

Fortinet

NSE4_FGT-6.4 Exam

Fortinet NSE 4 - FortiOS 6.4

Question: 1

Which three statements about a flow-based antivirus profile are correct? (Choose three.)

- A. IPS engine handles the process as a standalone.
- B. FortiGate buffers the whole file but transmits to the client simultaneously.
- C. If the virus is detected, the last packet is delivered to the client.
- D. Optimized performance compared to proxy-based inspection.
- E. Flow-based inspection uses a hybrid of scanning modes available in proxy-based inspection.

Answer: CDE

Question: 2

Refer to the exhibit.

```
STUDENT # get system session list
```

PROTO	EXPIRE	SOURCE	SOURCE-NAT	DESTINATION	DESTINATION-NAT
tcp	3598	10.0.1.10:2706	10.200.1.6:2706	10.200.1.254:80	-
tcp	3598	10.0.1.10:2704	10.200.1.6:2704	10.200.1.254:80	-
tcp	3596	10.0.1.10:2702	10.200.1.6:2702	10.200.1.254:80	-
tcp	3599	10.0.1.10:2700	10.200.1.6:2700	10.200.1.254:443	-
tcp	3599	10.0.1.10:2698	10.200.1.6:2698	10.200.1.254:80	-
tcp	3598	10.0.1.10:2696	10.200.1.6:2696	10.200.1.254:443	-
udp	174	10.0.1.10:2694	-	10.0.1.254:53	-
udp	173	10.0.1.10:2690	-	10.0.1.254:53	-

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

- A. Destination NAT is disabled in the firewall policy.
- B. One-to-one NAT IP pool is used in the firewall policy.
- C. Overload NAT IP pool is used in the firewall policy.
- D. Port block allocation IP pool is used in the firewall policy.

Answer: A

Question: 3

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.

Answer: CD

Question: 4

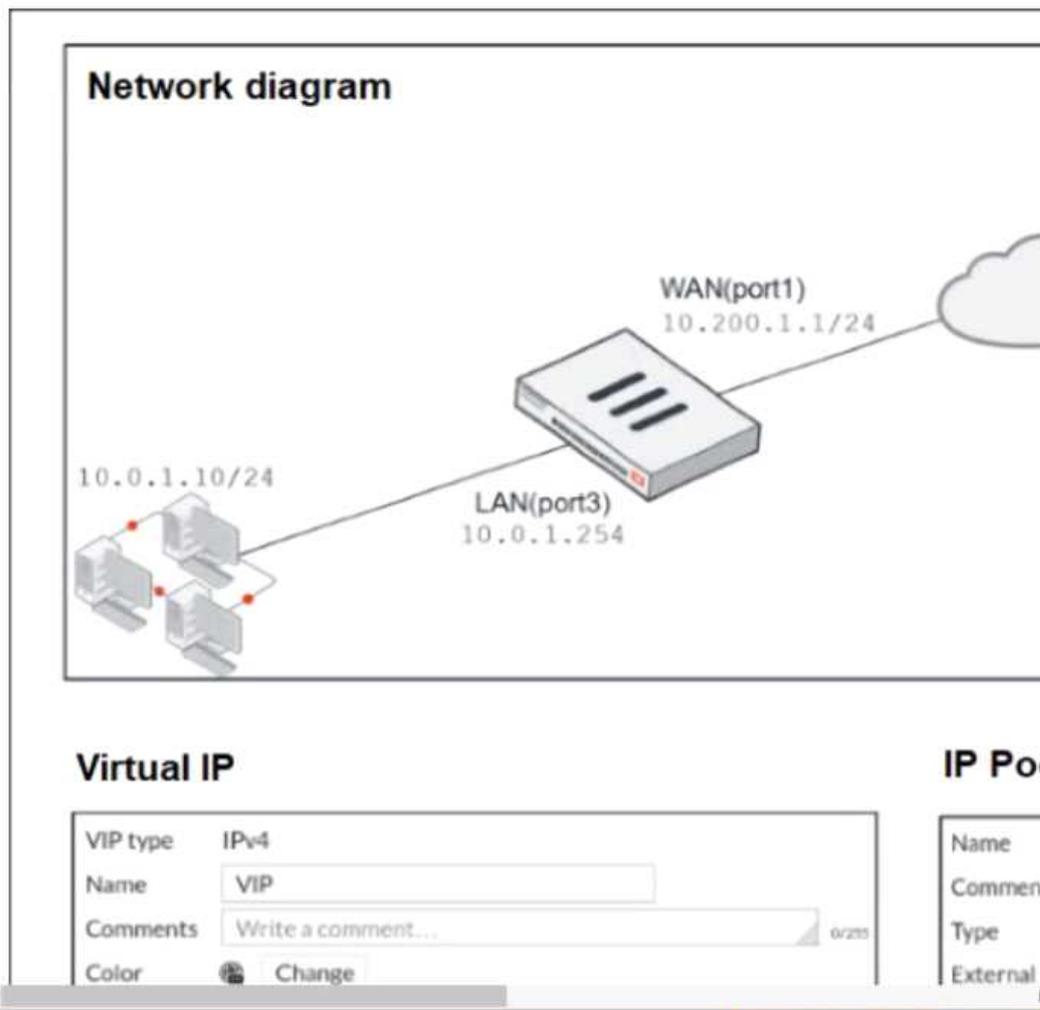
Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

- A. FortiCache
- B. FortiSIEM
- C. FortiAnalyzer
- D. FortiSandbox
- E. FortiCloud

Answer: BCD

Question: 5

Refer to the exhibit.



The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies 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 first firewall policy has NAT enabled using IP Pool. The second firewall policy is configured with a VIP as the destination address. Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0.1.10?

