NSE4_FGT-7.2 Q&As

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

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

https://www.certbus.com/nse4_fgt-7-2.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which statement is correct regarding the security fabric?

A. FortiManager is one of the required member devices.

B. FortiGate devices must be operating in NAT mode.

C. A minimum of two Fortinet devices is required.

D. FortiGate Cloud cannot be used for logging purposes.

Correct Answer: B

FortiGate Security 7.2 Study Guide (p.428): "You must have a minimum of two FortiGate devices at the core of the Security Fabric, plus one FortiAnalyzer or cloud logging solution. FortiAnalyzer Cloud or FortiGate Cloud can act as the cloud logging solution. The FortiGate devices must be running in NAT mode."

QUESTION 2

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.

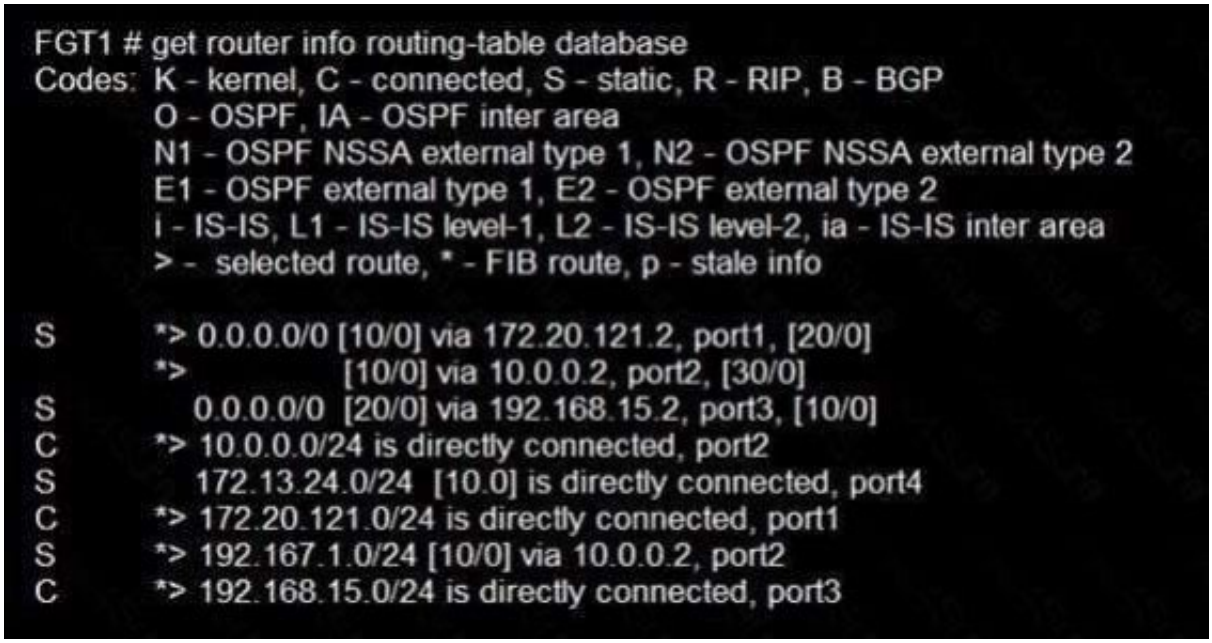
D. Interface Pair view is disabled.

Correct Answer: D

"If you use multiple source or destination interfaces, or the any interface in a firewall policy, you cannot separate policies into sections by interface pairs--some would be triplets or more. So instead, policies are then always displayed in a single list (By Sequence)."

QUESTION 3

Refer to the exhibit.



Given the routing database shown in the exhibit, which two statements are correct? (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.

