



Fortinet

Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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 2

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 3

Which two statements are true regarding FortiGate HA configuration synchronization? (Choose two.)

- A. Checksums of devices are compared against each other to ensure configurations are the same.
- B. Incremental configuration synchronization can occur only from changes made on the primary FortiGate device.
- C. Incremental configuration synchronization can occur from changes made on any FortiGate device within the HA cluster
- D. Checksums of devices will be different from each other because some configuration items are not synced to other HA members.

Answer: AB

Explanation:

In FortiGate HA (High Availability) configuration, checksums of device configurations are compared to ensure they are synchronized and identical across the cluster. Incremental synchronization can only happen from changes made on the primary device to ensure consistency and integrity across the cluster members. Changes made on non-primary devices do not initiate synchronization.

References:



FortiOS 7.4.1 Administration Guide: HA Configuration Synchronization

NEW QUESTION 4

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 5

Which three strategies are valid SD-WAN rule strategies for member selection? (Choose three.)

- A. Manual with load balancing
- B. Lowest Cost (SLA) with load balancing
- C. Best Quality with load balancing
- D. Lowest Quality (SLA) with load balancing
- E. Lowest Cost (SLA) without load balancing

Answer: ABC

Explanation:

FortiGate's SD-WAN rule strategies for member selection include the following:

- Manual with load balancing: This strategy allows an administrator to manually configure which SD-WAN member interfaces to use for specific traffic.
- Lowest Cost (SLA) with load balancing: This strategy prioritizes the link with the lowest cost that meets the SLA requirements.



Best Quality with load balancing: This strategy selects the link with the best performance metrics, such as latency, jitter, or packet loss.

Options D and E are incorrect because "Lowest Quality" is not a valid strategy, and "Lowest Cost without load balancing" contradicts the requirement for load balancing in the strategy name.

References:



FortiOS 7.4.1 Administration Guide: SD-WAN Rule Strategies

NEW QUESTION 6

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 7

Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

- A. Pre-shared key and certificate signature as authentication methods
- B. Extended authentication (XAuth) to request the remote peer to provide a username and password
- C. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
- D. No certificate is required on the remote peer when you set the certificate signature as the authentication method

Answer: AB

Explanation:

FortiGate supports both pre-shared key and certificate signature methods for IKEv1 authentication. These methods provide flexibility depending on the security requirements of the network. Additionally, FortiGate supports Extended Authentication (XAuth), which requests a username and password from the remote peer, enhancing security by adding an extra layer of authentication. The XAuth method does not necessarily make the authentication faster; it is an additional security measure.

References:



FortiOS 7.4.1 Administration Guide: IPsec VPN Configuration

NEW QUESTION 8

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 9

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.

