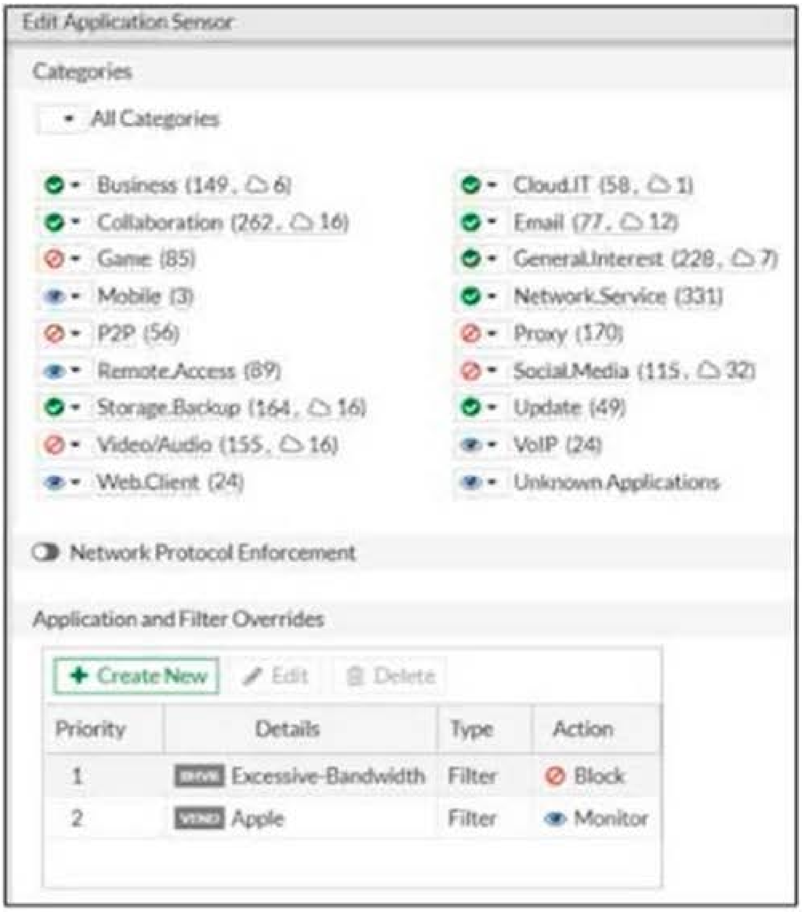
NSE4_FGT-7.2$^{\text{Q\&As}}$

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

QUESTION 1

Refer to the exhibit to view the application control profile.



