TestkingPDF

Try before you buy

Download a free sample of any of our exam questions and answers

Download Demo

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

Quality and Value

TestkingPDF Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our TestkingPDF testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

TestkingPDF offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.testkingpdf.com

Valid test online & stable pass king & latest PDF dumps

Exam : **NSE4_FGT-6.4**

Title : Fortinet NSE 4 - FortiOS 6.4

Vendor : Fortinet

Version : DEMO

NO.1 Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Exhibit A

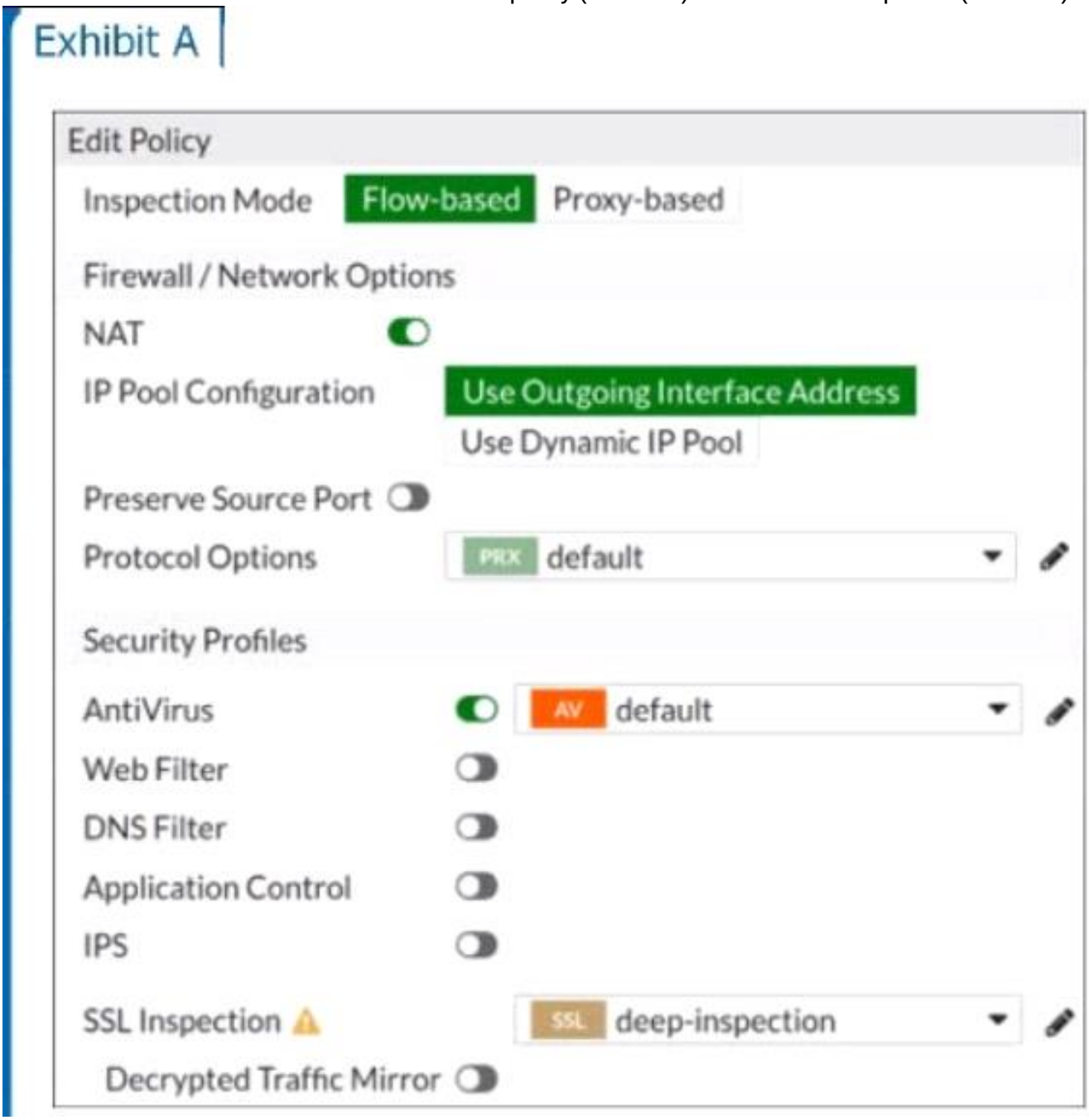
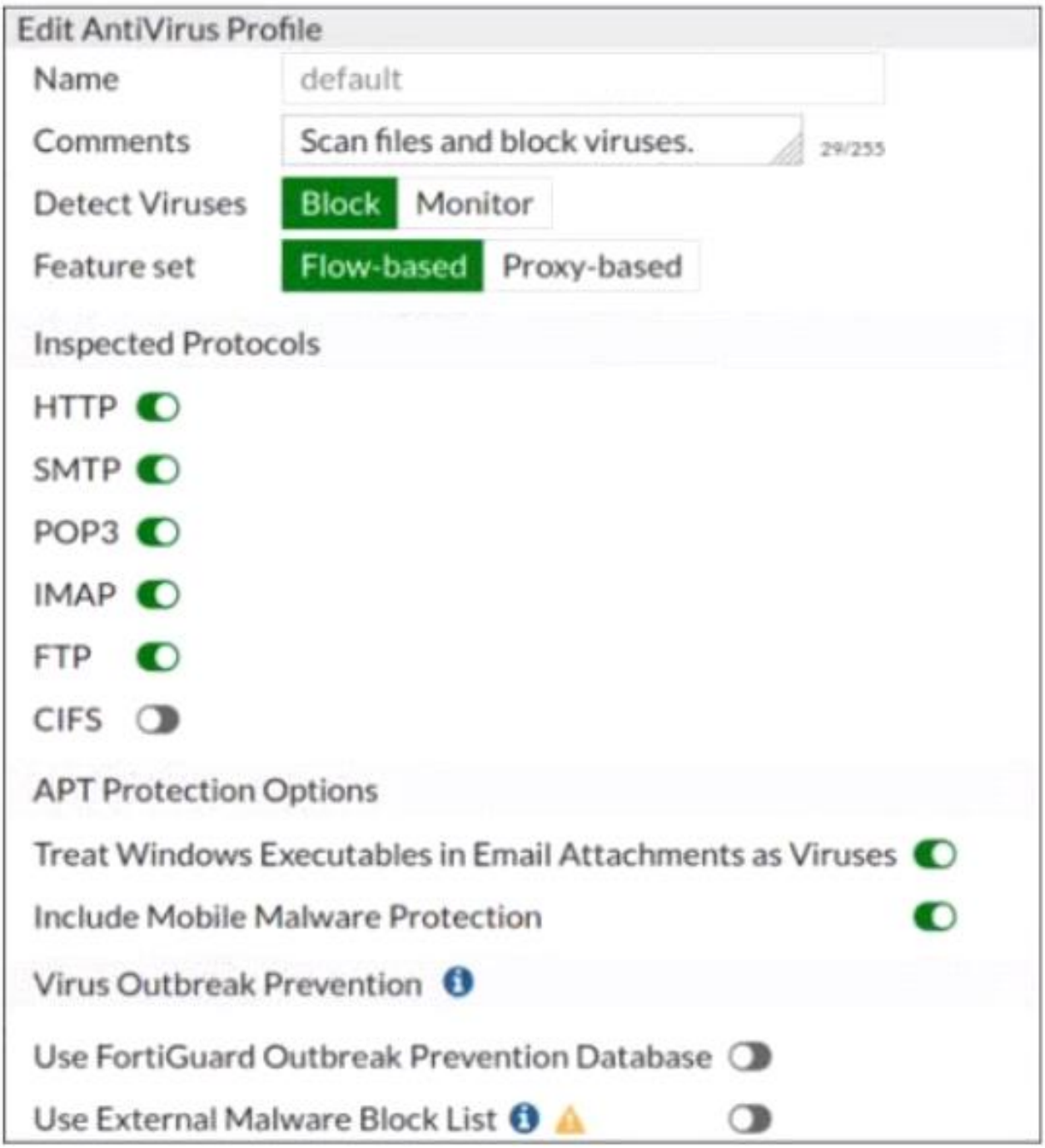


