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.pass4itsure.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

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.

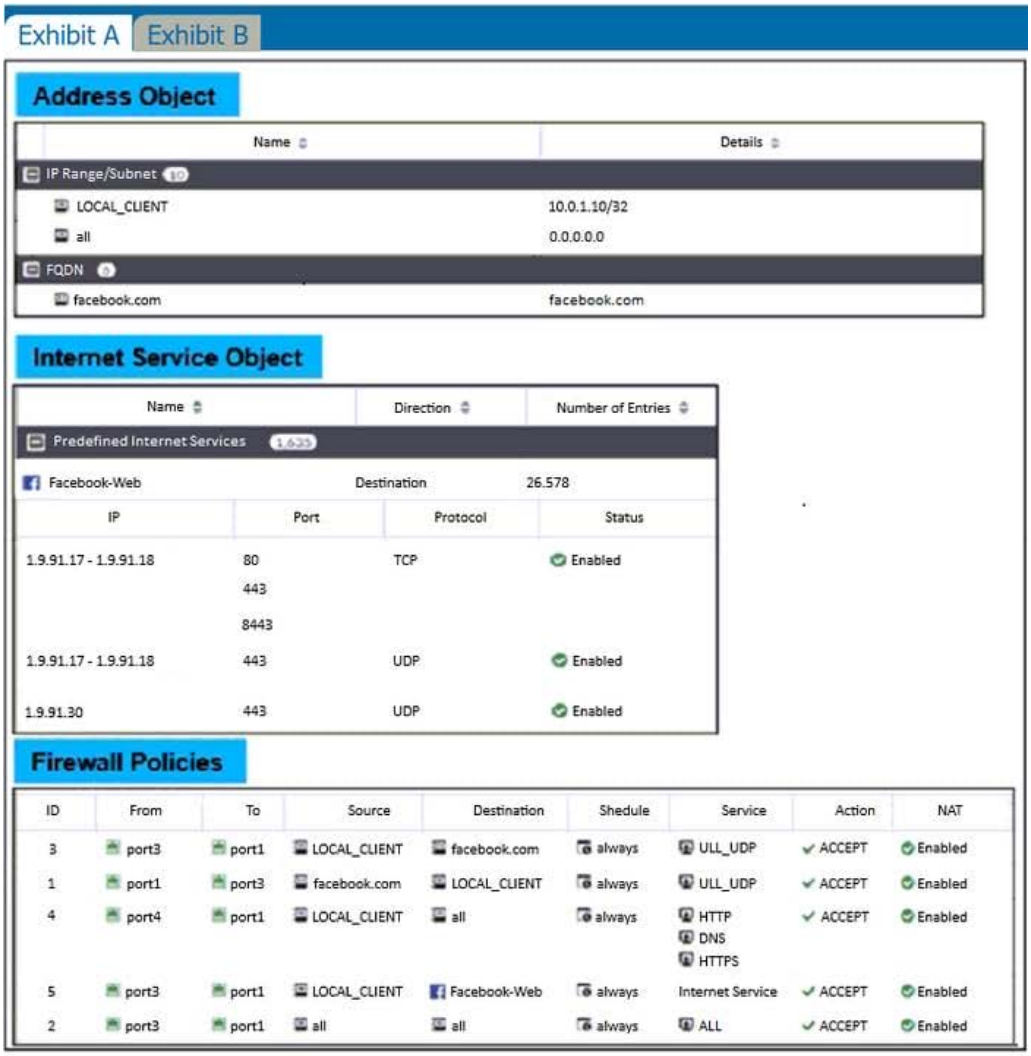


Exhibit A
Exhibit B
Address Object
Name
Details
IP Range/Subnet 10
LOCAL_CLIENT
10.0.1.10/32
all
0.0.0.0
FQDN 6
facebook.com
facebook.com
Internet Service Object
Name
Direction
Number of Entries
Predefined Internet Services 1,633
Facebook-Web
Destination
26,578
IP
Port
Protocol
Status
1.9.91.17 - 1.9.91.18
80
TCP
Enabled
443
8443
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
Search
Close

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.