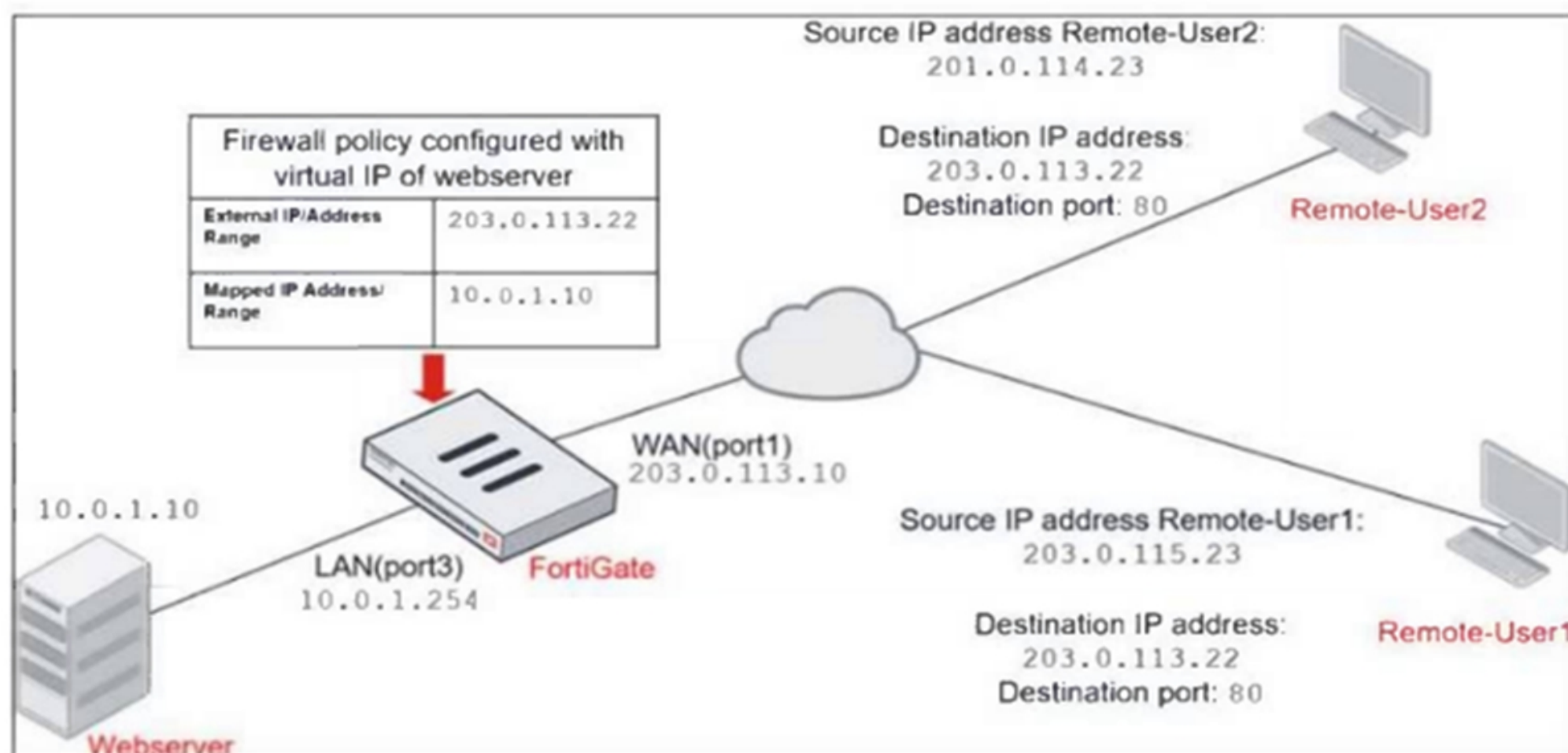
References:

- FortiOS 7.4.1 Administration Guide: HA election process

NEW QUESTION 10

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> WAN (port1) →  LAN (port3) 2</div></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 10

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 12

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:

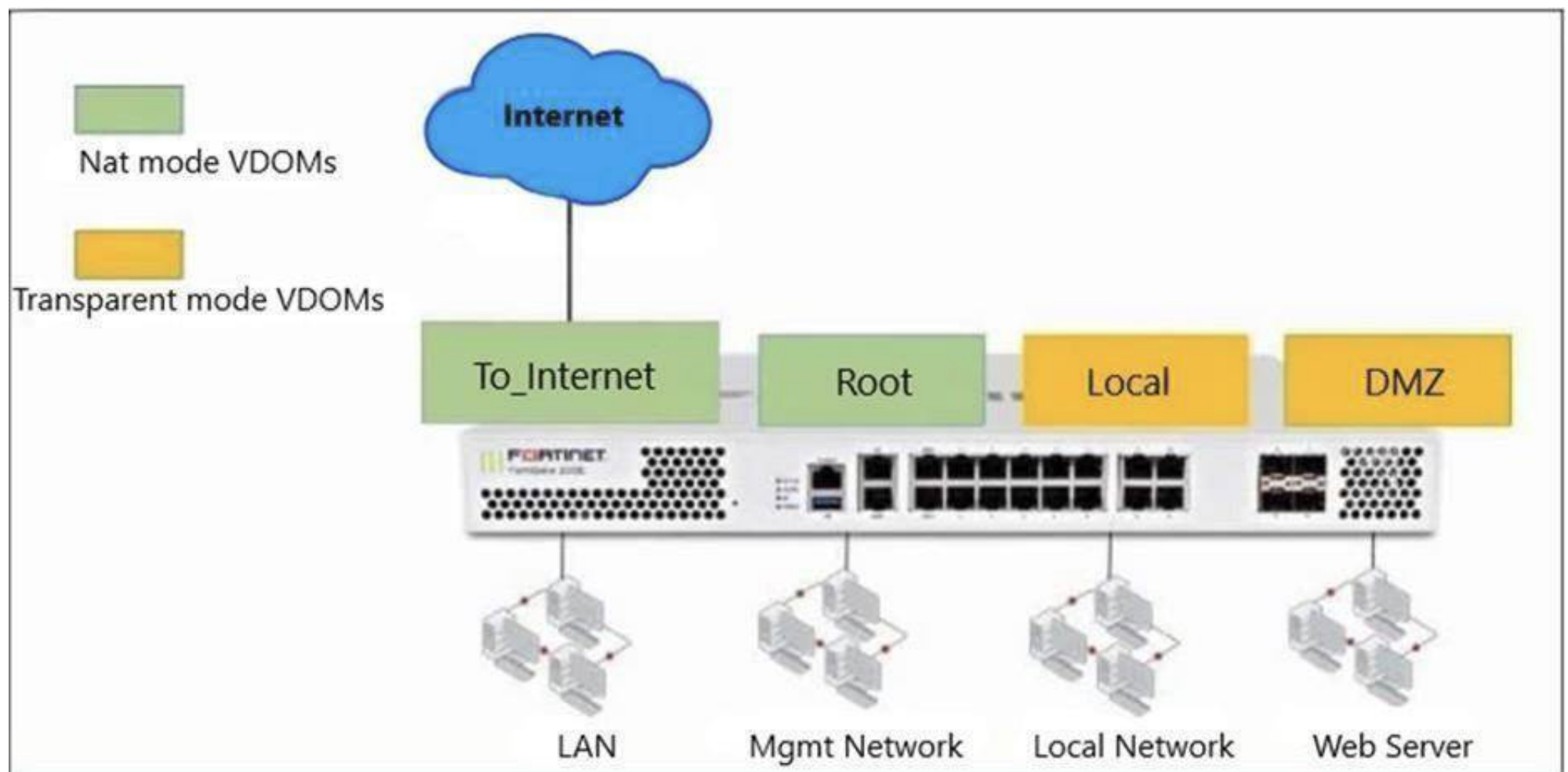
- A. The underlay zone contains port1 and: There is no mention in the exhibit about an "underlay zone" containing port1.
- B. The d-wan zone contains no member: This statement is irrelevant since the focus is on the zone's deletion, not its members.
- D. The virtual-wan-link zone contains no member: 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 15

Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode. The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem. With this configuration, which statement is true?

- A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
- B. A default static route is not required on the To_Internet VDOM to allow LAN users to access the internet.
- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
- D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: A

Explanation:

In this scenario, multiple Virtual Domains (VDOMs) are used, and each VDOM operates either in NAT mode or transparent mode:

- Root VDOM (management) and To_Internet VDOM are in NAT mode.
- DMZ VDOM and Local VDOM are in transparent mode.

To allow traffic between different VDOMs (e.g., Local and Root), inter-VDOM links must be configured.

Since Local VDOM is in transparent mode, it functions at Layer 2, meaning it requires an inter-VDOM link to pass traffic through the Root VDOM, which operates in NAT mode at Layer 3.

Why the other options are less appropriate:

- B. A default static route is not required on the To_Internet VDOM:

A default route is required on the To_Internet VDOM to send traffic from LAN users to the internet.

- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs:

Both Local and DMZ are in transparent mode and operate at Layer 2, so direct communication would require inter-VDOM links if passing through another VDOM.

