

## FCP\_FGT\_AD-7.4 Dumps

### FCP - FortiGate 7.4 Administrator

[https://www.certleader.com/FCP\\_FGT\\_AD-7.4-dumps.html](https://www.certleader.com/FCP_FGT_AD-7.4-dumps.html)



**NEW QUESTION 1**

Refer to the exhibit.

```
id=65308 trace_id=6 func=print_pkt_detail line=5895 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:21637  
->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=21637, seq=2."  
id=65308 trace_id=6 func=init_ip_session_common line=6076 msg="allocate a new session-00025d45, tun_id=0.0.0.  
0"  
id=65308 trace_id=6 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000 gw=10.200.1.254  
via port1"  
id=65308 trace_id=6 func=fw_forward_handler line=738 msg="Denied by forward policy check (policy 0)"
```

Why did FortiGate drop the packet?

- A. It matched an explicitly configured firewall policy with the action DENY
- B. It failed the RPF check.
- C. The next-hop IP address is unreachable.
- D. It matched the default implicit firewall policy

**Answer:** D

**Explanation:**

The debug trace output shows that the packet was "Denied by forward policy check (policy 0)." In FortiGate, policy ID 0 corresponds to the default implicit deny policy. This means that if a packet does not match any configured firewall policies, it is denied by the default implicit policy.

References:



FortiOS 7.4.1 Administration Guide: Firewall Policies

**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**

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, which shows a partial configuration from the remote authentication server.

Attribute	Value	Vendor	Actions
Fortinet-Group-Name	Training	Fortinet	 

Why does the FortiGate administrator need this configuration?

- A. To authenticate only the Training user group.
- B. To set up a RADIUS server Secret
- C. To authenticate and match the Training OU on the RADIUS server.
- D. To authenticate Any FortiGate user groups.

**Answer:** A

#### NEW QUESTION 6

FortiGate is integrated with FortiAnalyzer and FortiManager.

When a firewall policy is created, which attribute is added to the policy to improve functionality and to support recording logs to FortiAnalyzer or FortiManager?

- A. Log ID
- B. Policy ID
- C. (Sequence ID
- D. Universally Unique Identifier

**Answer:** D

#### Explanation:

When a firewall policy is created in FortiGate integrated with FortiAnalyzer and FortiManager, a Universally Unique Identifier (UUID) is added to the policy to support logging and management.

#### NEW QUESTION 7

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 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

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**

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.

