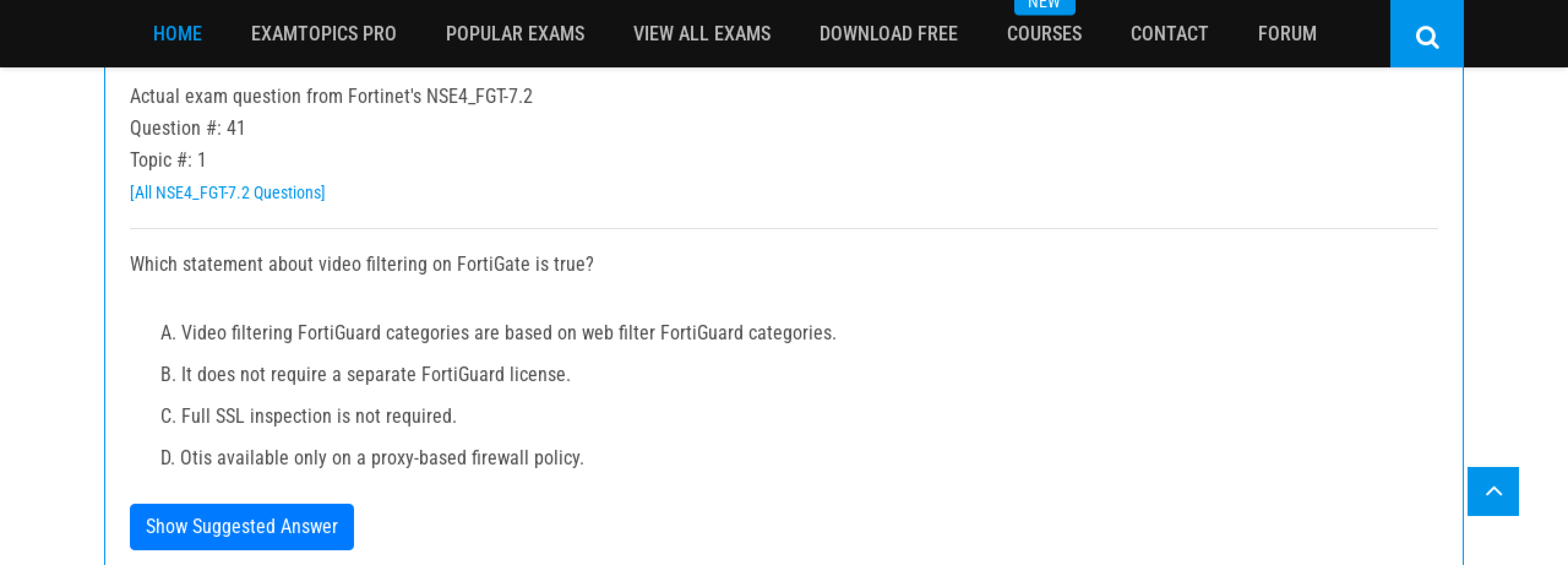
A. FTM

B. SSH

C. HTTPS

D. FortiTelemetry

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 41

Topic #: 1

[All NSE4_FGT-7.2 Questions]

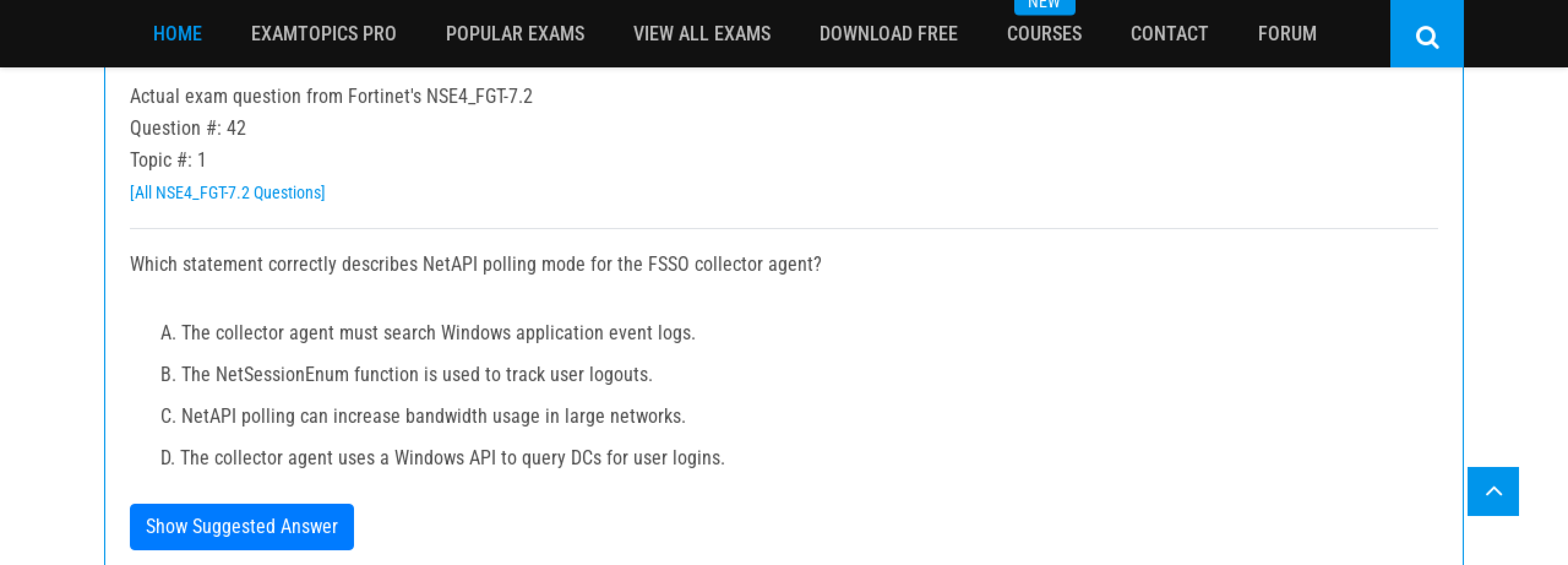
Which statement about video filtering on FortiGate is true?

A. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

B. It does not require a separate FortiGuard license.

C. Full SSL inspection is not required.

D. Otis available only on a proxy-based firewall policy.



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 42

Topic #: 1

[All NSE4_FGT-7.2 Questions]

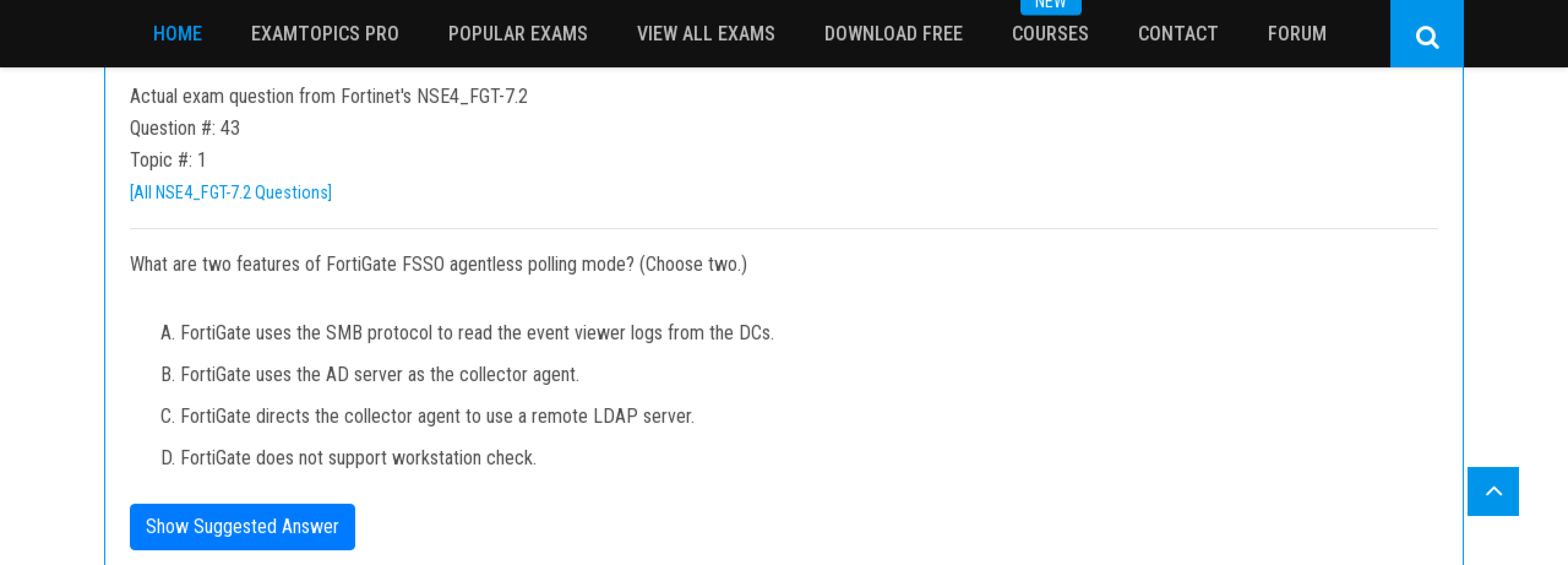
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The collector agent must search Windows application event logs.

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

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

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



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 43

Topic #: 1

[All NSE4_FGT-7.2 Questions]

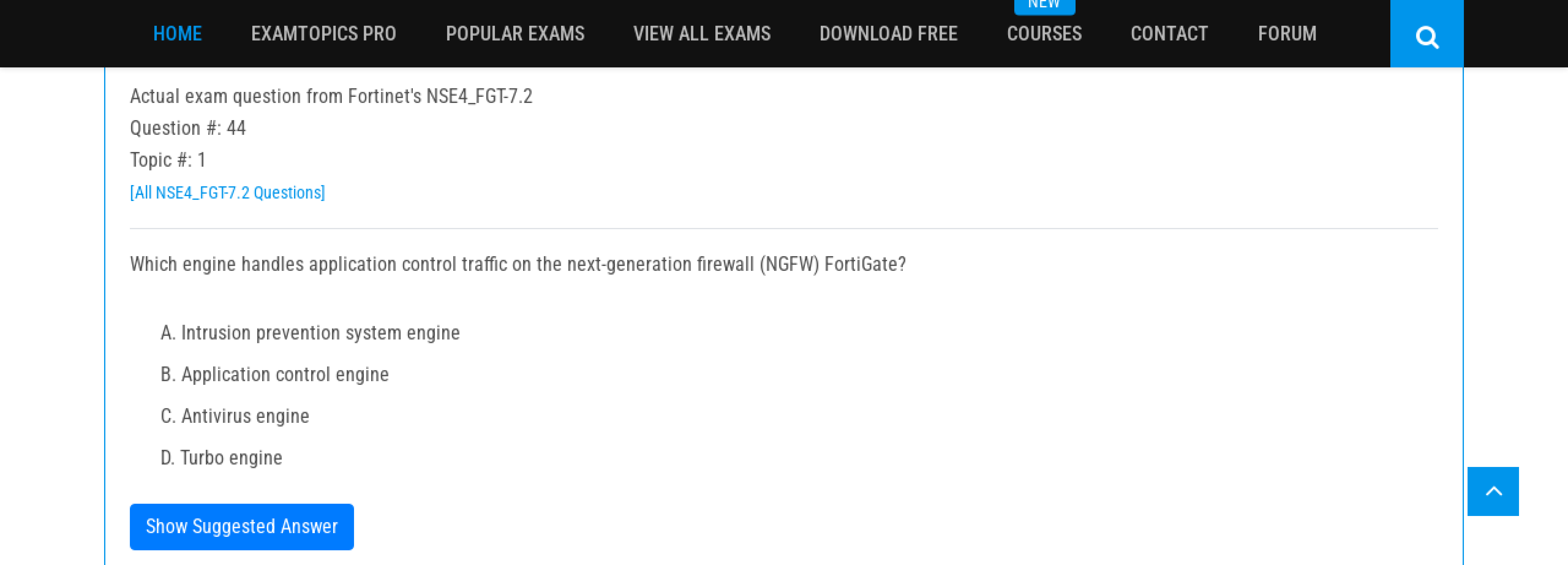
What are two features of FortiGate FSSO agentless polling mode? (Choose two.)

A. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

B. FortiGate uses the AD server as the collector agent.

C. FortiGate directs the collector agent to use a remote LDAP server.

D. FortiGate does not support workstation check.



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 44

Topic #: 1

[All NSE4_FGT-7.2 Questions]

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

A. Intrusion prevention system engine

B. Application control engine

C. Antivirus engine

D. Turbo engine

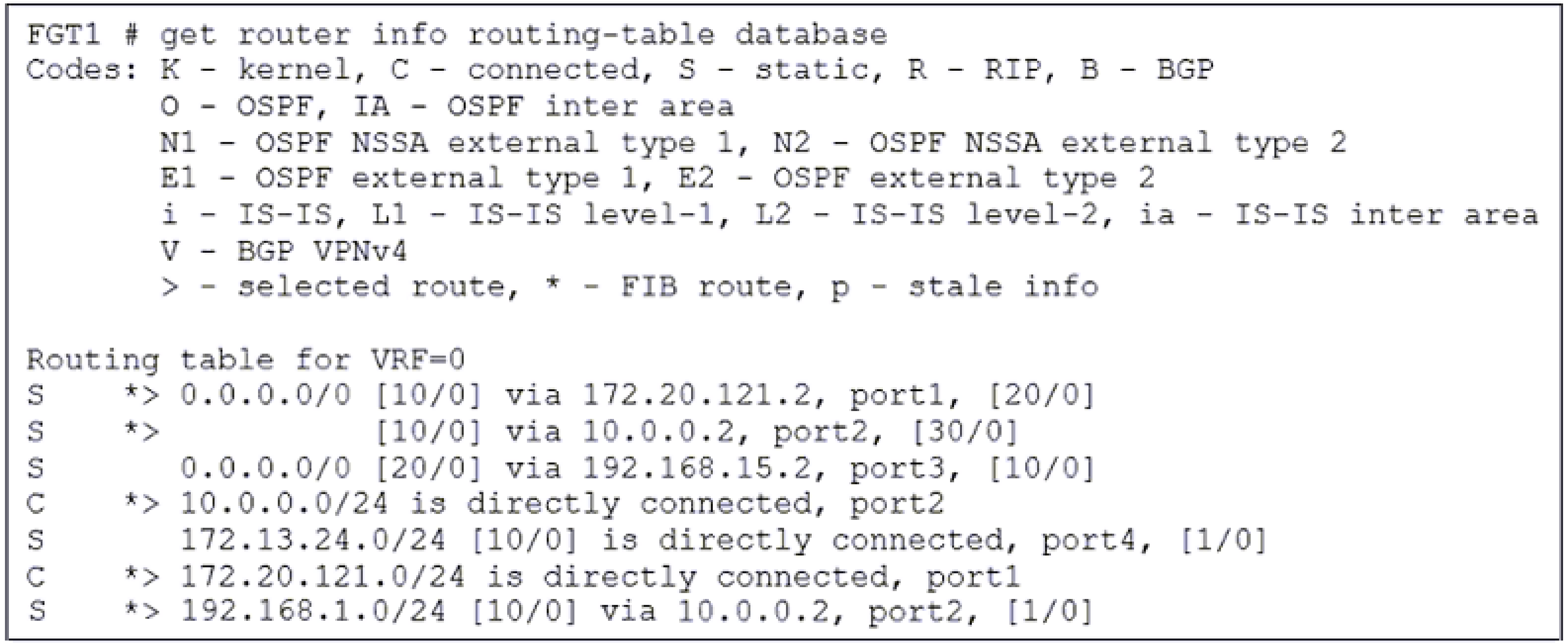
Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 45

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibit.



```
FGT1 # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S    *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
S    *>           [10/0] via 10.0.0.2, port2, [30/0]
S       0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C    *> 10.0.0.0/24 is directly connected, port2
S       172.13.24.0/24 [10/0] is directly connected, port4, [1/0]
C    *> 172.20.121.0/24 is directly connected, port1
S    *> 192.168.1.0/24 [10/0] via 10.0.0.2, port2, [1/0]
```

Based on the routing database shown in the exhibit, which two conclusions can you make about the routes? (Choose two.)

A. The port3 default route has the lowest metric.

B. The port1 and port2 default routes are active in the routing table.

C. The ports default route has the highest distance.

D. There will be eight routes active in the routing table.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 46
Topic #: 1
[All NSE4_FGT-7.2 Questions]

Refer to the exhibits.
The exhibits show a firewall policy (Exhibit A) and an antivirus profile (Exhibit B).

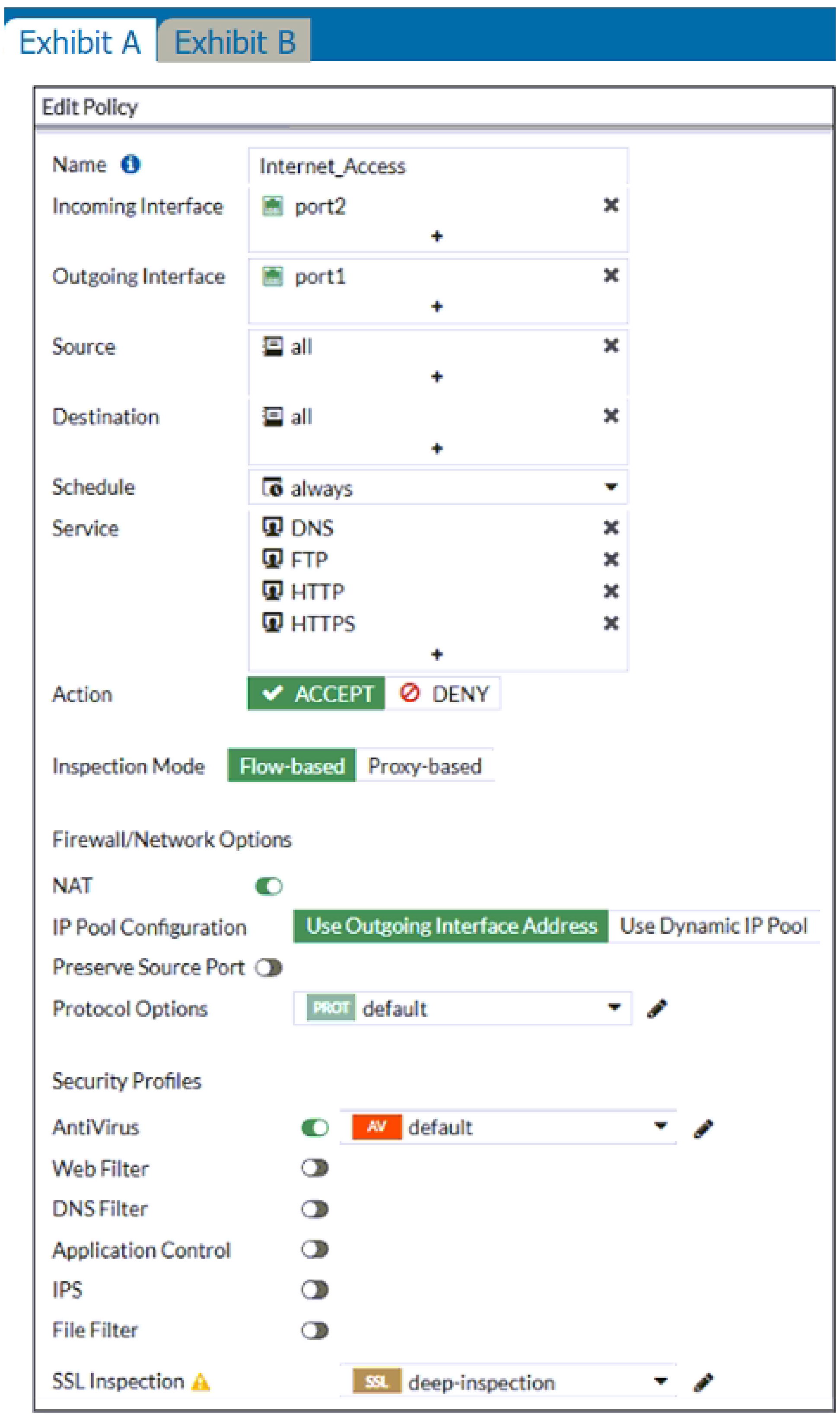


Exhibit A | Exhibit B

Edit 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

Firewall/Network Options
NAT: ●
IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool
Preserve Source Port: ○
Protocol Options: PROT default

Security Profiles
AntiVirus: ● AV default
Web Filter: ○
DNS Filter: ○
Application Control: ○
IPS: ○
File Filter: ○
SSL Inspection: SSL deep-inspection

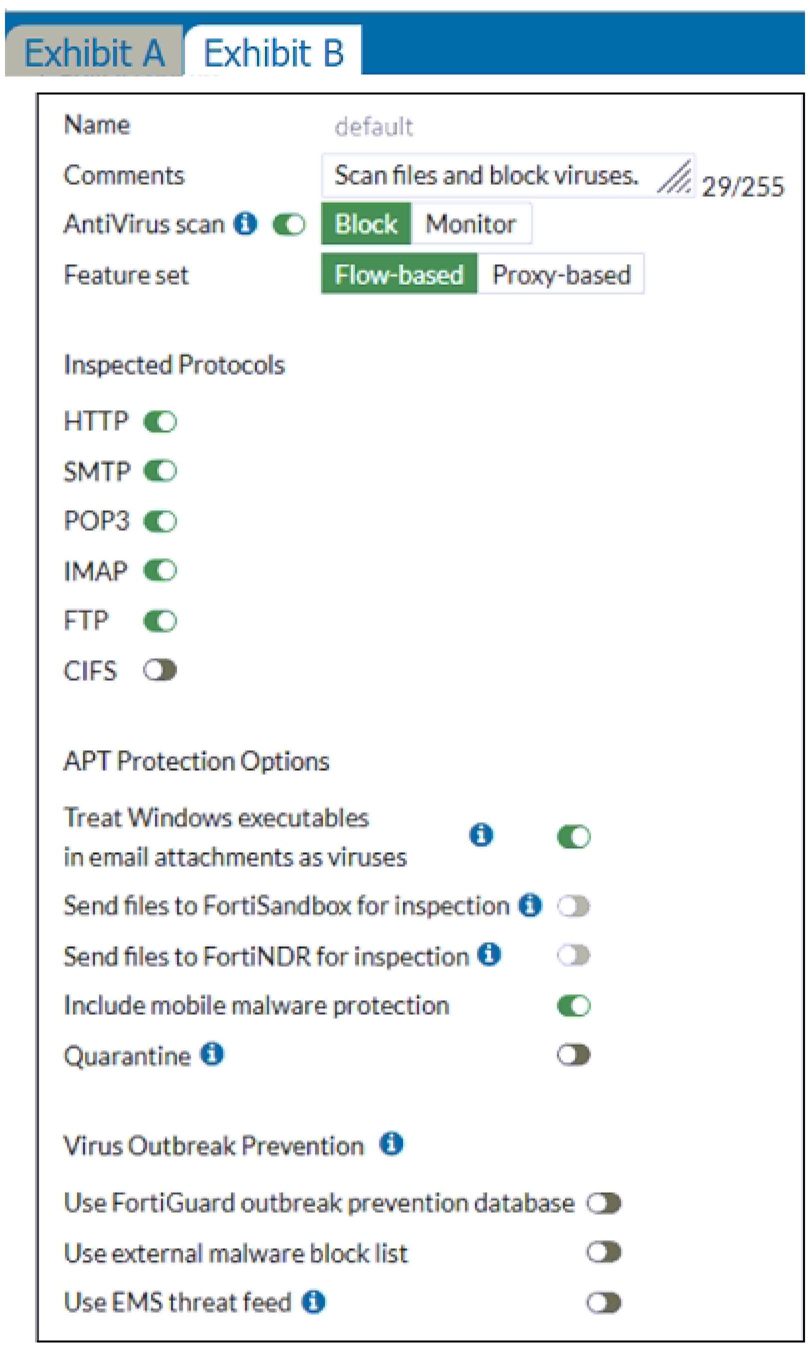


Exhibit A | Exhibit B

Name: default
Comments: Scan files and block viruses. 29/255
AntiVirus scan: ● Block | Monitor
Feature set: Flow-based | Proxy-based

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

APT Protection Options
Treat Windows executables in email attachments as viruses ●
Send files to FortiSandbox for inspection ○
Send files to FortiNDR for inspection ○
Include mobile malware protection ●
Quarantine ○

Virus Outbreak Prevention
Use FortiGuard outbreak prevention database ○
Use external malware block list ○
Use EMS threat feed ○

Why is the user unable to receive a block replacement message when downloading an infected file for the first time?

