

Fortinet

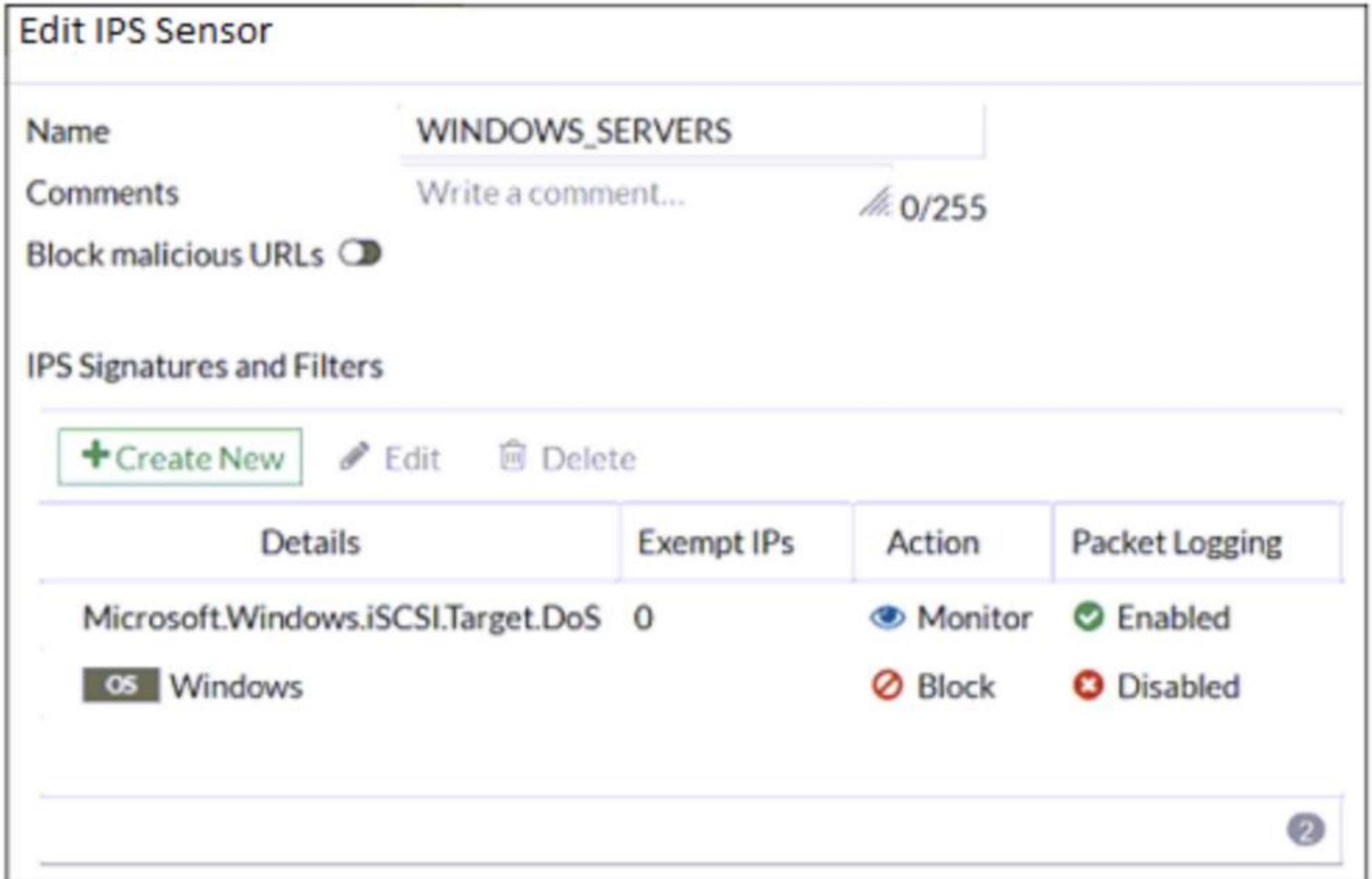
Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator



NEW QUESTION 1

Refer to the exhibit, which shows the IPS sensor configuration.



Edit IPS Sensor

Name:

Comments: 0/255

Block malicious URLs:

IPS Signatures and Filters

[+ Create New](#) [Edit](#) [Delete](#)

Details	Exempt IPs	Action	Packet Logging
Microsoft.Windows.iSCSI.Target.DoS OS Windows	0	<input checked="" type="radio"/> Monitor <input type="radio"/> Block	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled

2

If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

- A. The sensor will gather a packet log for all matched traffic.
- B. The sensor will reset all connections that match these signatures.
- C. The sensor will allow attackers matching the Microsoft.Windows.iSCSI.Target.DoS signature.
- D. The sensor will block all attacks aimed at Windows servers.

Answer: AC

Explanation:

The IPS sensor configuration shows that:

➤ The Microsoft.Windows.iSCSI.Target.DoS signature is set to "Monitor" with packet logging enabled, meaning that while traffic matching this signature will be allowed, it will also be logged for further analysis.

➤ The generic Windows filter is set to "Block," meaning that all other attacks matching this filter will be blocked. However, the sensor will not reset connections or log packets unless specified.

