Actual4Dump

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

http://www.actual4dump.com

Superb Exam Dumps Materials lead you to get your certification easily - Actual4dump

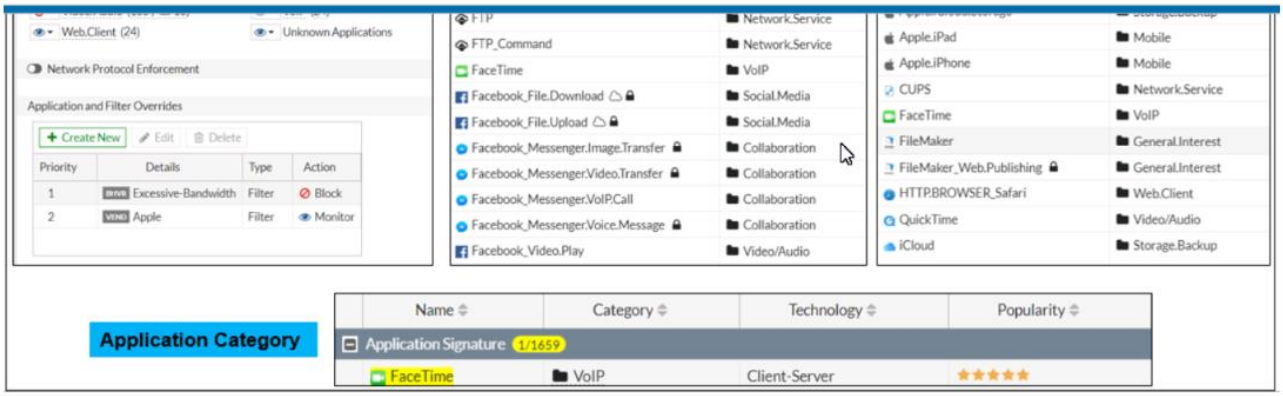
Exam : **C_HRHFC_2311**

Title : Fortinet NSE 4 - FortiOS 7.2

Vendor : Fortinet

Version : DEMO

NO.1 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 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.

Answer: A

NO.2 Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

A. System time

B. FortiGuaid update servers

C. Operating mode

D. NGFW mode

Answer: C,D

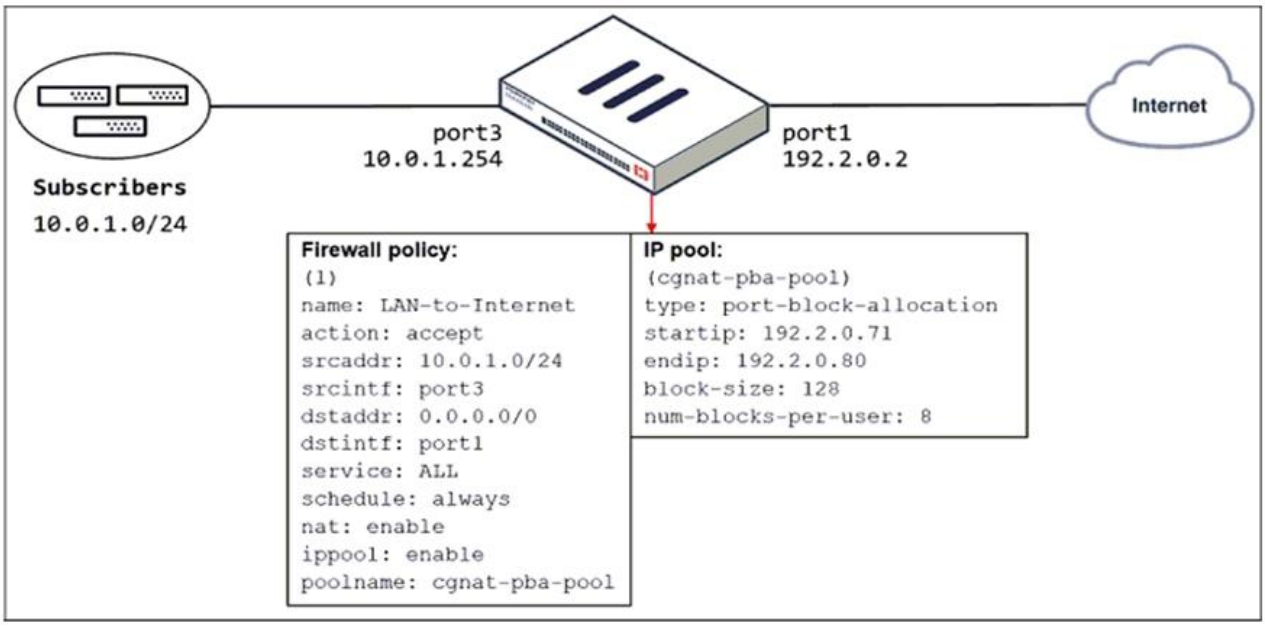
Explanation:

C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.

