NSE4_FGT-7.2 Q&As

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

QUESTION 1

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

A. SSH

B. HTTPS

C. FTM

D. FortiTelemetry

Correct Answer: AB

Reference: https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/995103/buildingsecurity-into-fortios

QUESTION 2

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

A. It limits the scanning of application traffic to the DNS protocol only.

B. It limits the scanning of application traffic to use parent signatures only.

C. It limits the scanning of application traffic to the browser-based technology category only.

D. It limits the scanning of application traffic to the application category only.

Correct Answer: C

FortiGate Security 7.2 Study Guide (p.317): "You can configure the URL Category within the same security policy; however, adding a URL filter causes application control to scan applications in only the browser-based technology category, for example, Facebook Messenger on the Facebook website."

QUESTION 3

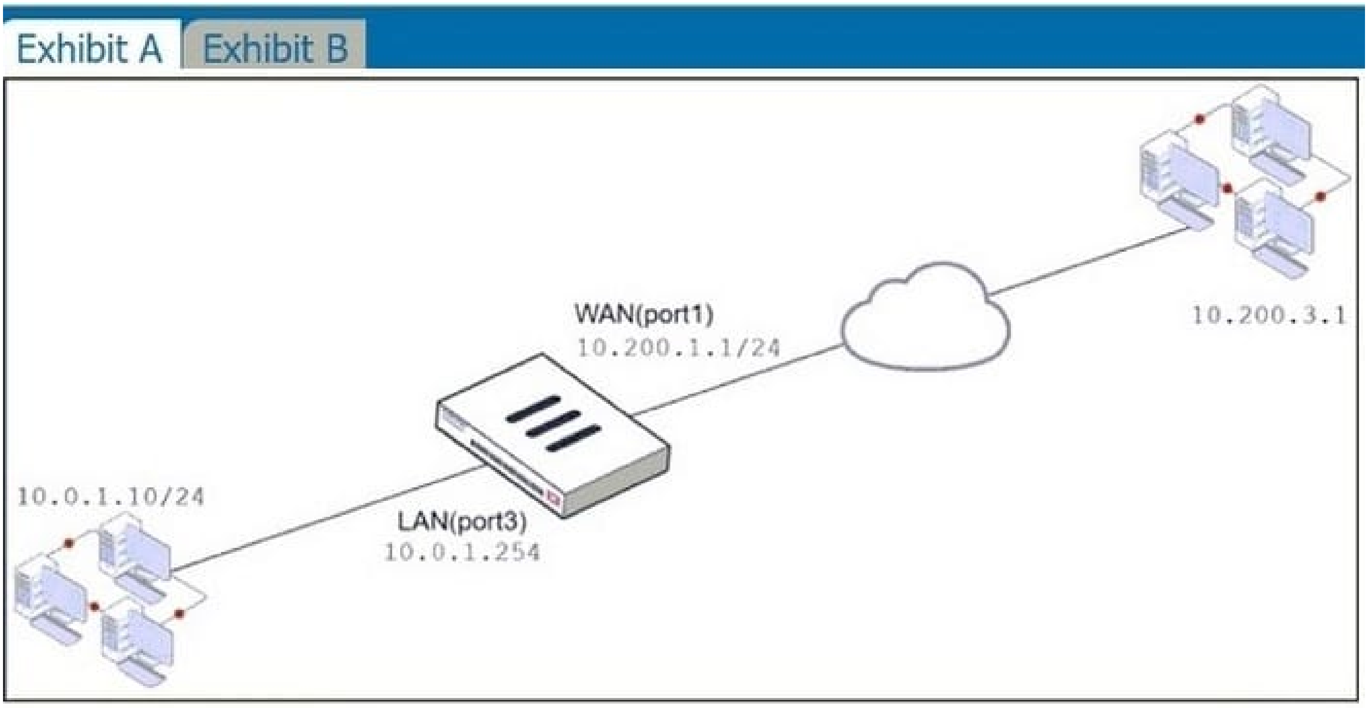
Refer to the exhibits.

