

# 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

WINDOWS\_SERVERS

Comments

Write a comment... 0/255

Block malicious URLs

☐

IPS Signatures and Filters

+ Create New

Edit

Delete

Details	Exempt IPs	Action	Packet Logging
Microsoft.Windows.iSCSI.Target.DoS	0	Monitor	Enabled
Windows		Block	Disabled

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

When FortiGate performs SSL/SSH full inspection, you can decide how it should react when it detects an invalid certificate. Which three actions are valid actions that FortiGate can perform when it detects an invalid certificate? (Choose three.)

- A. Allow & Warning
- B. Trust & Allow
- C. Allow
- D. Block & Warning
- E. Block

Answer: ADE

Explanation:

When FortiGate performs SSL/SSH full inspection and detects an invalid certificate, there are three valid actions it can take:

➤ Allow & Warning: This action allows the session but generates a warning.

➤ Block & Warning: This action blocks the session and generates a warning.

➤ Block: This action blocks the session without generating a warning.  
 Actions such as "Trust & Allow" or just "Allow" without additional configurations are not applicable in the context of handling invalid certificates.  
 References:  
 ➤ FortiOS 7.4.1 Administration Guide: Configuring SSL/SSH inspection profile

**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**  
 Refer to the exhibit.

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Critical-DIA	4 LOCAL_SUBNET	Slack-Slack Dropbox-Web Bloomberg		port1 port2
2	Non-Critical-DIA	4 LOCAL_SUBNET	Addicting.Games Social.Media	Bandwidth	port2
3	Default-Internet	4 LOCAL_SUBNET	4 REMOTE_SUBNET	Latency	port1 port2
Implicit 1					
	sd-wan	4 all	4 all	Source-Destination IP	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

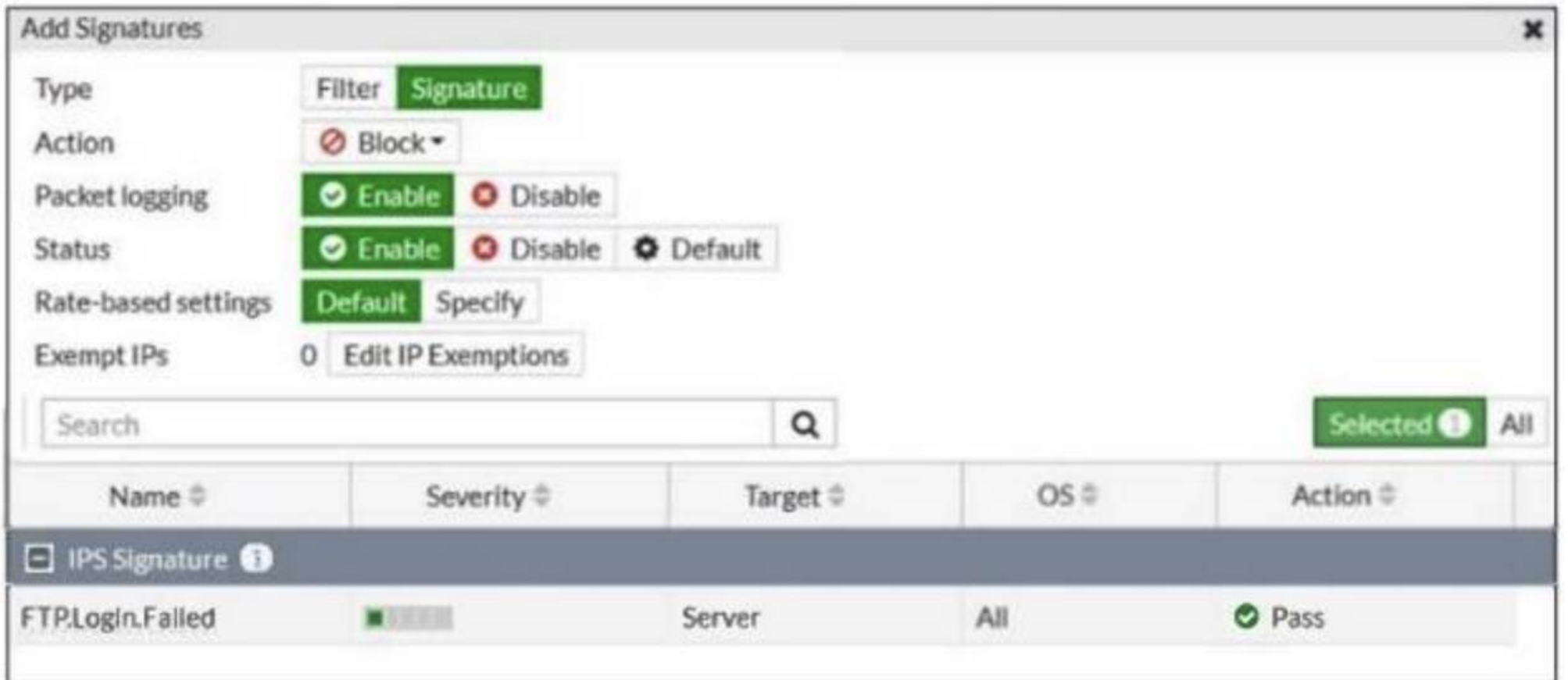
**NEW QUESTION 5**  
 An administrator manages a FortiGate model that supports NTurbo. How does NTurbo enhance performance for flow-based inspection?