Therefore, the sensor will allow attackers matching the specific DoS signature while blocking other attacks against Windows.

References:

➤ FortiOS 7.4.1 Administration Guide: IPS Configuration

NEW QUESTION 2

Refer to the exhibits, which show the firewall policy and an antivirus profile configuration.

Edit Antivirus Profile

Name: default

Comments: Scan files and block viruses.  29/255

AntiVirus scan  **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 

Send files to FortiSandbox for inspection 

Send files to FortiNDR for inspection 

Include mobile malware protection

Quarantine 

Virus Outbreak Prevention

Use FortiGuard outbreak prevention database

Use external malware block list

Use EMS threat feed 

Why is the user unable to receive a block replacement message when downloading an infected file for the first time?

- A. The intrusion prevention security profile must be enabled when using flow-based inspection mode.
- B. The option to send files to FortiSandbox for inspection is enabled.
- C. The firewall policy performs a full content inspection on the file.

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

Answer: D

Explanation:

In flow-based inspection mode, FortiGate sends a reset (RST) packet to the client instead of providing a replacement message, which causes the block message not to be displayed.

NEW QUESTION 3

What are two features of collector agent advanced mode? (Choose two.)

- A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
- B. Advanced mode supports nested or inherited groups.
- C. In advanced mode, security profiles can be applied only to user groups, not individual users.
- D. Advanced mode uses the Windows convention —NetBios: Domain\Username.

Answer: AD

Explanation:

Advanced mode allows for configuration as an LDAP client and supports group filtering directly on the FortiGate, as well as nested or inherited groups.

NEW QUESTION 4

Which inspection mode does FortiGate use for application profiles if it is configured as a profile-based next-generation firewall (NGFW)?

- A. Full content inspection
- B. Proxy-based inspection
- C. Certificate inspection
- D. Flow-based inspection

Answer: D

Explanation:

When FortiGate is configured in NGFW profile-based mode, it primarily uses flow-based inspection for application profiles. Flow-based inspection provides faster processing and lower latency by inspecting traffic in real-time without buffering, making it suitable for scenarios where performance is a priority.

References:

[FortiOS 7.4.1 Administration Guide: Inspection Modes](#)

NEW QUESTION 5

Refer to the exhibit.

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Critical-DIA	4 LOCAL_SUBNET	Slack-Slack Dropbox-Web Bloomberg		port1 <input checked="" type="checkbox"/> port2
2	Non-Critical-DIA	4 LOCAL_SUBNET	Addicting.Games Social.Media	Bandwidth	port2 <input checked="" type="checkbox"/>
3	Default-Internet	4 LOCAL_SUBNET	4 REMOTE_SUBNET	Latency	port1 port2
Implicit 1					
	sd-wan	4 all	4 all	Source-Destination IP	<input type="checkbox"/> any

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

- A. All traffic from a source IP to a destination IP is sent to the same interface.
- B. Traffic is sent to the link with the lowest latency.
- C. Traffic is distributed based on the number of sessions through each interface.
- D. All traffic from a source IP is sent to the same interface

Answer: A

Explanation:

For traffic that does not match any of the defined SD-WAN rules, the default implicit SD-WAN rule is applied. By default, the FortiGate uses a "source-destination IP-based" algorithm, which means all traffic from a specific source IP to a specific destination IP is sent through the same interface. This ensures that a consistent path is used for traffic between the same source and destination IP addresses. Options B, C, and D do not apply because the default algorithm does not prioritize by latency, session count, or source IP alone.

References:

[FortiOS 7.4.1 Administration Guide: SD-WAN Load Balancing Algorithms](#)

NEW QUESTION 6

An administrator manages a FortiGate model that supports NTurbo. How does NTurbo enhance performance for flow-based inspection?

- A. NTurbo offloads traffic to the content processor.
- B. NTurbo creates two inspection sessions on the FortiGate device.
- C. NTurbo buffers the whole file and then sends it to the antivirus engine.
- D. NTurbo creates a special data path to redirect traffic between the IPS engine its ingress and egress interfaces.