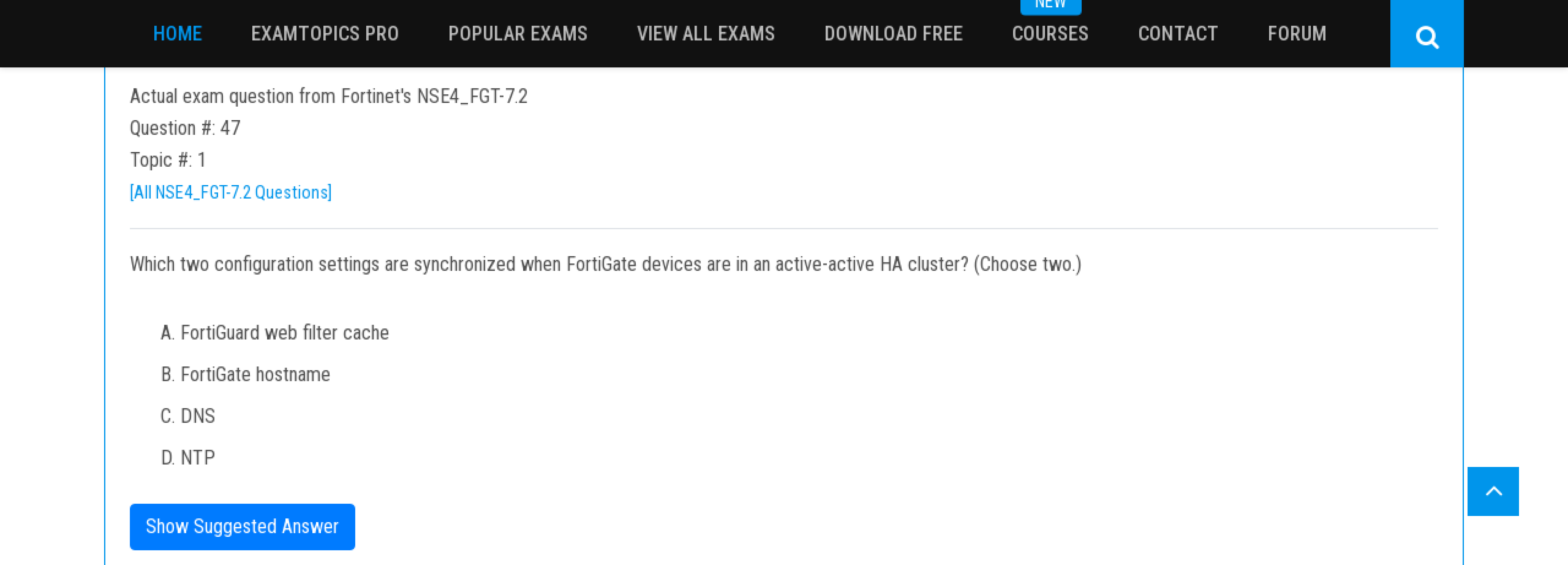
A. The firewall policy performs a full content inspection on the file.

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

C. Flow-based inspection is used, which resets the last packet to the user.

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

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 47

Topic #: 1

[All NSE4_FGT-7.2 Questions]

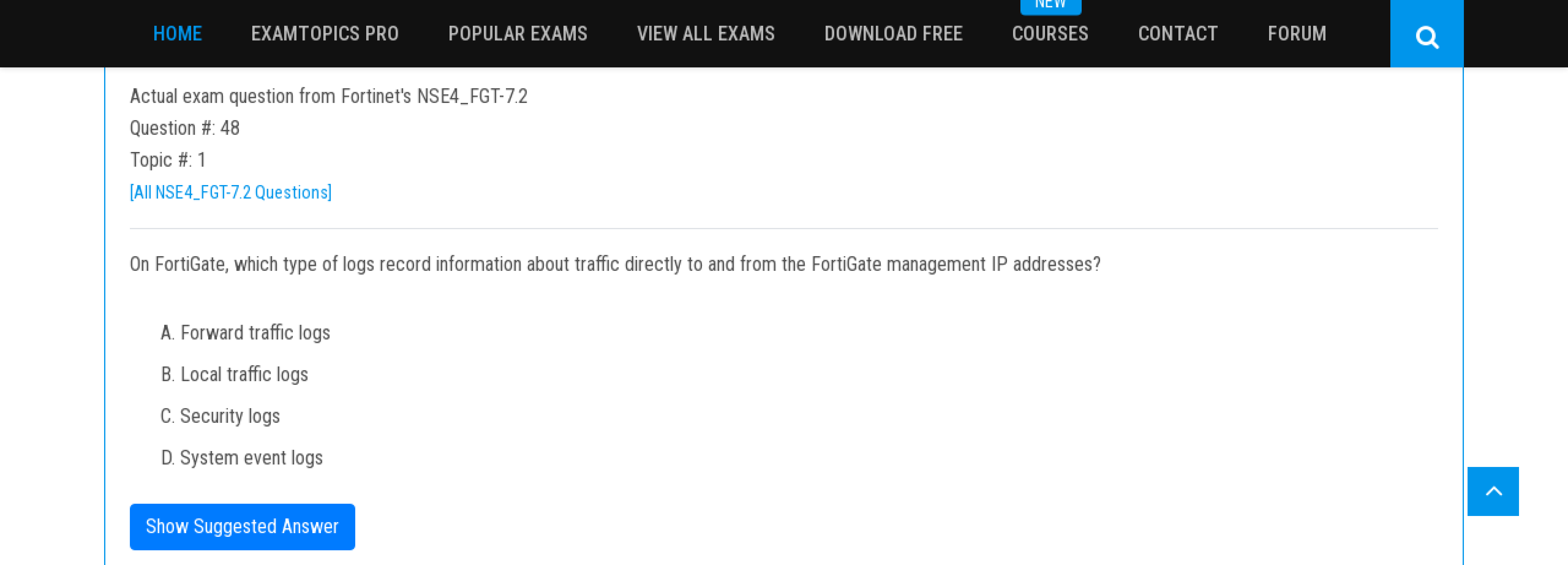
Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

A. FortiGuard web filter cache

B. FortiGate hostname

C. DNS

D. NTP



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 48

Topic #: 1

[All NSE4_FGT-7.2 Questions]

On FortiGate, which type of logs record information about traffic directly to and from the FortiGate management IP addresses?

A. Forward traffic logs

B. Local traffic logs

C. Security logs

D. System event logs

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

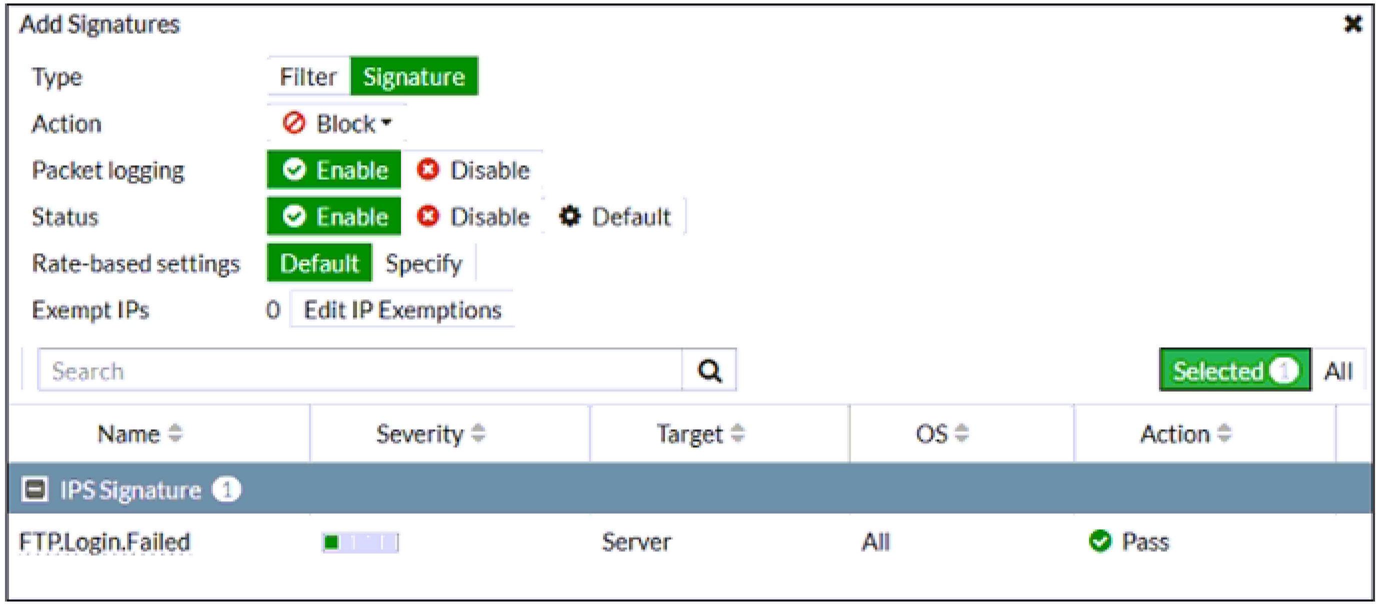
Question #: 49

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibit.

Review the intrusion prevention system (IPS) profile signature settings shown in 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
IPS Signature 1				
FTP.Login.Failed	■□□□□	Server	All	✓ Pass

What do you conclude when adding the FTP.Login.Failed signature to the IPS sensor profile?

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

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

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

D. The signature setting uses a custom rating threshold.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 50

Topic #: 1

[All NSE4_FGT-7.2 Questions]

An administrator configures outgoing interface any in a firewall policy.

What is the result of the policy list view?

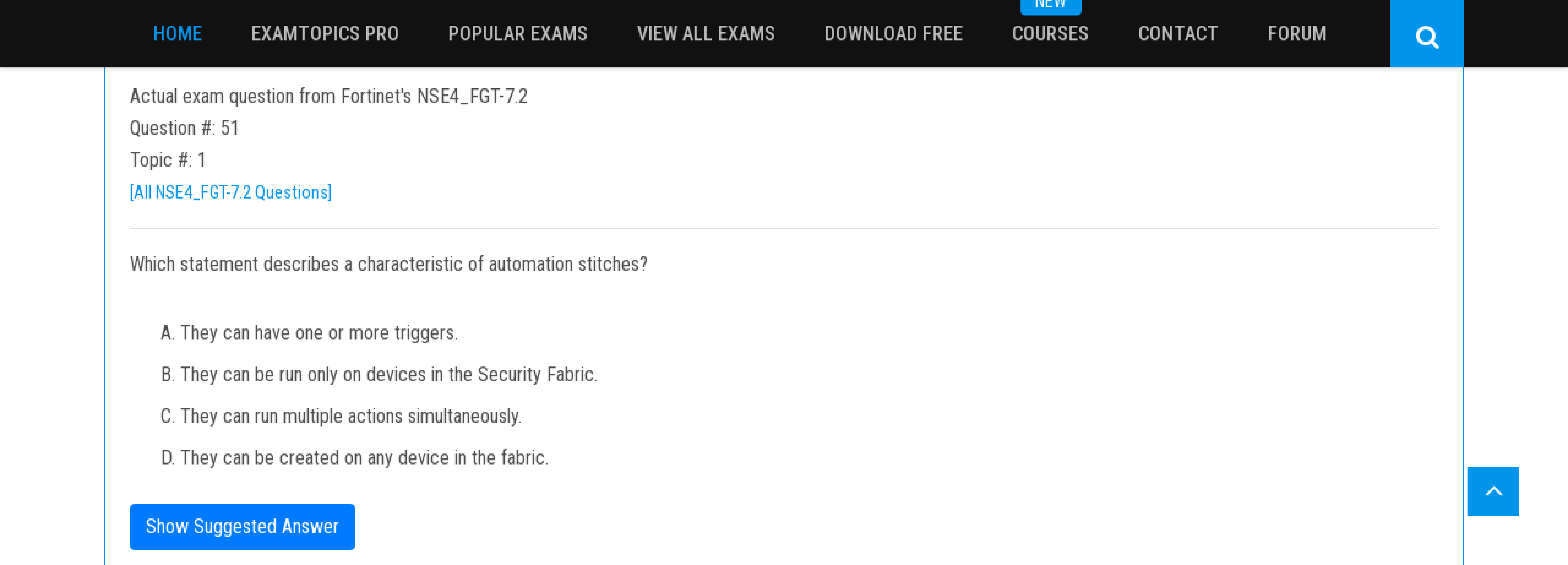
A. Search option is disabled.

B. Policy lookup is disabled.

C. By Sequence view is disabled.

D. Interface Pair view is disabled.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 51

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Which statement describes a characteristic of automation stitches?

A. They can have one or more triggers.

B. They can be run only on devices in the Security Fabric.

C. They can run multiple actions simultaneously.

D. They can be created on any device in the fabric.

Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 52

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibits.

Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object 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.