D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate_Infrastructure_6.4_Study_Guide

NO.3 Refer to the exhibit.

The exhibit shows a diagram of a FortiGate device connected to the network and the firewall policy and IP pool configuration on the FortiGate device.



Which two actions does FortiGate take on internet traffic sourced from the subscribers? (Choose two.)

A. FortiGate allocates port blocks per user, based on the configured range of internal IP addresses.

B. FortiGate allocates port blocks on a first-come, first-served basis.

C. FortiGate generates a system event log for every port block allocation made per user.

D. FortiGate allocates 128 port blocks per user.

Answer: B,C

Explanation:

FortiGate Security 7.2 Study Guide (p.109): "FortiGate allocates port blocks on a first-come, first-served basis." "For logging purposes, when FortiGate allocates a port block to a host, it generates a system event log to inform the administrator."

NO.4 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.

Answer: B,C

Explanation:

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://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-troubleshoot-FSSO-agentless-polling/ta-p/214349

NO.5 A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.
What is the reason for the certificate warning errors?
A. The matching firewall policy is set to proxy inspection mode.
B. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
C. The full SSL inspection feature does not have a valid license.
D. The browser does not trust the certificate used by FortiGate for SSL inspection.
Answer: D
Explanation:
FortiGate Security 7.2 Study Guide (p.235): "If FortiGate receives a trusted SSL certificate, then it generates a temporary certificate signed by the built-in Fortinet_CA_SSL certificate and sends it to the browser. If the browser trusts the Fortinet_CA_SSL certificate, the browser completes the SSL handshake. Otherwise, the browser also presents a warning message informing the user that the site is untrusted. In other words, for this function to work as intended, you must import the Fortinet_CA_SSL certificate into the trusted root CA certificate store of your browser."

NO.6 When configuring a firewall virtual wire pair policy, which following statement is true?
A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
B. Only a single virtual wire pair can be included in each policy.
C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
D. Exactly two virtual wire pairs need to be included in each policy.
Answer: A

NO.7 An administrator does not want to report the logon events of service accounts to FortiGate.
What setting on the collector agent is required to achieve this?
A. Add the support of NTLM authentication.
B. Add user accounts to Active Directory (AD).
C. Add user accounts to the FortiGate group fitter.
D. Add user accounts to the Ignore User List.
Answer: D

NO.8 What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)
A. FortiGate uses fewer resources.
B. FortiGate performs a more exhaustive inspection on traffic.
C. FortiGate adds less latency to traffic.
D. FortiGate allocates two sessions per connection.

Answer: A,C
Reference:
Flow-based inspection is a type of traffic inspection that is used by some firewall devices, including FortiGate, to analyze network traffic. It is designed to be more efficient and less resource-intensive than proxy-based inspection, and it offers several benefits over this approach.
Two benefits of flow-based inspection compared to proxy-based inspection are:
FortiGate uses fewer resources: Flow-based inspection uses fewer resources than proxy-based inspection, which can help to improve the performance of the firewall device and reduce the impact on overall system performance.
FortiGate adds less latency to traffic: Flow-based inspection adds less latency to traffic than proxy-based inspection, which can be important for real-time applications or other types of traffic that require low latency.