- 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 6**  
 Refer to the exhibit.



Name	Severity	Target	OS	Action
FTP.Login.Failed	Server	All		Pass

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 7**

Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

- A. The host field in the HTTP header.
- B. The server name indication (SNI) extension in the client hello message.
- C. The subject alternative name (SAN) field in the server certificate.
- D. The subject field in the server certificate.
- E. The serial number in the server certificate.

**Answer:** BCD

**Explanation:**

When SSL certificate inspection is enabled on a FortiGate device, the system uses the following three pieces of information to identify the hostname of the SSL server:

- > Server Name Indication (SNI) extension in the client hello message (B): The SNI is an extension in the client hello message of the SSL/TLS protocol. It indicates the hostname the client is attempting to connect to. This allows FortiGate to identify the server's hostname during the SSL handshake.
  - > Subject Alternative Name (SAN) field in the server certificate (C): The SAN field in the server certificate lists additional hostnames or IP addresses that the certificate is valid for. FortiGate inspects this field to confirm the identity of the server.
  - > Subject field in the server certificate (D): The Subject field contains the primary hostname or domain name for which the certificate was issued. FortiGate uses this information to match and validate the server's identity during SSL certificate inspection.
- The other options are not used in SSL certificate inspection for hostname identification:
- > Host field in the HTTP header (A): This is part of the HTTP request, not the SSL handshake, and is not used for SSL certificate inspection.
  - > Serial number in the server certificate (E): The serial number is used for certificate management and revocation, not for hostname identification.

References

- > FortiOS 7.4.1 Administration Guide - SSL/SSH Inspection, page 1802.
- > FortiOS 7.4.1 Administration Guide - Configuring SSL/SSH Inspection Profile, page 1799.

**NEW QUESTION 8**

A network administrator has configured an SSL/SSH inspection profile defined for full SSL inspection and set with a private CA certificate. The firewall policy that allows the traffic uses this profile for SSL inspection and performs web filtering. When visiting any HTTPS websites, the browser reports certificate warning errors.



What is the reason for the certificate warning errors?

- A. The SSL cipher compliance option is not enabled on the SSL inspection profil
- B. This setting is required when the SSL inspection profile is defined with a private CA certificate.
- C. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
- D. The browser does not recognize the certificate in use as signed by a trusted CA.
- E. With full SSL inspection it is not possible to avoid certificate warning errors at the browser level.

**Answer: C**

**Explanation:**

The certificate warning errors occur because the SSL inspection profile is configured to use a private CA certificate that is not recognized by the browser as being signed by a trusted CA. For the browser to trust the FortiGate's re-signed certificates, the CA certificate used by FortiGate for SSL inspection must be installed in the browser's trusted certificate store. Until the browser recognizes the certificate authority (CA) as trusted, it will continue to display warning errors when accessing HTTPS websites.

References:



FortiOS 7.4.1 Administration Guide: SSL/SSH Inspection Configuration

**NEW QUESTION 9**

Refer to the exhibits, which show the system performance output and the default configuration of high memory usage thresholds in a FortiGate.

