# NSE4_FGT-7.2$^{Q\&As}$

Fortinet NSE 4 - FortiOS 7.2

## Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

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

**QUESTION 1**

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

A. Fabric Connectors

B. Automation Stitches

C. Security Rating

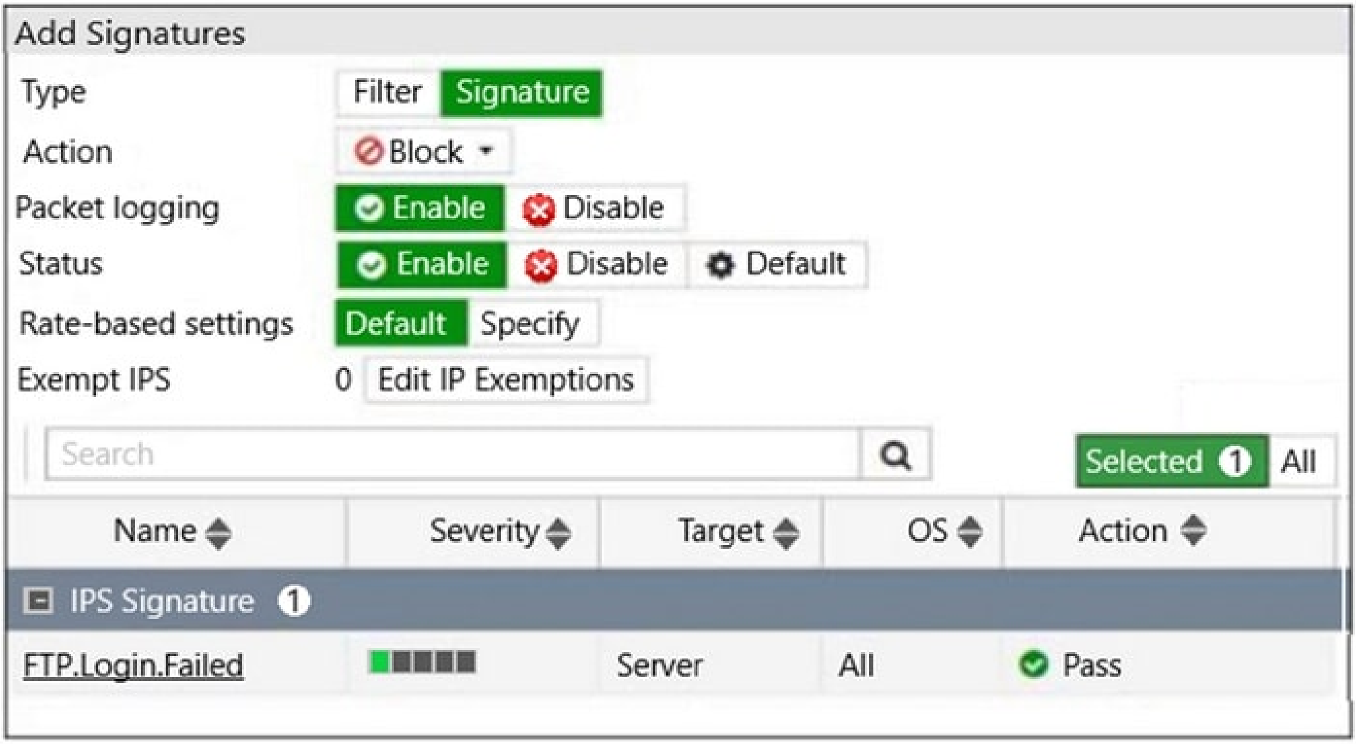
D. Logical Topology

Correct Answer: B

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

**QUESTION 2**

Refer to the exhibit.



Add Signatures

Type: Filter [✓ Signature]

Action: Block

Packet logging: [✓ Enable] Disable

Status: [✓ Enable] Disable Default

Rate-based settings: [✓ Default] Specify

Exempt IPS: 0 Edit IP Exemptions

Search | [✓ Selected 1] All

| Name | Severity | Target | OS | Action |
|---|---|---|---|---|
| IPS Signature 1 | | | | |
| FTP.Login.Failed | 🟩■■■■ | Server | All | ✓ Pass |