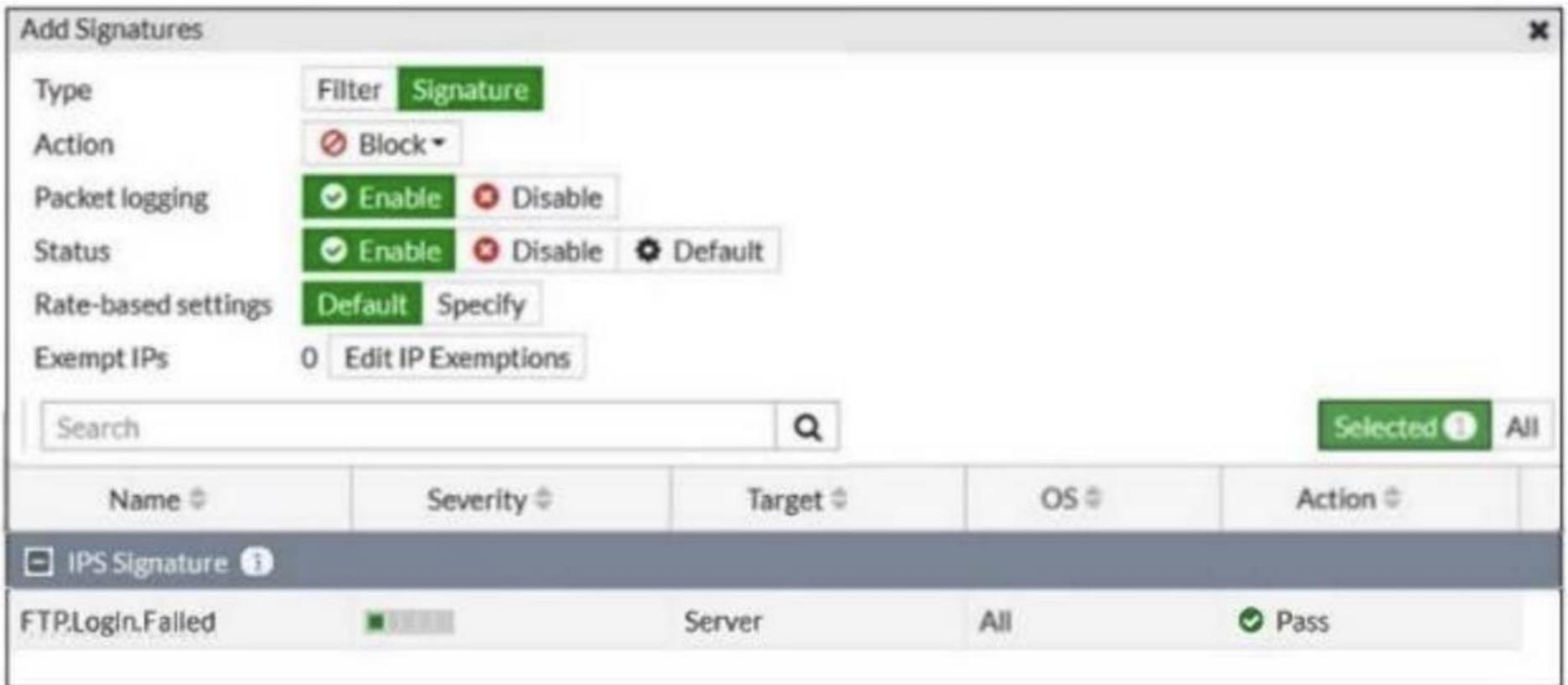
Answer: A

Explanation:

NTurbo enhances performance for flow-based inspection by offloading traffic to the content processor.

NEW QUESTION 7

Refer to the exhibit.



Review the intrusion prevention system (IPS) profile signature settings shown in the exhibit. What do you conclude when adding the FTP.Login.Failed signature to the IPS sensor profile?

- A. Traffic matching the signature will be allowed and logged.
- B. The signature setting uses a custom rating threshold.
- C. The signature setting includes a group of other signatures.
- D. Traffic matching the signature will be silently dropped and logged.

Answer: A

Explanation:

The exhibit shows that the "FTP.Login.Failed" IPS signature is set with the action "Pass" and packet logging enabled. This means that any traffic matching this signature will be allowed through the FortiGate, and the traffic details will be logged for monitoring and analysis purposes.

References:

- FortiOS 7.4.1 Administration Guide: IPS Signature Actions

NEW QUESTION 8

Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

- A. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN.
- B. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.
- C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
- D. The client FortiGate requires a manually added route to remote subnets.

Answer: BC

Explanation:

For SSL VPN to function correctly between two FortiGate devices, the following settings are required:

- B. The server FortiGate requires a CA certificate to verify the client FortiGate certificate: The server FortiGate must have a Certificate Authority (CA) certificate installed to authenticate and verify the certificate presented by the client FortiGate device.
 - C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate: The client FortiGate must have a client certificate that is signed by the same CA that the server FortiGate uses for verification. This ensures a secure SSL VPN connection between the two devices.
- The other options are not directly necessary for establishing SSL VPN:
- A. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN: This is incorrect as SSL VPN does not require a specific tunnel interface type; it typically uses an SSL VPN client profile.
 - D. The client FortiGate requires a manually added route to remote subnets: While routing may be necessary, it is not specifically required for the SSL VPN

functionality between two FortiGates.

References

- FortiOS 7.4.1 Administration Guide - Configuring SSL VPN, page 1203.
- FortiOS 7.4.1 Administration Guide - SSL VPN Authentication, page 1210.

NEW QUESTION 9

Which statement is a characteristic of automation stitches?

- A. They can be run only on devices in the Security Fabric.
- B. They can be created only on downstream devices in the fabric.
- C. They can have one or more triggers.
- D. They can run multiple actions at the same time.

Answer: C

Explanation:

Automation stitches on FortiGate can have one or more triggers, which are conditions or events that activate the automation stitch. The trigger defines when the automation stitch should execute the defined actions. Actions within a stitch can be executed sequentially or in parallel, depending on the configuration.

References:

- FortiOS 7.4.1 Administration Guide: Automation Stitches

NEW QUESTION 10

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 DNS over HTTPS.
- C. It uses DNS over TLS.
- D. It uses UDP 53.

Answer: D

Explanation:

By default, DNS queries to FortiGuard servers use UDP port 53.