NO.9 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.
Answer: B

NO.10 Which three statements explain a flow-based antivirus profile? (Choose three.)
A. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
B. If a virus is detected, the last packet is delivered to the client.
C. The IPS engine handles the process as a standalone.
D. FortiGate buffers the whole file but transmits to the client at the same time.
E. Flow-based inspection optimizes performance compared to proxy-based inspection.
Answer: A,D,E

NO.11 Refer to the exhibit to view the firewall policy
Why would the firewall policy not block a well-known virus, for
example eicar?
A. Web filter is not enabled on the firewall policy to complement the antivirus profile.
B. The firewall policy does not apply deep content inspection.
C. The firewall policy is not configured in proxy-based inspection mode.
D. The action on the firewall policy is not set to deny
Answer: B

NO.12 Which statement about video filtering on FortiGate is true?
A. Video filtering FortiGuard categories are based on web filter FortiGuard categories.
B. It does not require a separate FortiGuard license.
C. Full SSL inspection is not required.
D. its available only on a proxy-based firewall policy.
Answer: D
Explanation:

FortiGate Security 7.2 Study Guide (p.279): "To apply the video filter profile, proxy-based firewall polices currently allow you to enable the video filter profile. You must enable full SSL inspection on the firewall policy."
https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/860867/filtering-based-on-fortiguard-categories