Exhibit A Exhibit B

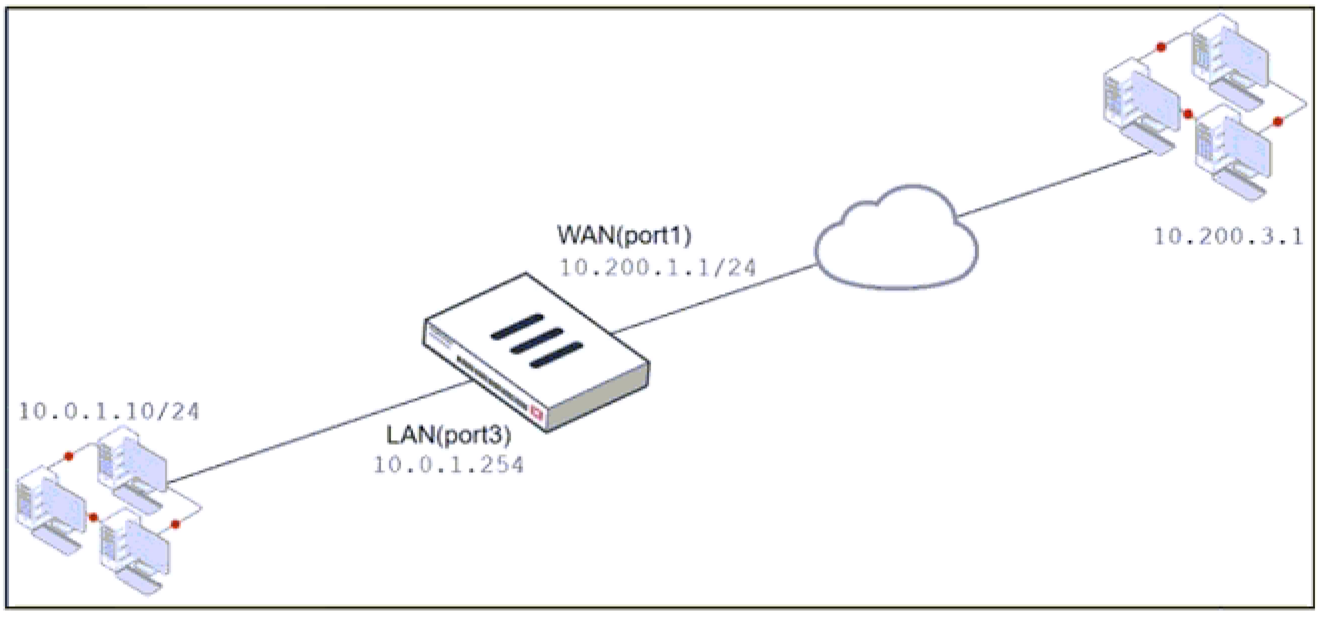
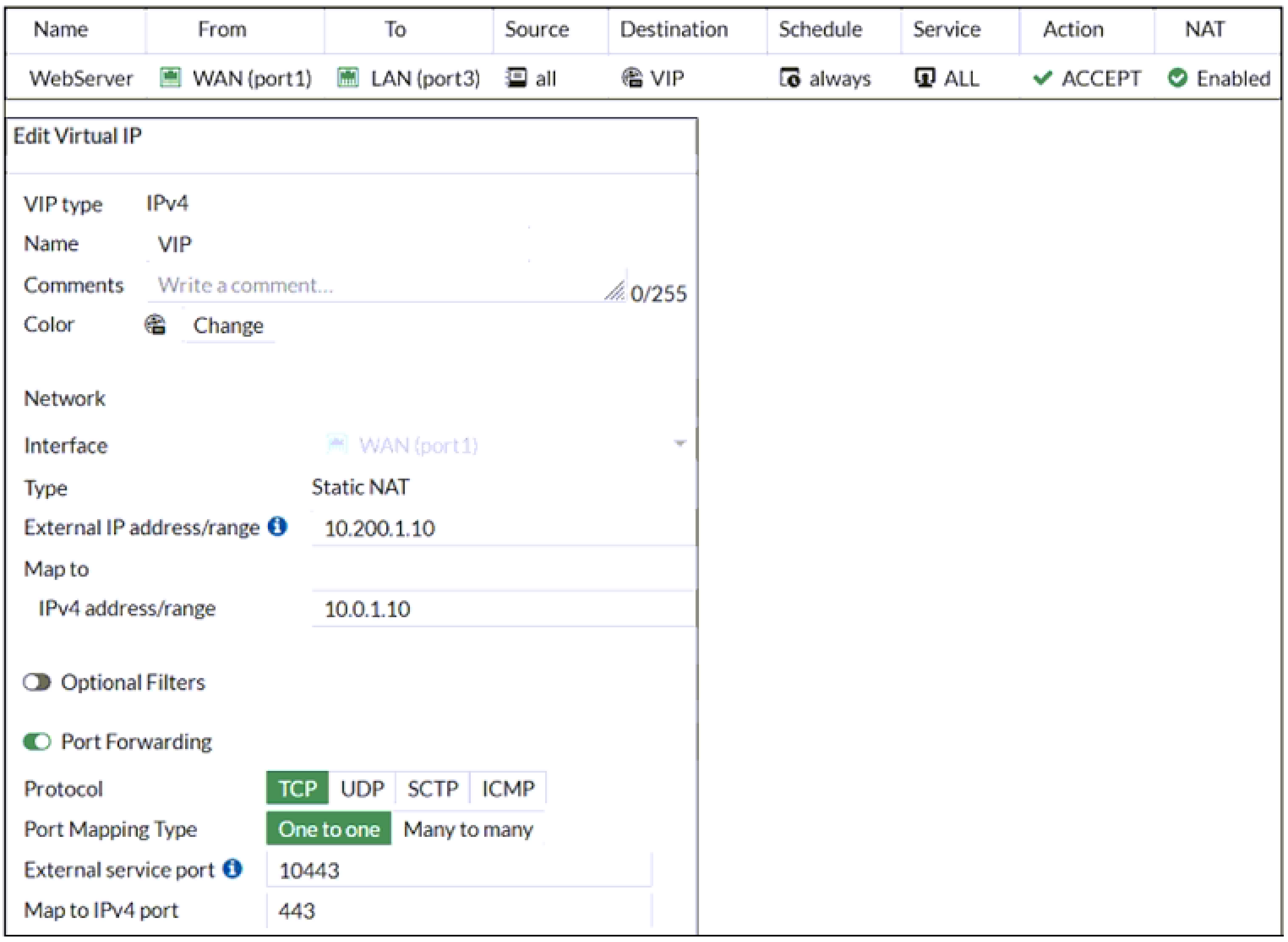


Exhibit A Exhibit B



Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	✓ ACCEPT	✓ Enabled

Edit Virtual IP

VIP type IPv4

Name VIP

Comments Write a comment... 0/255

Color Change

Network

Interface WAN (port1)

Type Static NAT

External IP address/range 10.200.1.10

Map to

IPv4 address/range 10.0.1.10

○ Optional Filters

● Port Forwarding

Protocol [✓ TCP] UDP SCTP ICMP

Port Mapping Type [✓ One to one] Many to many

External service port 10443

Map to IPv4 port 443

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

A. 10.0.1.254, 10.0.1.10, and 443, respectively

B. 10.0.1.254, 10.0.1.10, and 10443, respectively

C. 10.200.3.1, 10.0.1.10, and 443, respectively

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 53

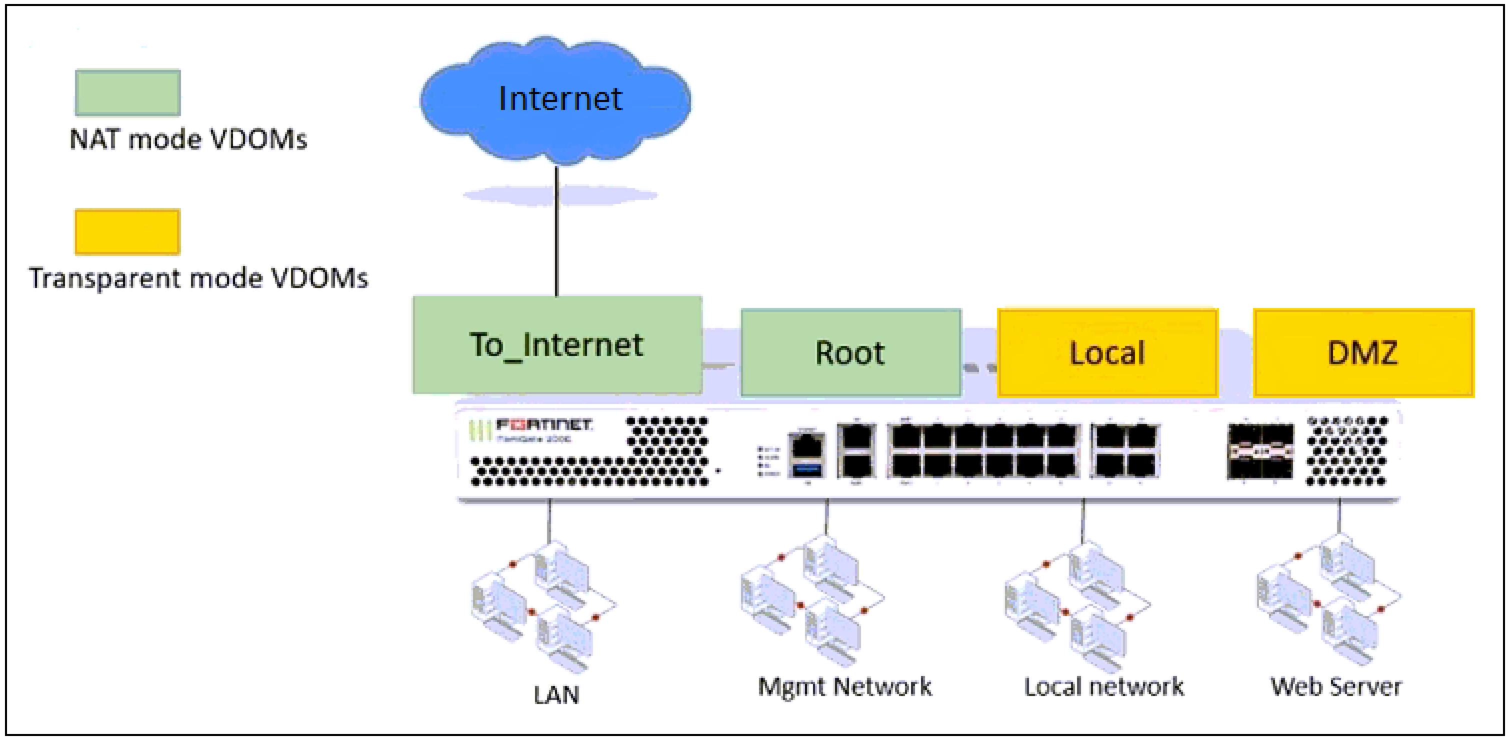
Topic #: 1

[All NSE4_FGT-7.2 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 the ISP modem.



What can you conclude about this configuration?

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

B. A default static route is not required on the To_Internet VDOM to allow LAN users to access the internet.

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

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

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

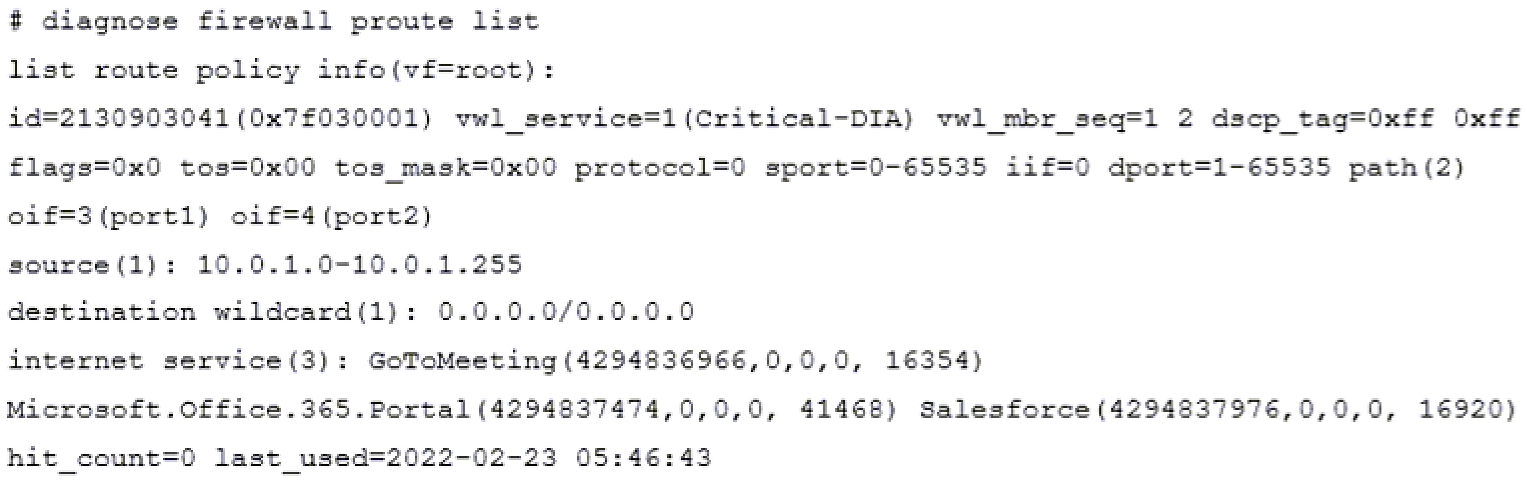
Question #: 54

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibit.