Exhibit B



Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

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

B. The firewall policy performs the full content inspection on the file.

C. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

D. The flow-based inspection is used, which resets the last packet to the user.

Answer: D

NO.2 An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

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

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

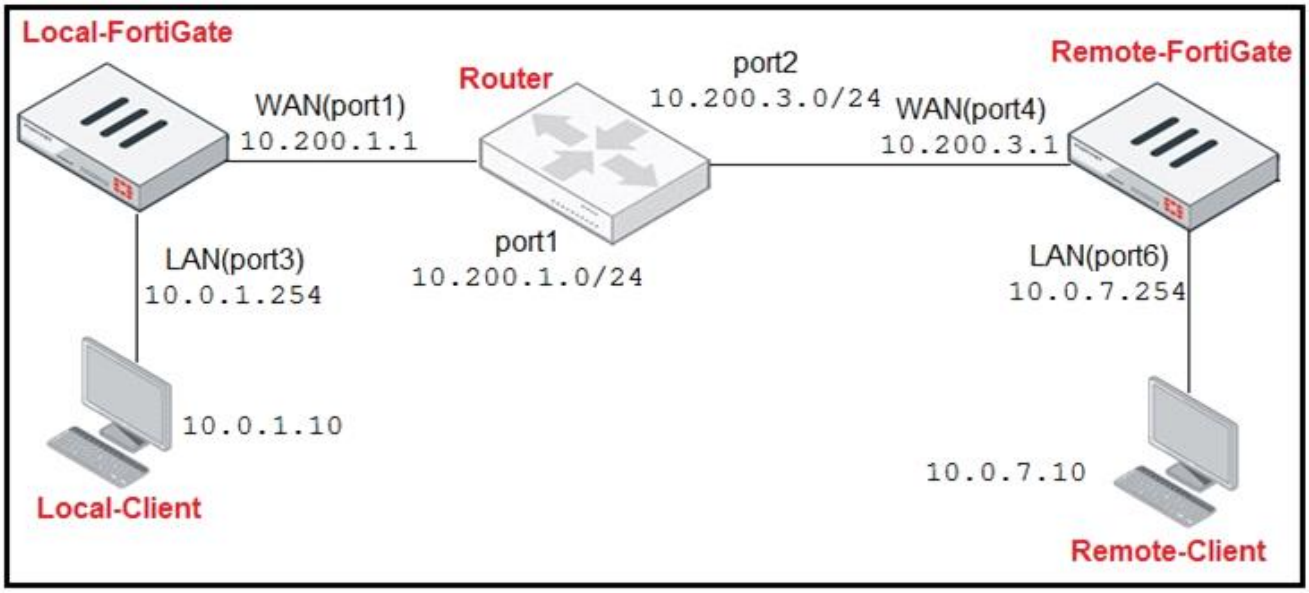
C. Strict RPF checks the best route back to the source using the incoming interface.

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

Answer: C

NO.3 Refer to the exhibit.

Network Diagram



Central SNAT Policies Local-FortiGate

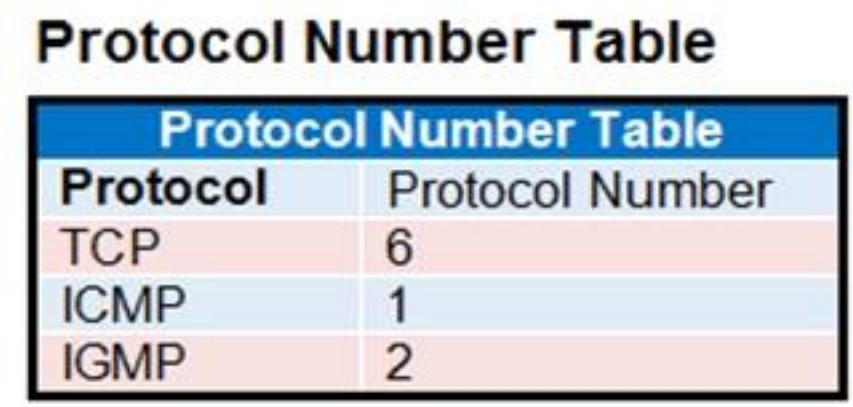
+ Create New | Edit | Delete | Search

ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

IP Pool Local-FortiGate

+ Create New | Edit | Clone | Delete | Search

Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	Enabled



The exhibit contains a network diagram, central SNAT policy, and IP pool 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.
A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1).
Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied.
Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