NO.13 To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

A. FortiManager

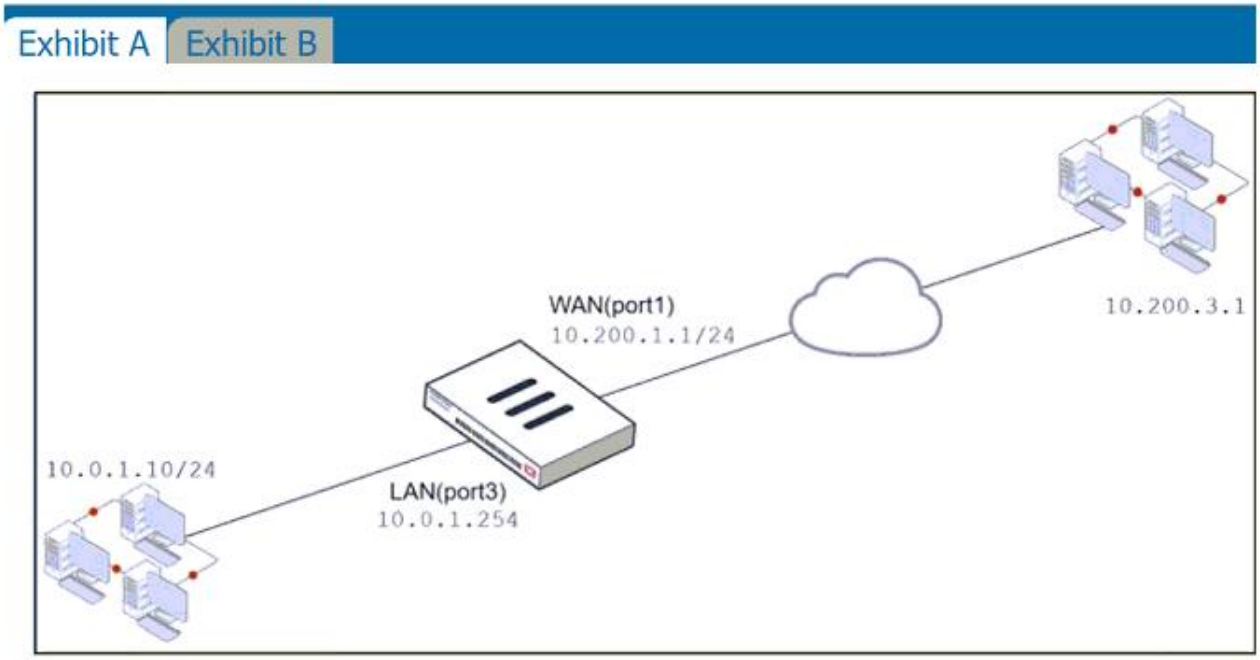
B. Root FortiGate

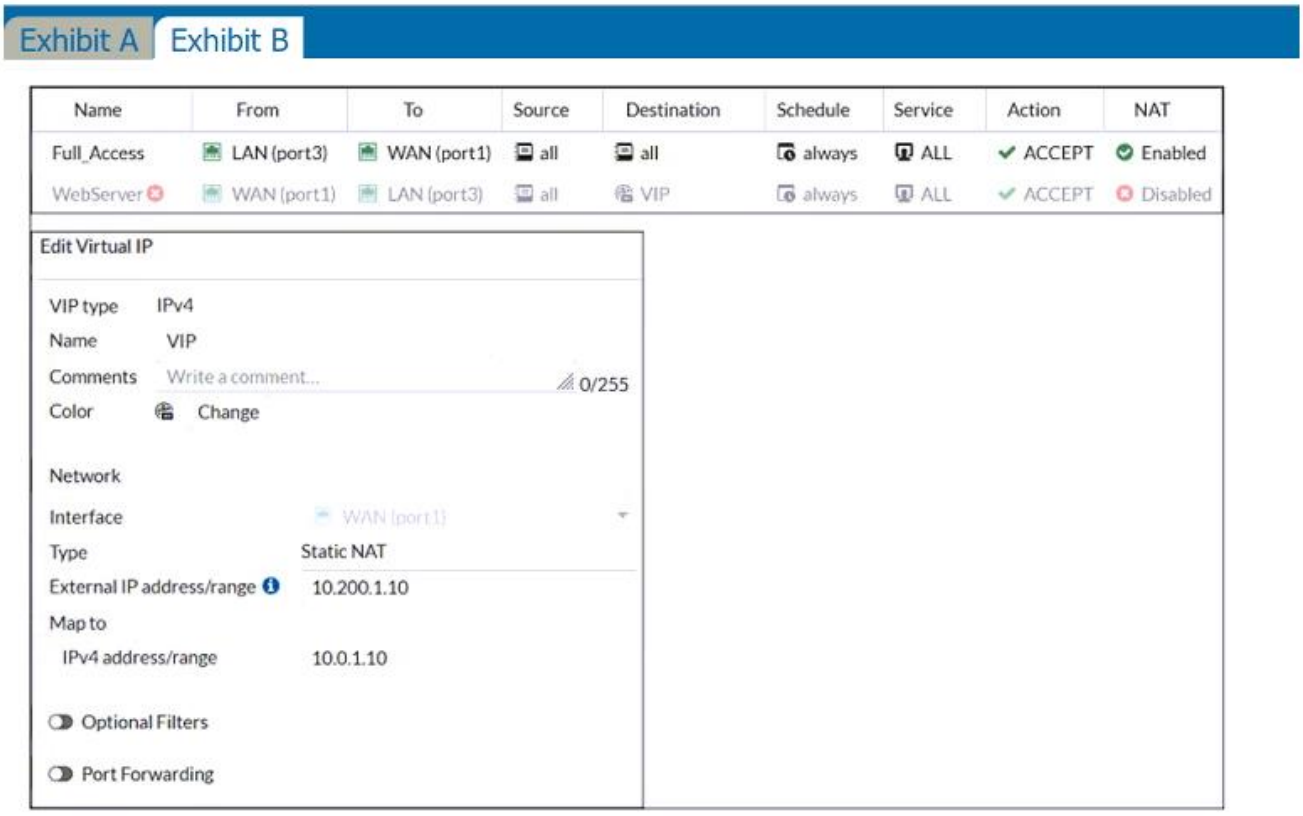
C. FortiAnalyzer

D. Downstream FortiGate

Answer: B

NO.14 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.