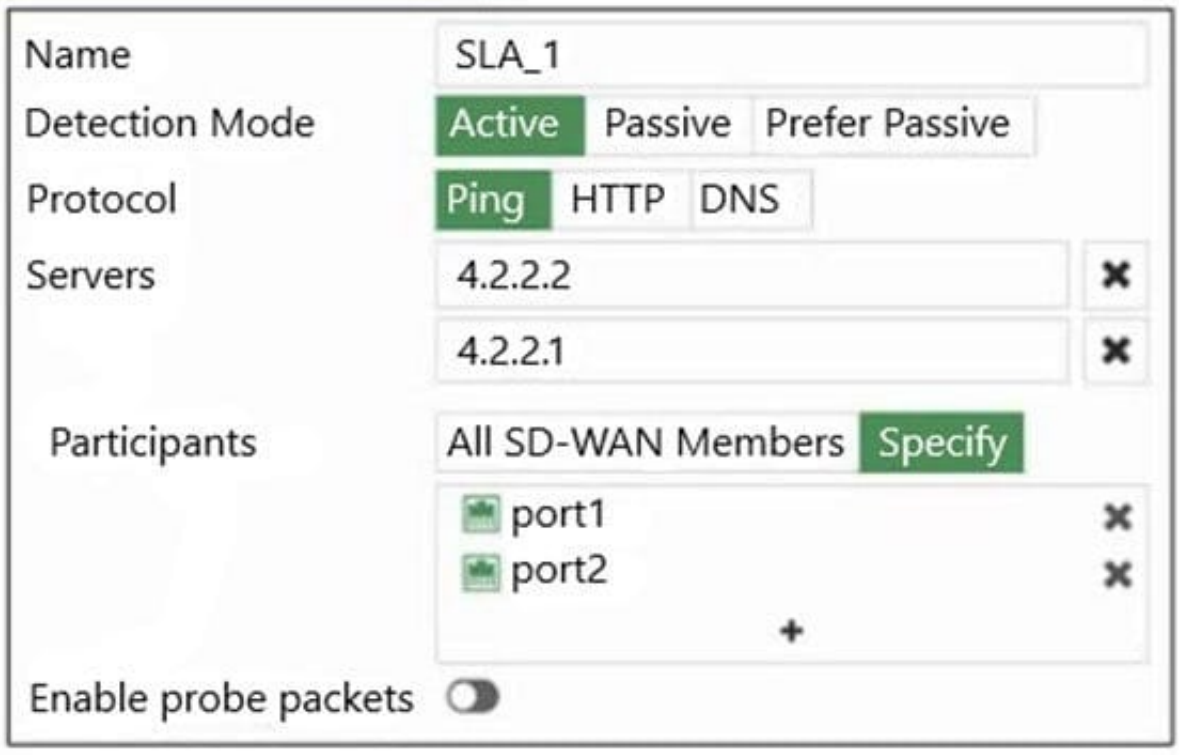
Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/6.2.12/cookbook/497952/policy-views-and-policy-lookup

We are looking for a policy that will allow or deny traffic from the source interface Port3 and source IP address 10.1.1.10 (LOCAL_CLIENT) to facebook.com TCP port 443 (HTTPS). There are only two policies that will match this traffic, policy ID 2 and 5. In FortiGate, firewall policies are evaluated from top to bottom. This means that the first policy that matches the traffic is applied, and subsequent policies are not evaluated. Based on the Policy Lookup criteria, Policy ID 5 will be highlighted

QUESTION 2

Refer to the exhibit.



An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic. Why is FortiGate not sending probes to 4.2.2.2 and 4.2.2.1 servers? (Choose two.)

A. The Detection Mode setting is not set to Passive.

B. Administrator didn\\'t configure a gateway for the SD-WAN members, or configured gateway is not valid.

C. The configured participants are not SD-WAN members.

D. The Enable probe packets setting is not enabled.

Correct Answer: BD

QUESTION 3

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

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

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

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

D. FortiGate forwards frames without changing the MAC address.

Correct Answer: AD

Reference: https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdfanddo cumentID=FD33113

QUESTION 4

Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

A. diagnose wad session list

B. diagnose wad session list | grep hook-preandandhook-out

C. diagnose wad session list | grep hook=preandandhook=out

D. diagnose wad session list | grep "hook=pre"and"hook=out"

Correct Answer: A

QUESTION 5

Which feature in the Security Fabric takes one or more actions based on event triggers?