NEW QUESTION 10

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

All traffic must be routed through the primary tunnel when both tunnels are up. The secondary tunnel must be used only if the primary tunnel goes down. In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover.

Which two key configuration changes must the administrator make on FortiGate to meet the requirements? (Choose two.)

- A. Enable Dead Peer Detection
- B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.
- C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
- D. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

Answer: AC

Explanation:

To configure redundant IPsec VPN tunnels on FortiGate with failover capability, the following two key configuration changes are required:

- A. Enable Dead Peer Detection (DPD): Dead Peer Detection is crucial for detecting if the remote peer is unreachable. By enabling DPD, FortiGate can quickly detect a dead tunnel, ensuring a faster failover to the secondary tunnel when the primary tunnel goes down.
- C. Configure a lower distance on the static route for the primary tunnel and a higher distance on the static route for the secondary tunnel: The static route with the lower distance (higher priority) will be used when both tunnels are operational. If the primary tunnel fails, the higher distance (lower priority) route for the secondary tunnel will take over, ensuring traffic is routed correctly.

The other options are not suitable:

- B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels:

This option is not directly related to the requirements of failover between two IPsec VPN tunnels.

- D. Configure a higher distance on the static route for the primary tunnel and a lower distance on the static route for the secondary tunnel: This would prioritize the secondary tunnel over the primary tunnel, which is opposite to the desired configuration.

References

- FortiOS 7.4.1 Administration Guide - Configuring IPsec VPN, page 1320.
- FortiOS 7.4.1 Administration Guide - Redundant VPN Configuration, page 1335.

NEW QUESTION 12

An administrator must enable a DHCP server on one of the directly connected networks on FortiGate. However, the administrator is unable to complete the process on the GUI to enable the service on the interface.

In this scenario, what prevents the administrator from enabling DHCP service?

- A. The role of the interface prevents setting a DHCP server.
- B. The DHCP server setting is available only on the CLI.

- C. Another interface is configured as the only DHCP server on FortiGate.
- D. The FortiGate model does not support the DHCP server.

Answer: A

Explanation:

FortiGate interfaces can be configured in different roles, such as WAN or LAN. If an interface is set as a "WAN" role, you cannot configure it to act as a DHCP server through the GUI. The interface role must be set to "LAN" or "Undefined" to allow DHCP server configuration.

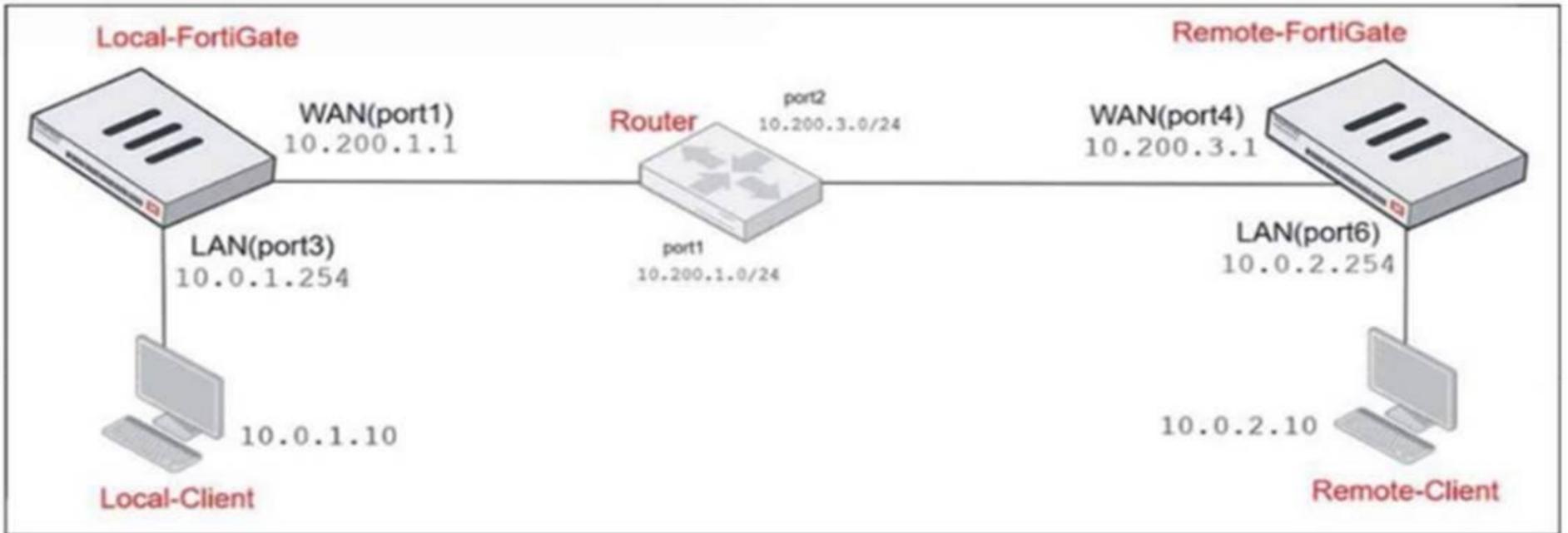
References:

- > FortiOS 7.4.1 Administration Guide: DHCP Server Configuration

NEW QUESTION 17

Refer to the exhibits.