- A. 10.200.1.1
- B. 10.200.3.1
- C. 10.200.1.100
- D. 10.200.1.10

Answer: A

Question: 6

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Exhibit A

Edit Policy

Inspection Mode **Flow-based** Proxy-based

Firewall / Network Options

NAT

IP Pool Configuration **Use Outgoing Interface Address**
Use Dynamic IP Pool

Preserve Source Port

Protocol Options **PRX** default 

Security Profiles

AntiVirus **AV** default 

Web Filter

DNS Filter

Application Control

IPS

SSL Inspection  **SSL** deep-inspection 

Decrypted Traffic Mirror

Exhibit B

Edit AntiVirus Profile

Name

Comments 29/255

Detect Viruses Block Monitor

Feature set Flow-based Proxy-based

Inspected Protocols

HTTP

SMTP

POP3

IMAP

FTP

CIFS

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses

Include Mobile Malware Protection

Virus Outbreak Prevention ⓘ

Use FortiGuard Outbreak Prevention Database

Use External Malware Block List ⓘ ⚠

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 firewall policy performs the full content inspection on the file.
- B. The flow-based inspection is used, which resets the last packet to the user.
- C. The volume of traffic being inspected is too high for this model of FortiGate.
- D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Answer: A

Question: 7

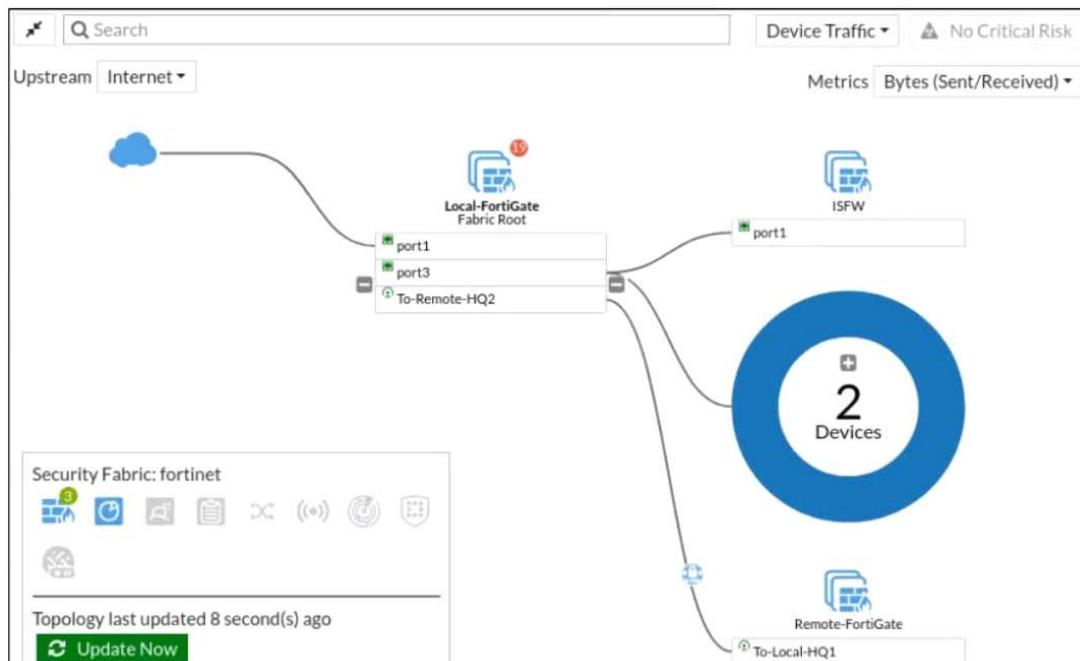
Which two statements about antivirus scanning mode are true? (Choose two.)

- A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
- B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.
- C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
- D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Answer: C, D

Question: 8

Refer to the exhibit.



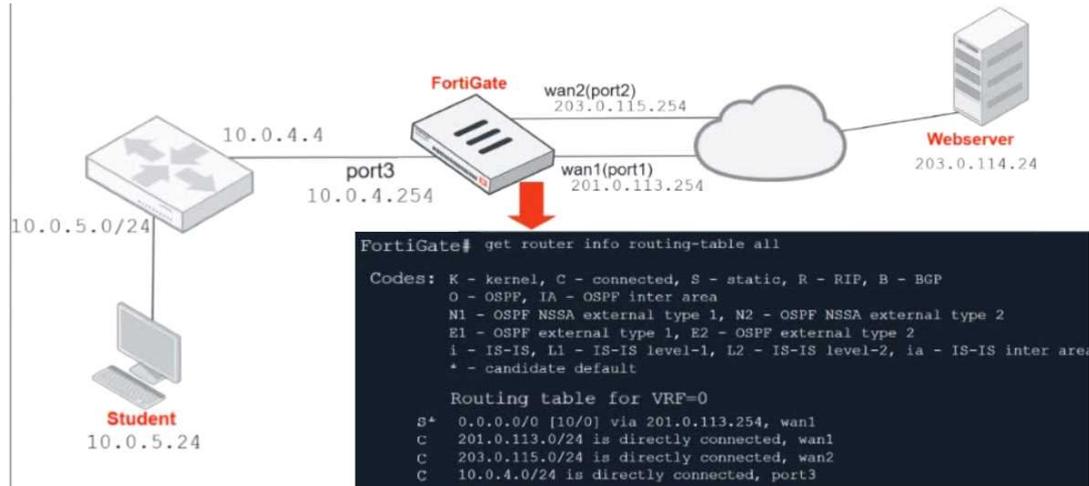
Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

- A. This security fabric topology is a logical topology view.
- B. There are 19 security recommendations for the security fabric.
- C. There are five devices that are part of the security fabric.
- D. Device detection is disabled on all FortiGate devices.

Answer: AD

Question: 9

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 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.

B.

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.

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: C