**System Performance output**

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 3 hours, 28 minutes
```

**Memory usage threshold settings**

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Based on the system performance output, what can be the two possible outcomes? (Choose two.)

- A. FortiGate will start sending all files to FortiSandbox for inspection.
- B. FortiGate has entered conserve mode.
- C. Administrators cannot change the configuration.
- D. Administrators can access FortiGate only through the console port.

**Answer: BC**

**Explanation:**

Based on the system performance output provided, the memory usage on the FortiGate device is at 90%, which is above the green threshold (82%) but below the red threshold (88%). Given this high memory usage, the FortiGate device will enter "conserve mode" to prevent further resource exhaustion. In conserve mode:



B. FortiGate has entered conserve mode: When the memory usage reaches or exceeds certain thresholds (in this case, the green and red thresholds), the FortiGate enters conserve mode to protect itself from running out of memory entirely. This mode limits some functionalities to reduce memory usage and avoid a potential system crash.



D. Administrators can access FortiGate only through the console port: During conserve mode, administrative access might be restricted, and administrators may only be able to connect to the device via the console port. This restriction is in place to ensure that the FortiGate can be managed directly, even under low resource conditions.

The other options are not correct:



A. FortiGate will start sending all files to FortiSandbox for inspection: This is unrelated to memory usage and conserve mode.



C. Administrators cannot change the configuration: While access may be limited, configuration changes can still be made via the console port.

References

- FortiOS 7.4.1 Administration Guide - Monitoring System Resources and Performance, page 325.
- FortiOS 7.4.1 Administration Guide - Conserve Mode, page 330.

#### NEW QUESTION 10

Which method allows management access to the FortiGate CLI without network connectivity?

- A. SSH console
- B. CLI console widget
- C. Serial console
- D. Telnet console

**Answer: C**

#### Explanation:

The serial console method allows management access to the FortiGate CLI without relying on network connectivity. This method involves directly connecting a computer to the FortiGate device using a serial cable (such as a DB-9 to RJ-45 cable or USB to RJ-45 cable) and using terminal emulation software to interact with the FortiGate CLI. This method is essential for situations where network-based access methods (such as SSH or Telnet) are not available or feasible.

References:

- FortiOS 7.4.1 Administration Guide: Console connection

#### 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**

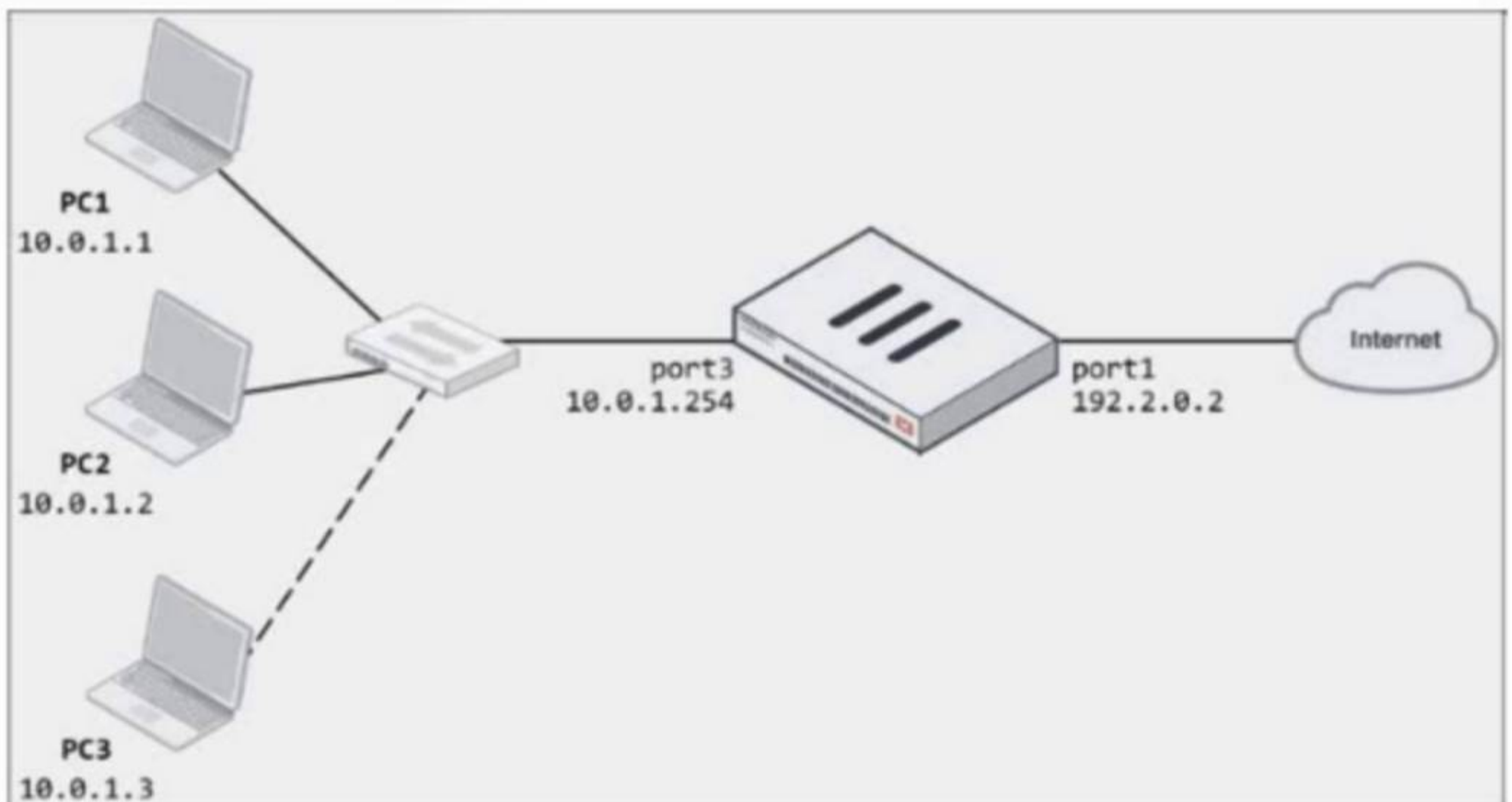
#### Explanation:

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

#### NEW QUESTION 13

Refer to the exhibits.

### Network diagram



## Dynamic IP pool

Edit Dynamic IP Pool


Name

internet-pool

Comments

Write a comment...  0/255

Type

One-to-One 

External IP Range 

192.2.0.10-192.2.0.11

ARP Reply

☒

# Firewall policy

Edit Policy

Name

LAN-to-Internet

Incoming Interface

LAN (port3)

×

Outgoing Interface

WAN (port1)

×

Source

all

×

Destination

all

×

Schedule

always

▼

Service

ALL

×

Action

✓ ACCEPT

⊘ DENY

Inspection Mode

Flow-based

Proxy-based

Firewall/Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

internet-pool

×

Preserve Source Port

Protocol Options

PROT

default

The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device. Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet.

Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)

- A. In the firewall policy configuration, add 10.