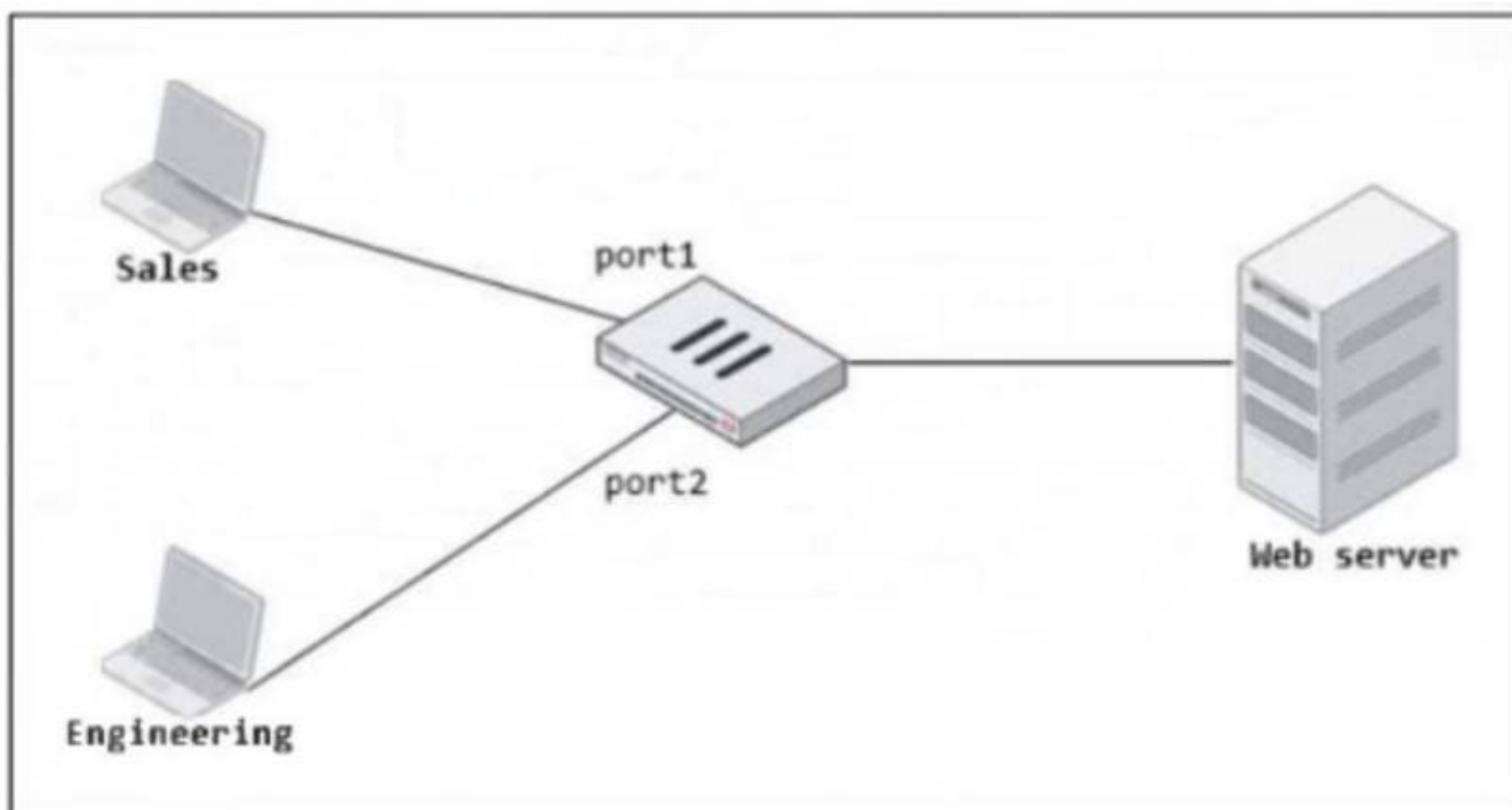
**Answer:** D

**Explanation:**

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

**NEW QUESTION 10**

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 11**

Refer to the exhibit to view the firewall policy.

## Firewall policy configuration

Edit Policy

Name	Internet_Access		
Incoming Interface	port2	+	✕
Outgoing Interface	port1	+	✕
Source	all	+	✕
Destination	all	+	✕
Schedule	always		
Service	<div> DNS ✕ </div> <div> FTP ✕ </div> <div> HTTP ✕ </div> <div> HTTPS ✕ </div> <div> +</div>		
Action	<div> <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY </div>		
Inspection Mode	<div> Flow-based Proxy-based </div>		

Firewall/Network Options

NAT

☒

IP Pool Configuration

Use Outgoing Interface Address
Use Dynamic IP Pool

Preserve Source Port
☐

Protocol Options

PROT default

Security Profiles

AntiVirus
☒

AV default

Web Filter
☐

DNS Filter
☐

Application Control
☐

IPS
☐

File Filter
☐

SSL Inspection

SSL certificate-inspection

Why would the firewall policy not block a well-known virus, for example eicar?

- A. The action on the firewall policy is not set to deny.
- B. The firewall policy is not configured in proxy-based inspection mode.
- C. Web filter is not enabled on the firewall policy to complement the antivirus profile.
- D. The firewall policy does not apply deep content inspection.