Network diagram



NAT IP pool configuration

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

Firewall policy

ID	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT
2	TCP traffic	all	REMOTE_FORTIGATE	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
6	PING traffic	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
7	IGMP traffic	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects. 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. Which IP address will be used to source NAT (SNAT) the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

- A. 10.200.1.1
- B. 10.200.1.149
- C. 10.200.1.99

Answer: C

Explanation:

The traffic from the user on Local-Client (10.0.1.10) pinging the IP address of Remote-FortiGate (10.200.3.1) will match the firewall policy with the service "PING traffic". According to the firewall policy:

- > Policy ID 6 is set for PING traffic and uses the NAT IP pool "SNAT-Remote1", which is defined as 10.200.1.99.

NEW QUESTION 21

Refer to the exhibit.

Firewall policies

ID	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN to WAN 1										
1	Full_Access	LAN (port3)	WAN (port1) WAN (port2)	all	all	always	ALL	ACCEPT	IP Pool	NAT
WAN to LAN 3										
2	Deny	WAN (port1)	LAN (port3)	Deny_IP	all	always	ALL	DENY		
3	Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
4	Webserver	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
Implicit 1										
0	Implicit Deny	any	any	all	all	always	ALL	DENY		

Which statement about this firewall policy list is true?

- A. The Implicit group can include more than one deny firewall policy.
- B. The firewall policies are listed by ID sequence view.
- C. The firewall policies are listed by ingress and egress interfaces pairing view.
- D. LAN to WA
- E. WAN to LA
- F. and Implicit are sequence grouping view lists.

Answer: C

Explanation:

The firewall policy list in the exhibit is arranged in the "Interface Pair View," where policies are grouped by their incoming (ingress) and outgoing (egress) interface pairs. Each section (LAN to WAN, WAN to LAN, etc.) groups policies based on these interface pairings. This view helps administrators quickly identify which policies apply to specific traffic flows between network interfaces. Options A and D are incorrect because the Implicit group typically does not include more than one deny policy, and there is no "sequence grouping view" in FortiGate. Option B is incorrect as the list is not displayed strictly by ID sequence.

References:

FortiOS 7.4.1 Administration Guide: Firewall Policy Views

NEW QUESTION 26

An employee needs to connect to the office through a high-latency internet connection. Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

- A. SSL VPN idle-timeout
- B. SSL VPN login-timeout
- C. SSL VPN dtls-hello-timeout
- D. SSL VPN session-ttl

Answer: C

Explanation:

For a high-latency internet connection, the SSL VPN setting that should be adjusted is:

* C. SSL VPN dtls-hello-timeout: This setting determines how long the FortiGate will wait for a DTLS hello message from the client. For high-latency connections, increasing this timeout will prevent SSL VPN negotiation failures caused by delays in receiving the DTLS hello message.

The other options are not suitable:

* A. SSL VPN idle-timeout: This setting controls the idle time allowed before a session is terminated, which is not relevant to the initial connection establishment.

* B. SSL VPN login-timeout: This setting controls the maximum time allowed for a user to log in, but does not affect connection negotiation.

* D. SSL VPN session-ttl: This setting controls the total time-to-live for an SSL VPN session but does not directly address issues caused by high latency.