The exhibit shows the output of a diagnose command.



```
# diagnose firewall proute list
list route policy info(vf=root):
id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-02-23 05:46:43
```

What does the output reveal about the policy route?

A. It is an ISDB route in policy route.

B. It is a regular policy route.

C. It is an ISDB policy route with an SDWAN rule.

D. It is an SDWAN rule in policy route.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

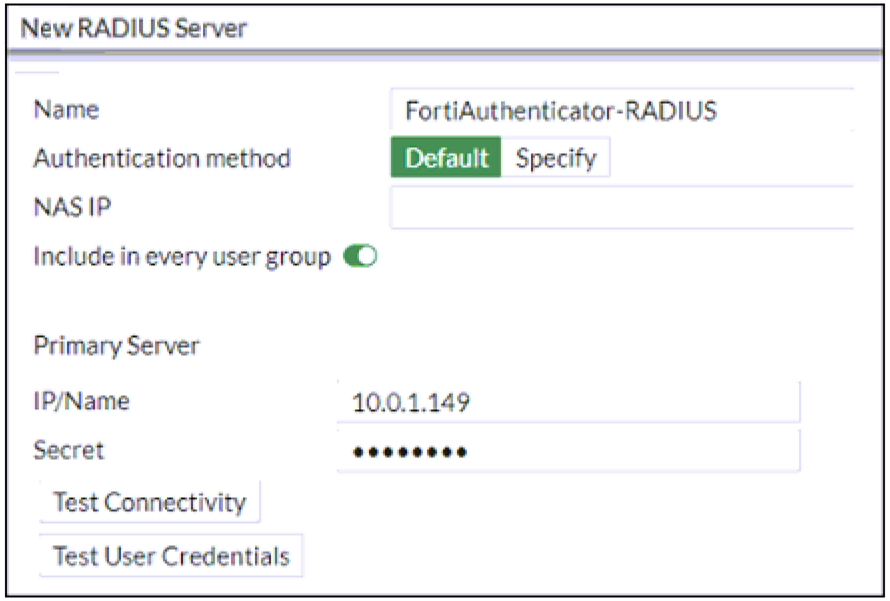
Question #: 55

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibit.

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



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: ●●●●●●●●●

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

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

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

C. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.

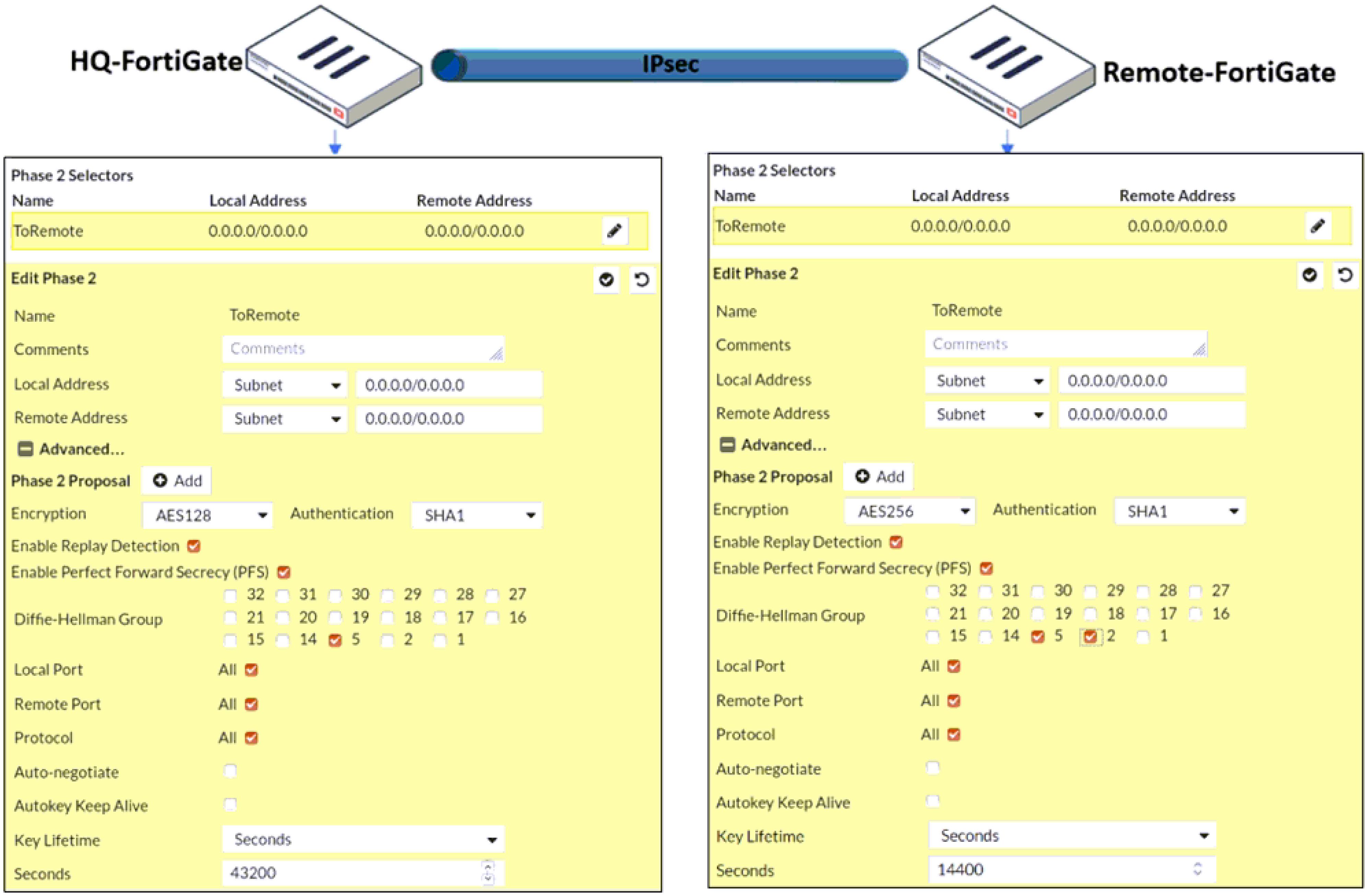
D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 56
Topic #: 1
[All NSE4_FGT-7.2 Questions]

Refer to the exhibit.

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.



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
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: 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

Based on the phase 2 configuration shown in the exhibit, which configuration change will bring phase 2 up?

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

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

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

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

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 57
Topic #: 1

[All NSE4_FGT-7.2 Questions]

An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings.
What is true about the DNS connection to a FortiGuard server?

A. It uses UDP 8888.

B. It uses UDP 53.

C. It uses DNS over HTTPS.

D. It uses DNS over TLS.

Show Suggested Answer

Actual exam question from Fortinet's NSE4_FGT-7.2

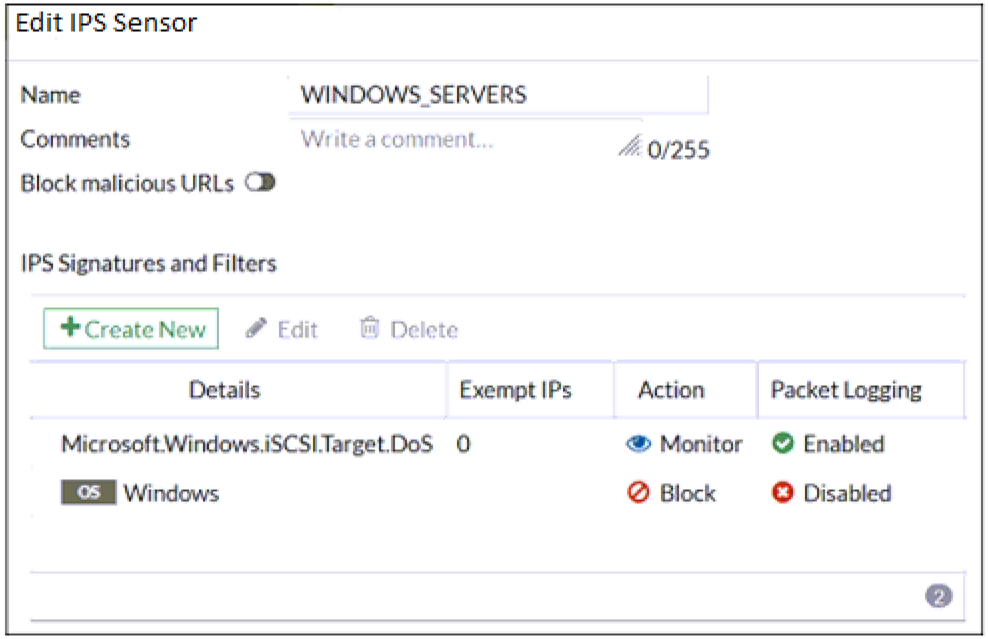
Question #: 58

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Refer to the exhibit.

The exhibit shows the IPS sensor configuration.



Edit IPS Sensor

Name WINDOWS_SERVERS

Comments Write a comment... 0/255

Block malicious URLs

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging
Microsoft.Windows.iSCSI.Target.DoS	0	Monitor	✓ Enabled
OS Windows		⊘ Block	✗ Disabled

If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

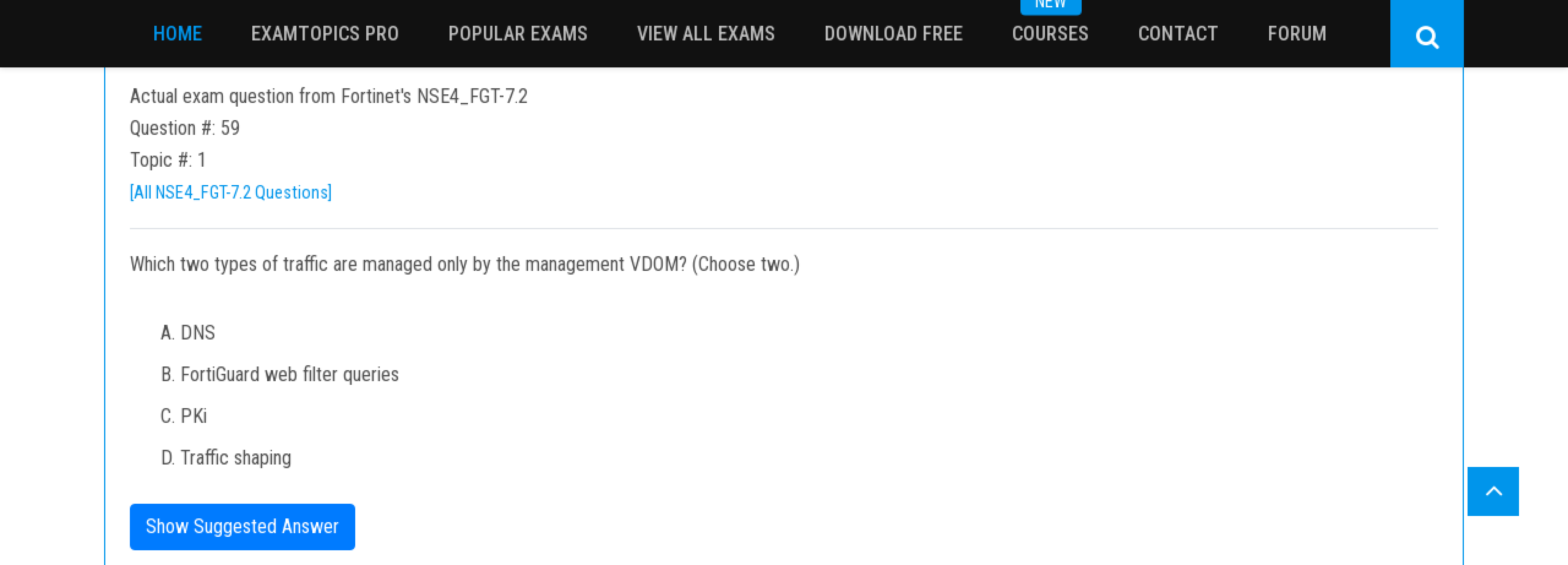
A. The sensor will gather a packet log for all matched traffic.