A. Fabric Connectors

B. Automation Stitches

C. Security Rating

D. Logical Topology

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/286973/fortinet-security-fabric

QUESTION 6

Which statement about the IP authentication header (AH) used by IPsec is true?

A. AH does not provide any data integrity or encryption.

B. AH does not support perfect forward secrecy.

C. AH provides data integrity bur no encryption.

D. AH provides strong data integrity but weak encryption.

Correct Answer: C

QUESTION 7

An administrator wants to simplify remote access without asking users to provide user credentials. Which access control method provides this solution?

A. ZTNA IP/MAC filtering mode

B. ZTNA access proxy

C. SSL VPN

D. L2TP

Correct Answer: B

FortiGate Infrastructure 7.2 Study Guide (p.165): "ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs."

This is true because ZTNA access proxy is a feature that allows remote users to access internal applications without requiring VPN or user credentials.

ZTNA access proxy uses a secure tunnel between the user\\'s device and the FortiGate, and authenticates the user based on device identity and context.

The user only needs to install a lightweight agent on their device, and the FortiGate will automatically assign them to the appropriate application group based on their device profile.

This simplifies remote access and enhances security by reducing the attack surface12

QUESTION 8

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 9

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 10

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

QUESTION 11

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

Correct Answer: B

FortiGate Infrastructure 7.2 Study Guide (p.198): "Tunnel mode requires FortiClient to connect to FortiGate. FortiClient adds a virtual network adapter identified as fortissl to the user\\'s PC. This virtual adapter dynamically receives an IP address from FortiGate each time FortiGate establishes a new VPN connection. Inside the tunnel, all traffic is SSL/TLS encapsulated. The main advantage of tunnel mode over web mode is that after the VPN is established, any IP network application running on the client can send traffic through the tunnel."

An SSL VPN tunnel allows remote users to establish a secure and encrypted Virtual Private Network (VPN) connection to the private network using the SSL/TLS protocol1. An SSL VPN tunnel can provide access to network resources such as FTP servers, as well as external applications running on the user\\'s PC1. An SSL VPN bookmark is a web link that provides access to network resources through the SSL VPN web portal1. It does not support external applications running on the user\\'s PC. Zero trust network access (ZTNA) is a security model that provides role-based application access to remote users without exposing the private network to the internet2. It does not use SSL/TLS protocol, but rather a proprietary ZTNA protocol. SSL VPN quick connection is a feature that allows users to connect to an SSL VPN tunnel without installing FortiClient or any other software on their PC3. It requires a web browser that supports Java or ActiveX. It does not support external applications running on the user\\'s PC.

QUESTION 12

Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

A. Heartbeat interfaces have virtual IP addresses that are manually assigned.

B. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.

C. Virtual IP addresses are used to distinguish between cluster members.

D. The primary device in the cluster is always assigned IP address 169.254.0.1.

Correct Answer: BC

QUESTION 13

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.

The administrator disabled the WebServer firewall policy.