- B. 3 as an address object in the source field.
- C. In the IP pool configuration, set endip to 192.2.0.12.
- D. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.
- E. In the IP pool configuration, set cype to overload.

Answer: BD

## Explanation:

To resolve the issue of PC3 not being able to access the internet, the administrator needs to adjust the IP pool configuration or the firewall policy. The following two options will fix the connectivity issue:

- B. In the IP pool configuration, set the ending IP to 192.2.0.12: The current IP pool range is 192.2.0.10-192.2.0.11, which only provides two IP addresses for network address translation (NAT). To allow PC3 to access the internet, the IP pool should be expanded to include an additional IP address by changing the end of the range to 192.2.0.12.

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>



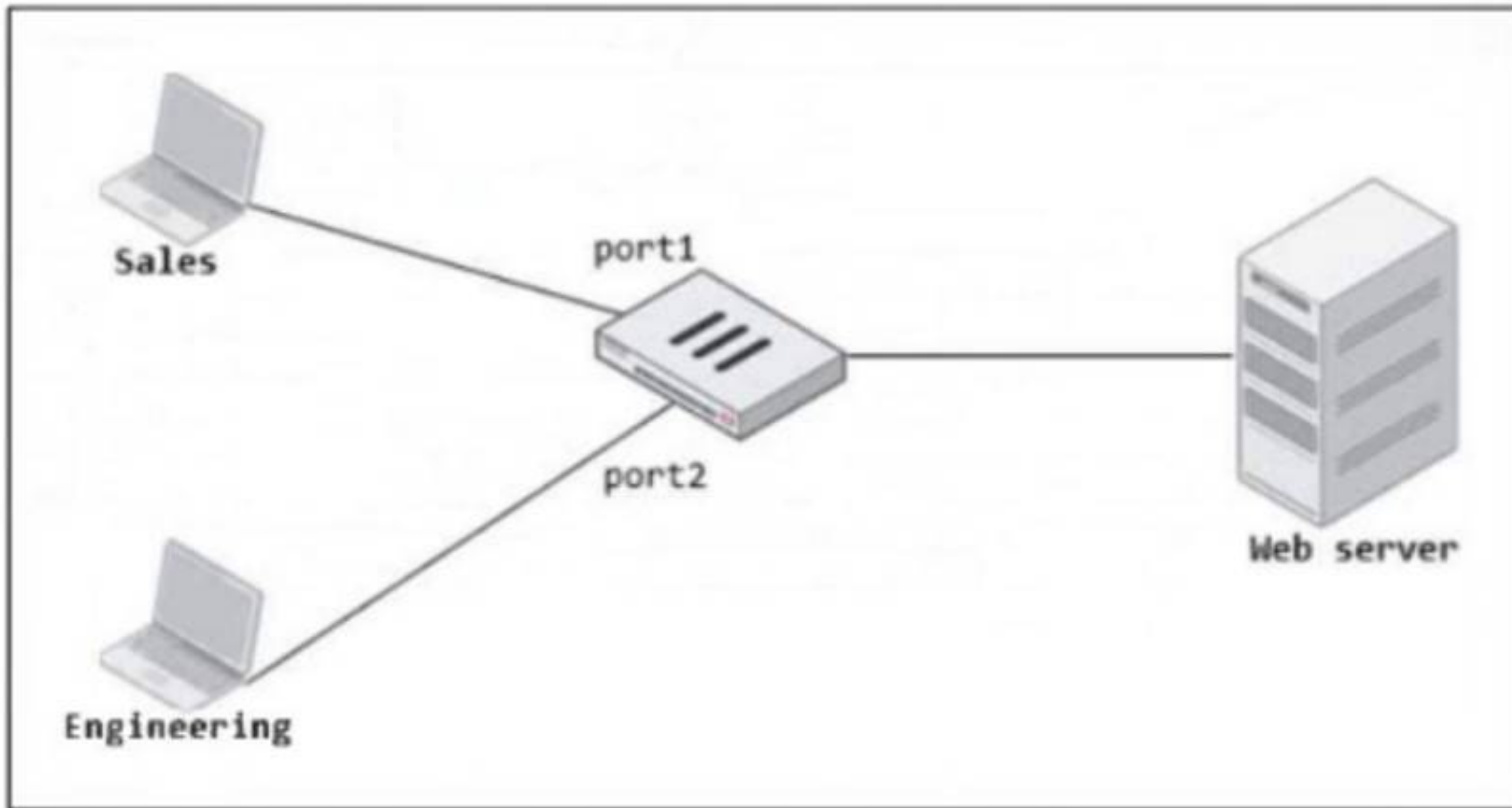
- D. In the IP pool configuration, set type to overload: Instead of using a one-to-one NAT, changing the type to overload will allow multiple internal addresses (such as PC1, PC2, and PC3) to share a single external IP address. This will solve the issue without needing additional public IP addresses. The other options are not suitable:
- A. In the firewall policy configuration, add 10.0.1.3 as an address object in the source field: This option is unnecessary since the firewall policy already allows all addresses from the source (LAN port3).
- C. Configure another firewall policy that matches only the address of PC3 as the source, and then place the policy on top of the list: This option is redundant and would not resolve the underlying issue with the IP pool configuration.

References

- FortiOS 7.4.1 Administration Guide - Configuring Firewall Policies, page 512.
- FortiOS 7.4.1 Administration Guide - Configuring NAT with IP Pools, page 518.

#### NEW QUESTION 14

Refer to the exhibit.



FortiGate has two separate firewall policies for Sales and Engineering to access the same web server with the same security profiles. Which action must the administrator perform to consolidate the two policies into one?

- A. Enable Multiple Interface Policies to select port1 and port2 in the same firewall policy
- B. Create an Interface Group that includes port1 and port2 to create a single firewall policy
- C. Select port1 and port2 subnets in a single firewall policy.
- D. Replace port1 and port2 with the any interface in a single firewall policy.

**Answer: B**

#### Explanation:

To consolidate the two separate firewall policies for Sales and Engineering departments accessing the same web server, you can create an Interface Group that includes both port1 (Sales) and port2 (Engineering). Once the Interface Group is created, you can use this group as a single incoming interface in a single firewall policy. This approach reduces the number of policies, making management more efficient.

References:

- FortiOS 7.4.1 Administration Guide: Firewall Policy Configuration

#### NEW QUESTION 19

Refer to the exhibit showing a FortiGuard connection debug output.

## FortiGuard connection debug output

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-filter
Status      : Enable
License     : Contract

Service     : Antispam
Status      : Disable

Service     : Virus Outbreak Prevention
Status      : Disable

Num. of servers : 1
Protocol     : https
Port        : 443
Anycast     : Enable
Default servers : Included

-- Server List (Thu Jun  9 11:26:56 2022) --

IP           Weight  RTT  Flags  TZ  FortiGuard-requests  Curr Lost  Total Lost  Updated Time
173.243.141.16  -8    18   DI    0      4          0         0  Thu Jun  9 11:26:24 2022
12.34.97.18    20    30      1      1          0         0  Thu Jun  9 11:26:24 2022
210.7.96.18    160   305      9      0          0         0  Thu Jun  9 11:26:24 2022
```