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

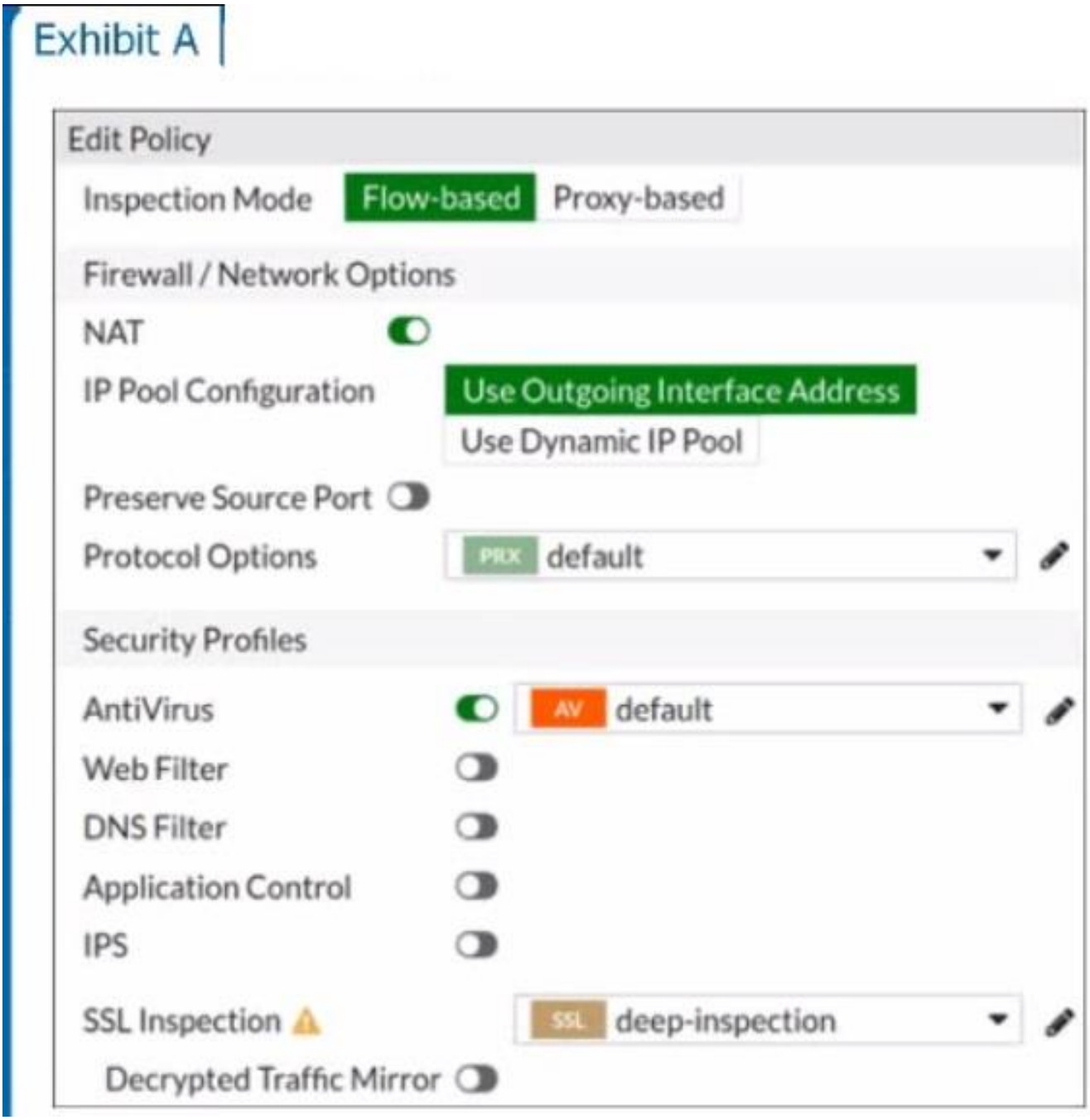
Answer: C

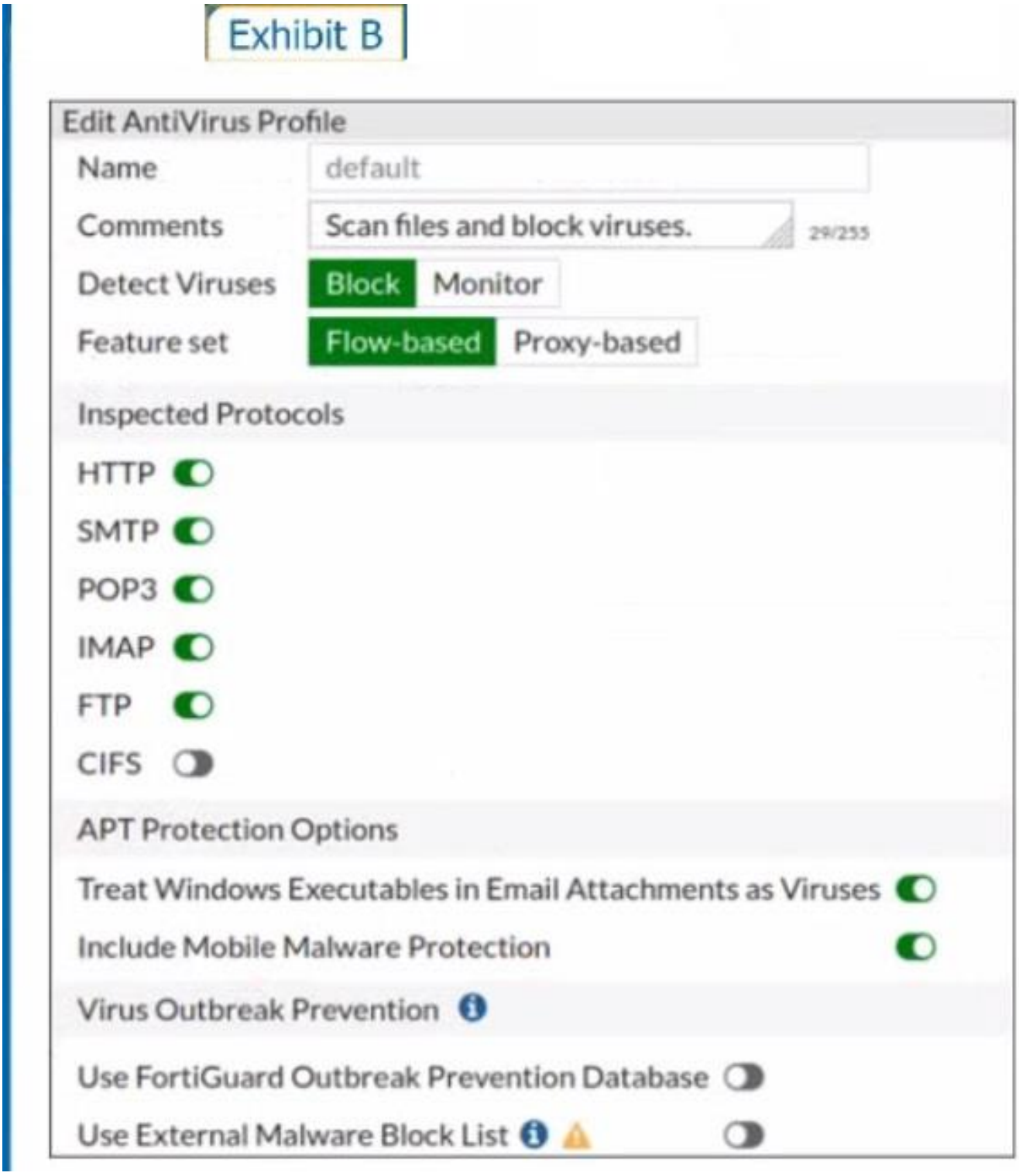
Explanation:

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.

NO.15 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



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.