Edit Application Sensor

Categories

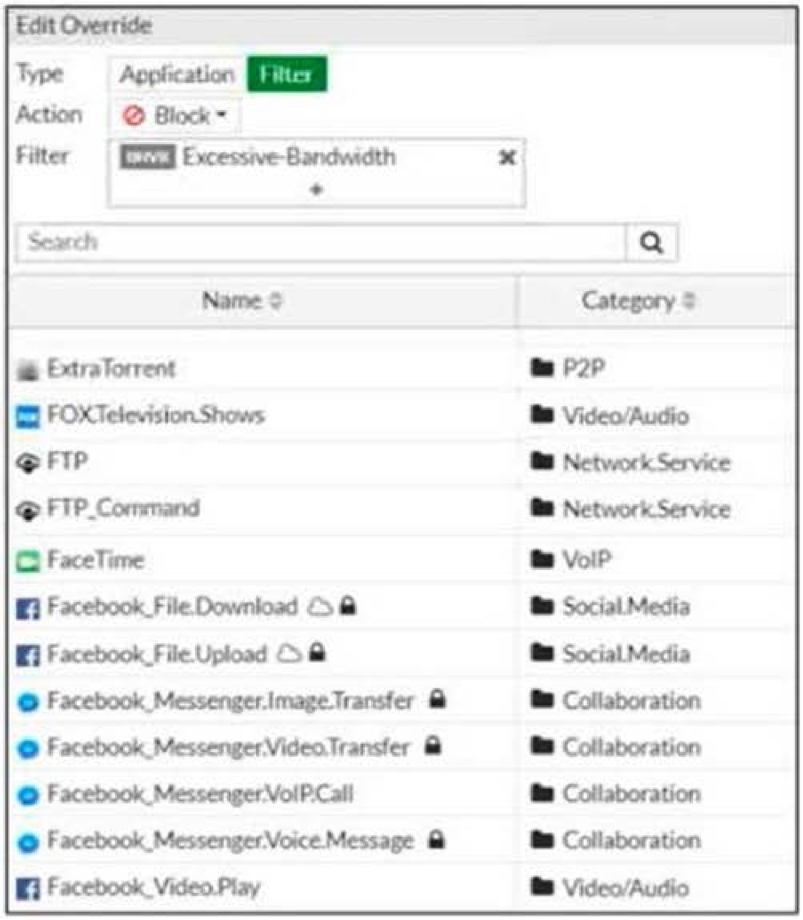
All Categories

✓	Business (149, ☁ 6)	✓	Cloud.IT (58, ☁ 1)
✓	Collaboration (262, ☁ 16)	✓	Email (77, ☁ 12)
⊘	Game (85)	✓	General.Interest (228, ☁ 7)
👁	Mobile (3)	✓	Network.Service (331)
⊘	P2P (56)	⊘	Proxy (170)
👁	Remote.Access (89)	⊘	Social.Media (115, ☁ 32)
✓	Storage.Backup (164, ☁ 16)	✓	Update (49)
⊘	Video/Audio (155, ☁ 16)	👁	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