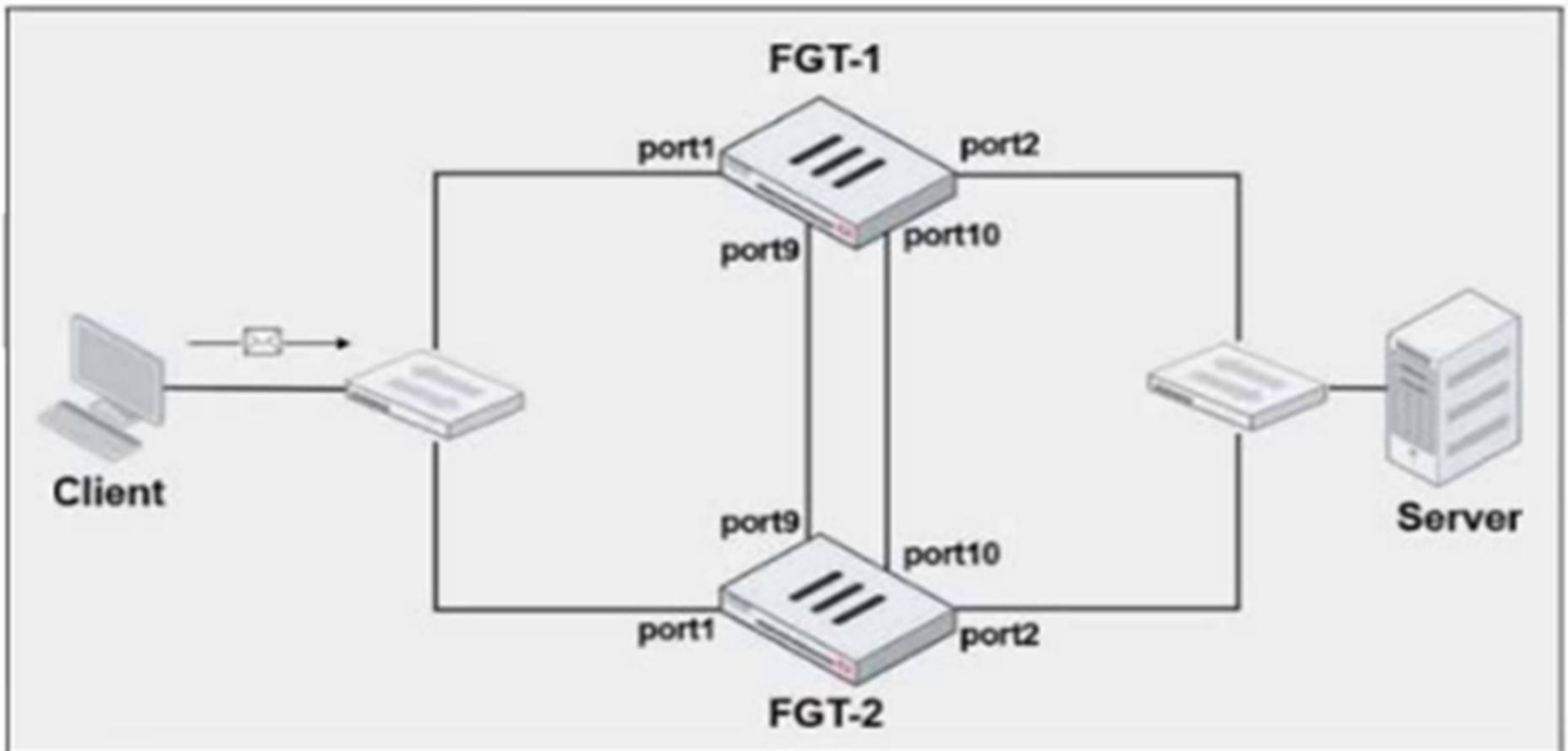
References

FortiOS 7.4.1 Administration Guide - SSL VPN Configuration, page 1415.

NEW QUESTION 29

Refer to the exhibits.

FortiGate HA cluster topology



Current HA status

```

# get system ha status
...
Configuration Status:
  FGVM010000064692(updated 4 seconds ago): in-sync
  FGVM010000064692 checksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
  FGVM010000065036(updated 4 seconds ago): in-sync
  FGVM010000065036 checksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
...
Primary       : FGT-1, FGVM010000064692, HA cluster index = 1
Secondary     : FGT-2, FGVM010000065036, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1
  
```

New FortiGate HA configuration

```
FGT-1
#config system ha
  set group-id 3
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port9" 50 "port10" 50
  set session-pickup enable
  set override disable
  set priority 90
  set monitor port3
```

```
FGT-2
#config system ha
  set group-id 3
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port9" 50 "port10" 50
  set session-pickup enable
  set override enable
  set priority 110
  set monitor port3
```

FGT-1 and FGT-2 are updated with HA configuration commands shown in the exhibit.
 What would be the expected outcome in the HA cluster?

- A. FGT-1 will remain the primary because FGT-2 has lower priority.
- B. FGT-2 will take over as the primary because it has the override enable setting and higher priority than FGT-1.
- C. FGT-1 will synchronize the override disable setting with FGT-2.
- D. The HA cluster will become out of sync because the override setting must match on all HA members.

Answer: B

NEW QUESTION 34

Refer to the exhibit.

```

FGT1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
V - BGP VPNv4
* - candidate default

Routing table for VRF=0
S    0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]
C    172.20.121.0/24 is directly connected, port1
C    172.20.168.0/24 is directly connected, port2
C    172.20.167.0/24 is directly connected, port3
S    10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
S    10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0]
S    10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]

```

Which route will be selected when trying to reach 10.20.30.254?

- A. 10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0]
- B. 10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
- C. 10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
- D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]

Answer: A

Explanation:

The correct route selected when trying to reach 10.20.30.254 is 10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0].

Prefix Length: The routing process prioritizes routes with the most specific (longest) prefix. In this case, 10.20.30.0/24 has a shorter prefix than 10.20.30.0/26 (option C), but it still matches the target address 10.20.30.254. The /24 subnet includes all addresses from 10.20.30.0 to 10.20.30.255, so 10.20.30.254 falls within this range.

• **Administrative Distance and Metric:** In the exhibit, all routes have the same administrative distance (AD) and metric, meaning they are considered equal in terms of preference. Hence, the prefix length becomes the primary factor for route selection.

Why the other options are less appropriate:



B. 10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]

• This route is for a different subnet, 10.30.20.0/24, which does not include the target address 10.20.30.254. Therefore, it is not a valid match.



C. 10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]

• Although this has a more specific prefix (/26), which means it should cover a smaller range of addresses, the /26 subnet only includes addresses from 10.20.30.0 to 10.20.30.63. The target address 10.20.30.254 does not fall within this range, so this route will not be selected.



D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]

• This is a default route (0.0.0.0/0) used for any address that doesn't match a more specific route.

Since 10.20.30.254 matches the 10.20.30.0/24 route (option A), the default route will not be selected.