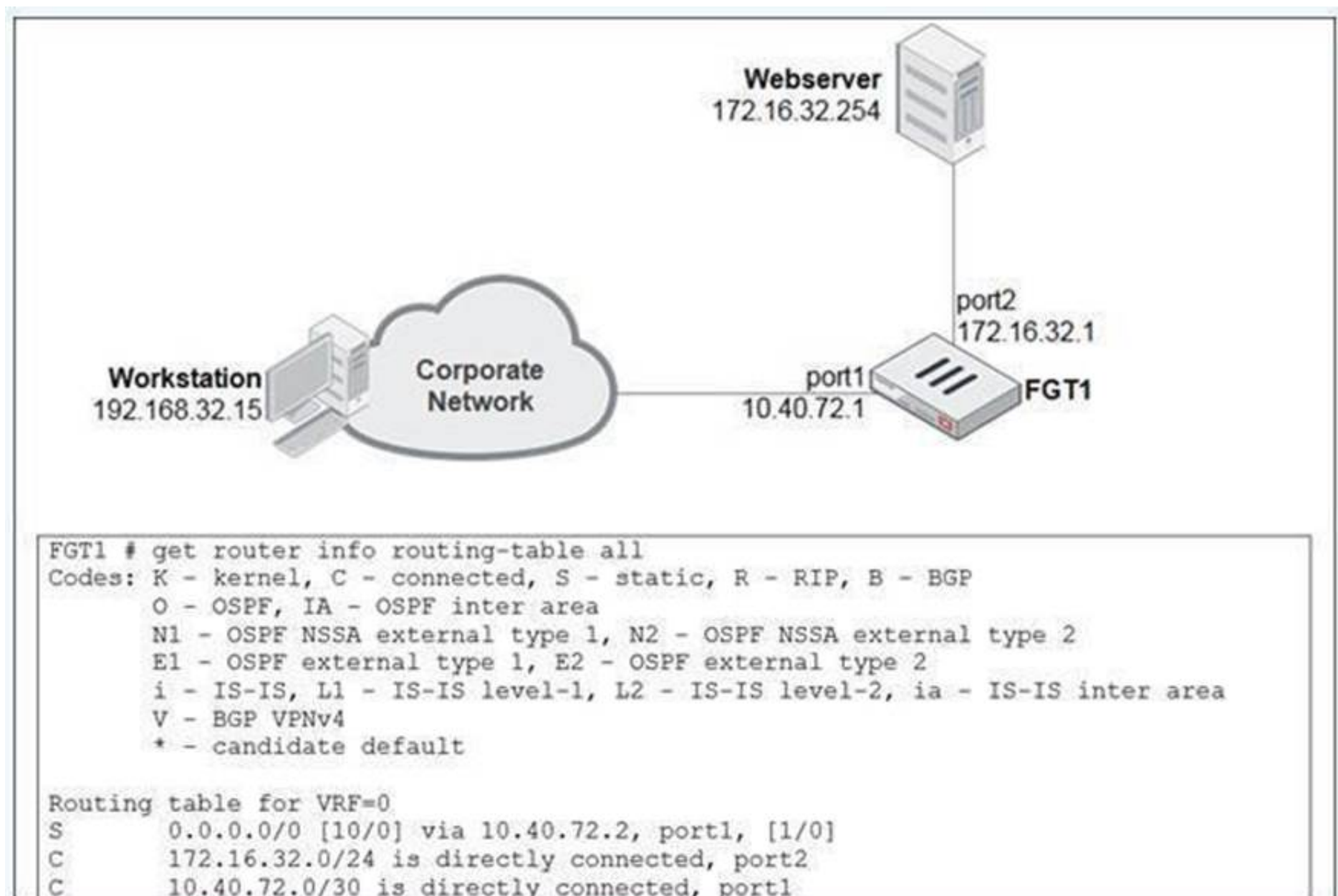
- D. Inter-VDOM links are not required between the Root and To_Internet VDOMs:

Even if the Root VDOM is only used for management, it still requires inter-VDOM links to communicate with other VDOMs (like To_Internet) in the Security Fabric.

NEW QUESTION 16

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 17

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 20

.....

Relate Links

100% Pass Your FCP_FGT_AD-7.4 Exam with Exam Bible Prep Materials

https://www.exambible.com/FCP_FGT_AD-7.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>