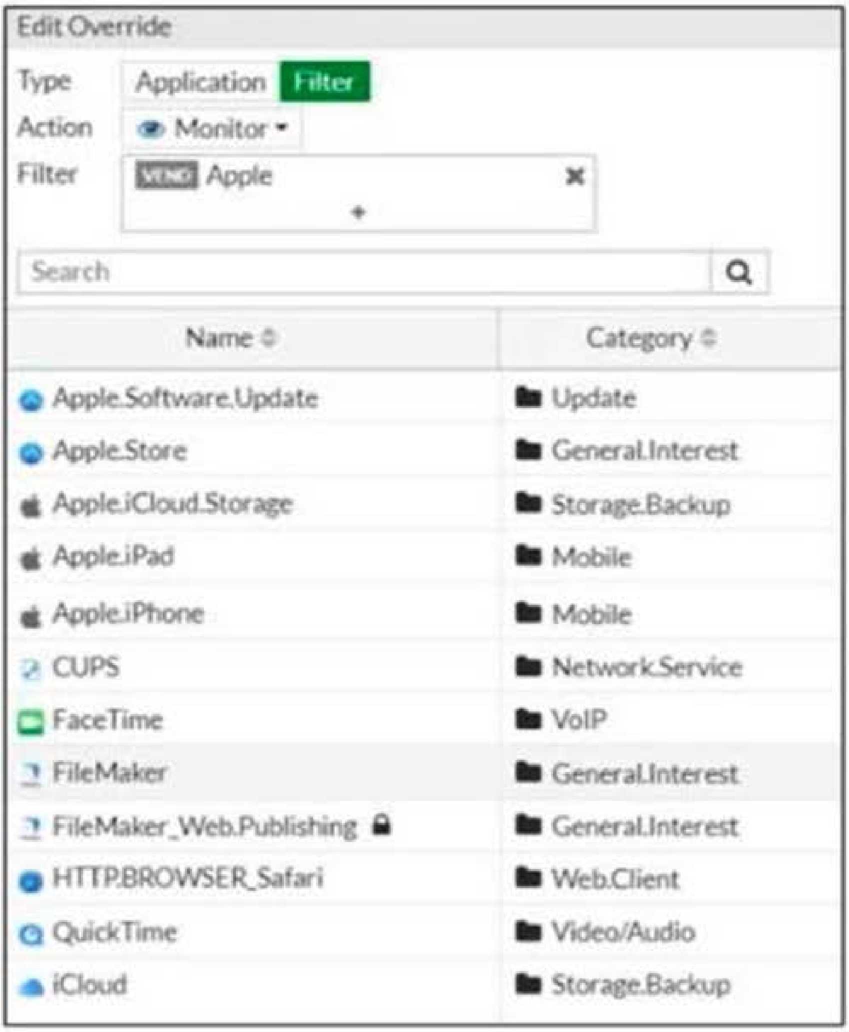
Edit Override

Type: Application **Filter**

Action: ⊘ Block

Filter: BHVR Excessive-Bandwidth ✖

Name	Category
ExtraTorrent	P2P
FOXTelevision.Shows	Video/Audio
FTP	Network.Service
FTP_Command	Network.Service
FaceTime	VoIP
Facebook_File.Download ☁ 🔒	Social.Media
Facebook_File.Upload ☁ 🔒	Social.Media
Facebook_Messenger.Image.Transfer 🔒	Collaboration
Facebook_Messenger.Video.Transfer 🔒	Collaboration
Facebook_Messenger.VoIP.Call	Collaboration
Facebook_Messenger.Voice.Message 🔒	Collaboration
Facebook_Video.Play	Video/Audio

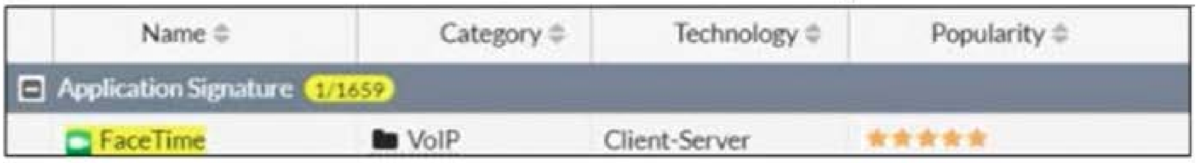


Edit Override

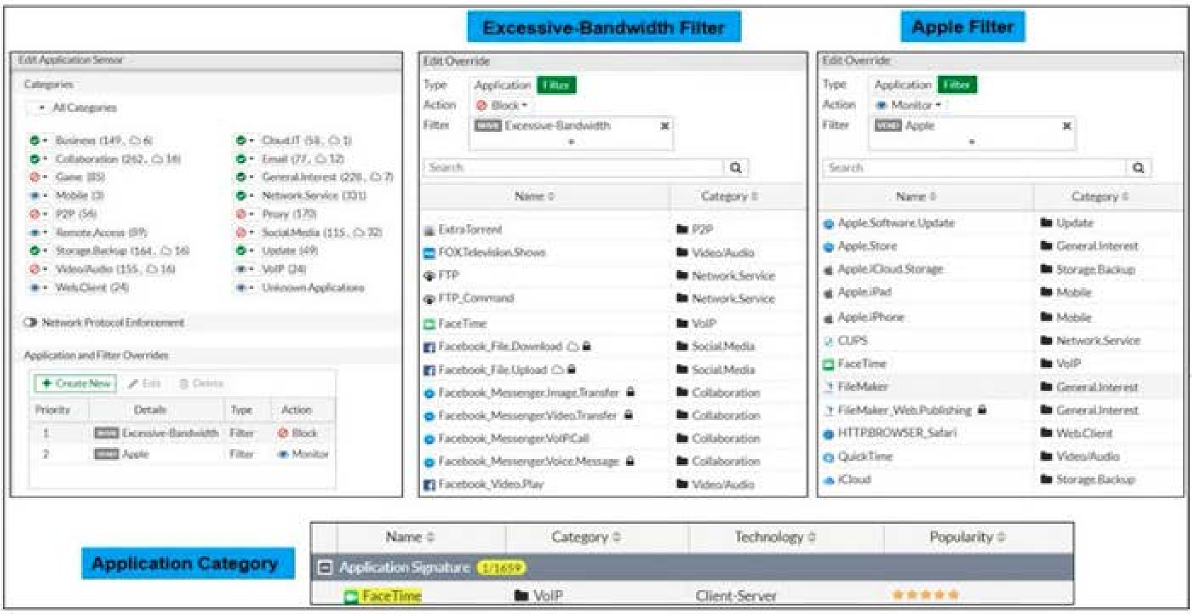
Type: Application **Filter**
Action: Monitor ▾
Filter: VENDOR Apple ✖ +