A. 10.200.1.149
B. 10.200.1.99
C. 10.200.1.49
D. 10.200.1.1
Answer: B

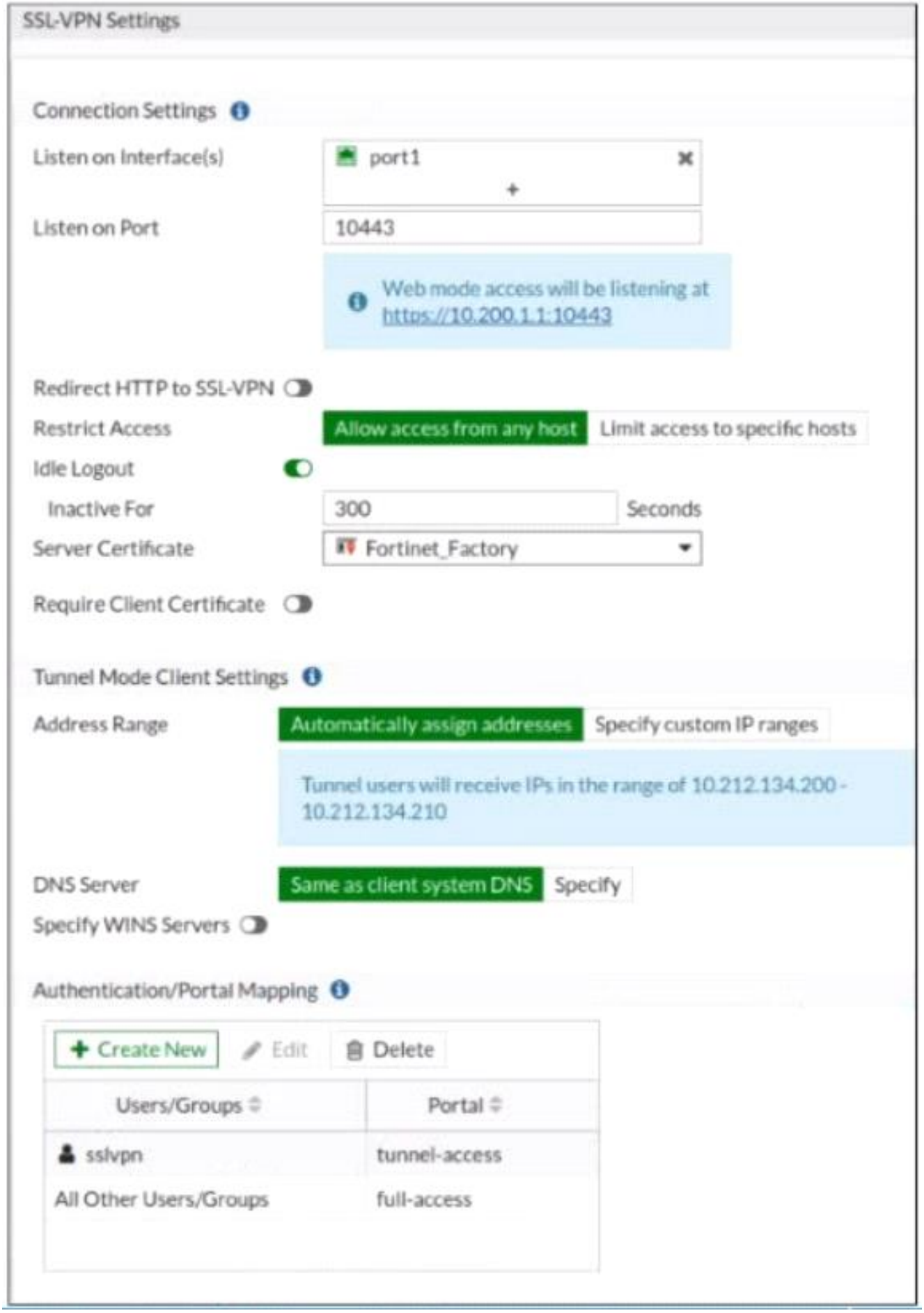
NO.4 Which security feature does FortiGate provide to protect servers located in the internal networks from attacks such as SQL injections?