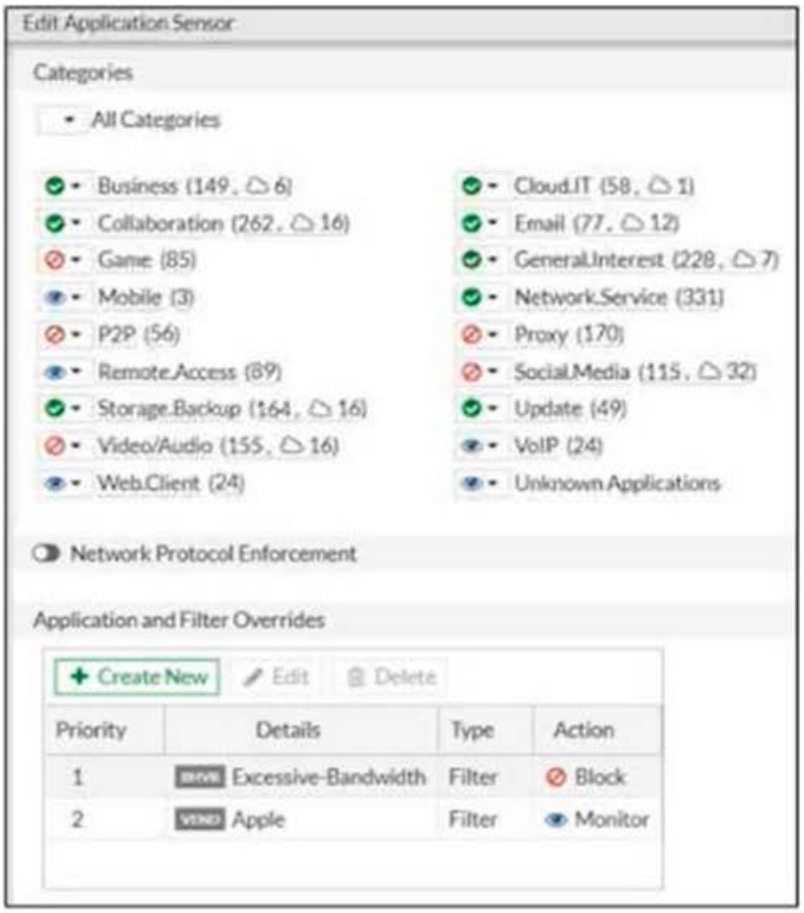
D. There will be eight routes active in the routing table.