Search

Name	Category
Apple.Software.Update	Update
Apple.Store	General.Interest
Apple.iCloud.Storage	Storage.Backup
Apple.iPad	Mobile
Apple.iPhone	Mobile
CUPS	Network.Service
FaceTime	VoIP
FileMaker	General.Interest
FileMaker_Web.Publishing 🔒	General.Interest
HTTP.BROWSER_Safari	Web.Client
QuickTime	Video/Audio
iCloud	Storage.Backup



Name	Category	Technology	Popularity
Application Signature 1/1659			
FaceTime	VoIP	Client-Server	★★★★★



Edit Application Sensor

Categories

All Categories

Business (149, ☁ 6)	Cloud.IT (58, ☁ 1)
Collaboration (262, ☁ 18)	Email (77, ☁ 12)
Game (85)	General.Interest (228, ☁ 7)
Mobile (3)	Network.Service (331)
P2P (56)	Proxy (170)
Remote.Access (89)	Social.Media (115, ☁ 32)
Storage.Backup (164, ☁ 16)	Update (49)
Video/Audio (155, ☁ 16)	VoIP (24)
Web.Client (24)	Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New | Edit | Delete

Priority	Details	Type	Action
1	VENDOR Excessive-Bandwidth	Filter	Block
2	VENDOR Apple	Filter	Monitor

Application Category

Excessive-Bandwidth Filter

Edit Override

Type: Application **Filter**
Action: Block ▾
Filter: VENDOR Excessive-Bandwidth ✖ +

Search

Name	Category
ExtraTorrent	P2P
FOXTelevision.Shows	Video/Audio
FTP	Network.Service
FTP_Command	Network.Service
FaceTime	VoIP
Facebook_File.Download ☁ 🔒	Social.Media
Facebook_File.Upload ☁ 🔒	Social.Media
Facebook_Messenger.Image.Transfer 🔒	Collaboration
Facebook_Messenger.Video.Transfer 🔒	Collaboration
Facebook_Messenger.VoIP.Call	Collaboration
Facebook_Messenger.Voice.Message 🔒	Collaboration
Facebook_Video.Play	Video/Audio

Apple Filter

Edit Override

Type: Application **Filter**
Action: Monitor ▾
Filter: VENDOR Apple ✖ +

Search

Name	Category
Apple.Software.Update	Update
Apple.Store	General.Interest
Apple.iCloud.Storage	Storage.Backup
Apple.iPad	Mobile
Apple.iPhone	Mobile
CUPS	Network.Service
FaceTime	VoIP
FileMaker	General.Interest
FileMaker_Web.Publishing 🔒	General.Interest
HTTP.BROWSER_Safari	Web.Client
QuickTime	Video/Audio
iCloud	Storage.Backup

Name	Category	Technology	Popularity
Application Signature 1/1659			
FaceTime	VoIP	Client-Server	★★★★★

Based on the configuration, what will happen to Apple FaceTime?

A. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration

B. Apple FaceTime will be allowed, based on the Apple filter configuration.

C. Apple FaceTime will be allowed only if the filter in Application and Filter Overrides is set to Learn

D. Apple FaceTime will be allowed, based on the Categories configuration.

Correct Answer: A

QUESTION 2

In an explicit proxy setup, where is the authentication method and database configured?

A. Proxy Policy

B. Authentication Rule

C. Firewall Policy

D. Authentication scheme

Correct Answer: D

QUESTION 3

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 the above requirement?