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

A. The signature setting uses a custom rating threshold.

B. The signature setting includes a group of other signatures.

C. Traffic matching the signature will be allowed and logged.

D. Traffic matching the signature will be silently dropped and logged.

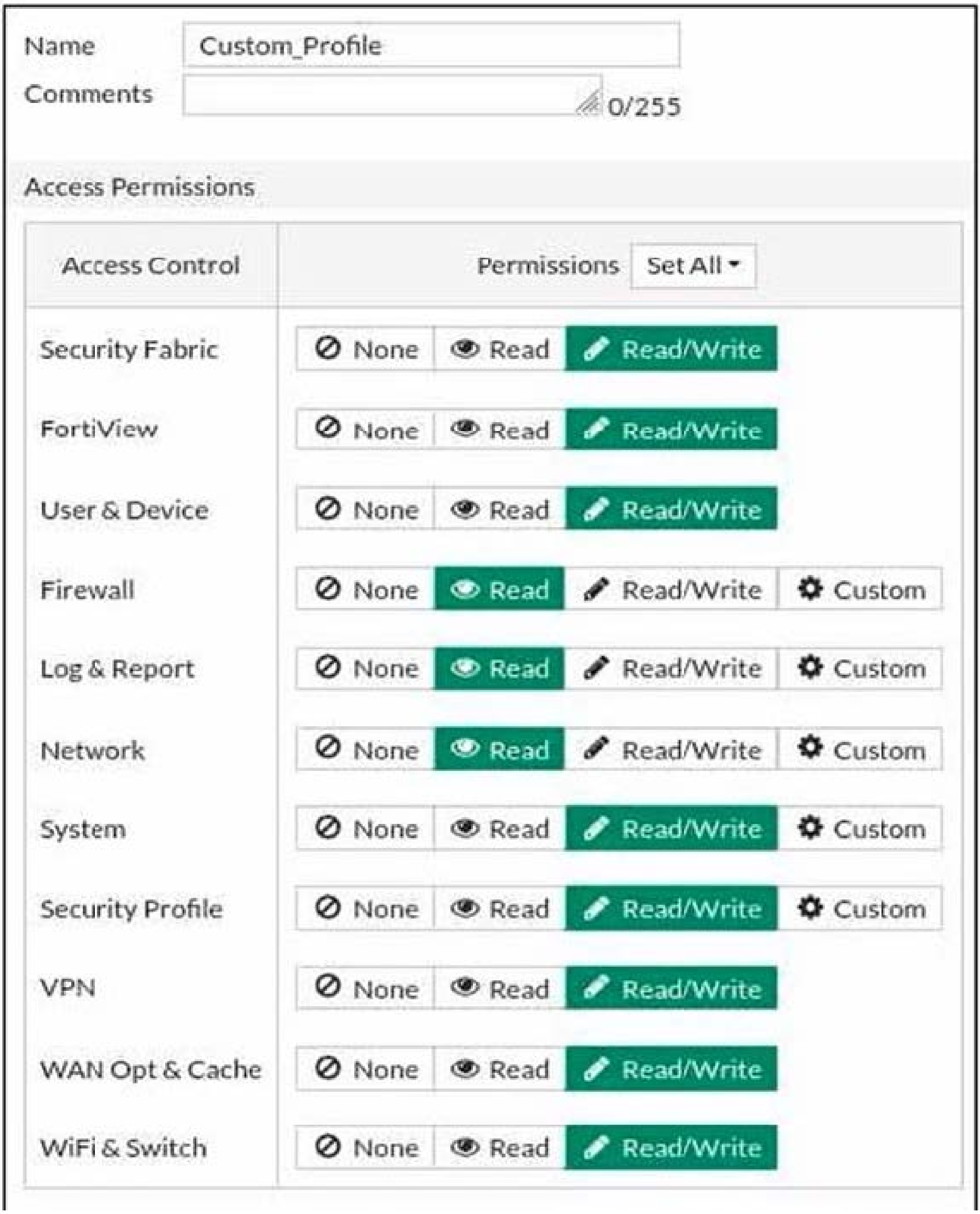
Correct Answer: D

Select Block to silently drop traffic matching any of the signatures included in the entry. So, while the default action would be \\'Pass\\' for this signature the administrator is specifically overriding that to set the Block action. To use the default action the setting would have to be \\'Default\\'.

Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

**QUESTION 3**

Refer to the exhibit.



| | |
|---|---|
| Name | Custom_Profile |
| Comments | 0/255 |

Access Permissions

| Access Control | Permissions Set All ▾ |
|---|---|
| Security Fabric | None · Read · [✓ Read/Write] |
| FortiView | None · Read · [✓ Read/Write] |
| User & Device | None · Read · [✓ Read/Write] |
| Firewall | None · [✓ Read] · Read/Write · Custom |
| Log & Report | None · [✓ Read] · Read/Write · Custom |
| Network | None · [✓ Read] · Read/Write · Custom |
| System | None · Read · [✓ Read/Write] · Custom |
| Security Profile | None · Read · [✓ Read/Write] · Custom |
| VPN | None · Read · [✓ Read/Write] |
| WAN Opt & Cache | None · Read · [✓ Read/Write] |
| WiFi & Switch | None · Read · [✓ Read/Write] |

Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?

A. Custom permission for Network

B. Read/Write permission for Log and Report

C. CLI diagnostics commands permission

D. Read/Write permission for Firewall

Correct Answer: C

https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220

### QUESTION 4

Which statement about video filtering on FortiGate is true?

A. Full SSL Inspection is not required.

B. It is available only on a proxy-based firewall policy.

C. It inspects video files hosted on file sharing services.

D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/190873/video-filtering

### QUESTION 5

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 6

Which timeout setting can be responsible for deleting SSL VPN associated sessions?