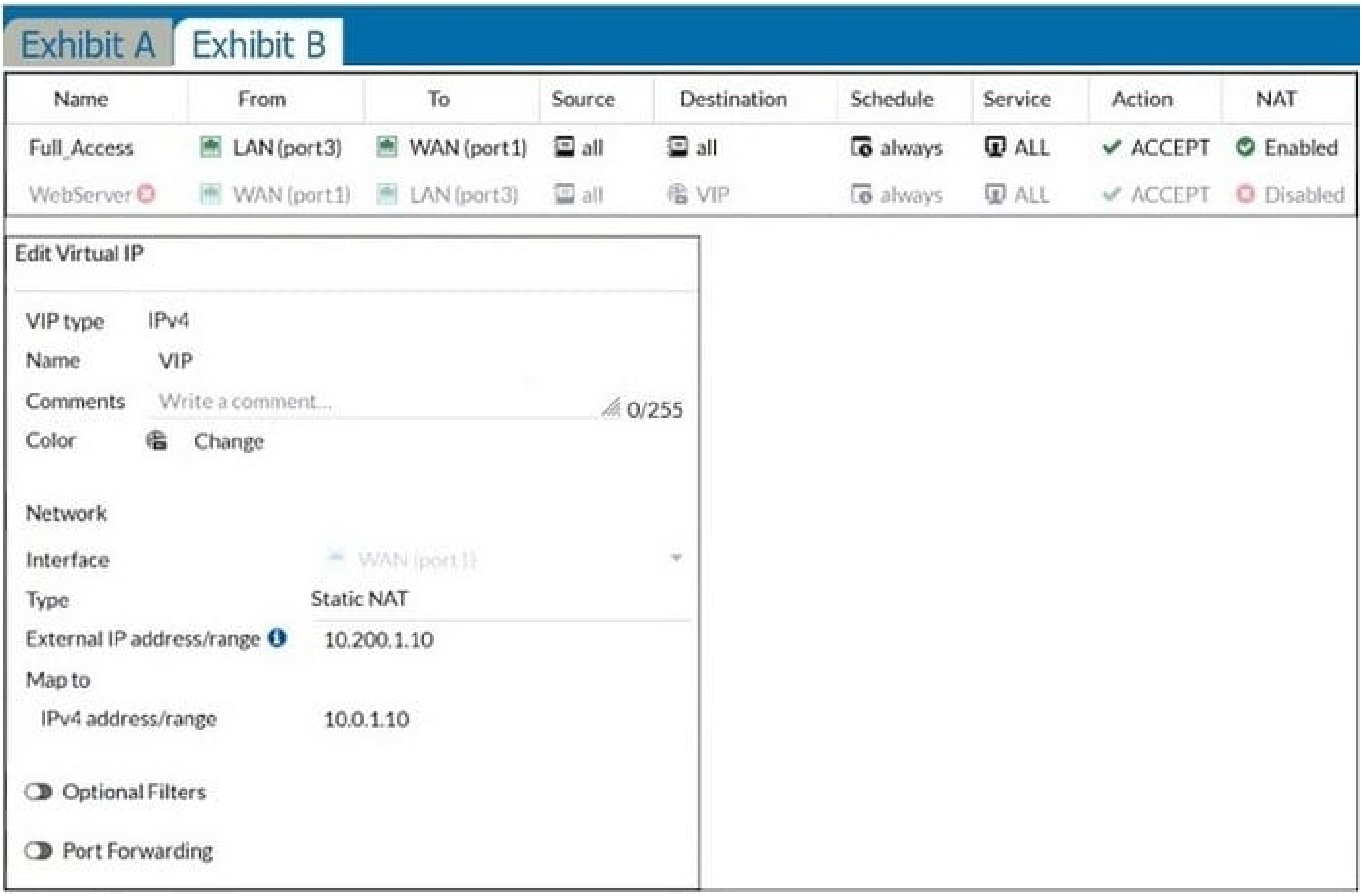
Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.

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.