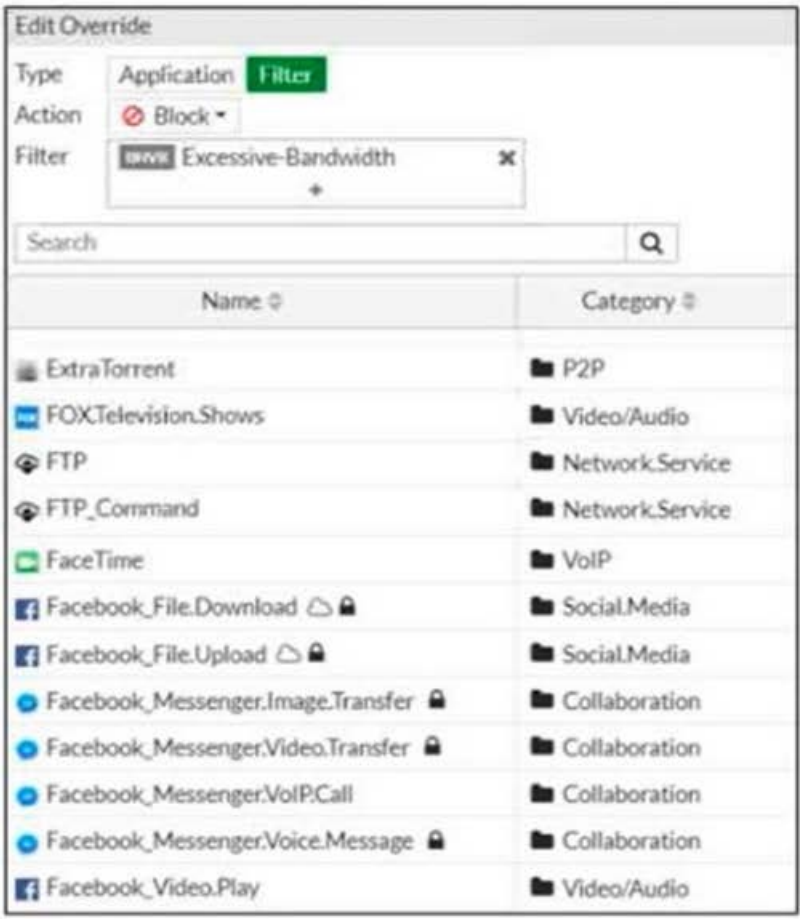
Correct Answer: BC

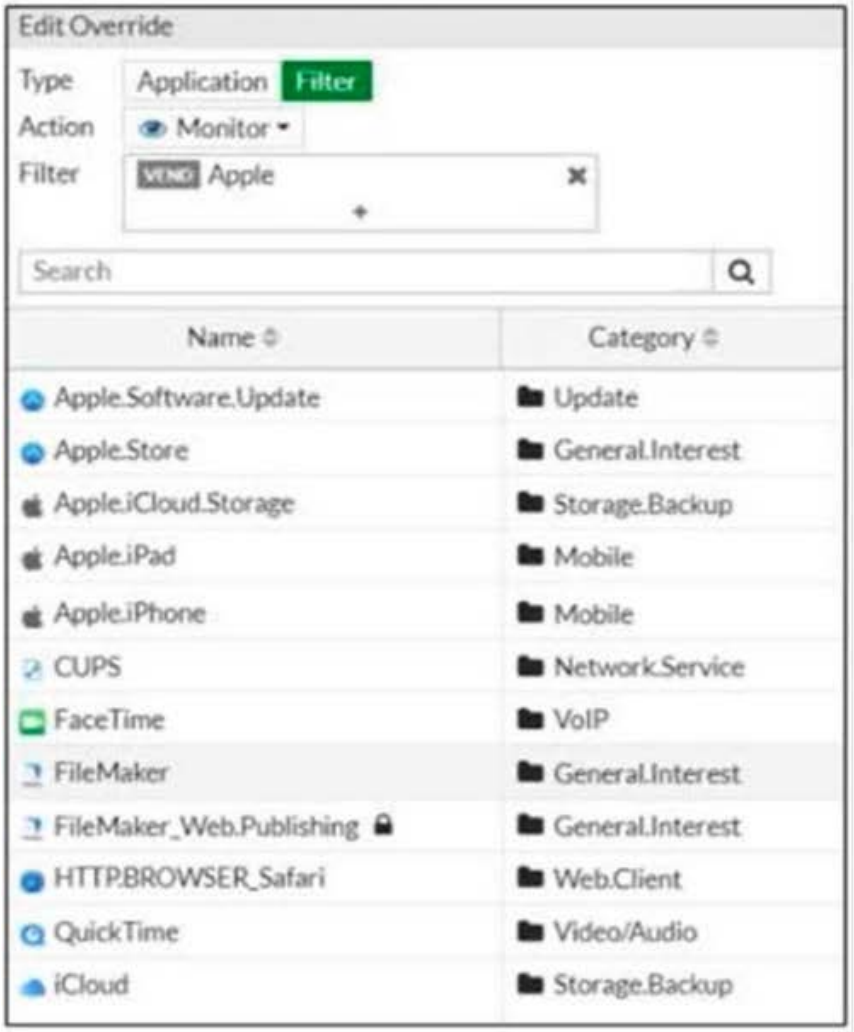
https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-identify-Inactive-Routes-in-the-Routing/ta-p/197595

QUESTION 4

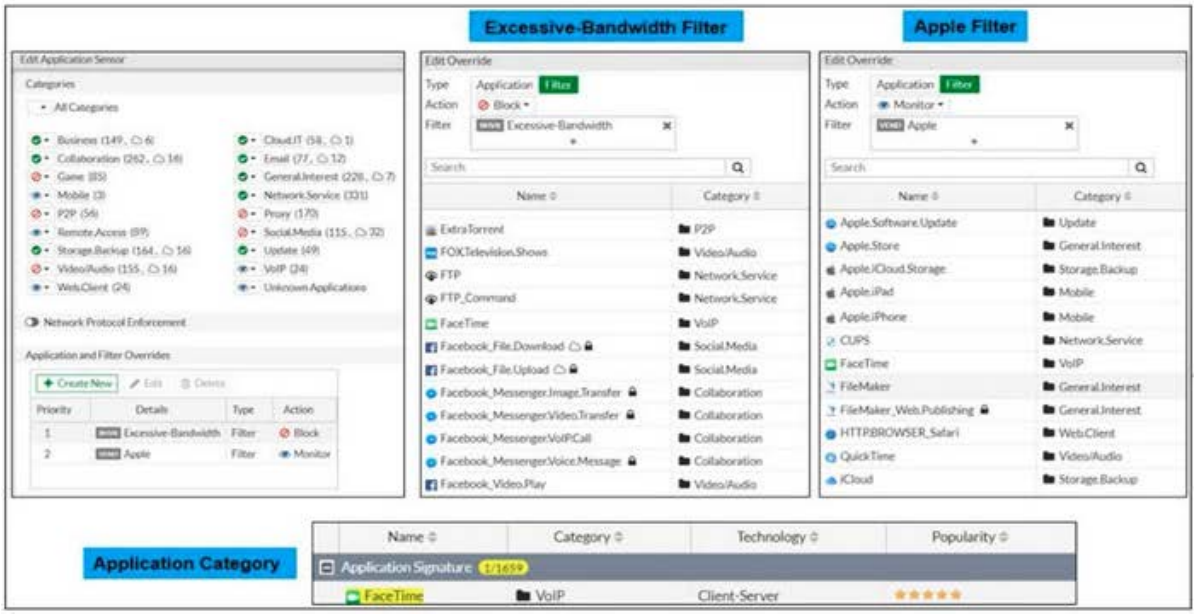
Refer to the exhibit to view the application control profile.