A. SSL VPN idle-timeout

B. SSL VPN http-request-body-timeout

C. SSL VPN login-timeout

D. SSL VPN dtls-hello-timeout

Correct Answer: A

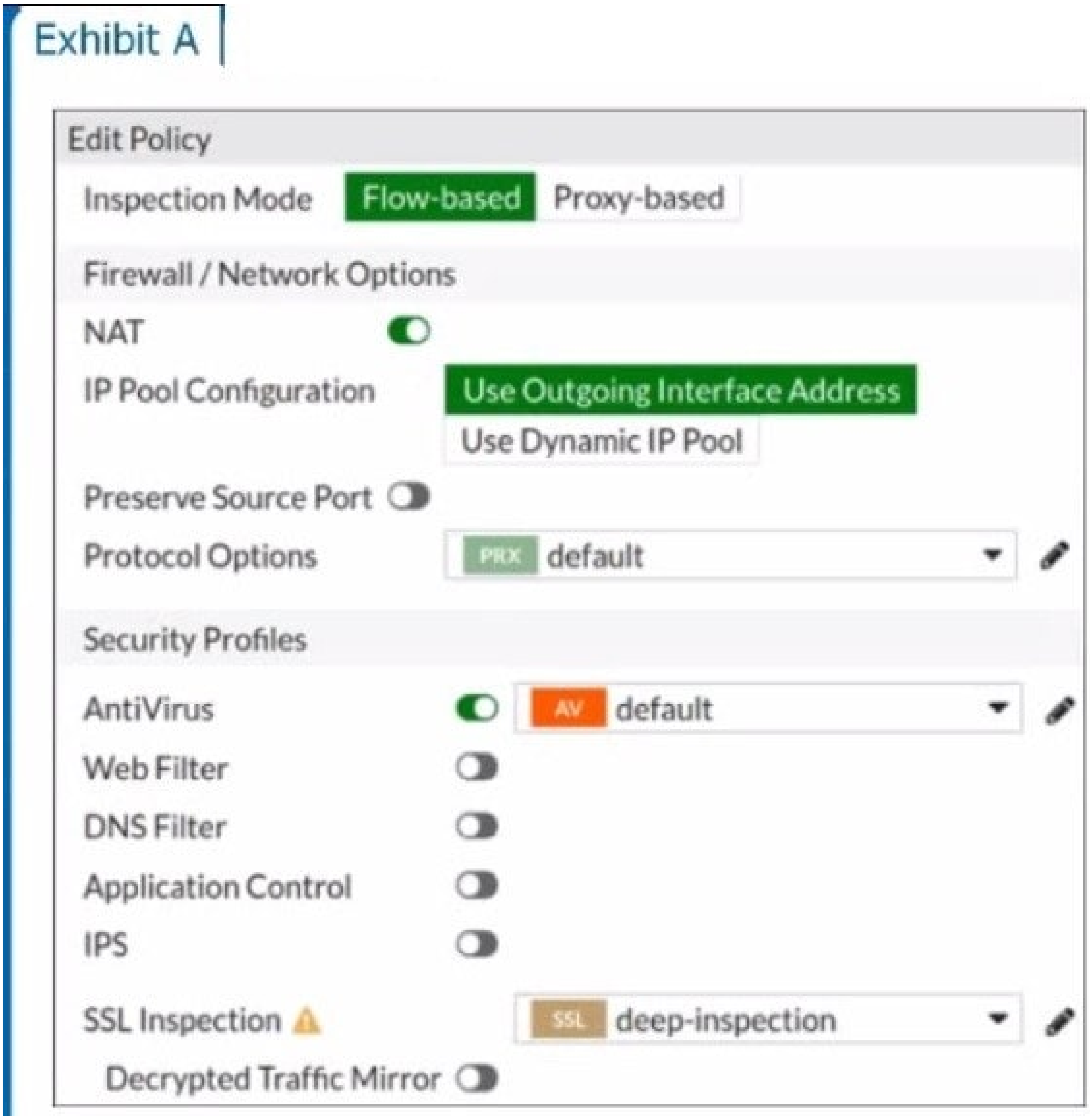
Reference: https://community.fortinet.com/t5/FortiGate/Technical-Tip-SSL-VPN-disconnection-issues-when-connectedwith/ta-p/207851#:~:text=By%20default%2C%20a%20SSL%2DVPN,hours%20due%20to%20auth%2Dtimeout

The SSL VPN idle-timeout setting determines how long an SSL VPN session can be inactive before it is terminated. When an SSL VPN session becomes inactive (for example, if the user closes the VPN client or disconnects from the network), the session timer begins to count down. If the timer reaches the idle-timeout value before the user reconnects or sends any new traffic, the session will be terminated and the associated resources (such as VPN tunnels and virtual interfaces) will be deleted.