A. Disabled

B. On Demand

C. Enabled

D. On Idle

Correct Answer: D

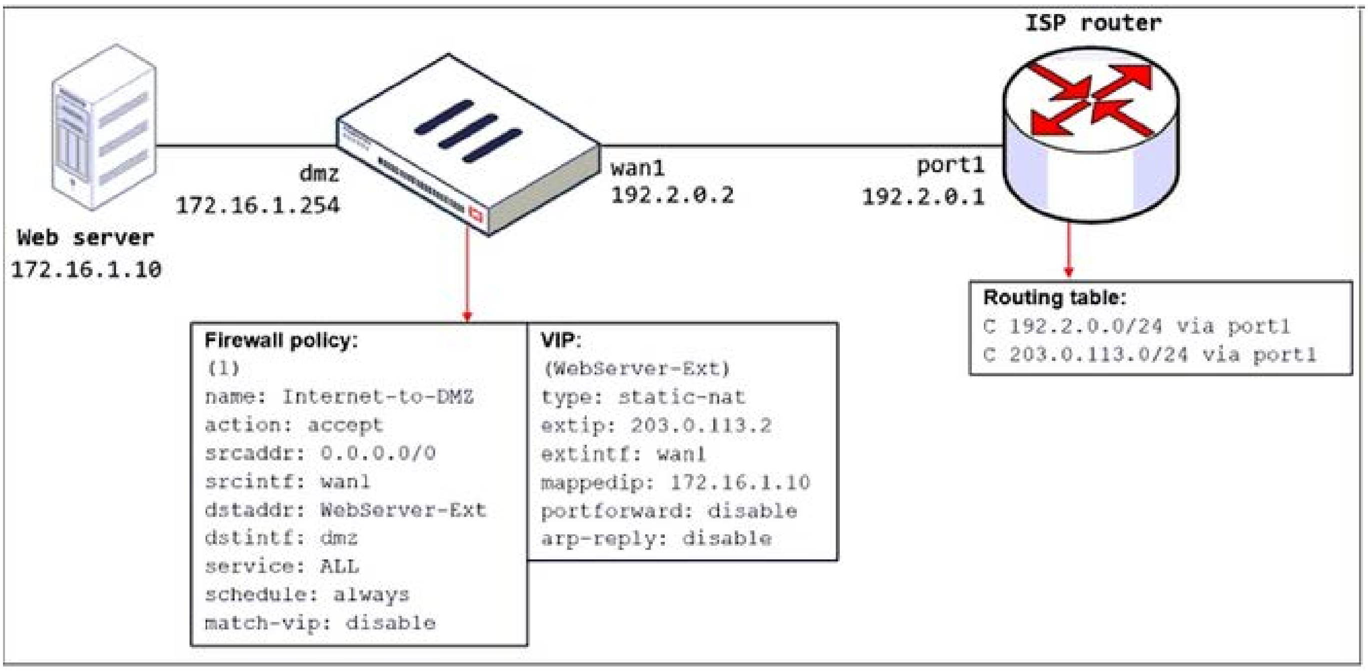
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD40813

QUESTION 4

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.



```
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
```

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

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.

