NSE4_FGT-7.0$^{Q\&As}$

Fortinet NSE 4 - FortiOS 7.0

Pass Fortinet NSE4_FGT-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

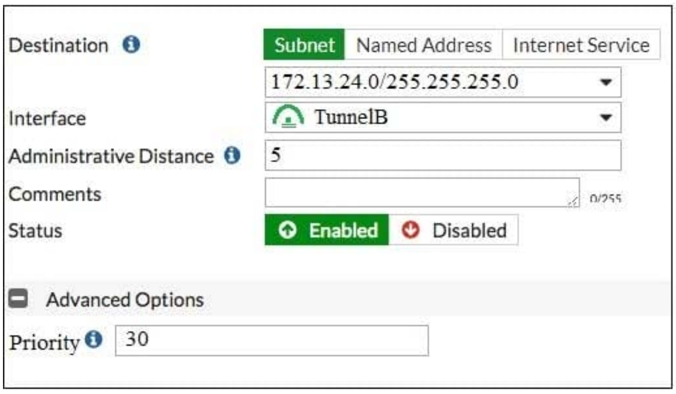
https://www.pass2lead.com/nse4_fgt-7-0.html

100% Passing Guarantee
100% Money Back Assurance

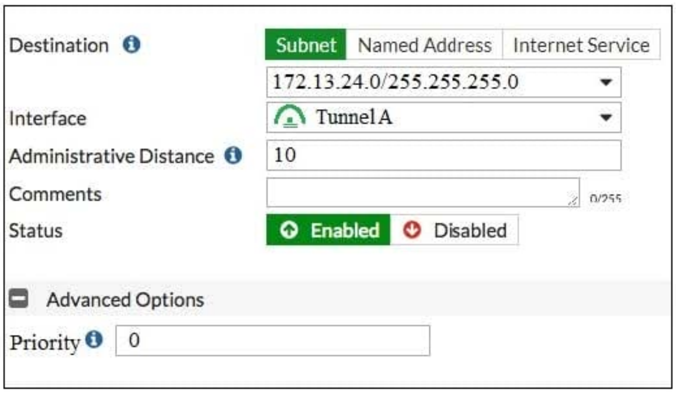
Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

View the exhibit.



Destination: Subnet | Named Address | Internet Service
172.13.24.0/255.255.255.0
Interface: TunnelB
Administrative Distance: 5
Comments: 0/255
Status: Enabled | Disabled
Advanced Options
Priority: 30



Destination: Subnet | Named Address | Internet Service
172.13.24.0/255.255.255.0
Interface: Tunnel A
Administrative Distance: 10
Comments: 0/255
Status: Enabled | Disabled
Advanced Options
Priority: 0

Which of the following statements are correct? (Choose two.)