**QUESTION 7**

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

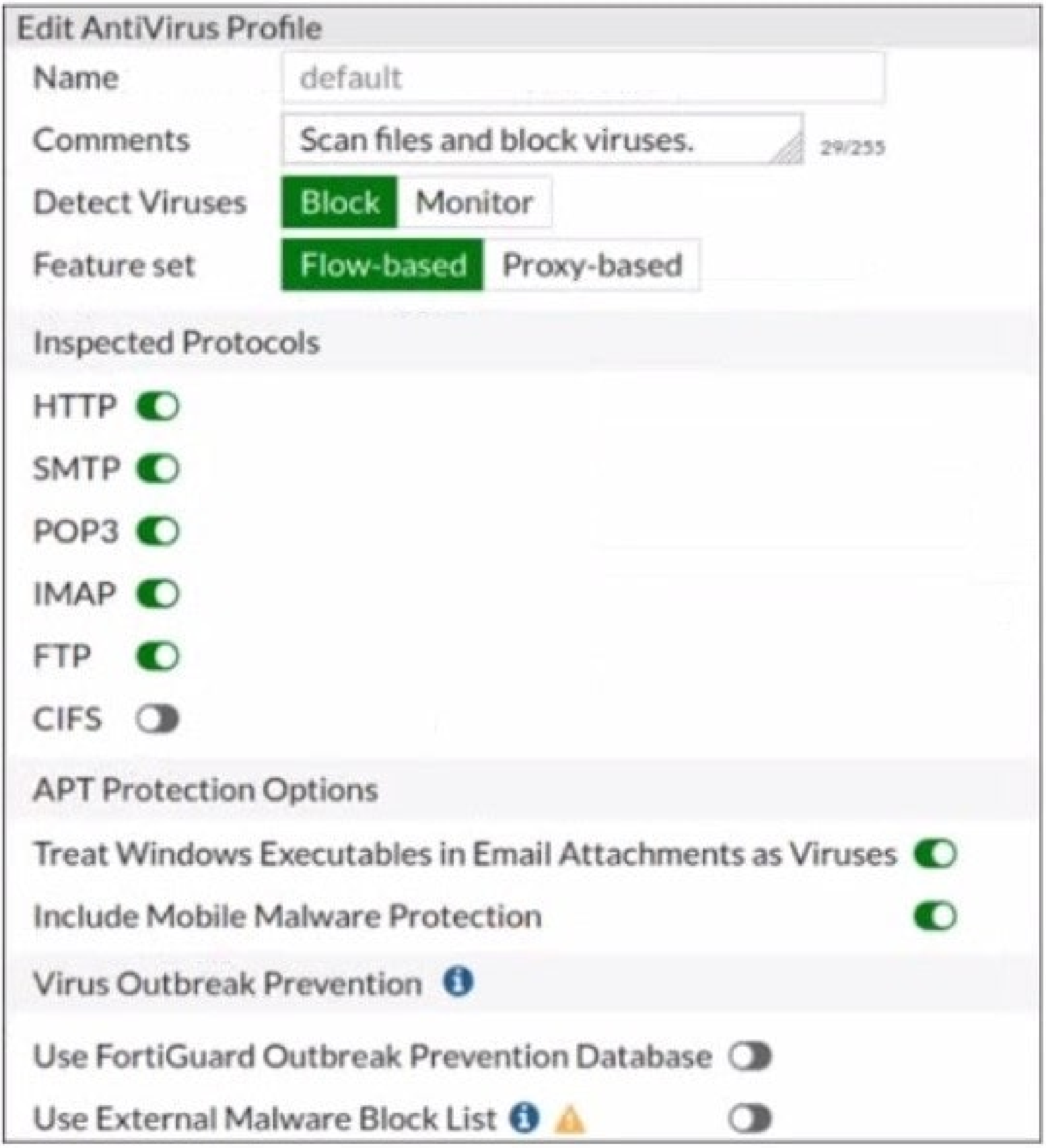
Firewall / Network Options

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 (selected) | Monitor

Feature set: Flow-based (selected) | 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