Based on the output, which two facts does the administrator know about the FortiGuard connection? (Choose two.)

- A. One server was contacted to retrieve the contract information.
- B. There is at least one server that lost packets consecutively.
- C. A local FortiManager is one of the servers FortiGate communicates with.
- D. FortiGate is using default FortiGuard communication settings.

**Answer:** AD

### Explanation:

The debug output indicates that FortiGate connected to one server (173.243.141.16) to retrieve contract information as it shows four FortiGuard requests without any packet loss, which confirms the connection to the server. Additionally, the default FortiGuard communication settings are being used, as indicated by the use of the HTTPS protocol on port 443, which is the default setting for FortiGuard connections.

References:



FortiOS 7.4.1 Administration Guide: FortiGuard Connection Settings

## NEW QUESTION 22

An administrator configured a FortiGate to act as a collector for agentless polling mode. What must the administrator add to the FortiGate device to retrieve AD user group information?

- A. LDAP server
- B. RADIUS server
- C. DHCP server
- D. Windows server

**Answer:** A

### Explanation:

To retrieve AD user group information in agentless polling mode, the administrator must add an LDAP server to the FortiGate device.

## NEW QUESTION 25

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 28**

What is the primary FortiGate election process when the HA override setting is disabled?

- A. Connected monitored ports > Priority > System uptime > FortiGate serial number  
B. Connected monitored ports > System uptime > Priority > FortiGate serial number  
C. Connected monitored ports > Priority > HA uptime > FortiGate serial number  
D. Connected monitored ports > HA uptime > Priority > FortiGate serial number

**Answer:** A

**Explanation:**

When the HA override setting is disabled, FortiGate uses the primary election process based on the following criteria:

- Connected monitored ports: The unit with the most monitored ports up is preferred.
- Priority: The unit with the highest priority is preferred.
- System uptime: The unit with the longest uptime is preferred.
- FortiGate serial number: Used as the final criterion to break any remaining ties.

References:

- FortiOS 7.4.1 Administration Guide: HA election process

**NEW QUESTION 32**

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:**

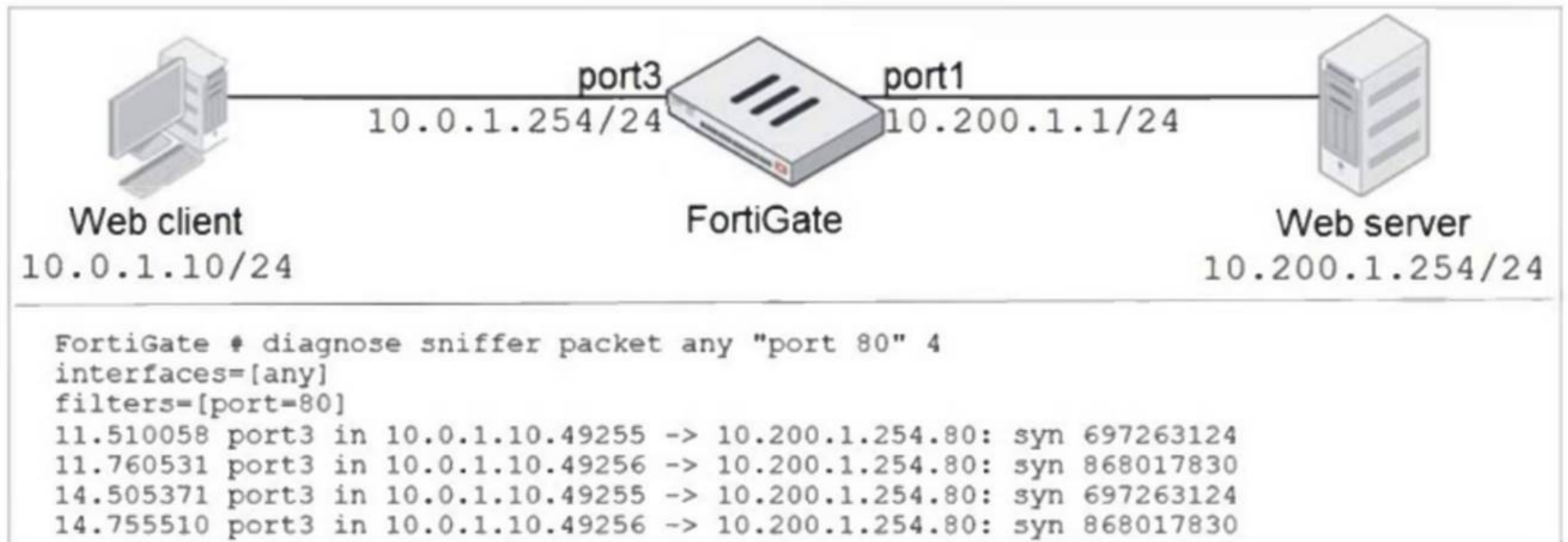
The firewall policy list in the exhibit is arranged in the "Interface Pair View," where policies are grouped by their incoming (ingress) and outgoing (egress) interface pairs. Each section (LAN to WAN, WAN to LAN, etc.) groups policies based on these interface pairings. This view helps administrators 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 36**  
Refer to the exhibit.