A. Antivirus
B. Denial of Service
C. Web application firewall
D. Application control
Answer: C

NO.5 How do you format the FortiGate flash disk?

A. Load the hardware test (HQIP) image.
B. Select the format boot device option from the BIOS menu.
C. Load a debug FortiOS image.
D. Execute the CLI command execute formatlogdisk.
Answer: B

NO.6 Refer to the exhibits.


SSL-VPN Settings
Connection Settings
Listen on Interface(s)
port1
Listen on Port
10443
Web mode access will be listening at https://10.200.1.1:10443
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Server Certificate
Fortinet_Factory
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
Authentication/Portal Mapping
Create New
Edit
Delete
Users/Groups
Portal
sslvpn
tunnel-access
All Other Users/Groups
full-access

The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

A. Change the Server IP address.

B. Change the SSL VPN portal to the tunnel.

C. Change the SSL VPN port on the client.

D. Change the idle-timeout.

Answer: C

NO.7 Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

A. SSH

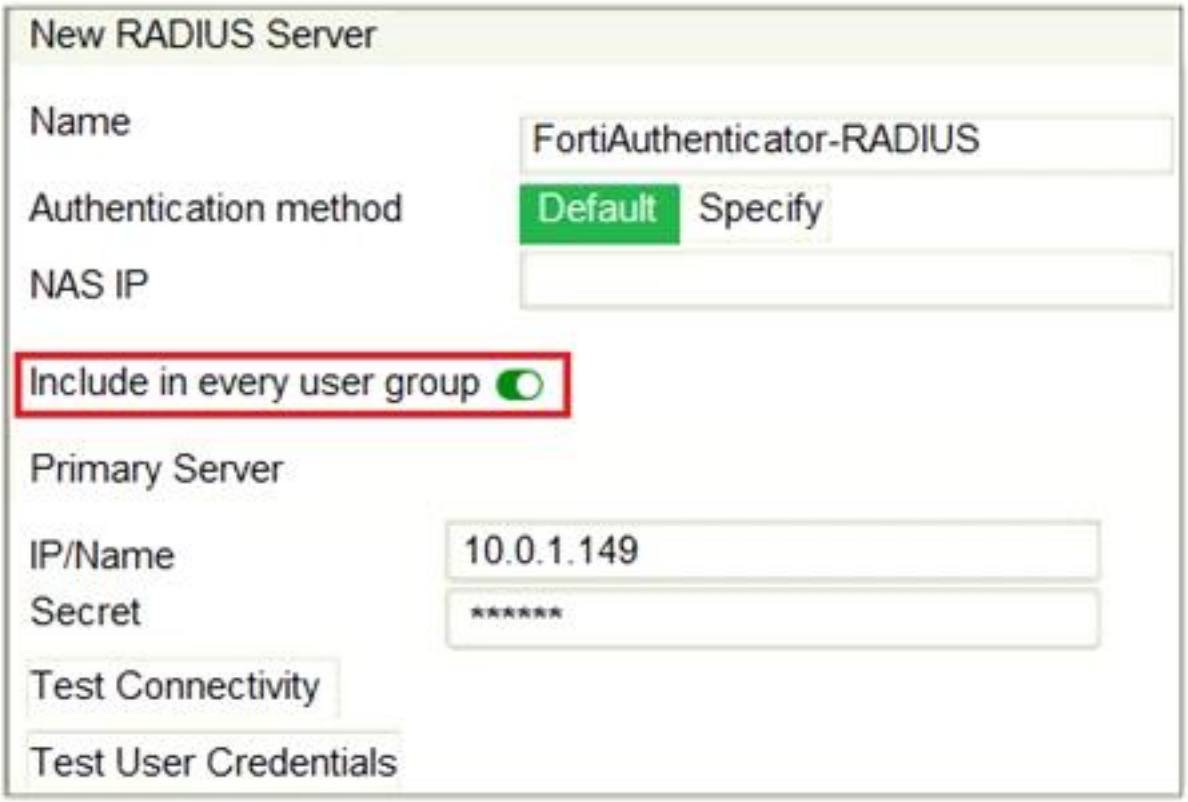
B. HTTPS

C. FTM

D. FortiTelemetry

Answer: A,B

NO.8 Refer to the exhibit, which contains a radius server configuration.