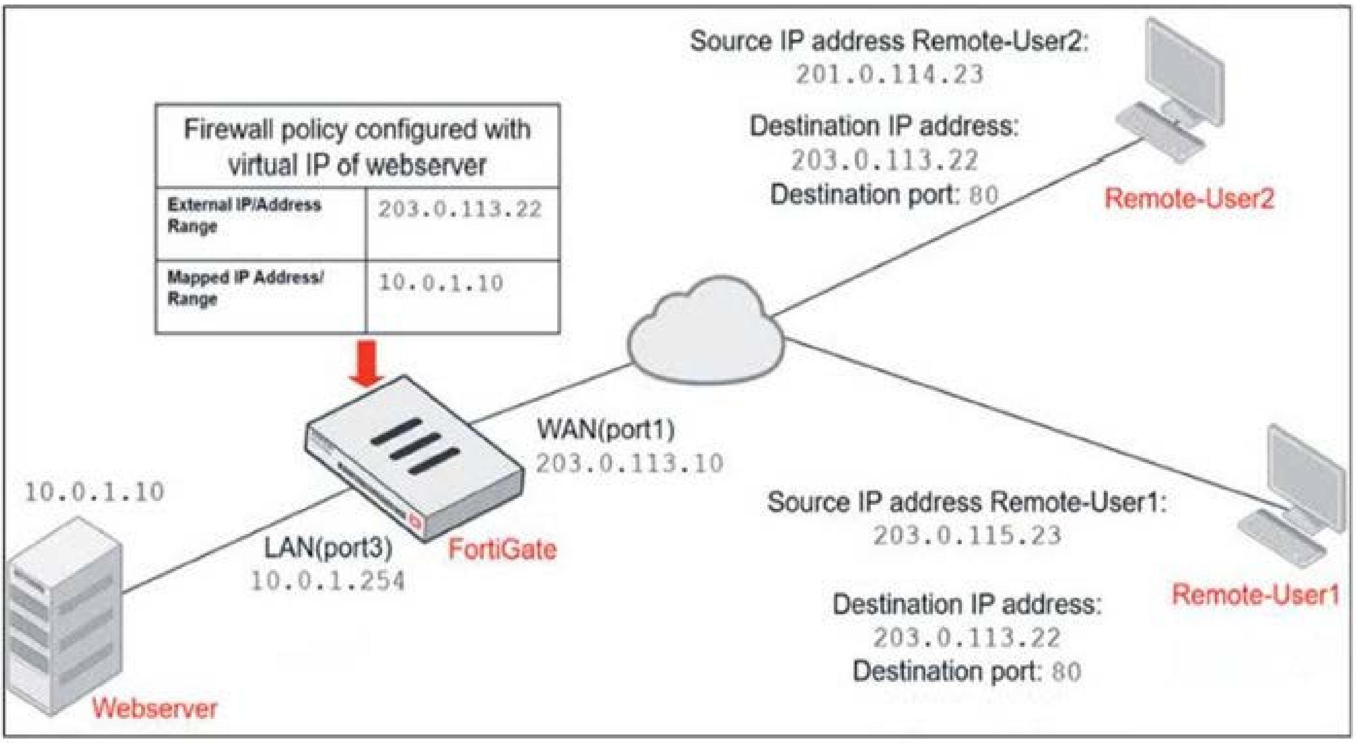
ONL"; If the virus is detected at the";STAR"; of the connection, the IPS engine sends the block replacement message immediately When a virus is detected on a TCP session (FIRST TIME), but where";SOME PACKET"; have been already forwarded to the receiver, FortiGate "resets the connection" and does not 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.