Exhibit A | Exhibit B

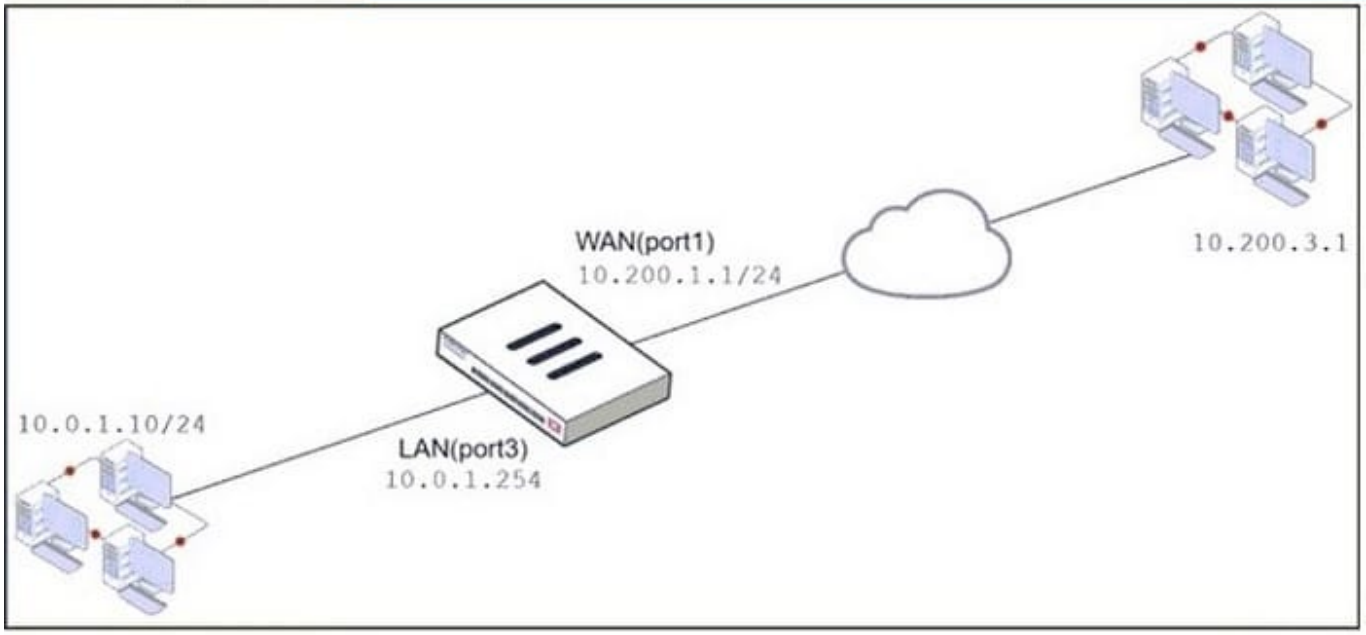


Exhibit A | Exhibit B

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

Which IP address will be used to source NAT the traffic, if a user with address 10.0.1.10 connects over SSH to the host with address 10.200.3.1?