An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option.
What will be the impact of using Include in every user group option in a RADIUS configuration?

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

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

Answer: B

NO.9 Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)

A. Disable FortiAnalyzer logging for a downstream FortiGate device.

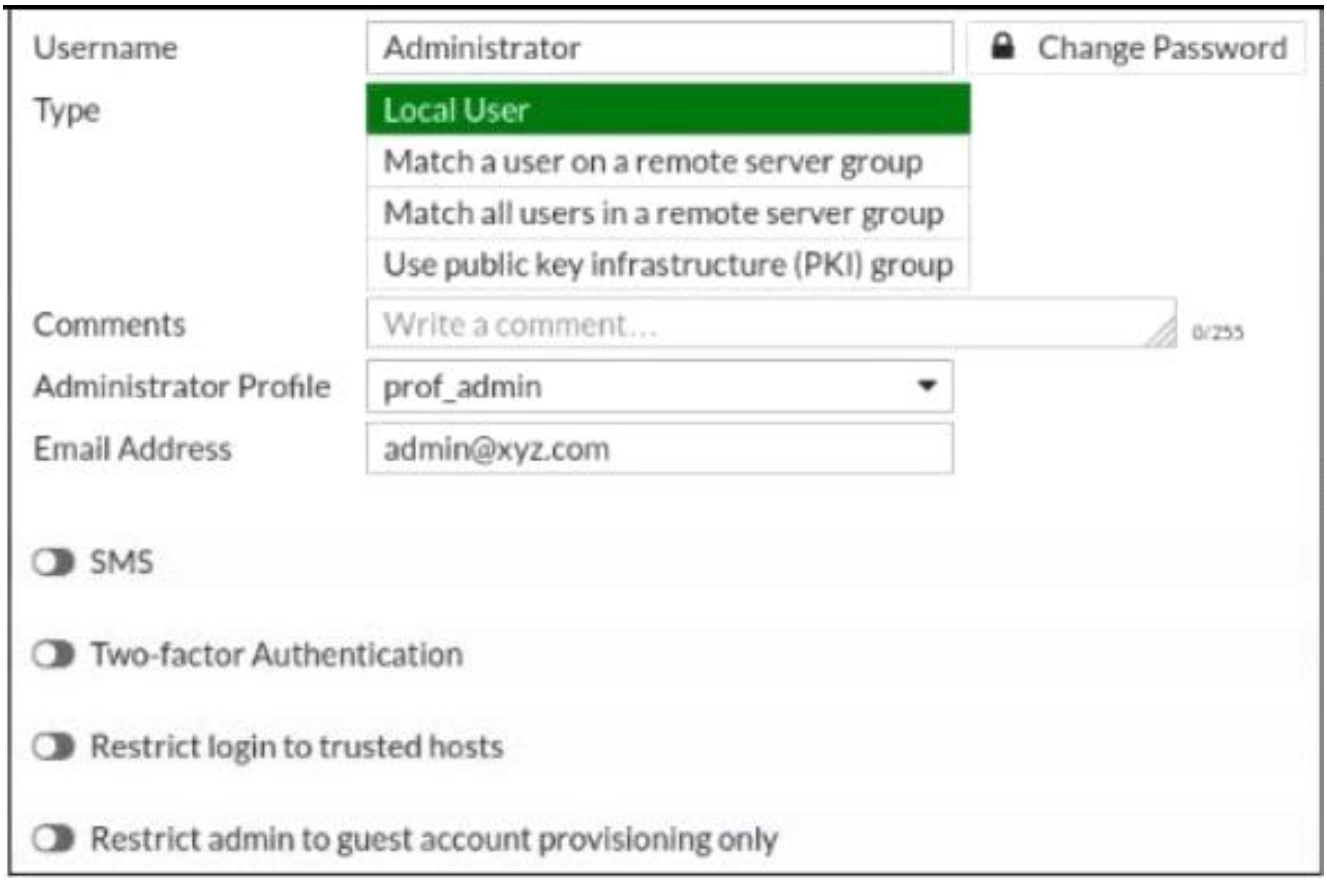
B. Log in to a downstream FortiSwitch device.