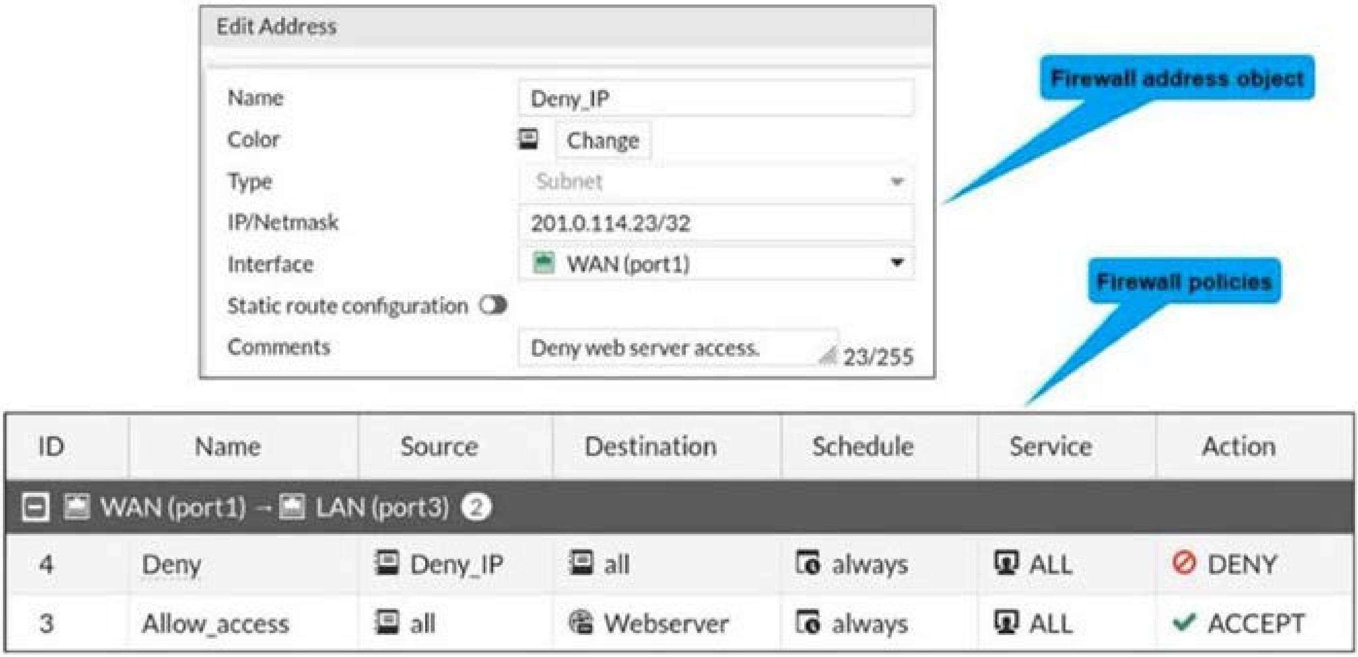
**QUESTION 8**

Refer to the exhibits.

The exhibits show a network diagram and firewall configurations.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver. Remote-User2 must not be able to access the Webserver.





Edit Address

| | |
|---|---|
| Name | Deny_IP |
| Color | Change |
| Type | Subnet |
| IP/Netmask | 201.0.114.23/32 |
| Interface | WAN (port1) |
| Static route configuration | ○ |
| Comments | Deny web server access. 23/255 |

| ID | Name | Source | Destination | Schedule | Service | Action |
|---|---|---|---|---|---|---|
| WAN (port1) → LAN (port3) 2 | | | | | | |
| 4 | Deny | Deny_IP | all | always | ALL | DENY |
| 3 | Allow_access | all | Webserver | always | ALL | ✓ ACCEPT |

In this scenario, which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

A. Disable match-vip in the Deny policy.

B. Set the Destination address as Deny_IP in the Allow-access policy.

C. Enable match vip in the Deny policy.

D. Set the Destination address as Web_server in the Deny policy.

Correct Answer: BC

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta-p/189641

The exhibits show a network diagram and firewall configurations for a FortiGate unit that has two policies: Allow_access and Deny. The Allow_access policy allows traffic from the WAN (port1) interface to the LAN (port3) interface with the destination address of VIP and the service of HTTPS. The VIP object maps the external IP address 10.200.1.10 and port 10443 to the internal IP address 10.0.1.10 and port 443 of the Webserver. The Deny policy denies traffic from the WAN (port1) interface to the LAN (port3) interface with the source address of Deny_IP and the destination address of All. In this scenario, the administrator wants to deny Webserver access for Remote-User2, who has the IP address 10.200.3.2, which is included in the Deny_IP address object. Remote- User1, who has the IP address 10.200.3.1, must be able to access the Webserver. To achieve this goal, the administrator can make two changes to deny Webserver access for Remote-User2: Set the Destination address as Webserver in the Deny policy. This will make the Deny policy more specific and match only the traffic that is destined for the Webserver\\'s internal IP address, instead of any destination address. Enable matchvip in the Deny policy. This will make the Deny policy apply to traffic that matches a VIP object, instead of ignoring it1. This way, the Deny policy will block Remote-User2\\'s traffic that uses the VIP object\\'s external IP address and port.

**QUESTION 9**

By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers.

Which CLI command will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering?

A. set fortiguard-anycast disable

B. set webfilter-force-off disable

C. set webfilter-cache disable

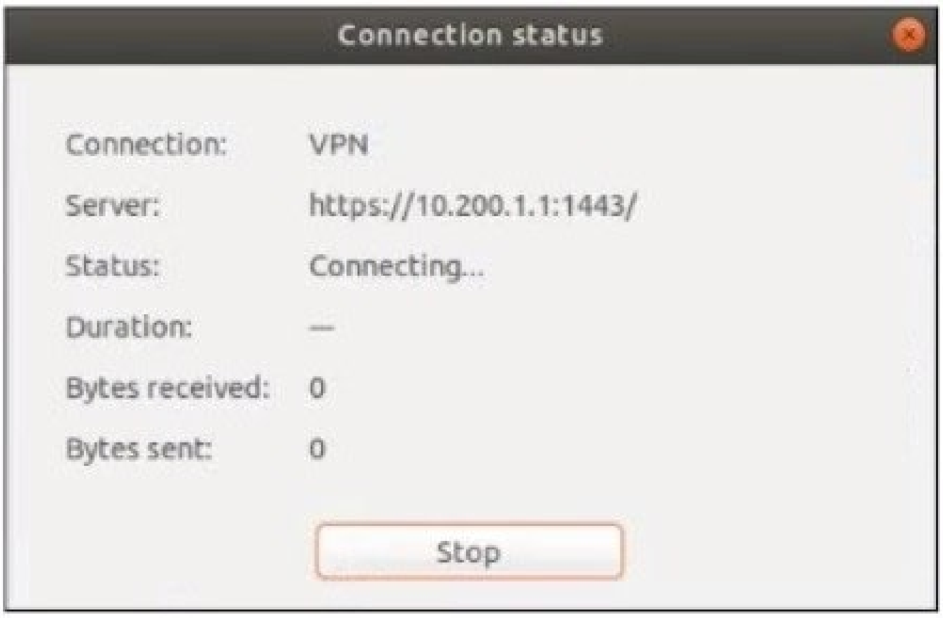
D. set protocol tcp

Correct Answer: A

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD48294

**QUESTION 10**

Refer to the exhibits.