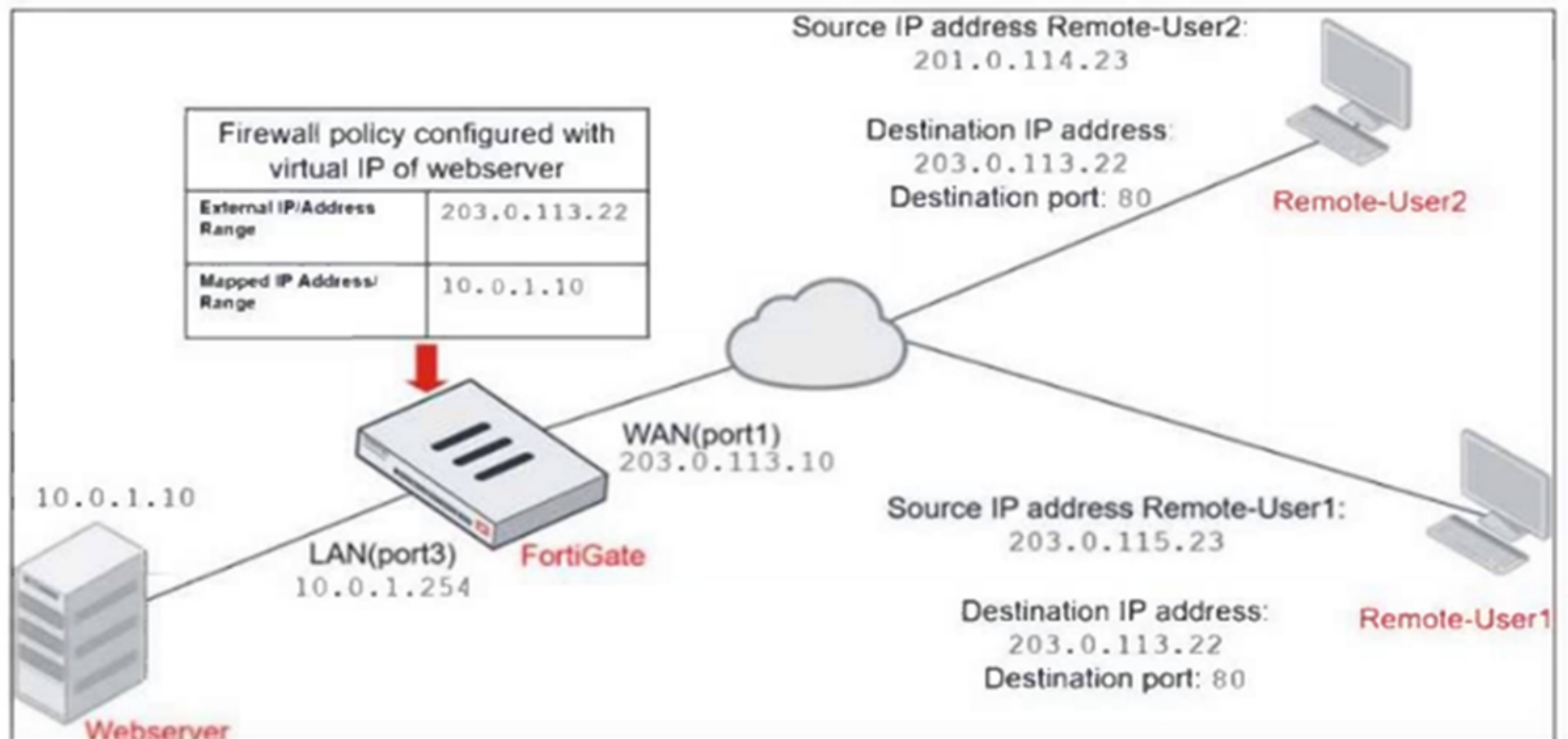
In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit.  
What should the administrator do next, to troubleshoot the problem?

- A. Execute a debug flow.
- B. Capture the traffic using an external sniffer connected to port1.
- C. Execute another sniffer on FortiGate, this time with the filter "host 10.0.1.10".
- D. Run a sniffer on the web server.

**Answer: A**

**NEW QUESTION 37**  
Refer to the exhibits.

**Network diagram**





Firewall address object

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

Firewall policies

ID	Name	Source	Destination	Schedule	Service	Action
<div><div></div> WAN (port1) → LAN (port3) 2</div>						
4	Deny	<div> Deny_IP</div>	<div> all</div>	<div> always</div>	<div> ALL</div>	<div> DENY</div>
3	Allow_access	<div> all</div>	<div> Webserver</div>	<div> always</div>	<div> ALL</div>	<div> ACCEPT</div>

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration. An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. The policy should work such that Remote-User1 must be able to access the Webserver while preventing Remote-User2 from accessing the Webserver. Which two configuration changes can the administrator make to the policy to deny Webserver access for Remote-User2? (Choose two.)