A. This setup requires at least two firewall policies with the action set to IPsec.

B. Dead peer detection must be disabled to support this type of IPsec setup.

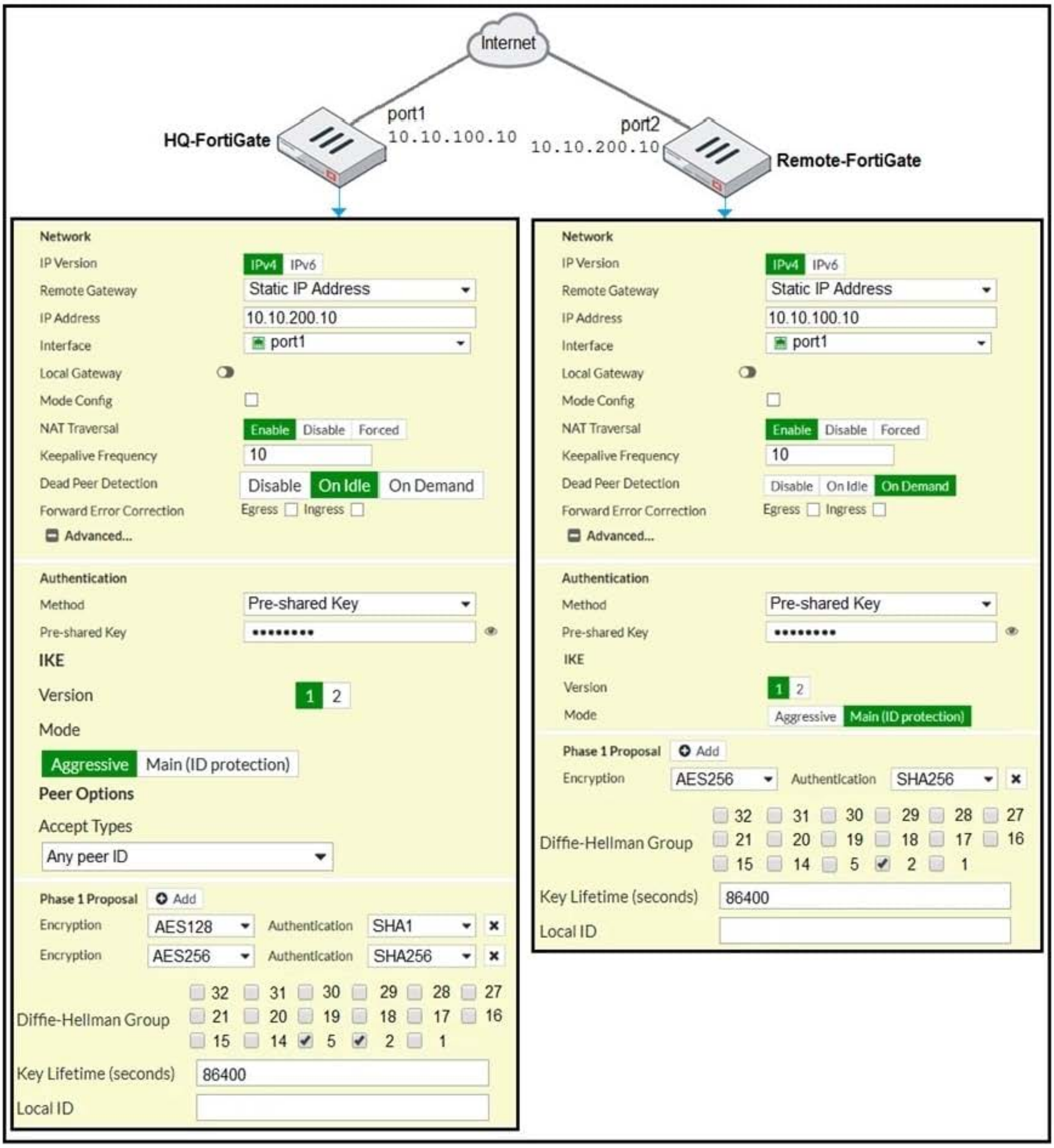
C. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.

D. This is a redundant IPsec setup.

Correct Answer: CD

QUESTION 2

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 preshared 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.