C. Shut down/reboot a downstream FortiGate device.

D. Ban or unban compromised hosts.

Answer: A,C

NO.10 Refer to the exhibit.



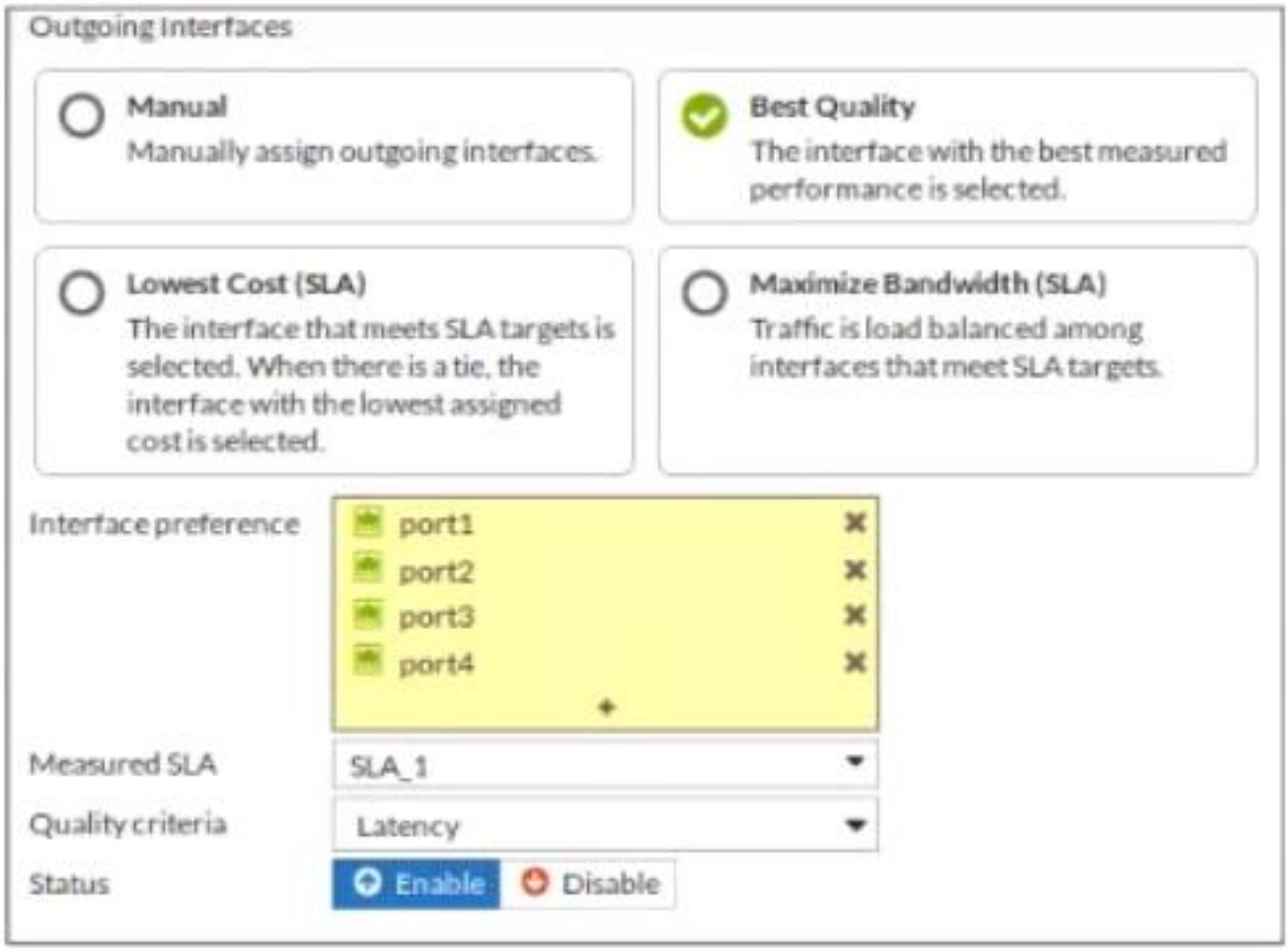
The global settings on a FortiGate device must be changed to align with company security policies. What does the Administrator account need to access the FortiGate global settings?