NEW QUESTION 36

Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

FortiGate SD-WAN zone configuration



Based on the exhibit, which statement is true?

- A. The underlay zone contains port1 and
- B. The d-wan zone contains no member.
- C. The d-wan zone cannot be deleted.
- D. The virtual-wan-link zone contains no member.

Answer: C

Explanation:

In FortiGate's SD-WAN configuration, the d-wan zone is a system default SD-WAN zone that is automatically created and cannot be deleted. This zone is used to manage dynamic WAN links for SD-WAN traffic balancing and routing. It ensures that multiple WAN interfaces can be grouped and managed effectively for WAN link optimization.

Why the other options are less appropriate:

- A. The underlay zone contains port1 and: There is no mention in the exhibit about an "underlay zone" containing port1.
- B. The d-wan zone contains no member: This statement is irrelevant since the focus is on the zone's deletion, not its members.
- D. The virtual-wan-link zone contains no member: This is unrelated to the core fact that the d-wan zone cannot be deleted.

Reference:

FortiOS 7.4.1 Administration Guide: SD-WAN Zone Configuration

NEW QUESTION 38

Which of the following methods can be used to configure FortiGate to perform source NAT (SNAT) for outgoing traffic?

- A. Configure a static route pointing to the external interface.
- B. Enable the "Use Outgoing Interface Address" option in a firewall policy.
- C. Create a virtual server with an external IP address.
- D. Deploy an IPsec VPN tunnel with NAT enabled.

Answer: B

Explanation:

To configure source NAT (SNAT) for outgoing traffic on FortiGate, one of the most common methods is to enable the "Use Outgoing Interface Address" option in a firewall policy. This option ensures that the source IP address of packets leaving the FortiGate device is replaced by the IP address of the outgoing interface. This is typically done when traffic is exiting a private network to access the internet, requiring source NAT to translate the private IP addresses to a public IP.

Why the other options are less appropriate:

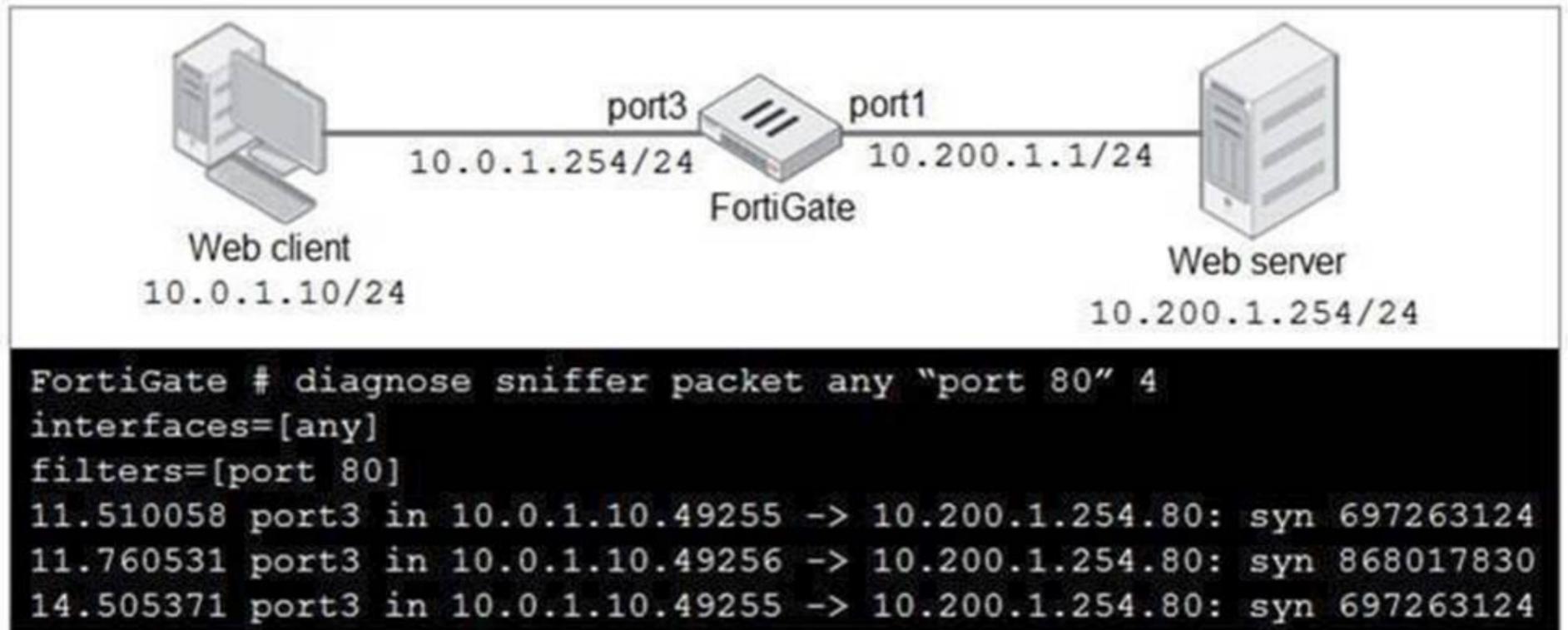
- * A. Configure a static route pointing to the external interface: A static route is used to direct

traffic, but it does not configure SNAT. It determines where packets are sent but does not modify the source IP.