Connection status

Connection: VPN

Server: https://10.200.1.1:1443/

Status: Connecting...

Duration: —

Bytes received: 0

Bytes sent: 0

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 SSL VPN port on the client.

B. Change the Server IP address.

C. Change the idle-timeout.

D. Change the SSL VPN portal to the tunnel.

Correct Answer: A

Reference: https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/150494

**QUESTION 11**

On FortiGate, which type of logs record information about traffic directly to and from the FortiGate management IP addresses?

A. System event logs

B. Forward traffic logs

C. Local traffic logs

D. Security logs

Correct Answer: C

Reference: https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/476970 Traffic logs record the traffic flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through FortiGate, this type of logging is also called firewall policy logging. Firewall policies control all traffic attempting to pass through the FortiGate unit, between FortiGate interfaces, zones, and VLAN sub-interfaces. FortiGate Security 7.2 Study Guide (p.176): "Local traffic logs contain information about traffic directly to and from the FortiGate management IP addresses. They also include connections to the GUI and FortiGuard queries."

**QUESTION 12**

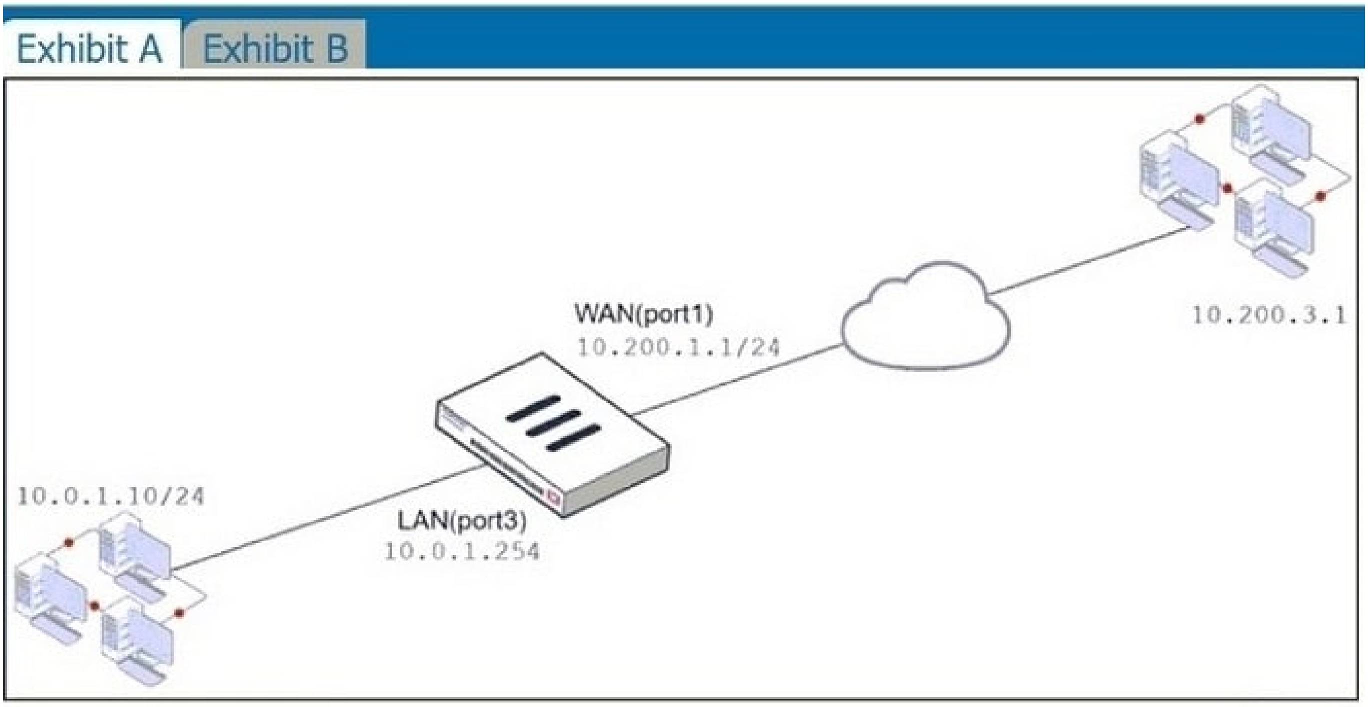
Refer to the exhibits.