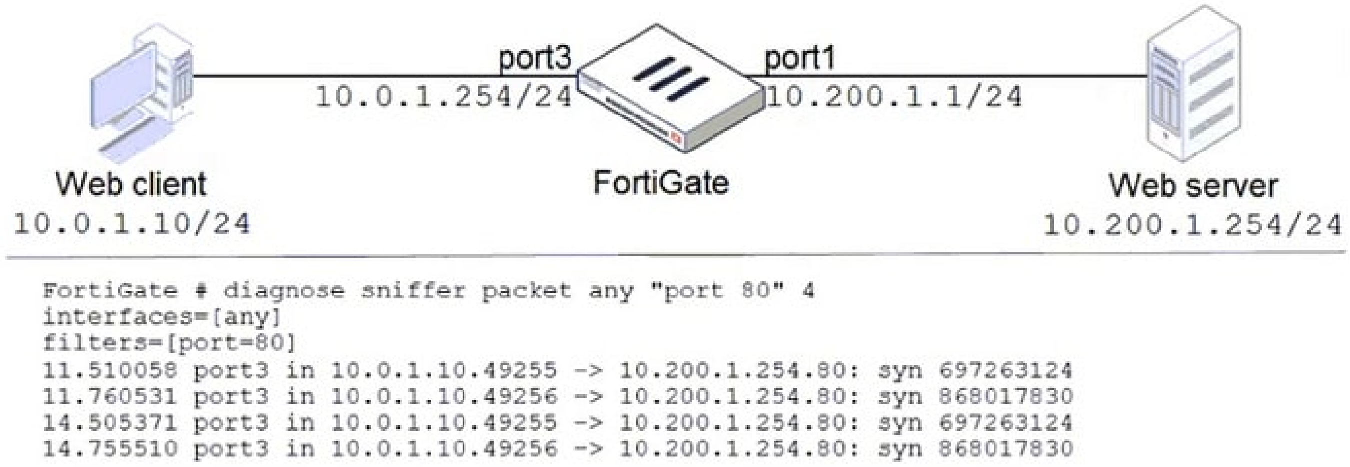
Correct Answer: B

FortiGate Security 7.2 Study Guide (p.115): "Enabling ARP reply is usually not required in most networks because the routing tables on the adjacent devices contain the correct next hop information, so the networks are reachable. However, sometimes the routing configuration is not fully correct, and having ARP reply enabled can solve the issue for you. For this reason, it\\'s a best practice to keep ARP reply enabled."

QUESTION 5

Refer to the exhibit.

In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit.



```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port=80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
14.755510 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
```

What should the administrator do next, to troubleshoot the problem?

A. Execute a debug flow.

B. Capture the traffic using an external sniffer connected to port1.

C. Execute another sniffer on FortiGate, this time with the filter "host 10.0.1.10".

D. Run a sniffer on the web server.

Correct Answer: A

QUESTION 6

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. 1.0/24

B. 192. 168.0.0/24

C. 192. 168.2.0/24

D. 192. 168.3.0/24

Correct Answer: C

For an IPsec VPN between site A and site B, the administrator has configured the local quick mode selector for site A as 192.168.1.0/24 and the remote quick mode selector as 192.168.2.0/24. This means that the VPN will allow traffic to and from the 192.168.1.0/24 subnet at site A to reach the 192.168.2.0/24 subnet at site B.

To complete the configuration, the administrator must configure the local quick mode selector for site B. To do this, the administrator must use the same subnet as the remote quick mode selector for site A, which is 192.168.2.0/24. This will allow traffic to and from the 192.168.2.0/24 subnet at site B to reach the 192.168.1.0/24 subnet at site A.

Therefore, the administrator must configure the local quick mode selector for site B as 192.168.2.0/24.

QUESTION 7

An administrator has a requirement to keep an application session from timing out on port 80.

What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)

A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.

B. Create a new service object for HTTP service and set the session TTL to never

C. Set the TTL value to never under config system-ttl

D. Set the session TTL on the HTTP policy to maximum

Correct Answer: BC

QUESTION 8

An administrator is running the following sniffer command:

Which three pieces of Information will be Included in me sniffer output? {Choose three.)

A. Interface name

B. Packet payload

C. Ethernet header

D. IP header

E. Application header

Correct Answer: ABD

QUESTION 9

Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

A. To detect intermediary NAT devices in the tunnel path.

B. To dynamically change phase 1 negotiation mode aggressive mode.

C. To encapsulation ESP packets in UDP packets using port 4500.

D. To force a new DH exchange with each phase 2 rekey.

Correct Answer: AC

QUESTION 10

The IPS engine is used by which three security features? (Choose three.)

A. Antivirus in flow-based inspection

B. Web filter in flow-based inspection

C. Application control

D. DNS filter

E. Web application firewall

Correct Answer: ABC

FortiGate Security 7.2 Study Guide (p.385): "The IPS engine is responsible for most of the features shown in this lesson: IPS and protocol decoders. It\\'s also responsible for application control, flow-based antivirus protection, web filtering, and email filtering."