Answer: B

Explanation:

The firewall policy shown in the exhibit is configured in flow-based inspection mode. In flow-based inspection, certain security features, such as deep content inspection, might not be as effective as in proxy- based mode. Proxy-based inspection is necessary for thorough content inspection, which includes identifying and blocking well-known viruses like EICAR.

References:

> FortiOS 7.4.1 Administration Guide: Inspection Modes

NEW QUESTION 15

Refer to the exhibit.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port3 → port1 ⓘ									
1	Full_Access	Remote-users 4 LOCAL_SUB...	4 all	always	HTTP HTTPS ALL_ICMP	✓ ACCEPT	✓ NAT	Standard	Category_Monitor SSL certificate-inspection

FortiGate is configured for firewall authentication. When attempting to access an external website, the user is not presented with a login prompt. What is the most likely reason for this situation?

- A. The Service DNS is required in the firewall policy.
- B. The user is using an incorrect user name.
- C. The Remote-users group is not added to the Destination.
- D. No matching user account exists for this user.

Answer: A

Explanation:

Firewall authentication generally requires the DNS service to be enabled in the firewall policy to correctly resolve hostnames during the authentication process. If DNS is not allowed in the firewall policy, the FortiGate cannot resolve external domains, and as a result, the user may not be presented with the login prompt when attempting to access an external website.

References:

> FortiOS 7.4.1 Administration Guide: Firewall Authentication Configuration

NEW QUESTION 19

Refer to the exhibit.

## FortiGate routing database

```
Local-FortiGate # get router info routing-table database
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
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S      0.0.0.0/0 [20/0] via 10.200.2.254, port2, [1/0]
S      *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C      *> 10.0.1.0/24 is directly connected, port3
C      *> 10.200.1.0/24 is directly connected, port1
C      *> 10.200.2.0/24 is directly connected, port2
C      *> 172.16.100.0/24 is directly connected, port8
```

Which two statements are true about the routing entries in this database table? (Choose two.)

- A. All of the entries in the routing database table are installed in the FortiGate routing table.
- B. The port2 interface is marked as inactive.
- C. Both default routes have different administrative distances.
- D. The default route on port2 is marked as the standby route.

**Answer:** CD

### Explanation:

The routing table in the exhibit shows two default routes (0.0.0.0/0) with different administrative distances:



The default route through port2 has an

administrative distance of 20.



The default route through port1 has an administrative distance of 10.

Administrative distance determines the priority of the route; a lower value is preferred. Here, the route through port1 with an administrative distance of 10 is the preferred route. The route through port2 with an administrative distance of 20 acts as a standby or backup route. If the primary route (port1) fails or is unavailable, traffic will then be routed through port2.

Regarding the statement that the port2 interface is marked as inactive, there is no indication in the routing table that port2 is inactive. Similarly, all the routes displayed are not necessarily installed in the FortiGate routing table, as the table could include both active and backup routes.

References:



FortiOS 7.4.1 Administration Guide: Default route configuration



FortiOS 7.4.1 Administration Guide: Routing table

## NEW QUESTION 22

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 26



The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile. Which order must FortiGate use when the web filter profile has features such as safe search enabled?

- A. FortiGuard category filter and rating filter
- B. Static domain filter, SSL inspection filter, and external connectors filters
- C. DNS-based web filter and proxy-based web filter
- D. Static URL filter, FortiGuard category filter, and advanced filters

Answer: D

Explanation:

FortiGate applies web filters in the following order: Static URL filter, FortiGuard category filter, Web content filter, Web script filter, and Antivirus scanning.

NEW QUESTION 28

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 32

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 35

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 36

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 41

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 45

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.