Edit Application Sensor
Categories
All Categories
Business (149, 6)
Collaboration (262, 16)
Game (85)
Mobile (3)
P2P (56)
Remote.Access (89)
Storage.Backup (164, 16)
Video/Audio (155, 16)
Web.Client (24)
Cloud.IT (58, 1)
Email (77, 12)
General.Interest (228, 7)
Network.Service (331)
Proxy (170)
Social.Media (115, 32)
Update (49)
VoIP (24)
Unknown Applications
Network Protocol Enforcement
Application and Filter Overrides
Create New
Edit
Delete
Priority
Details
Type
Action
1
Excessive-Bandwidth
Filter
Block
2
Apple
Filter
Monitor


Edit Override
Type
Application
Filter
Action
Block
Filter
Excessive-Bandwidth
Search
Name
Category
ExtraTorrent
P2P
FOX.Television.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
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


Excessive-Bandwidth Filter
Apple Filter
Application Category

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 5

Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

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

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

C. FortiGate does not support workstation check .

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

Correct Answer: BC

You can deploy FSSO w/o installing an agent. FG polls the DCs directly, instead of receiving logon info indirectly from a collector agent.

Because FG collects all of the data itself, agentless polling mode requires greater system resources, and it doesn\\'t scale as easily.

Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there\\'s no collector agent, FG uses the SMB protocol to read the event viewer logs from the DCs.

FG acts as a collector. It \\'s responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent.

Reference: https://kb.fortinet.com/kb/documentLink .do?externalID=FD47732 https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-troubleshoot-FSSO-agentless-polling/ta-p/214349

QUESTION 6

Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

A. Proxy-based inspection

B. Certificate inspection

C. Flow-based inspection

D. Full Content inspection

Correct Answer: AC

QUESTION 7

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

A. By default, FortiGate uses WINS servers to resolve names.

B. By default, the SSL VPN portal requires the installation of a client\\'s certificate.

C. By default, split tunneling is enabled.

D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Correct Answer: D

QUESTION 8

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.

Correct Answer: B

FortiGate Security 7.2 Study Guide (p.192): "if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecure network. You can choose the level of SSL protection used by configuring the enc-algorithm setting on the CLI."

QUESTION 9

Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?

A. VDOMs without ports with connected devices are not displayed in the topology.

B. Downstream devices can connect to the upstream device from any of their VDOMs.

C. Security rating reports can be run individually for each configured VDOM.

D. Each VDOM in the environment can be part of a different Security Fabric.

Correct Answer: A

FortiGate Security 7.2 Study Guide (p.436): "When you configure FortiGate devices in multi-vdom mode and add them

to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. Only the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable Device Detection on ports you want to have displayed in the Security Fabric. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single Security Fabric."

QUESTION 10

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

A. Full Content inspection

B. Proxy-based inspection

C. Certificate inspection

D. Flow-based inspection

Correct Answer: D

QUESTION 11

An administrator must disable RPF check to investigate an issue.

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

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

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

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

D. Enable asymmetric routing at the interface level.

Correct Answer: B

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955

QUESTION 12

In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

A. The IP version of the sources and destinations in a firewall policy must be different.

B. The Incoming Interface. Outgoing Interface. Schedule, and Service fields can be shared with both IPv4 and IPv6.

C. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.

D. The IP version of the sources and destinations in a policy must match.

E. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Correct Answer: BDE

QUESTION 13

Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

A. FortiCache

B. FortiSIEM

C. FortiAnalyzer

D. FortiSandbox

E. FortiCloud

Correct Answer: BCE

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-and-reporting-overview

QUESTION 14

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

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

A. Antivirus scanning

B. File filter

C. DNS filter

D. Intrusion prevention

Correct Answer: AD

Security policy: If the traffic is allowed as per the consolidated policy, FortiGate will then process it based on the security policy to analyze additional criteria, such as URL categories for web filtering and application control. Also, if enabled, the security policy further inspects traffic using security profiles such as IPS and AV.

QUESTION 15

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

A. FortiGate acts as an FDS server.

B. FortiGate acts as an HTTP reverse proxy.

C. FortiGate acts as DNS server.

D. FortiGate acts as router.

Correct Answer: B

Reference: https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigate-sslvpn-40-mr3.pdf