QUESTION 11

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

A. Warning

B. Exempt

C. Allow

D. Learn

Correct Answer: AC

QUESTION 12

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.

B. Only secondary FortiGate devices are rebooted.

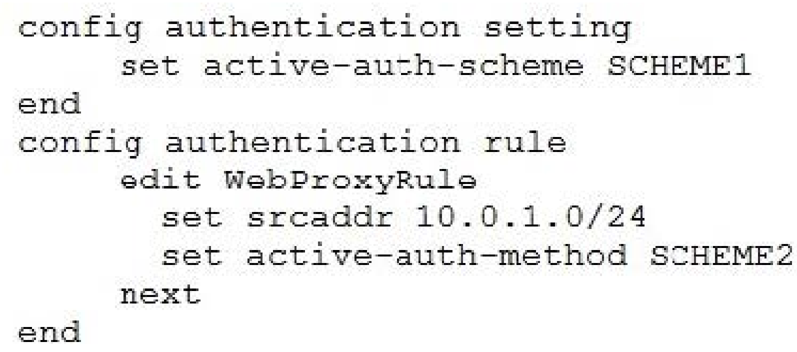
C. Uninterruptable upgrade is enabled by default.

D. Traffic load balancing is temporally disabled while upgrading the firmware.

Correct Answer: CD

QUESTION 13

Examine this FortiGate configuration: How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?



```
config authentication setting
     set active-auth-scheme SCHEME1
end
config authentication rule
     edit WebProxyRule
       set srcaddr 10.0.1.0/24
       set active-auth-method SCHEME2
     next
end
```

A. It always authorizes the traffic without requiring authentication.

B. It drops the traffic.

C. It authenticates the traffic using the authentication scheme SCHEME2.

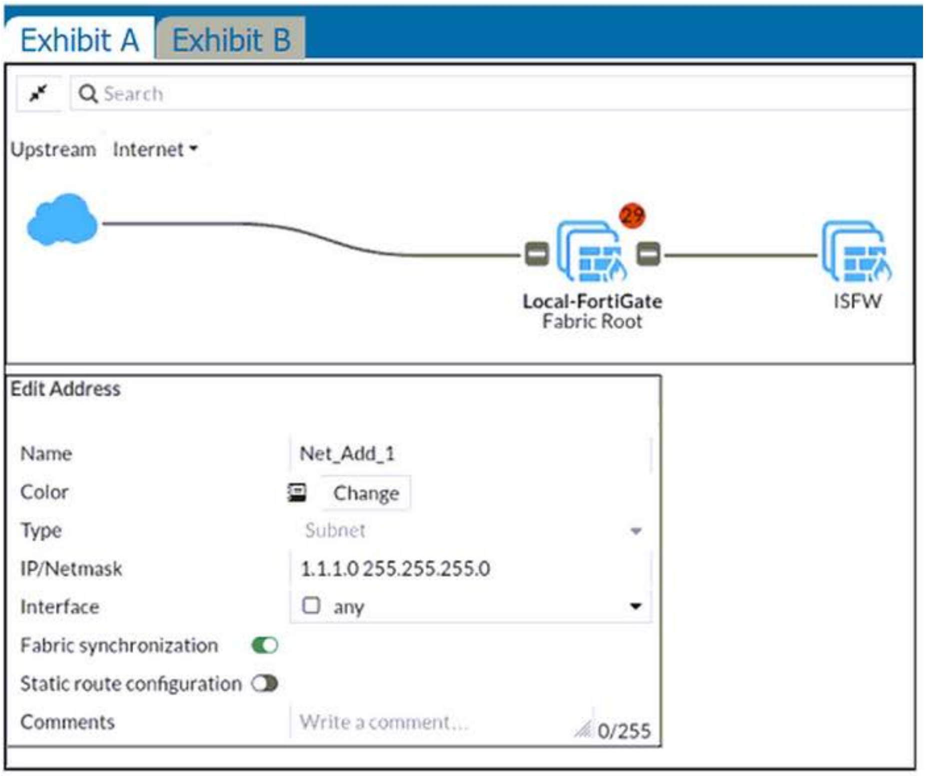
D. It authenticates the traffic using the authentication scheme SCHEME1.