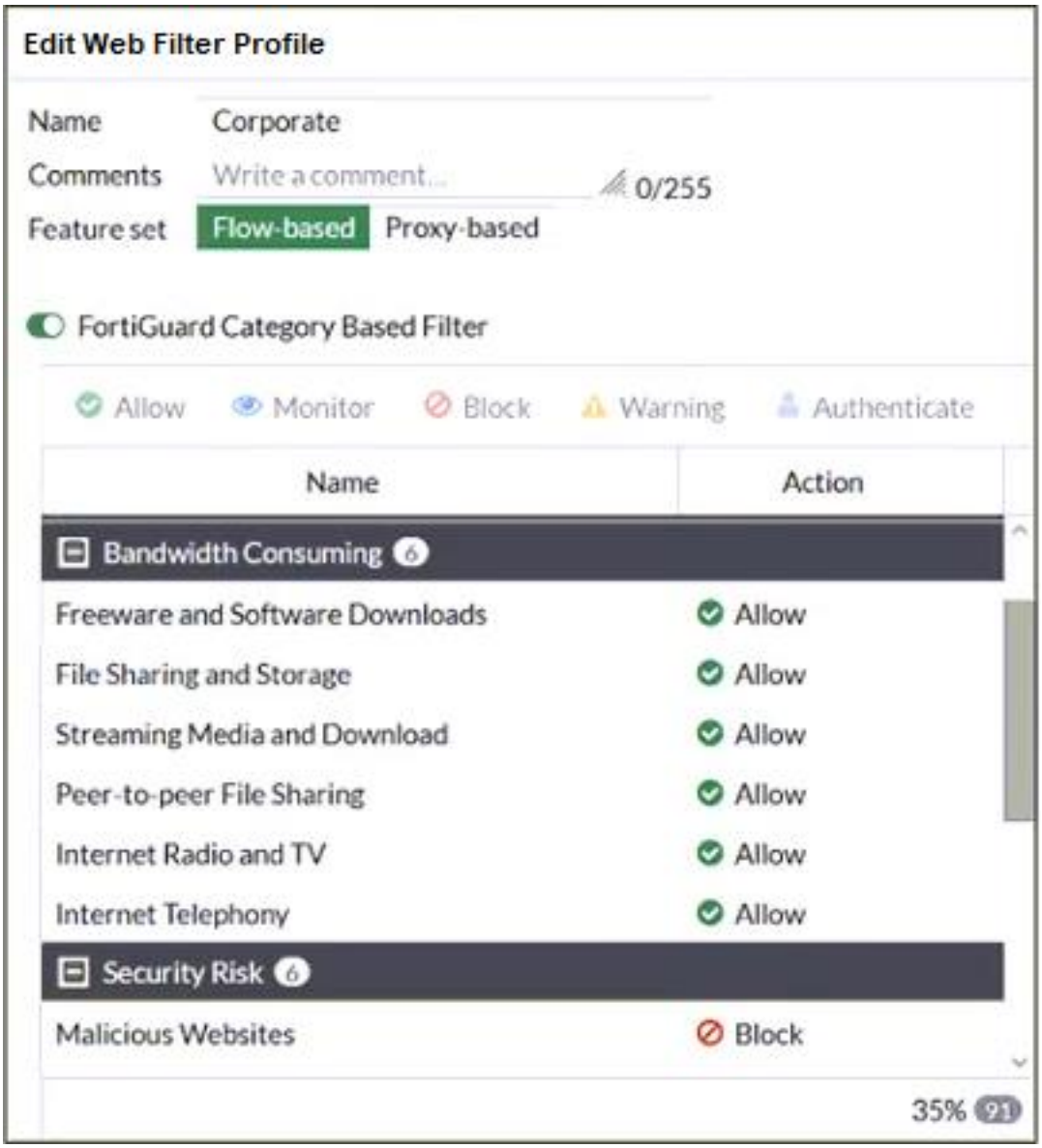
Answer: B

Explanation:

* "ONLY" If the virus is detected at the "START" 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 PACKETS" 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.

NO.16 An administrator has a requirement to keep an application session from timing out on port 80. What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)
A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
B. Create a new service object for HTTP service and set the session TTL to never
C. Set the TTL value to never under config system-ttl
D. Set the session TTL on the HTTP policy to maximum
Answer: B,C

NO.17 Refer to the exhibit.
The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.
An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.



What are two solutions for satisfying the requirement? (Choose two.)

A. Configure a separate firewall policy with action Deny and an FQDN address object for *.download.com as destination address.

B. Configure a web override rating for download.com and select Malicious Websites as the subcategory.

C. Set the Freeware and Software Downloads category Action to Warning.

D. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

Answer: B,D

Explanation:

FortiGate Security 7.2 Study Guide (p.268-269): "If you want to make an exception, for example, rather than unblock access to a potentially unwanted category, change the website to an allowed category. You can also do the reverse. You can block a website that belongs to an allowed category." "Static URL filtering is another web filter feature. Configured URLs in the URL filter are checked against the visited websites. If a match is found, the configured action is taken. URL filtering has the same patterns as static domain filtering: simple, regular expressions, and wildcard." B) Configure a web override rating for download.com and select Malicious Websites as the subcategory.

This is true because a web override rating is a feature that allows the administrator to change the FortiGuard category of a specific website or domain, and apply a different action to it based on the web filter profile. By configuring a web override rating for download.com and selecting Malicious Websites as the subcategory, the administrator can block access to download.com, which belongs to the Freeware and Software Downloads category by default, without affecting other websites in the same category. The Malicious Websites category has the action Block in the web filter profile shown in the exhibit.
D) Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.
This is true because a static URL filter entry is a feature that allows the administrator to define custom rules for filtering specific URLs or domains, and apply an action to them based on the web filter profile. By configuring a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively, the administrator can block access to download.com and any subdomains or paths under it, without affecting other websites in the Freeware and Software Downloads category. The static URL filter entries have higher priority than the FortiGuard category based filter entries in the web filter profile.

NO.18 If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

A. A CRL

B. A person

C. A subordinate CA

D. A root CA

Answer: D