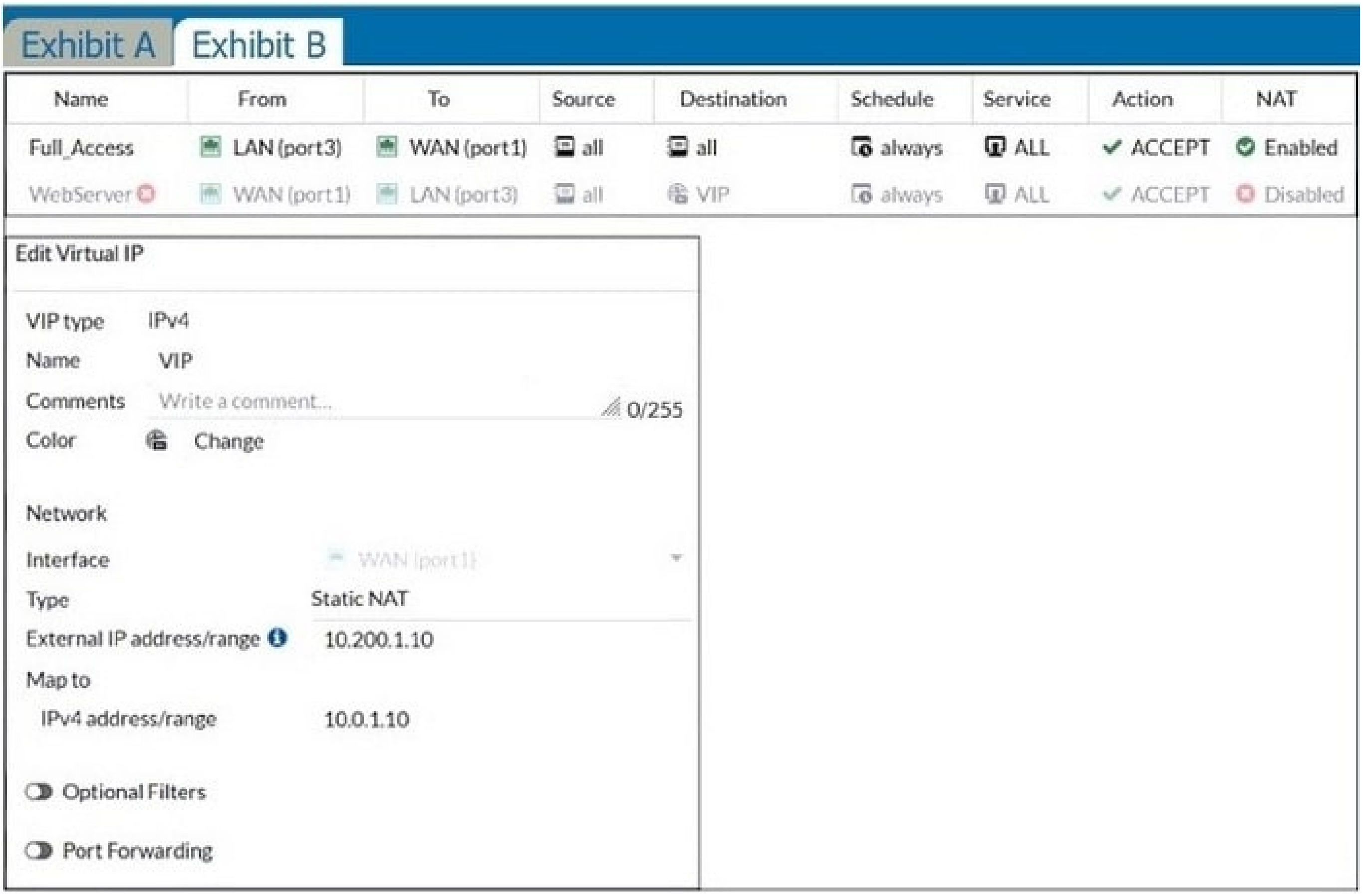
Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.

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 13**

Which two statements are correct about a software switch on FortiGate? (Choose two.)

A. It can be configured only when FortiGate is operating in NAT mode

B. Can act as a Layer 2 switch as well as a Layer 3 router

C. All interfaces in the software switch share the same IP address

D. It can group only physical interfaces

Correct Answer: AC

**QUESTION 14**

An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings.

What is true about the DNS connection to a FortiGuard server?

A. It uses UDP 8888.

B. It uses UDP 53.

C. It uses DNS over HTTPS.

D. It uses DNS overTLS.

Correct Answer: D

FortiGate Security 7.2 Study Guide (p.15): "When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic."

When using FortiGuard servers for DNS, FortiOS defaults to using DNS over TLS (DoT) to secure the DNS traffic1. DNS over TLS is a protocol that encrypts and authenticates DNS queries and responses using the Transport Layer Security (TLS) protocol2. This prevents eavesdropping, tampering, and spoofing of DNS data by third parties. The default FortiGuard DNS servers are 96.45.45.45 and 96.45.46.46, and they use the hostname globalsdns.fortinet.net1. The FortiGate verifies the server hostname using the server-hostname setting in the system dns configuration1.

**QUESTION 15**

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