Correct Answer: D

"What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting"

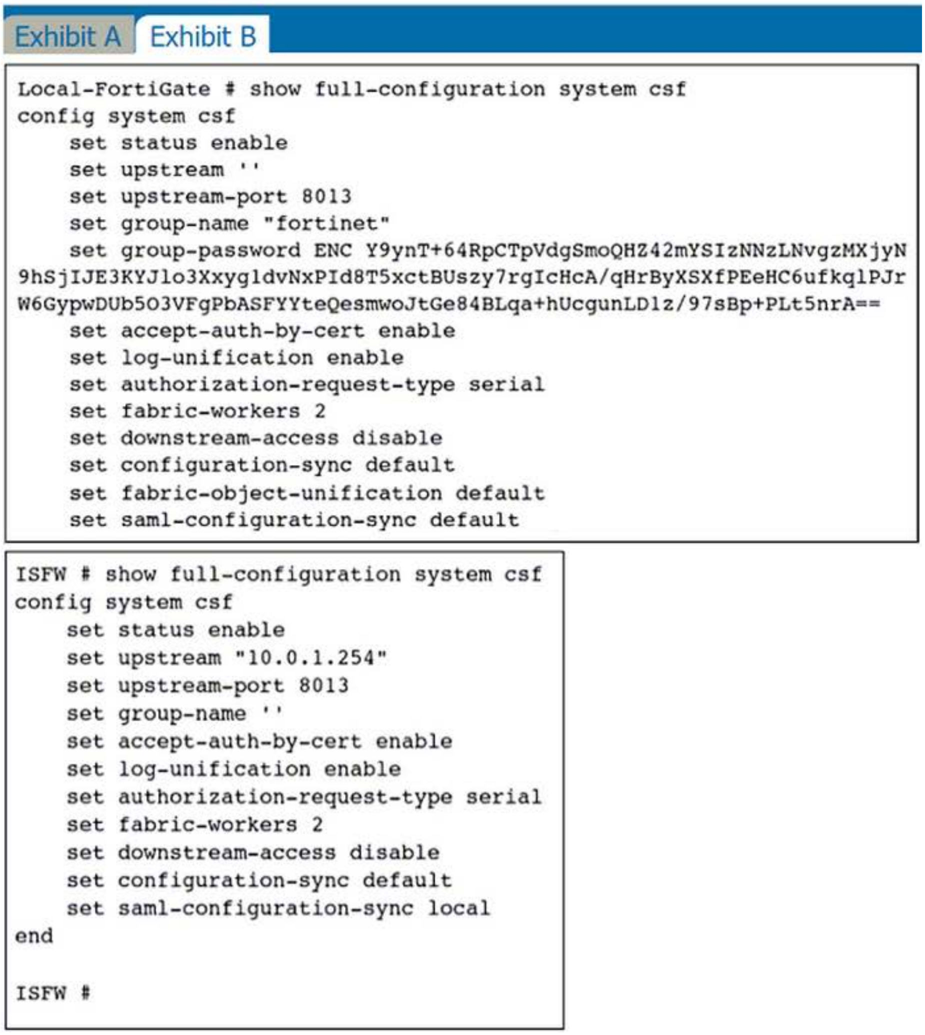
QUESTION 14

Refer to the exhibits.



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
9hSjIJE3KYJlo3Xxygl dvNxPId8T5xctBUszy7rgIcHcA/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 #
```

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). 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.

Correct Answer: C

Reference: https://docs.fortinet.com/document/fortigate/6.4.5/administration-guide/880913/synchronizing-objects-across-the-security-fabric

QUESTION 15

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

Correct Answer: AC