A. 10.200.1.10

B. 10.0.1.254

C. 10.200.1.1

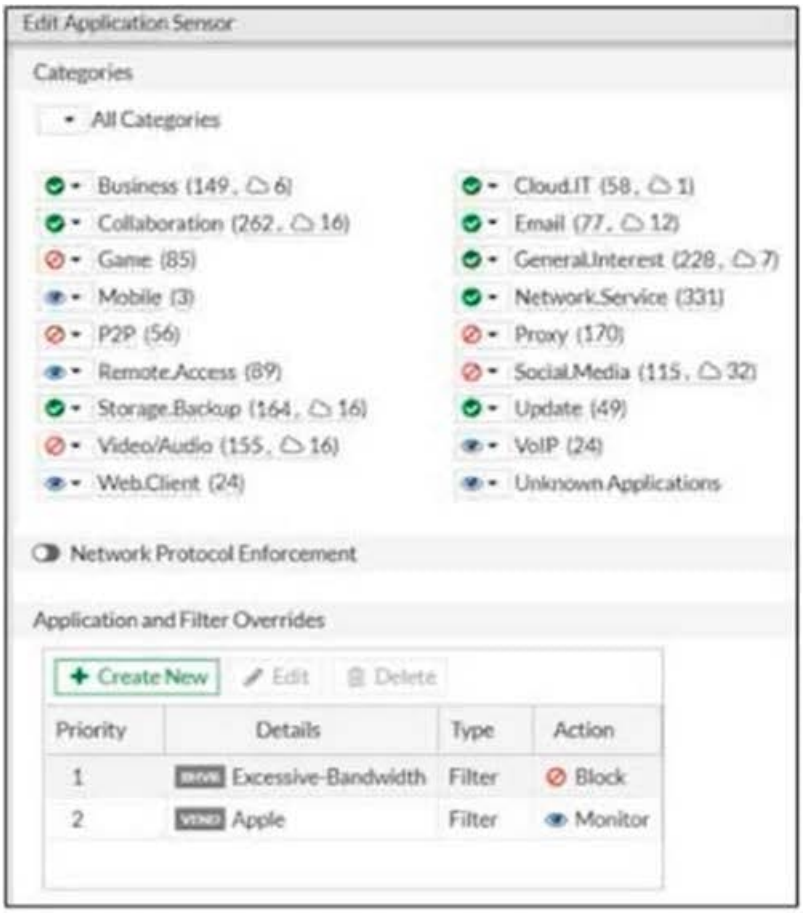
D. 10.200.3.1

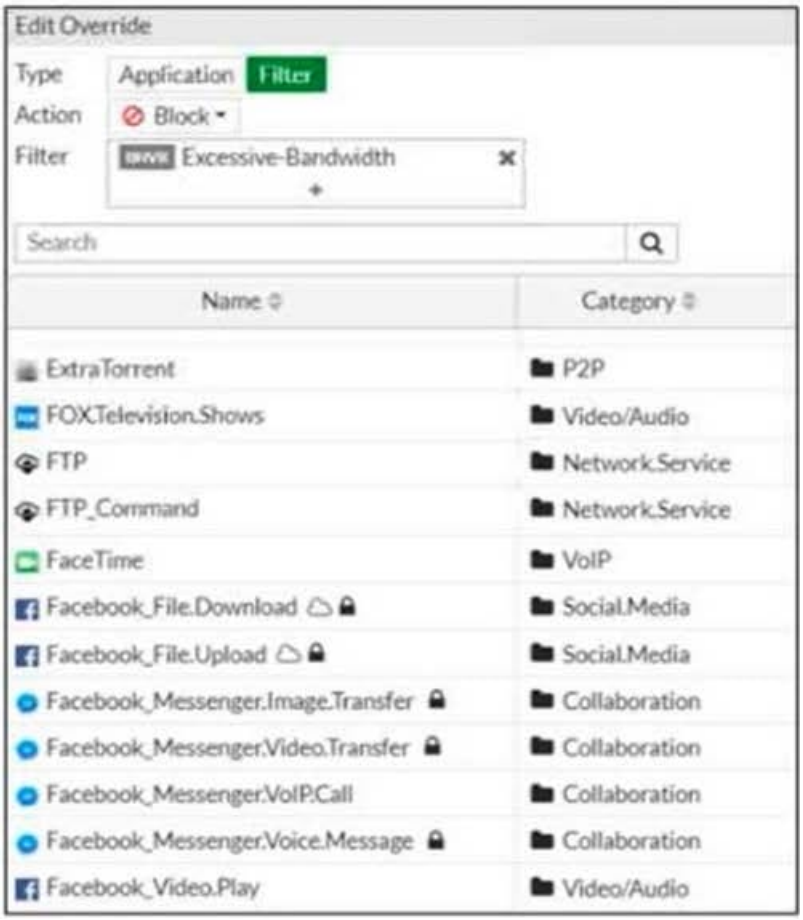
Correct Answer: C

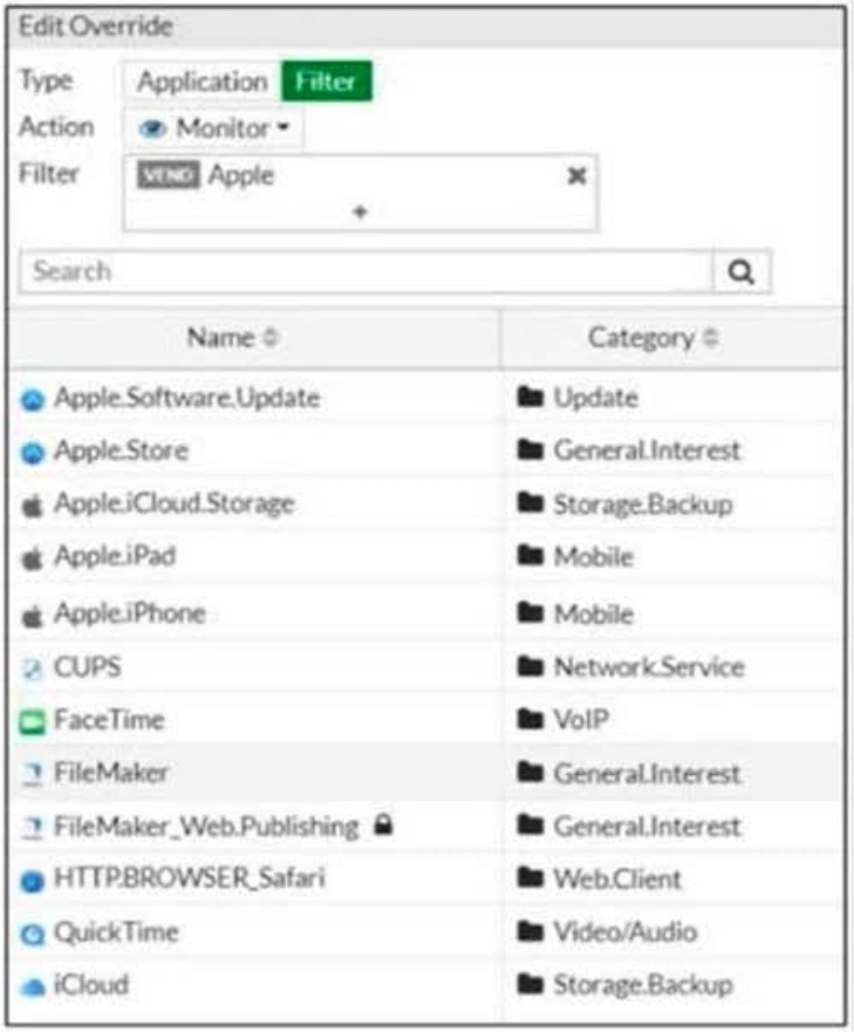
Traffic is coming from LAN to WAN, matches policy Full_Access which has NAT enable, so traffic uses source IP address of outgoing interface. Simple SNAT.