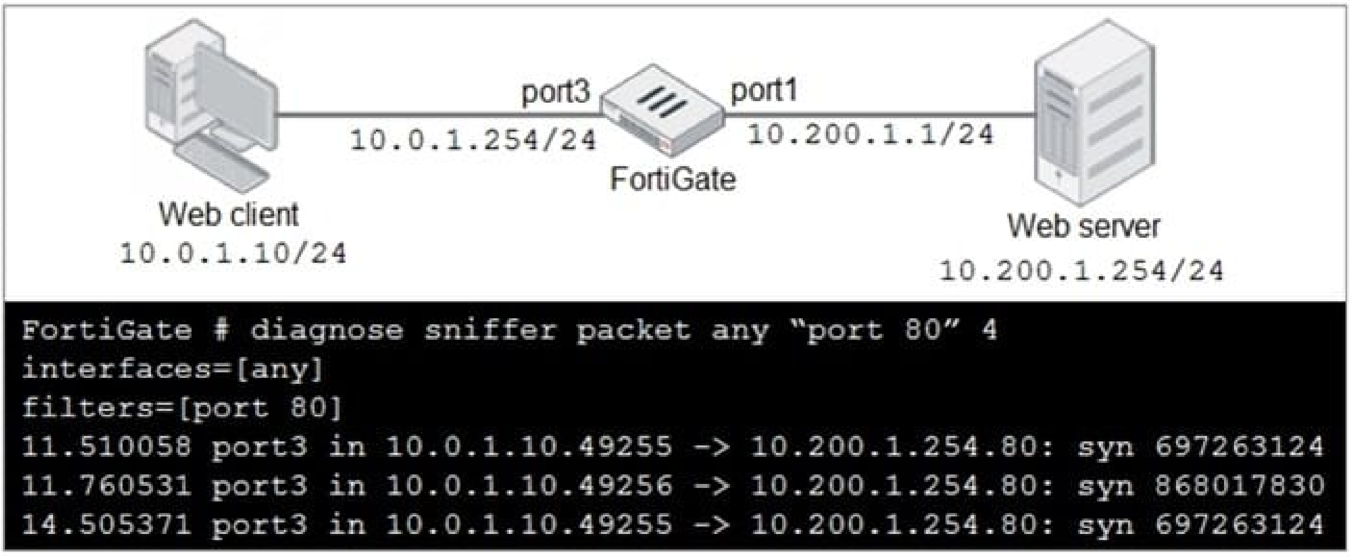
C. On HQ-FortiGate, disable Diffie-Helman group 2.