B. The sensor will reset all connections that match these signatures.

C. The sensor will block all attacks aimed at Windows servers.

D. The sensor will allow attackers matching the Microsoft Windows.iSCSI.Target.DoS signature.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 59

Topic #: 1

[All NSE4_FGT-7.2 Questions]

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

A. DNS

B. FortiGuard web filter queries

C. PKi

D. Traffic shaping

Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 60
Topic #: 1
[All NSE4_FGT-7.2 Questions]

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

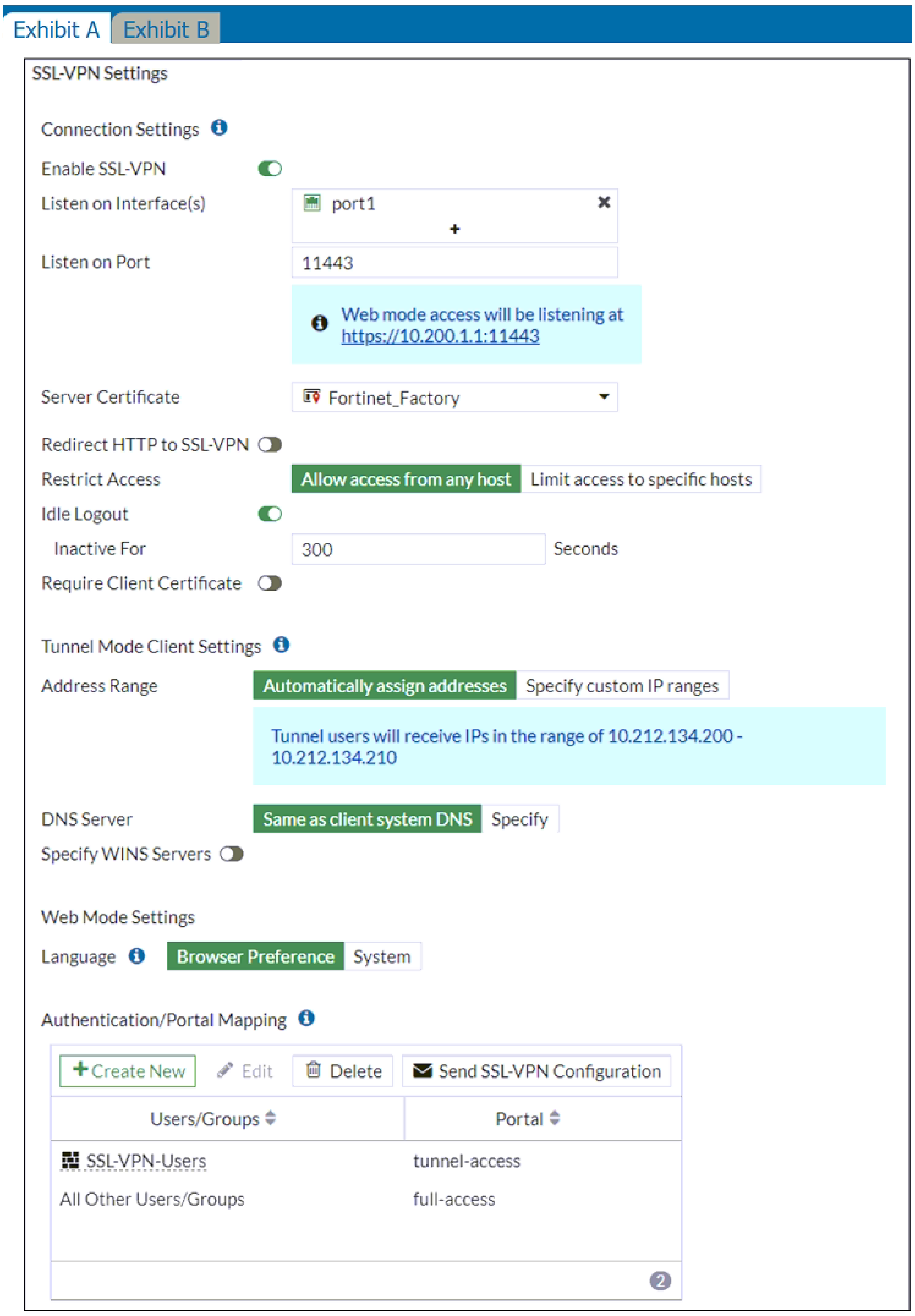


Exhibit A Exhibit B

SSL-VPN Settings

Connection Settings

Enable SSL-VPN ●

Listen on Interface(s): port1 ✖ +

Listen on Port: 11443

Web mode access will be listening at https://10.200.1.1:11443

Server Certificate: Fortinet_Factory

Redirect HTTP to SSL-VPN ○

Restrict Access: [✓ Allow access from any host] Limit access to specific hosts

Idle Logout ●

Inactive For: 300 Seconds

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 ○

Web Mode Settings

Language: [✓ Browser Preference] System

Authentication/Portal Mapping

Users/Groups	Portal
SSL-VPN-Users	tunnel-access
All Other Users/Groups	full-access

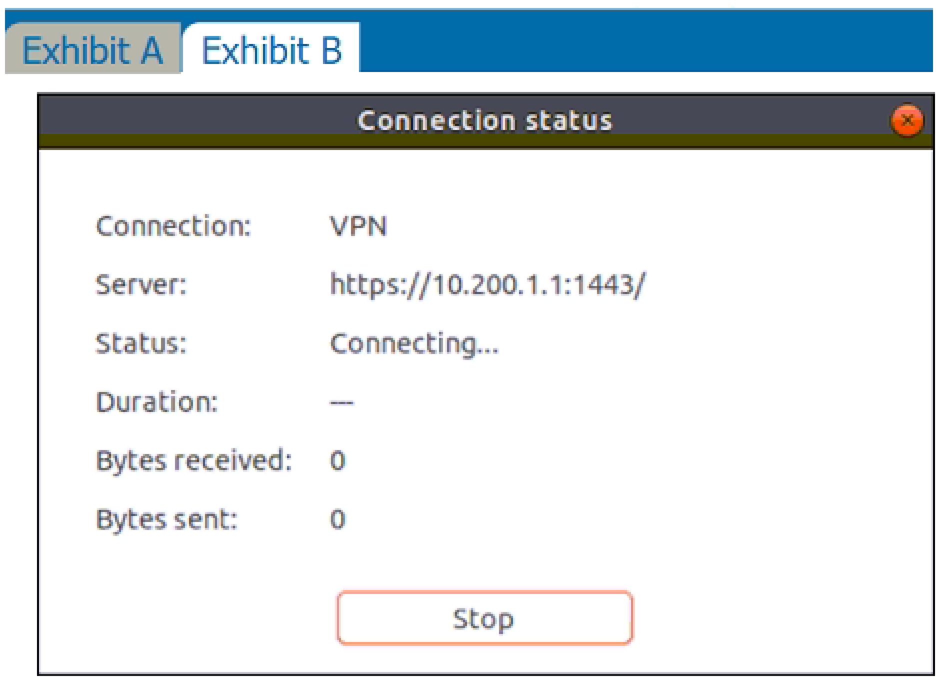


Exhibit A Exhibit B

Connection status

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

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

A. Change the SSL VPN port on the client.

B. Change the idle-timeout.

C. Change the SSL VPN portal to the tunnel.

D. Change the server IP address.

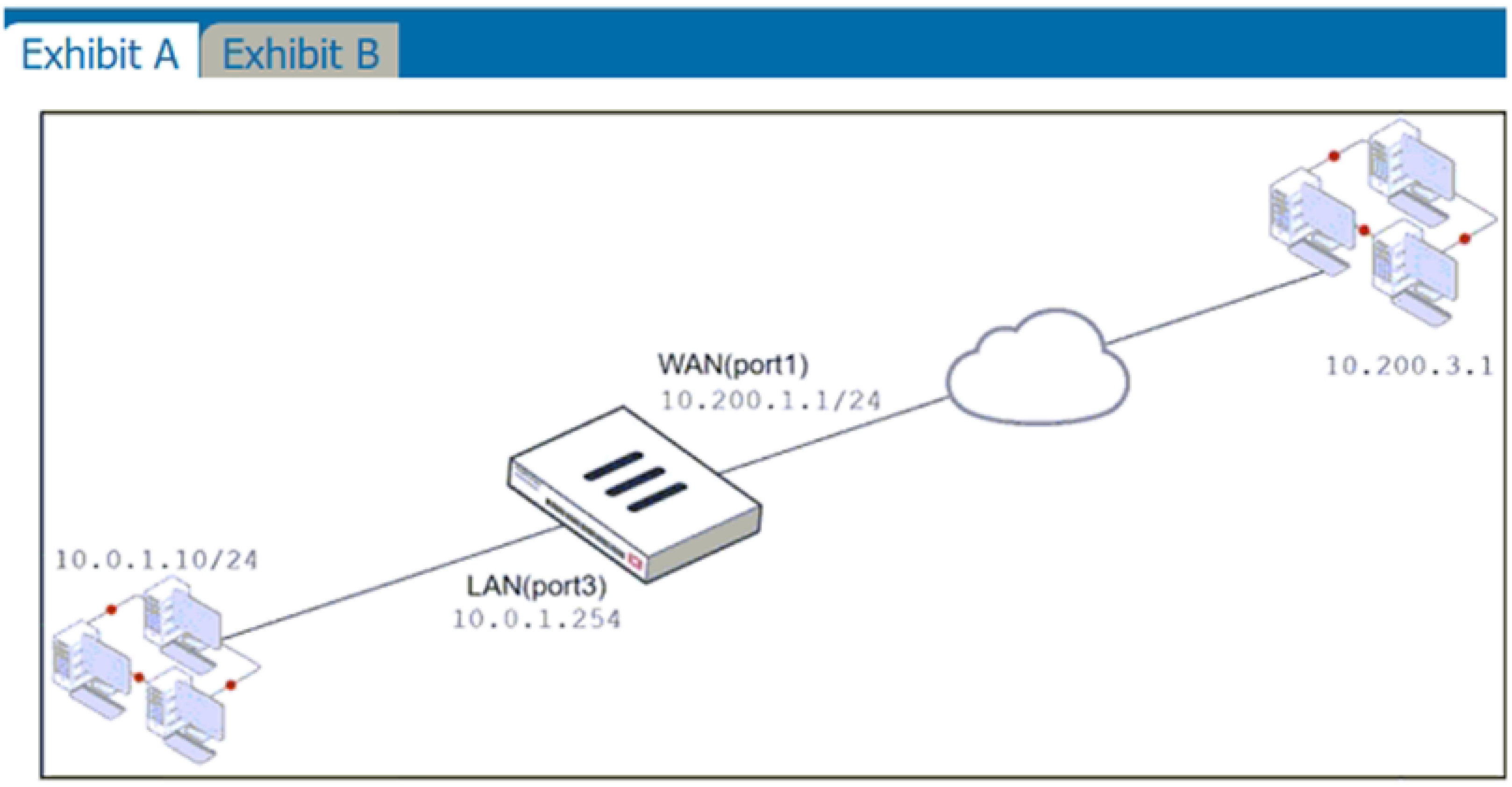
Show Suggested Answer

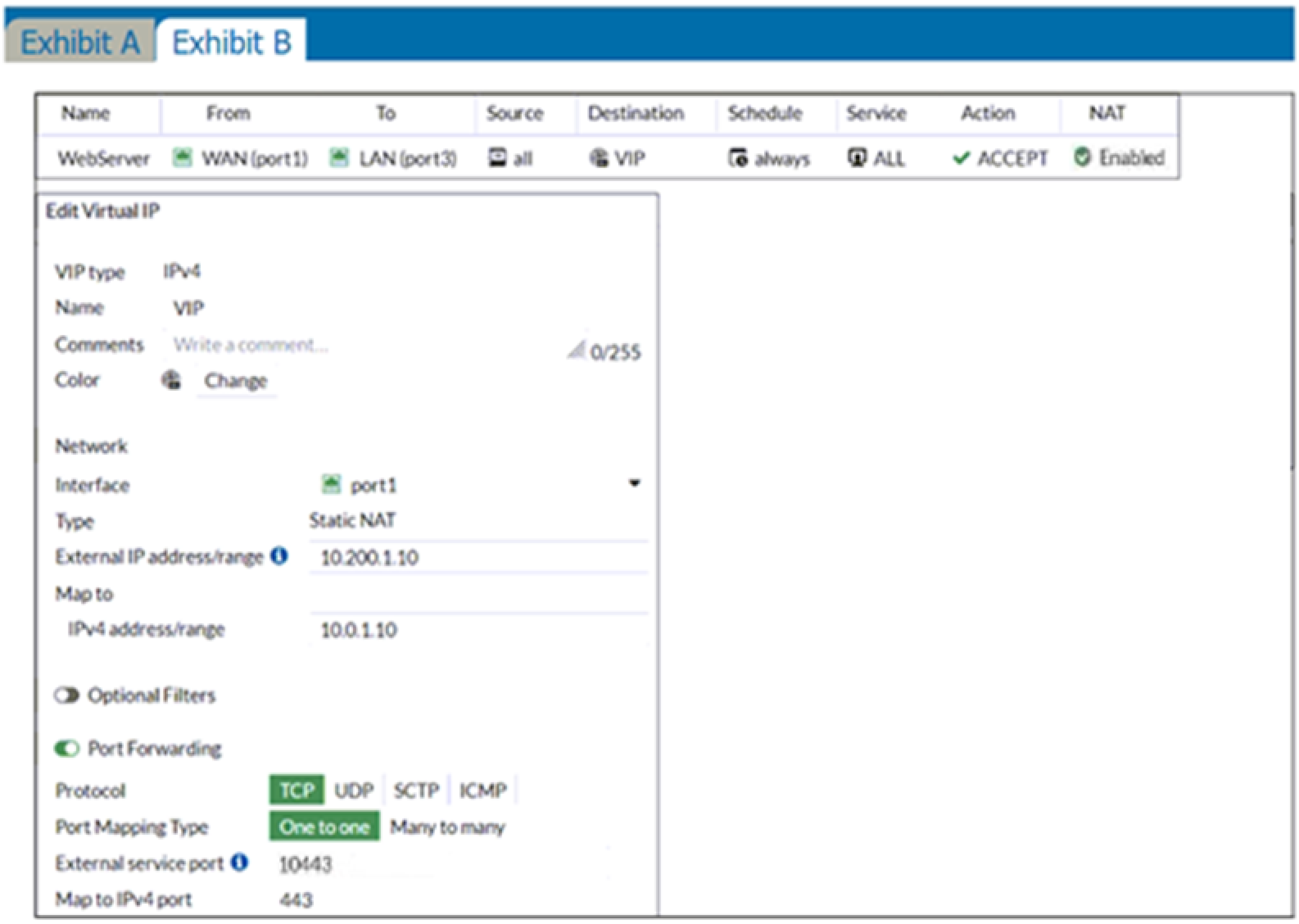
Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 61
Topic #: 1
[All NSE4_FGT-7.2 Questions]

Refer to the exhibits.

Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object 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.





Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	✓ ACCEPT	Enabled

Edit Virtual IP

VIP type IPv4
Name VIP
Comments Write a comment... 0/255
Color Change

Network
Interface port1
Type Static NAT
External IP address/range 10.200.1.10
Map to
IPv4 address/range 10.0.1.10

Optional Filters

Port Forwarding
Protocol **TCP** UDP SCTP ICMP
Port Mapping Type **One to one** Many to many
External service port 10443
Map to IPv4 port 443

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

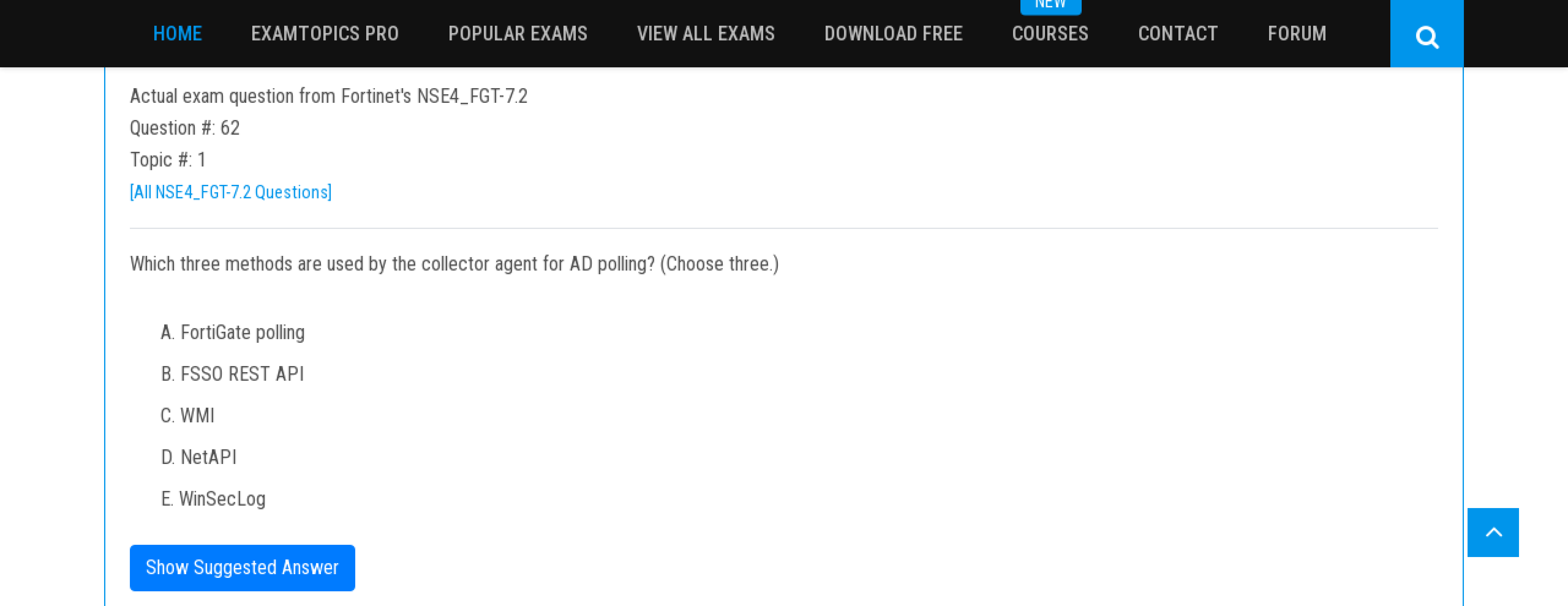
A. 10.0.1.254, 10.0.1.10, and 443, respectively

B. 10.0.1.254, 10.200.1.10, and 443, respectively

C. 10.200.3.1, 10.0.1.10, and 443, respectively

D. 10.0.1.254, 10.0.1.10, and 10443, respectively

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 62

Topic #: 1

[All NSE4_FGT-7.2 Questions]

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

A. FortiGate polling

B. FSSO REST API

C. WMI

D. NetAPI

E. WinSecLog

Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 63

Topic #: 1

[All NSE4_FGT-7.2 Questions]

What are two functions of the ZTNA rule? (Choose two.)

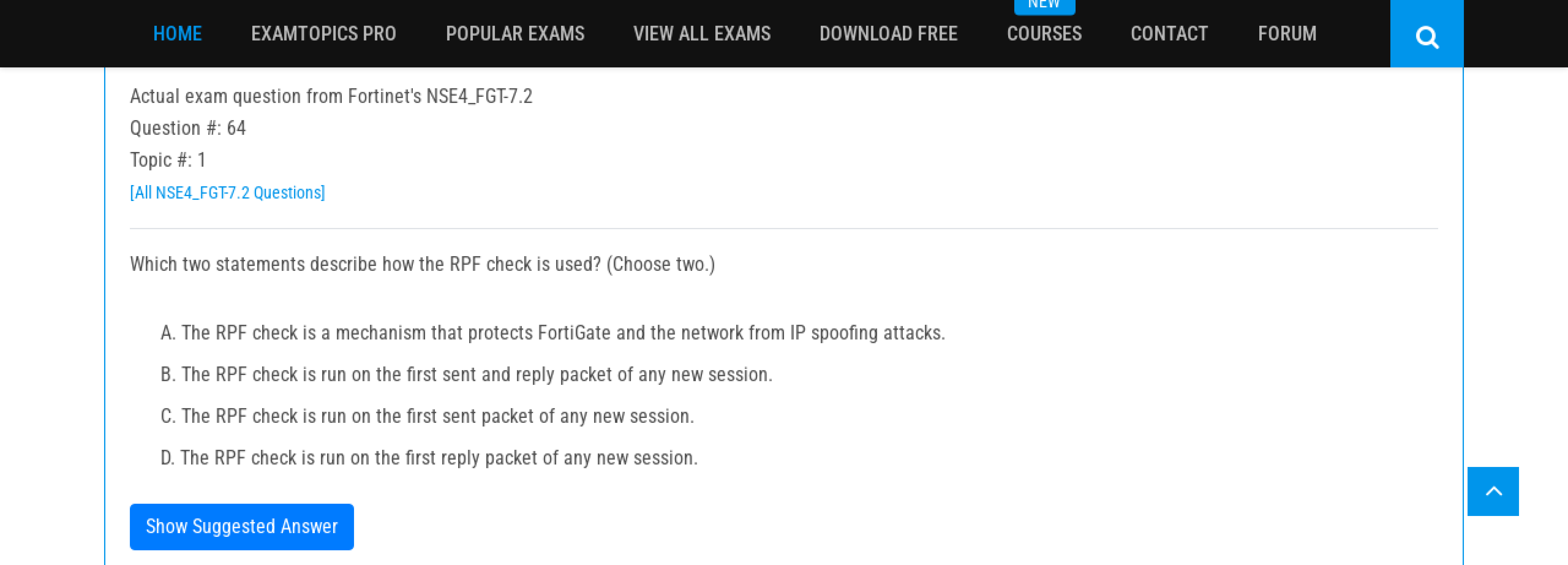
A. It redirects the client request to the access proxy.

B. It applies security profiles to protect traffic.

C. It defines the access proxy.

D. It enforces access control.

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 64

Topic #: 1

[All NSE4_FGT-7.2 Questions]

Which two statements describe how the RPF check is used? (Choose two.)

A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

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

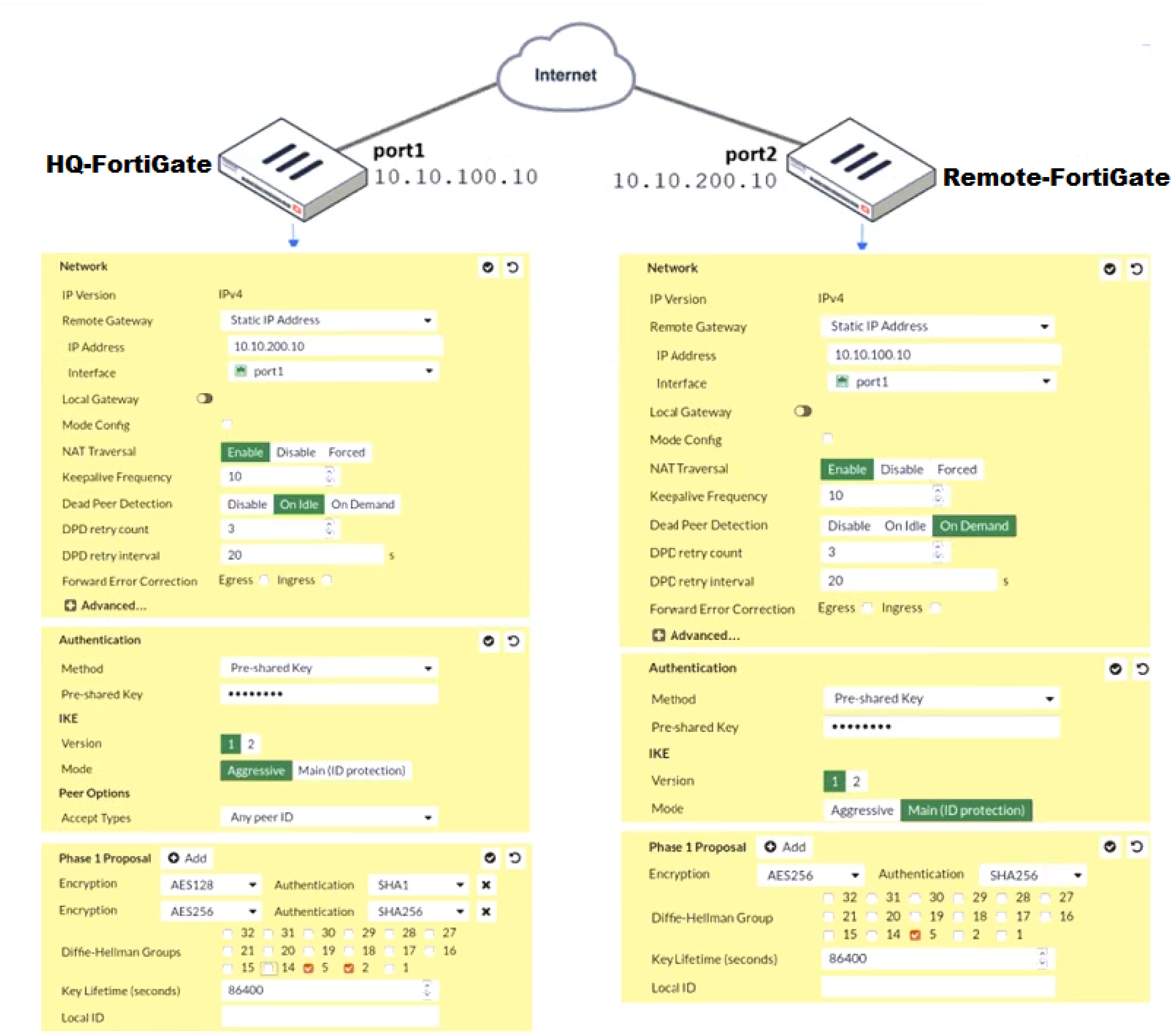
C. The RPF check is run on the first sent packet of any new session.