QUESTION 14

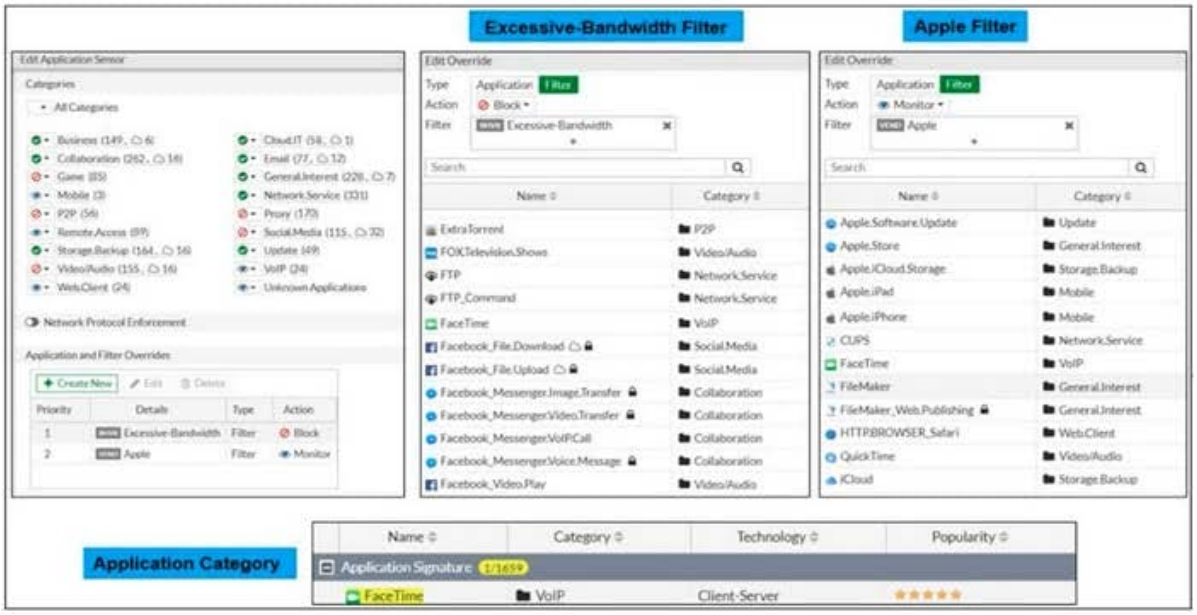
Refer to the exhibit to view the application control profile.


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
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 15

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