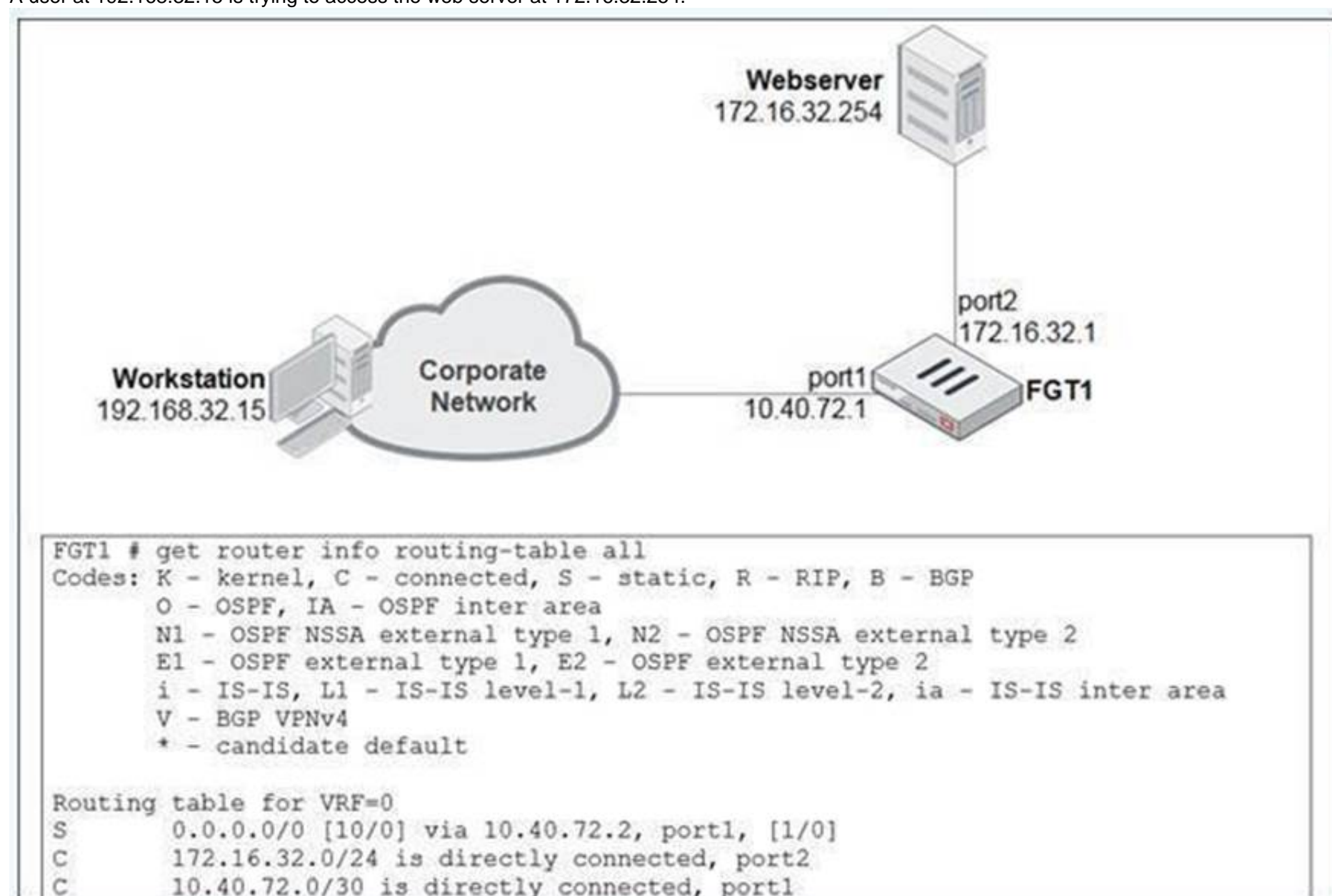
• B. Set the session TTL on the SSLVPN policy to maximum:

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 48

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 50**

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 53**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your FCP\_FGT\_AD-7.4 Exam with Our Prep Materials Via below:**

[https://www.certleader.com/FCP\\_FGT\\_AD-7.4-dumps.html](https://www.certleader.com/FCP_FGT_AD-7.4-dumps.html)