- A. Enable match-vip in the Deny policy.

B. Set the Destination address as Webserver in the Deny policy.

C. Disable match-vip in the Deny policy.

D. Set the Destination address as Deny\_IP in the Allow\_access policy.

Answer: AB

NEW QUESTION 39

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 41**

Which two IP pool types are useful for carrier-grade NAT deployments? (Choose two.)

- A. Port block allocation
- B. Fixed port range
- C. One-to-one
- D. Overload

**Answer:** AB

**Explanation:**

In carrier-grade NAT (CGNAT) deployments, specific IP pool types are used to manage large-scale NAT translations efficiently. The correct IP pool types for CGNAT are:

- A. Port block allocation: This type of IP pool allocates a block of ports from a single public IP to multiple clients. It allows efficient use of a limited number of public IPs by distributing port ranges among users, which is crucial for carrier-grade NAT environments where a large number of users need access to the internet.

- B. Fixed port range: In this type, each client is assigned a fixed range of ports, ensuring that the same public IP and port range are used consistently. This helps in reducing the complexity and overhead of managing dynamic port assignments, which is particularly useful in large-scale CGNAT setups.

Why the other options are less appropriate:

- C. One-to-one: One-to-one NAT is used for mapping a single private IP address to a single public IP address. This is not efficient for carrier-grade NAT because CGNAT is designed to allow multiple clients to share a smaller number of public IPs.

- D. Overload: Overload, also known as PAT (Port Address Translation), maps multiple private IPs to a single public IP by differentiating connections based on port numbers. While commonly used in regular NAT setups, CGNAT benefits more from port block allocation and fixed port range due to th

**NEW QUESTION 42**

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 46**

Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.



## IPS Sensor

Edit IPS Sensor
WINDOWS\_SERVER
[View IPS Signatures]

Name: EMAIL-SERVER-IPS
Comments:

IPS Signatures

Add Signatures
Delete
Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
SMTPLoginBruteForce			Server	TCP_SMT	All	Block	

IPS Filters

Add Filter
Edit Filter
Delete

Filter Details	Action	Packet Logging
Location: server Protocol: SMTP	Block	

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
<input checked="" type="checkbox"/>	IMAPLoginBruteForce	60	10	Source IP	Block	None
<input type="checkbox"/>	Digiplex Asterisk SIP/TCP Connection Class DoS	5	1	Any	Block	None

Apply

## DoS Policy

Incoming Interface: port1

Source Address: all

Destination Address: all

Services: ALL

### L3 Anomalies

Name	Status	Logging	Pass	Block	Action
ip_src_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block	
ip_dst_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block	

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

- A. SMTP.Login.Brute.Force
- B. IMAP.Login.brute.Force
- C. ip\_src\_session
- D. Location: server Protocol: SMTP

**Answer:** B

#### Explanation:

When FortiGate evaluates potential attacks, the IPS sensor follows a specific processing order based on the configuration of filters, signatures, and anomaly thresholds. In this case:

- The IPS sensor is configured with IMAP.Login.brute.Force, which comes first in the order of evaluation.
- FortiGate prioritizes based on signature definitions in the sensor, and since IMAP.Login.brute.Force appears higher in the configuration, it will be evaluated before the other signatures and anomalies.

Why the other options are less appropriate:

- A. SMTP.Login.Brute.Force: This would be evaluated after IMAP.Login.brute.Force, based on the sensor configuration hierarchy.
- C. ip\_src\_session: This is part of the DoS policy and does not come into play until after IPS signatures are evaluated.
- D. Location: server Protocol: SMTP: This appears to be part of the broader IPS sensor rule, but it is not the first item in the evaluation chain.



#### NEW QUESTION 51

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.