A. Enable restrict access to trusted hosts
B. Enable two-factor authentication
C. Change Administrator profile
D. Change password
Answer: C

NO.11 What is the primary FortiGate election process when the HA override setting is disabled?

A. Connected monitored ports > HA uptime > Priority > FortiGate Serial number
B. Connected monitored ports > System uptime > Priority > FortiGate Serial number
C. Connected monitored ports > Priority > HA uptime > FortiGate Serial number
D. Connected monitored ports > Priority > System uptime > FortiGate Serial number
Answer: A

NO.12 Refer to the exhibit.




```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4.287) sla_map=0x
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5.685) sla_map=0x
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4.287) sla_map=0x
```

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check.
Which interface will be selected as an outgoing interface?

A. port4
B. port2
C. port3
D. port1

Answer: D
Explanation:
Port 1 shows the lowest latency.

NO.13 Refer to the exhibit.

Which contains a network diagram and routing table output.
The Student is unable to access Webserver.
What is the cause of the problem and what is the solution for the problem?

A. The first reply packet for Student failed the RPF check.
This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.

B. The first packet sent from Student failed the RPF check.
This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.

C. The first reply packet for Student failed the RPF check.
This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

D. The first packet sent from Student failed the RPF check.
This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

Answer: D

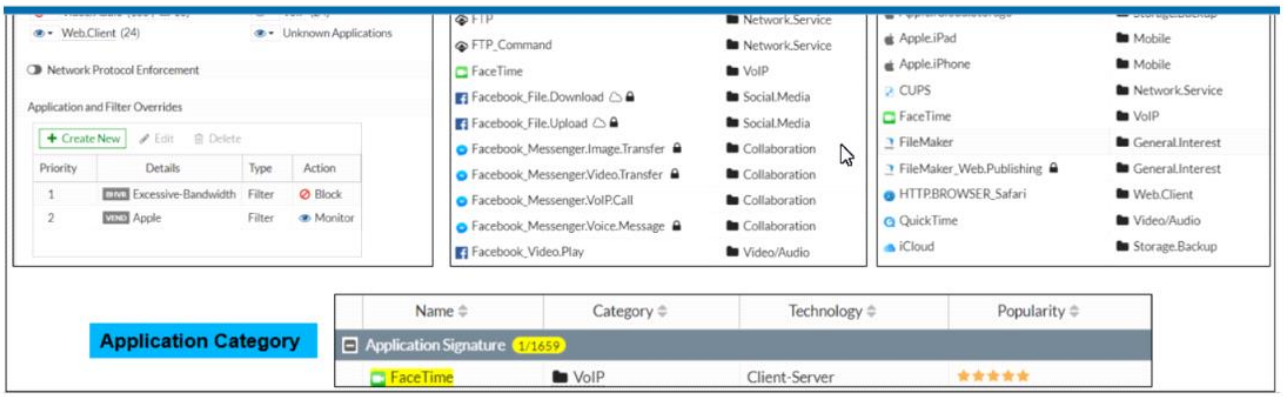
NO.14 Refer to the exhibit.

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 as shown in the exhibit.
What should the administrator do next to troubleshoot the problem?

A. Run a sniffer on the web server.
B. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10"
C. Capture the traffic using an external sniffer connected to port1.
D. Execute a debug flow.
Answer: D

NO.15 An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.16.1.0/24 and the remote quick mode selector is 192.16.2.0/24. How must the administrator configure the local quick mode selector for site B?
A. 192.168.3.0/24
B. 192.168.2.0/24
C. 192.168.0.0/8
D. 192.168.1.0/24
Answer: B

NO.16 Refer to the exhibit to view the application control profile.



Based on the configuration, what will happen to Apple FaceTime?
A. Apple FaceTime will be allowed only if the filter in Application and Filter Overrides is set to Learn
B. Apple FaceTime will be allowed, based on the Apple filter configuration.
C. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration
D. Apple FaceTime will be allowed, based on the Categories configuration.
Answer: C