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

Correct Answer: AD

QUESTION 3

Refer to 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
```

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 as shown in the exhibit.

What should the administrator do next to troubleshoot the problem?

A. Run a sniffer on the web server.

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

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

D. Execute a debug flow.

Correct Answer: D

QUESTION 4

Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

A. FortiGate points the collector agent to use a remote LDAP server.

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

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

D. FortiGate queries AD by using the LDAP to retrieve user group information.

Correct Answer: CD

Fortigate Infrastructure 7.0 Study Guide P.272-273 https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732

QUESTION 5

Which downstream FortiGate VDOM is used to join the Security Fabric when split-task VDOM is enabled on all FortiGate devices?

A. Root VDOM

B. FG-traffic VDOM

C. Customer VDOM

D. Global VDOM

Correct Answer: A

QUESTION 6

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.

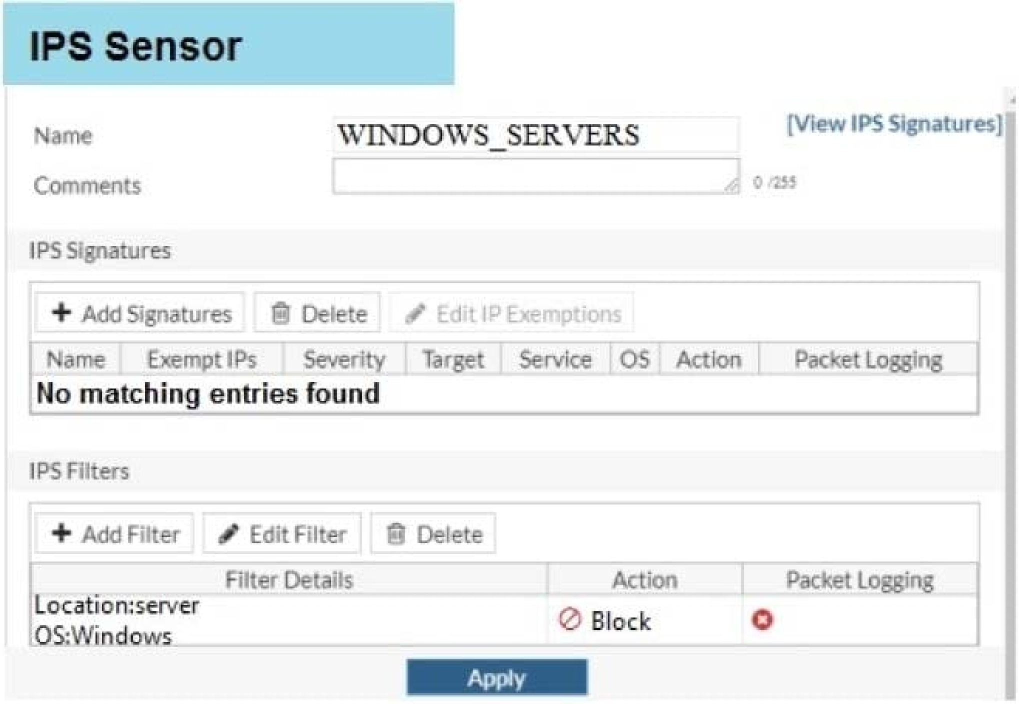
D. SLA targets are used only when referenced by an SD-WAN rule.

Correct Answer: BD

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-sla-sla-targets

QUESTION 7

Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.



Name WINDOWS_SERVERS

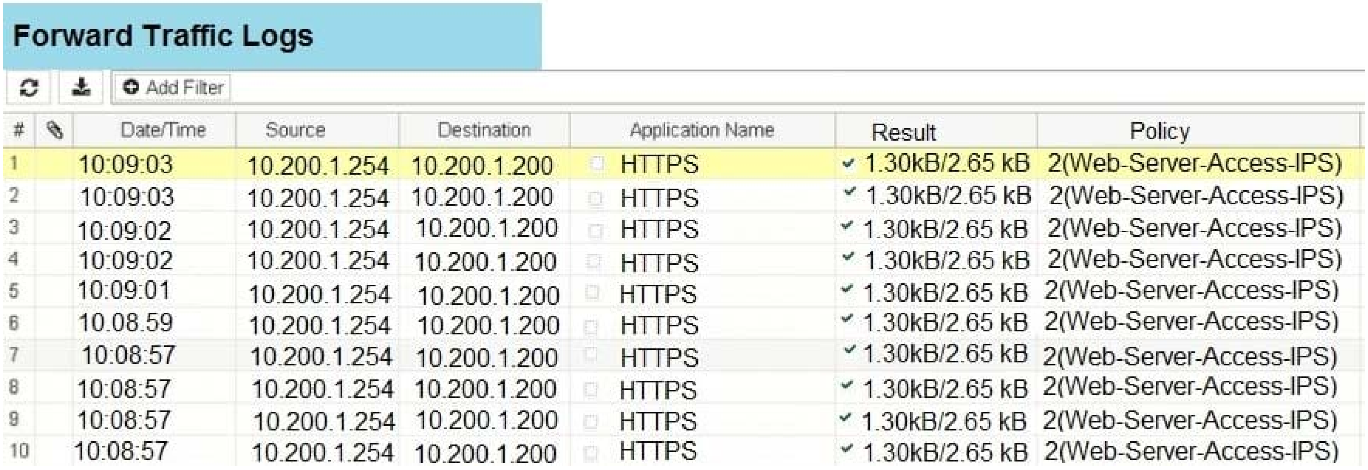
Comments 0 /255

IPS Signatures

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

IPS Filters

Filter Details	Action	Packet Logging
Location:server OS:Windows	⊘ Block	●



#		Date/Time	Source	Destination	Application Name	Result	Policy
1		10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