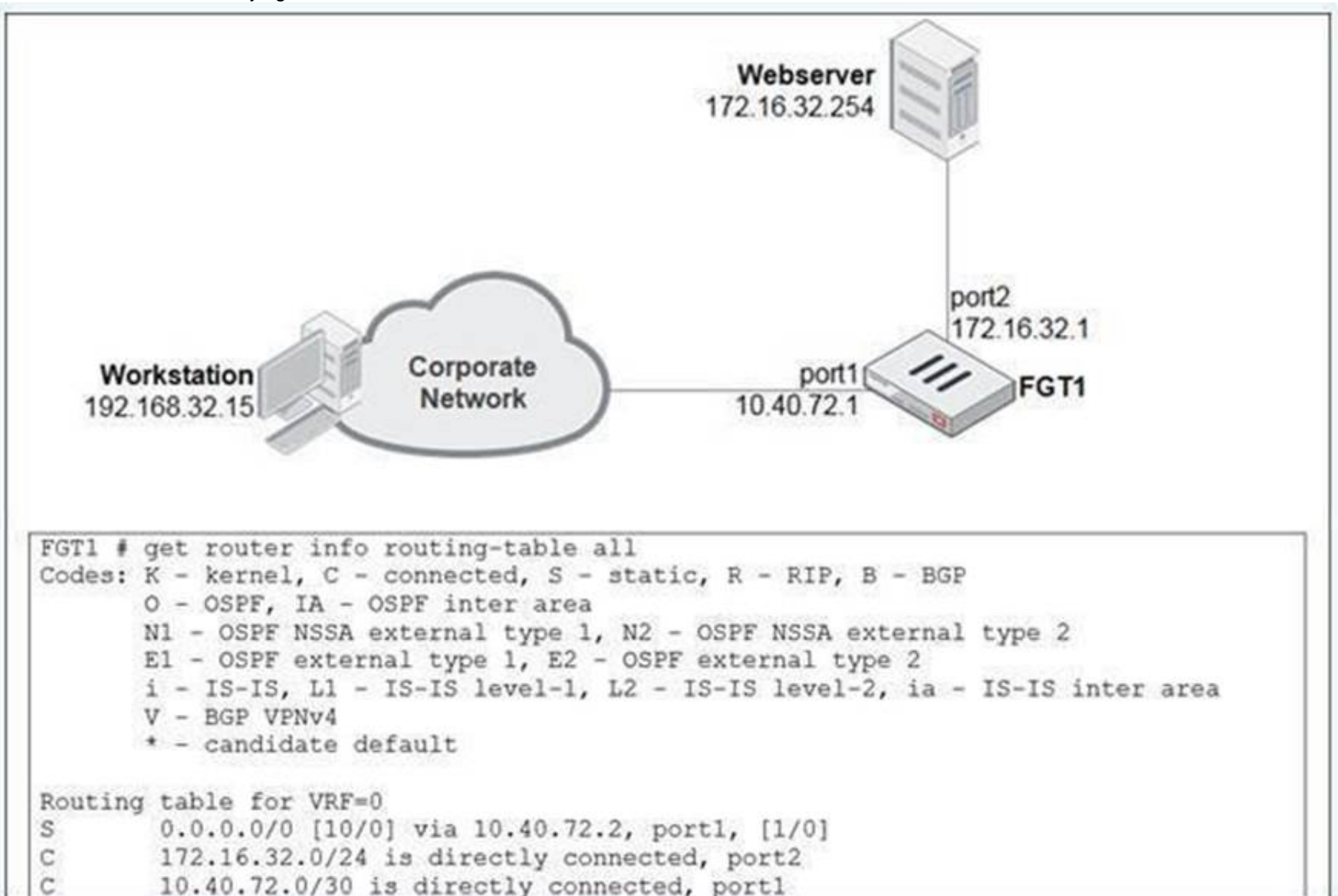
- B. Set the session TTL on the SSLVPN policy to maximum:

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 55

View the exhibit.

A user at 192.168.32.15 is trying to access the web server at 172.16.32.254.



Which two statements best describe how the FortiGate will perform reverse path forwarding (RPF) checks on this traffic? (Choose two.)

- A. Strict RPF check will deny the traffic.
- B. Loose RPF check will allow the traffic.
- C. Strict RPF check will allow the traffic.
- D. Loose RPF check will deny the traffic.

**Answer:** BC

**Explanation:**

When FortiGate performs reverse path forwarding (RPF) checks, it can operate in two modes: Strict RPF and Loose RPF. Here's how these two checks work:

In strict RPF, FortiGate checks whether the best route back to the source IP of the packet (in this case, 192.168.32.15) goes through the same interface on which the packet was received. If the best return path uses a different interface, the packet is denied. Based on the scenario:

o C. Strict RPF check will allow the traffic:

If the return path for 192.168.32.15 matches the interface where the traffic was received, the strict RPF check will allow the traffic.

• Loose RPF Check:

In loose RPF, FortiGate only checks if there is any route back to the source IP of the packet, regardless of the interface. This is a more permissive check, and if a route exists, the packet will be allowed.

o B. Loose RPF check will allow the traffic:

Since loose RPF requires only that a valid route to the source exists, the traffic is allowed.

Why the other options are less appropriate:

• A. Strict RPF check will deny the traffic:

This would only happen if the return route didn't match the incoming interface, which is not indicated here.

• D. Loose RPF check will deny the traffic:

Loose RPF is more permissive, so it will not deny the traffic as long as a valid route to the source IP exists.

**NEW QUESTION 57**

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 61**

Which three criteria can FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

A. Services defined in the firewall policy

B. Highest to lowest priority defined in the firewall policy

C. Destination defined as Internet Services in the firewall policy

D. Lowest to highest policy ID number

E. Source defined as Internet Services in the firewall policy

**Answer:** ACE

**Explanation:**

• A. Services defined in the firewall policy: FortiGate uses the service specified in the firewall policy to match traffic. Services define the types of traffic (like HTTP, FTP) that the policy will apply to.

• C. Destination defined as Internet Services in the firewall policy: Policies can be matched based on the destination being categorized as Internet Services, allowing specific handling of such traffic.

• E. Source defined as Internet Services in the firewall policy: Similarly, traffic from sources categorized as Internet Services can be matched and processed according to the policy configuration.

Why the other options are less relevant:

• B. Highest to lowest priority defined in the firewall policy: Policies are processed from top to bottom, not by priority. The highest priority policy is processed first, but this is about the order of policy processing rather than criteria for matching traffic.

• D. Lowest to highest policy ID number: Policies are processed from the top of the list (the lowest policy ID) to the bottom (the highest policy ID), which is about the processing order rather than matching criteria.

**NEW QUESTION 64**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questons 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 FirstTry
- \* FCP\_FGT\_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The FCP\\_FGT\\_AD-7.4 Practice Test Here](#)**