- C. Create a virtual server with an external IP address: Virtual servers are used to provide destination NAT (DNAT) for incoming traffic, not SNAT for outgoing traffic.
- D. Deploy an IPsec VPN tunnel with NAT enabled: While IPsec VPN tunnels can be configured with NAT traversal, this is not the typical method for configuring SNAT for general outgoing internet traffic.

NEW QUESTION 39

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. Capture the traffic using an external sniffer connected to port1.
- C. Execute another sniffer in the FortiGate, this time with the filter ??host 10.0.1.10??
- D. Execute a debug flow.

Answer: D

Explanation:

The next step for troubleshooting the problem would be to execute a debug flow on the FortiGate. The debug flow command provides detailed insights into how FortiGate handles the traffic, including whether the traffic is being dropped, allowed, or forwarded to the correct interface. It helps in identifying issues like firewall policy misconfigurations, routing issues, or NAT problems.

- A. Run a sniffer on the web server: While this might help diagnose server-side issues, the initial focus should be on the FortiGate, as the problem might lie in the firewall configuration or traffic handling.
- B. Capture the traffic using an external sniffer connected to port1: This may provide packetlevel information, but it's more useful to first analyze FortiGate's internal decision-making process with a debug flow.
- C. Execute another sniffer in the FortiGate, this time with the filter ??host 10.0.1.10??: Running a sniffer on the specific host might give more packet details, but the debug flow provides more comprehensive information on how the firewall processes the packets. Thus, using the debug flow will offer a more direct understanding of how the traffic is being processed or blocked within FortiGate.

NEW QUESTION 40

Consider the topology:

Application on a Windows machine <--(SSL VPN) -->FGT--> Telnet to Linux server.

An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout. The administrator has already verified that the issue is not caused by the application or Linux server.

This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.

What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

- A. Set the maximum session TTL value for the TELNET service object.
- B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.
- C. Create a new service object for TELNET and set the maximum session TTL.
- D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

Answer: CD

Explanation:

The issue with the idle session timing out after 90 minutes can be resolved by adjusting the session Time-To-Live (TTL) for the TELNET service used over the SSL VPN connection. Here's how the administrator can address the problem:

- C. Create a new service object for TELNET and set the maximum session TTL: By creating a new service object specifically for TELNET and setting a custom maximum session TTL, the administrator can ensure that the TELNET session does not time out prematurely. This way, the session will last longer or indefinitely, depending on the configured TTL.

- D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy:
Creating a dedicated firewall policy for SSL VPN traffic and placing it above the existing one allows the administrator to apply the new TELNET service object with a longer session TTL. This will ensure the new policy with the adjusted settings takes precedence for TELNET traffic.

Why the other options are less appropriate:

- A. Set the maximum session TTL value for the TELNET service object:

This would work if you were adjusting an existing TELNET service object. However, creating a new service object for TELNET and applying it in the firewall policy (as described in options C and D) is more granular and won't affect other services using the same TELNET object.

- B. Set the session TTL on the SSLVPN policy to maximum:

While this would extend the session timeout for the entire SSL VPN traffic, it could affect other services running through the SSL VPN, which may not be desirable. This option would lack the necessary specificity for only the TELNET traffic.

NEW QUESTION 45

Which two statements correctly describe the differences between IPsec main mode and IPsec aggressive mode? (Choose two.)

- A. The first packet of aggressive mode contains the peer ID, while the first packet of main mode does not.
- B. Main mode cannot be used for dialup VPNs, while aggressive mode can.
- C. Aggressive mode supports XAuth, while main mode does not.
- D. Six packets are usually exchanged during main mode, while only three packets are exchanged during aggressive mode.

Answer: AD

Explanation:

The differences between IPsec main mode and IPsec aggressive mode are mainly in the number of packets exchanged and the level of security provided during the negotiation process. Here's the breakdown:

- A. The first packet of aggressive mode contains the peer ID, while the first packet of main mode does not:

In aggressive mode, the peer's identity is sent in the first packet, making the process faster but less secure because the peer's identity is not encrypted. In main mode, the peer's identity is protected and only exchanged after the encryption is established, offering more security.

- D. Six packets are usually exchanged during main mode, while only three packets are exchanged during aggressive mode:

Main mode involves a more detailed negotiation process, requiring the exchange of six packets. Aggressive mode, on the other hand, reduces this to three packets, speeding up the connection but sacrificing some security in the process.

Why the other options are less appropriate:

- B. Main mode cannot be used for dialup VPNs, while aggressive mode can:

This is incorrect. Main mode can be used for dialup VPNs as long as the peer's IP is known or configured in advance.

- C. Aggressive mode supports XAuth, while main mode does not:

Both main mode and aggressive mode can support XAuth (eXtended Authentication) if needed.

NEW QUESTION 49

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCP_FGT_AD-7.4 Practice Exam Features:

- * FCP_FGT_AD-7.4 Questions and Answers Updated Frequently
- * FCP_FGT_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FGT_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * FCP_FGT_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FGT_AD-7.4 Practice Test Here](#)