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

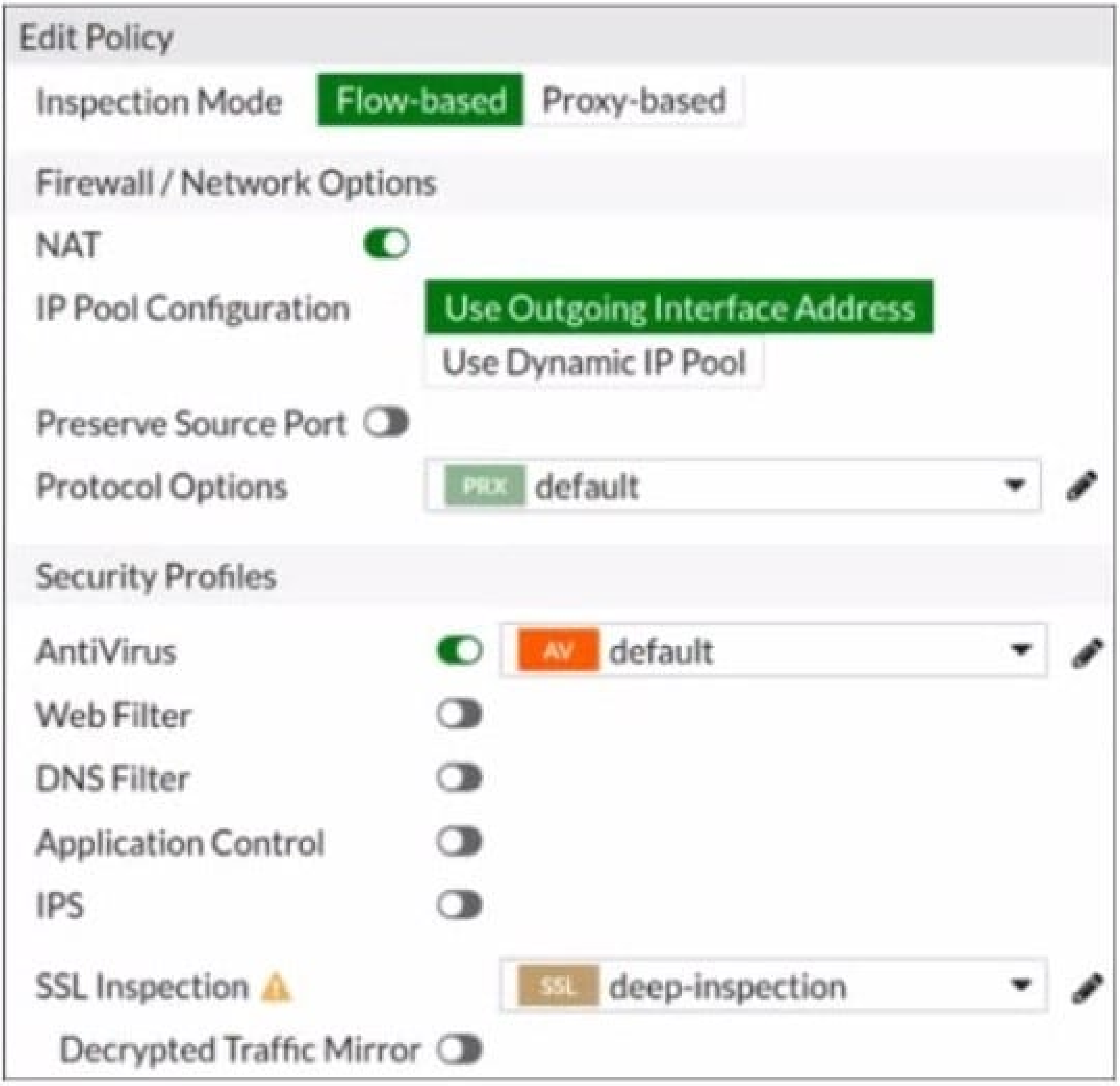
Correct Answer: C

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 4

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 (selected) | Proxy-based

Firewall / Network Options

NAT: ●

IP Pool Configuration: Use Outgoing Interface Address (selected) | Use Dynamic IP Pool