2		10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
3		10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
4		10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
5		10:09:01	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
6		10.08.59	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
7		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
8		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
9		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
10		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)

An administrator has configured the WINDOWS_SERVERS IPS sensor in an attempt to determine whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic.

What is a possible reason for this?

A. The IPS filter is missing the Protocol: HTTPS option.

B. The HTTPS signatures have not been added to the sensor.

C. A DoS policy should be used, instead of an IPS sensor.

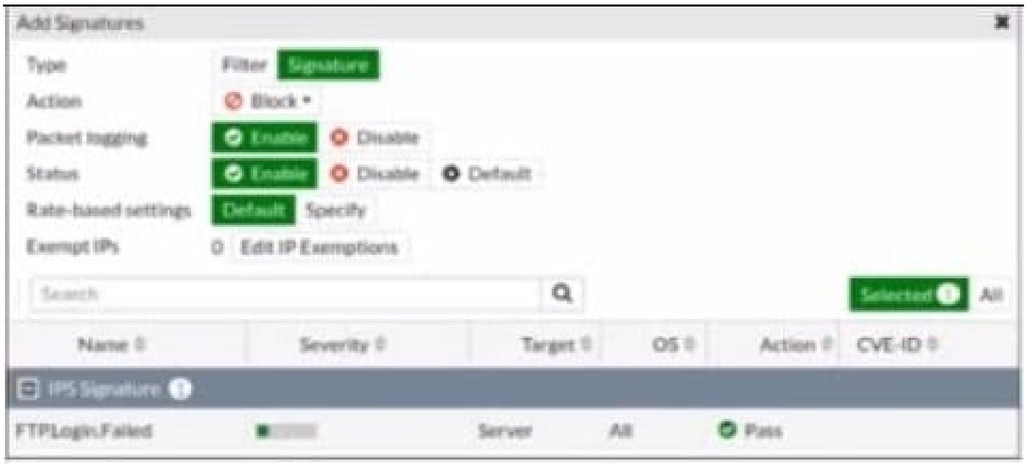
D. A DoS policy should be used, instead of an IPS sensor.

E. The firewall policy is not using a full SSL inspection profile.

Correct Answer: E

QUESTION 8

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

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. The signature setting uses a custom rating threshold.

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

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

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

Correct Answer: D

Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

QUESTION 9

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

B. To finish any inspection operations

C. To remove the NAT operation

D. To generate logs

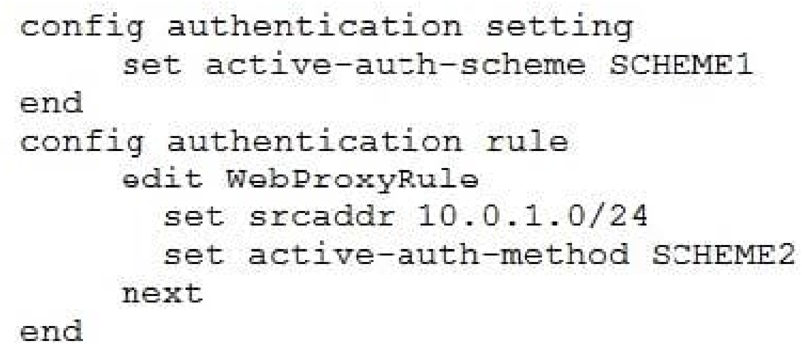
Correct Answer: A

TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an

entry in the firewall session table.

QUESTION 10

Examine this FortiGate configuration:



```
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
```

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

A. It always authorizes the traffic without requiring authentication.

B. It drops the traffic.

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

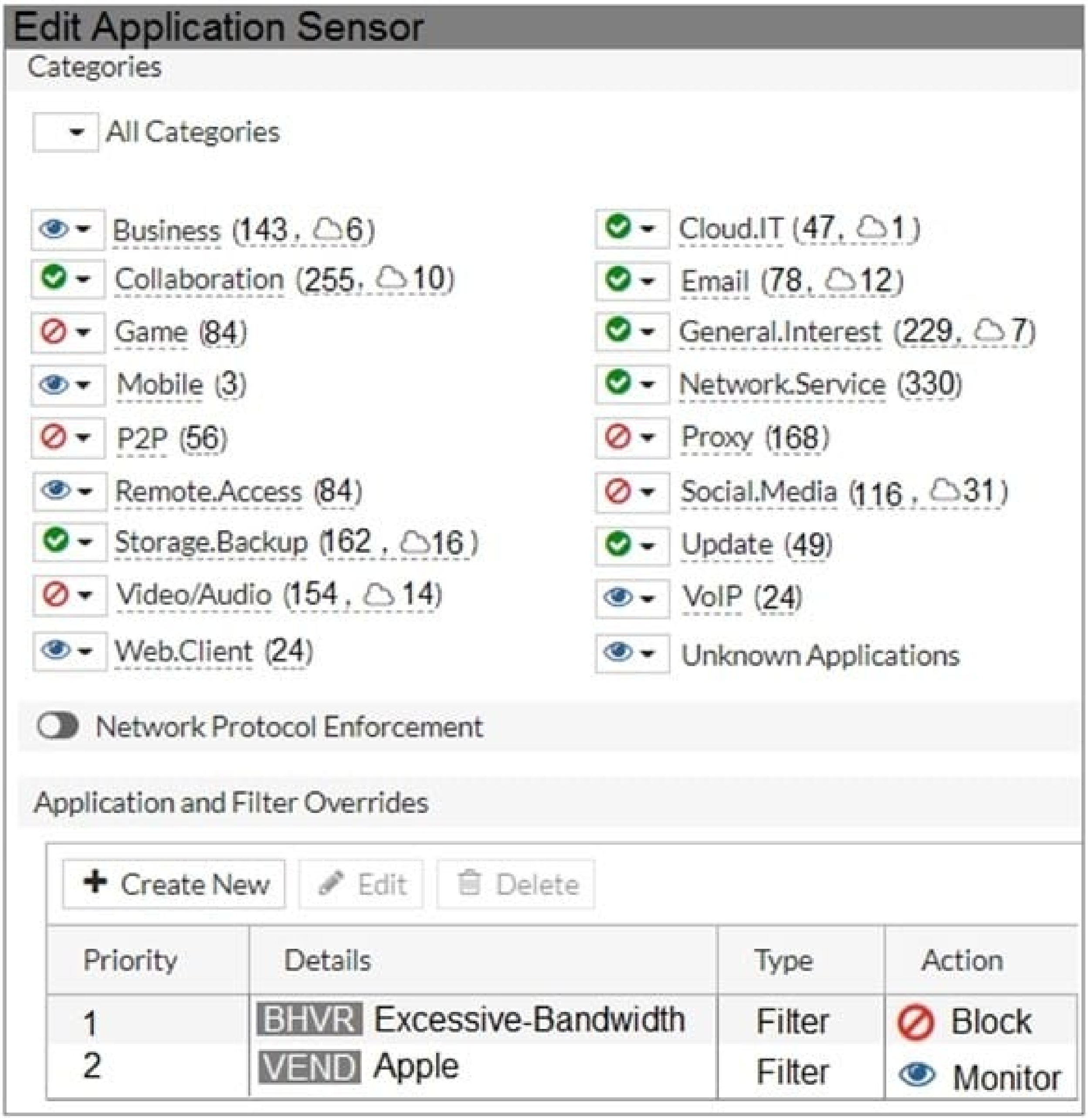
D. It authenticates the traffic using the authentication scheme SCHEME1.

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 11

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.

Correct Answer: C

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.

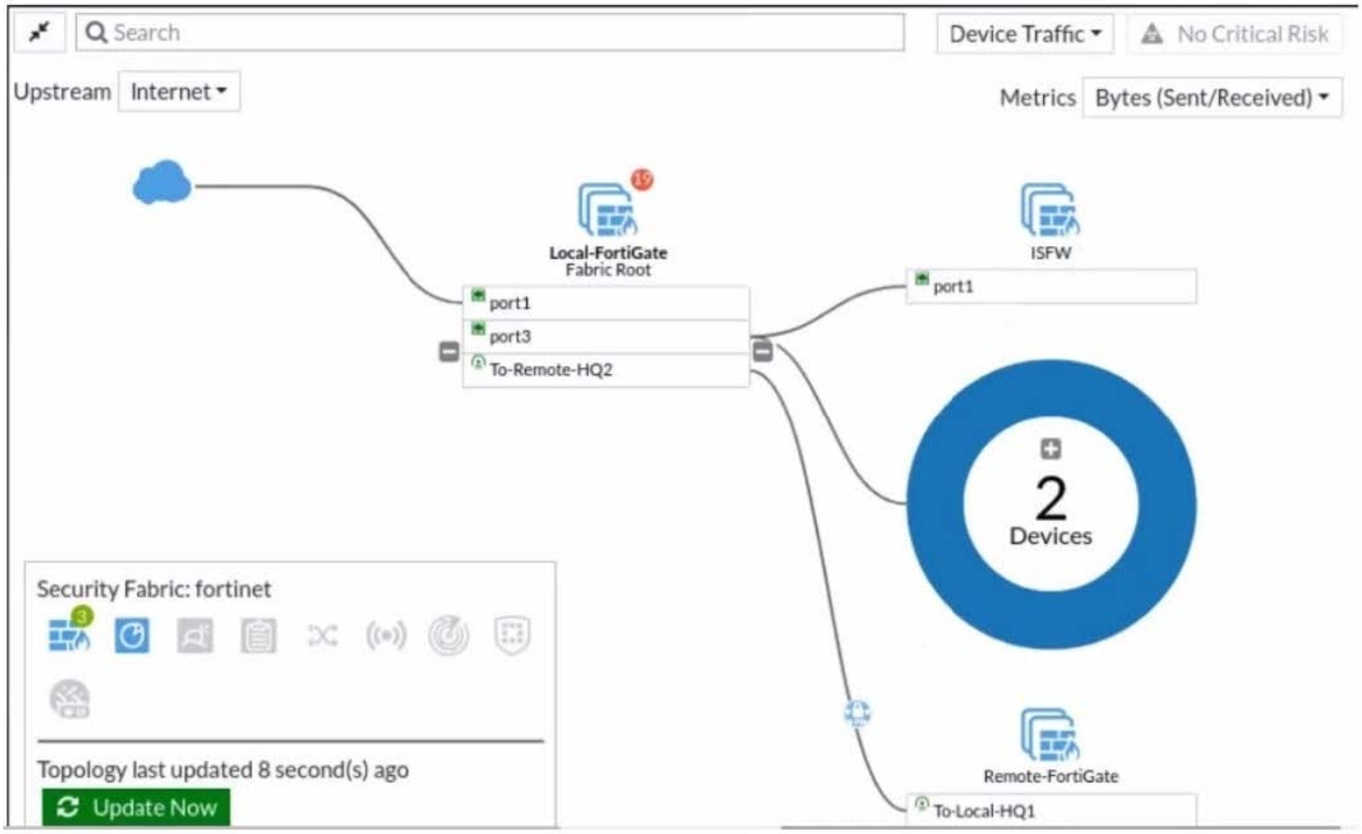
C. Uninterruptable upgrade is enabled by default.

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

Correct Answer: CD

QUESTION 13

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.

Correct Answer: CD

https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results
https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology

QUESTION 14

Which statement about video filtering on FortiGate is true?

A. Full SSL Inspection is not required.

B. It is available only on a proxy-based firewall policy.

C. It inspects video files hosted on file sharing services.

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

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/190873/video-filtering

QUESTION 15

Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

A. get system status

B. get system performance status

C. diagnose sys top

D. get system arp

Correct Answer: D

"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

Latest NSE4_FGT-7.0 Dumps NSE4_FGT-7.0 Study Guide NSE4_FGT-7.0 Braindumps