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

Actual exam question from Fortinet's NSE4_FGT-7.2
Question #: 65
Topic #: 1
[All NSE4_FGT-7.2 Questions]

Refer to the exhibit.

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 failed to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.



HQ-FortiGate

Network
IP Version: IPv4
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
DPD retry count: 3
DPD retry interval: 20 s
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 Groups: ☐ 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
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]
DPD retry count: 3
DPD retry interval: 20 s
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:

Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes can the administrator make to bring phase 1 up? (Choose two.)

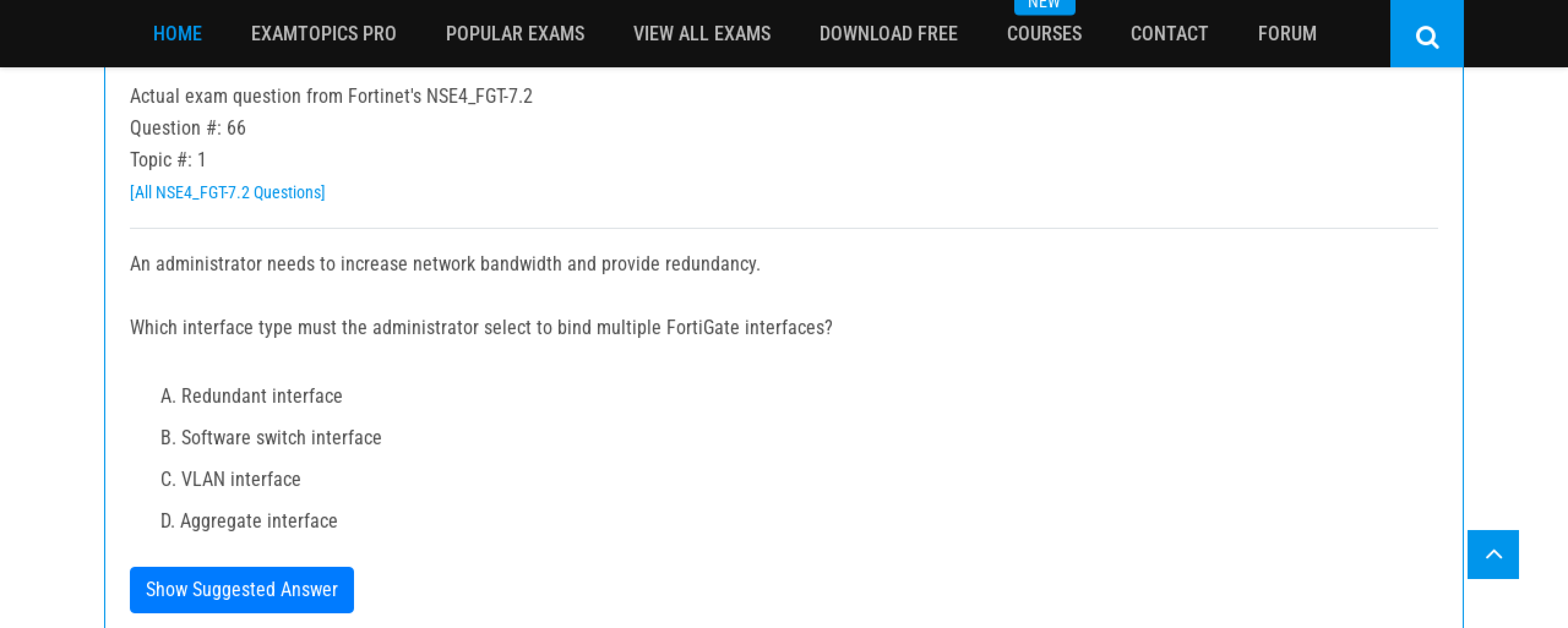
A. On both FortiGate devices, set Dead Peer Detection to On Demand.

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

C. On HO-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-7.2

Question #: 66

Topic #: 1

[All NSE4_FGT-7.2 Questions]

An administrator needs to increase network bandwidth and provide redundancy.

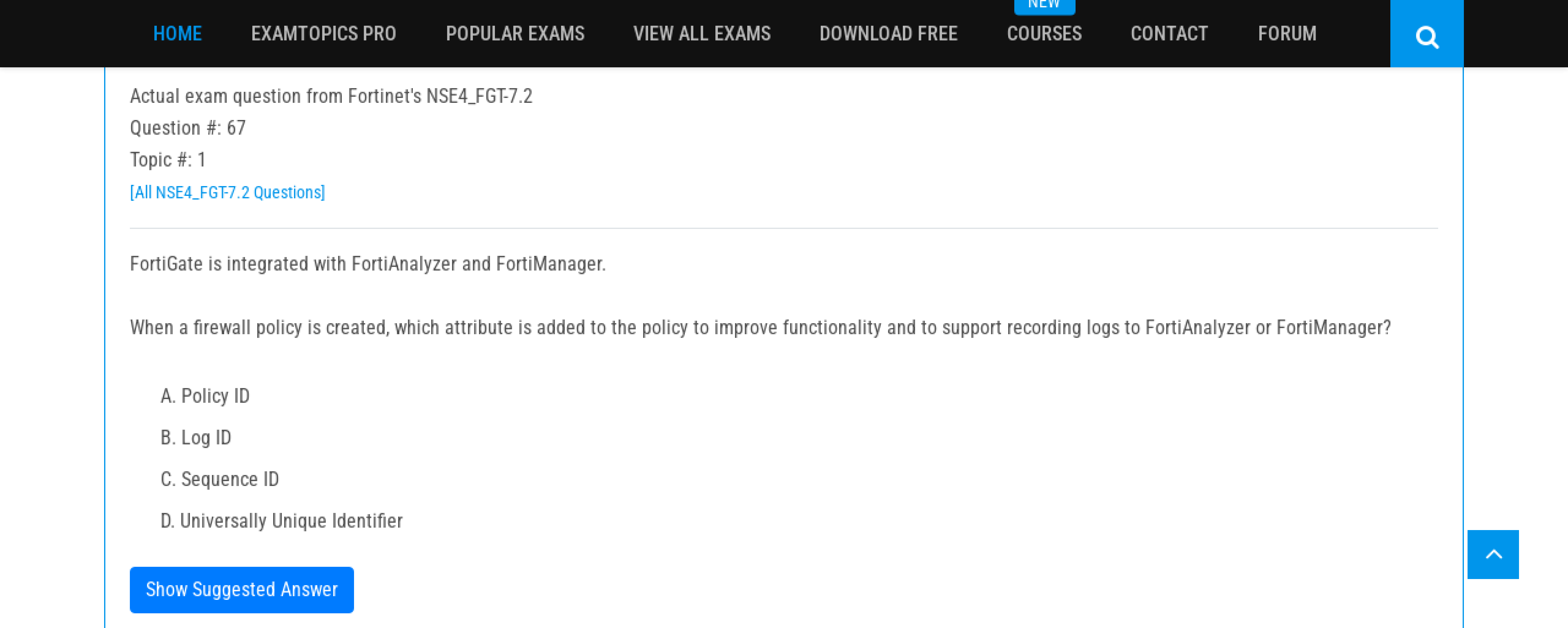
Which interface type must the administrator select to bind multiple FortiGate interfaces?

A. Redundant interface

B. Software switch interface

C. VLAN interface

D. Aggregate interface



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 67

Topic #: 1

[All NSE4_FGT-7.2 Questions]

FortiGate is integrated with FortiAnalyzer and FortiManager.

When a firewall policy is created, which attribute is added to the policy to improve functionality and to support recording logs to FortiAnalyzer or FortiManager?

A. Policy ID

B. Log ID

C. Sequence ID

D. Universally Unique Identifier

Actual exam question from Fortinet's NSE4_FGT-7.2

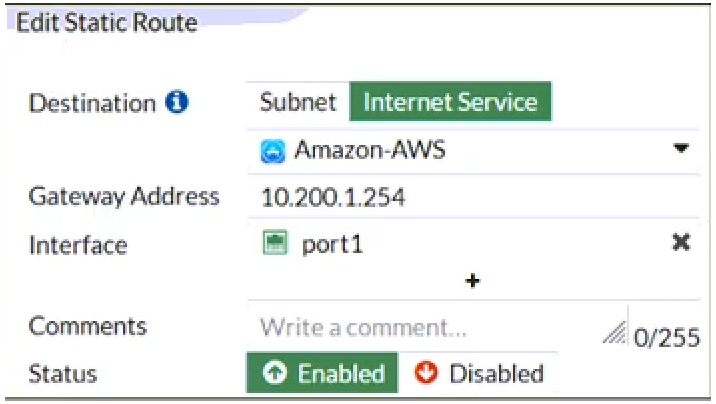
Question #: 68

Topic #: 1

[All NSE4_FGT-7.2 Questions]

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

An administrator created a static route for Amazon Web Services.



Edit Static Route

Destination	Subnet / Internet Service (selected)
	Amazon-AWS
Gateway Address	10.200.1.254
Interface	port1
Comments	Write a comment... 0/255
Status	Enabled (selected) / Disabled

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

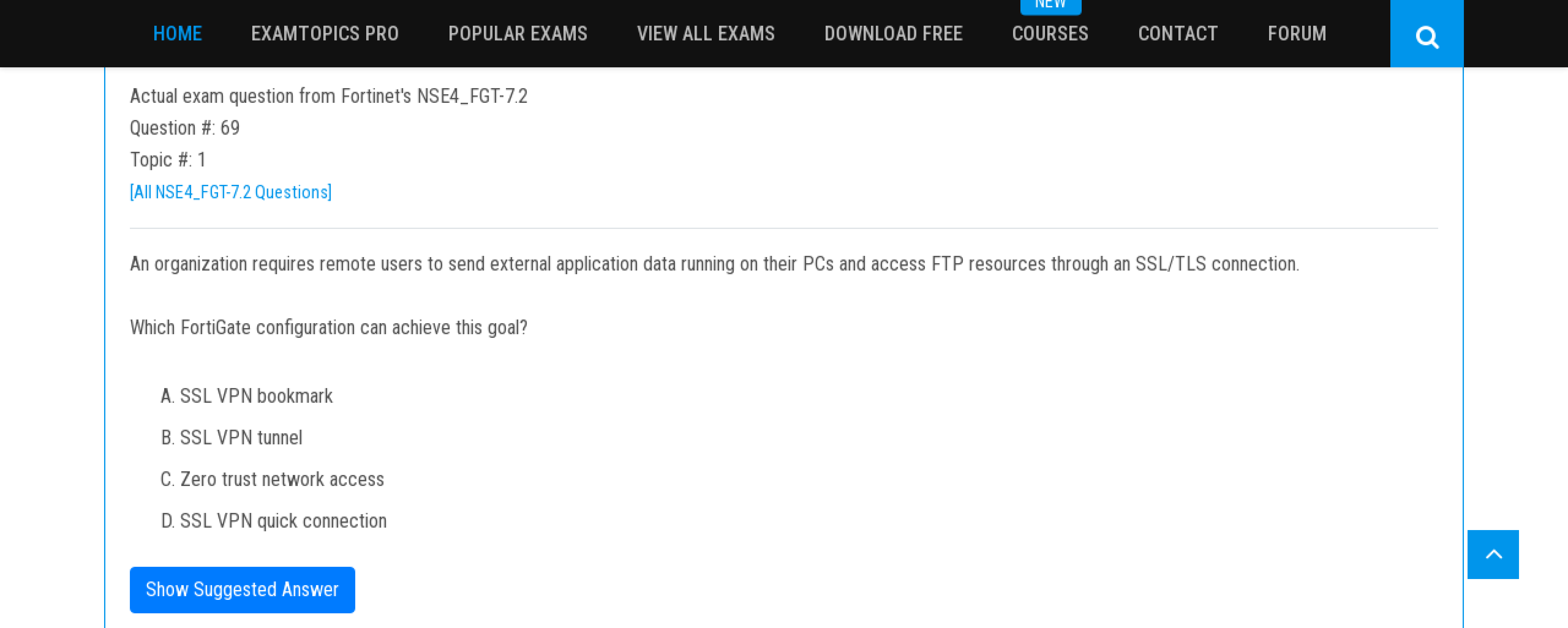
A. get router info routing-table database

B. diagnose firewall route list

C. get internet-service route list

D. get router info routing-table all

Show Suggested Answer



Actual exam question from Fortinet's NSE4_FGT-7.2

Question #: 69

Topic #: 1

[All NSE4_FGT-7.2 Questions]

An organization requires remote users to send external application data running on their PCs and access FTP resources through an SSL/TLS connection.

Which FortiGate configuration can achieve this goal?

A. SSL VPN bookmark

B. SSL VPN tunnel

C. Zero trust network access

D. SSL VPN quick connection

Show Suggested Answer