Preserve Source Port: ○

Protocol Options: PRX default

Security Profiles

AntiVirus: ● AV default

Web Filter: ○

DNS Filter: ○

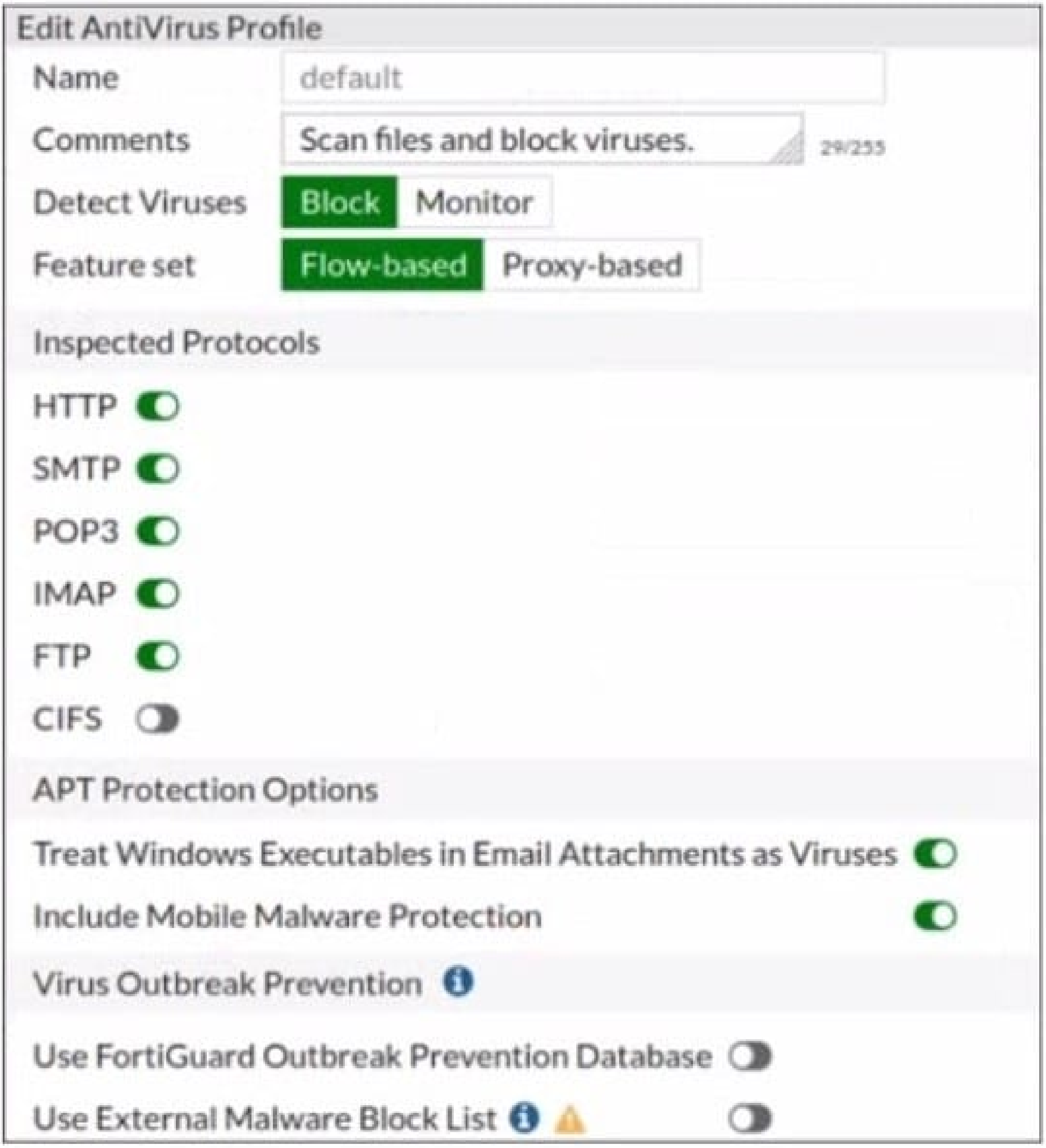
Application Control: ○

IPS: ○

SSL Inspection ⚠: SSL deep-inspection

Decrypted Traffic Mirror: ○

Exhibit B



Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 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.

Correct Answer: B

ONL"; If the virus is detected at the";STAR"; of the connection, the IPS engine sends the block replacement message immediately When a virus is detected on a TCP session (FIRST TIME), but where";SOME PACKET"; have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can\\'t be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again. In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

QUESTION 5

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