



Fortinet

Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

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

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 3

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 4

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 5

Refer to the exhibit.

Name	Severity	Target	OS	Action
IPS Signature				
FTP.Login.Failed	Low	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 6

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 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

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 9

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 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

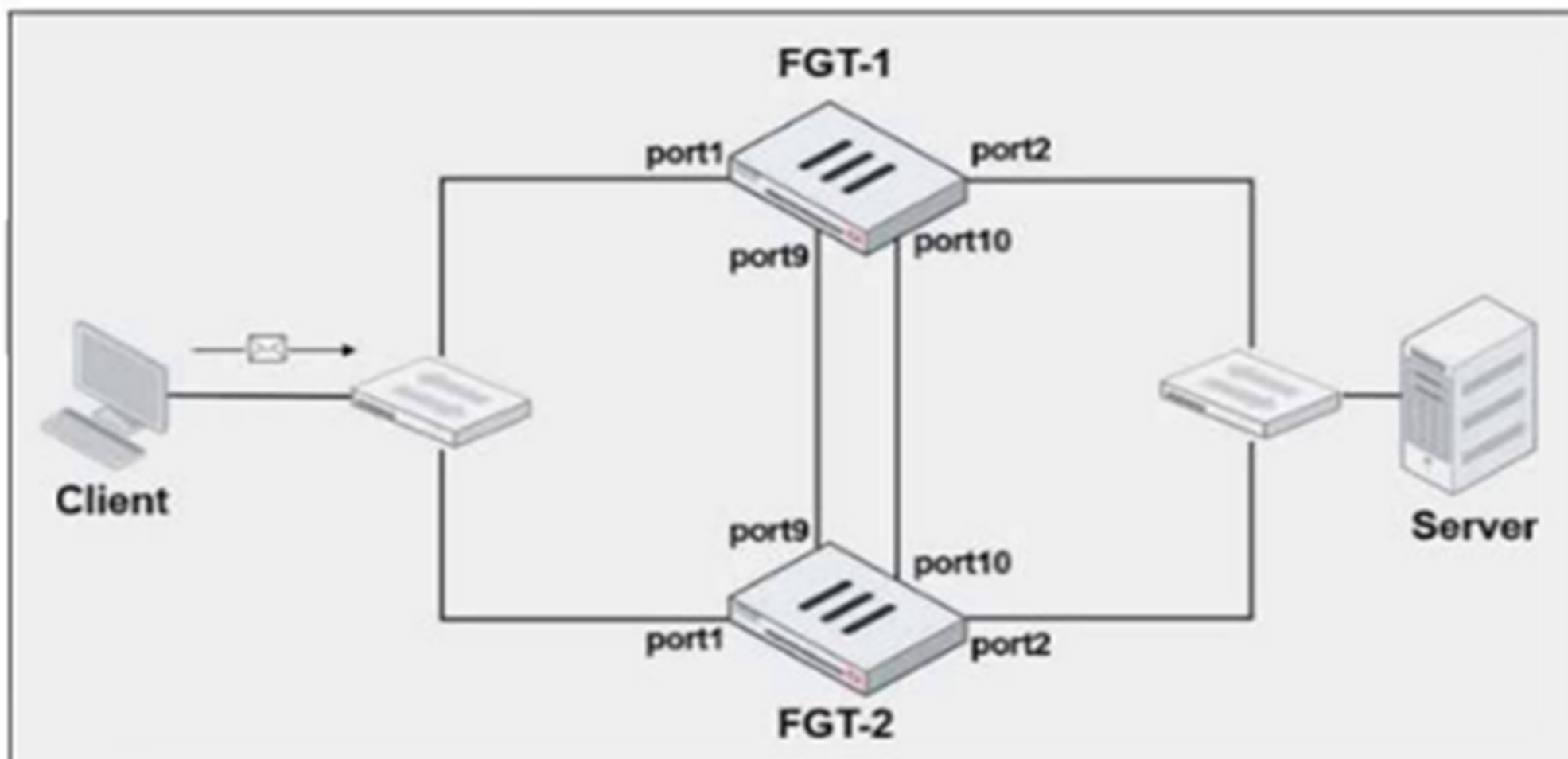


FortiOS 7.4.1 Administration Guide: Routing table

NEW QUESTION 10

Refer to the exhibits.

FortiGate HA cluster topology



Current HA status

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

New FortiGate HA configuration

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

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

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

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

Answer: B

NEW QUESTION 12

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:

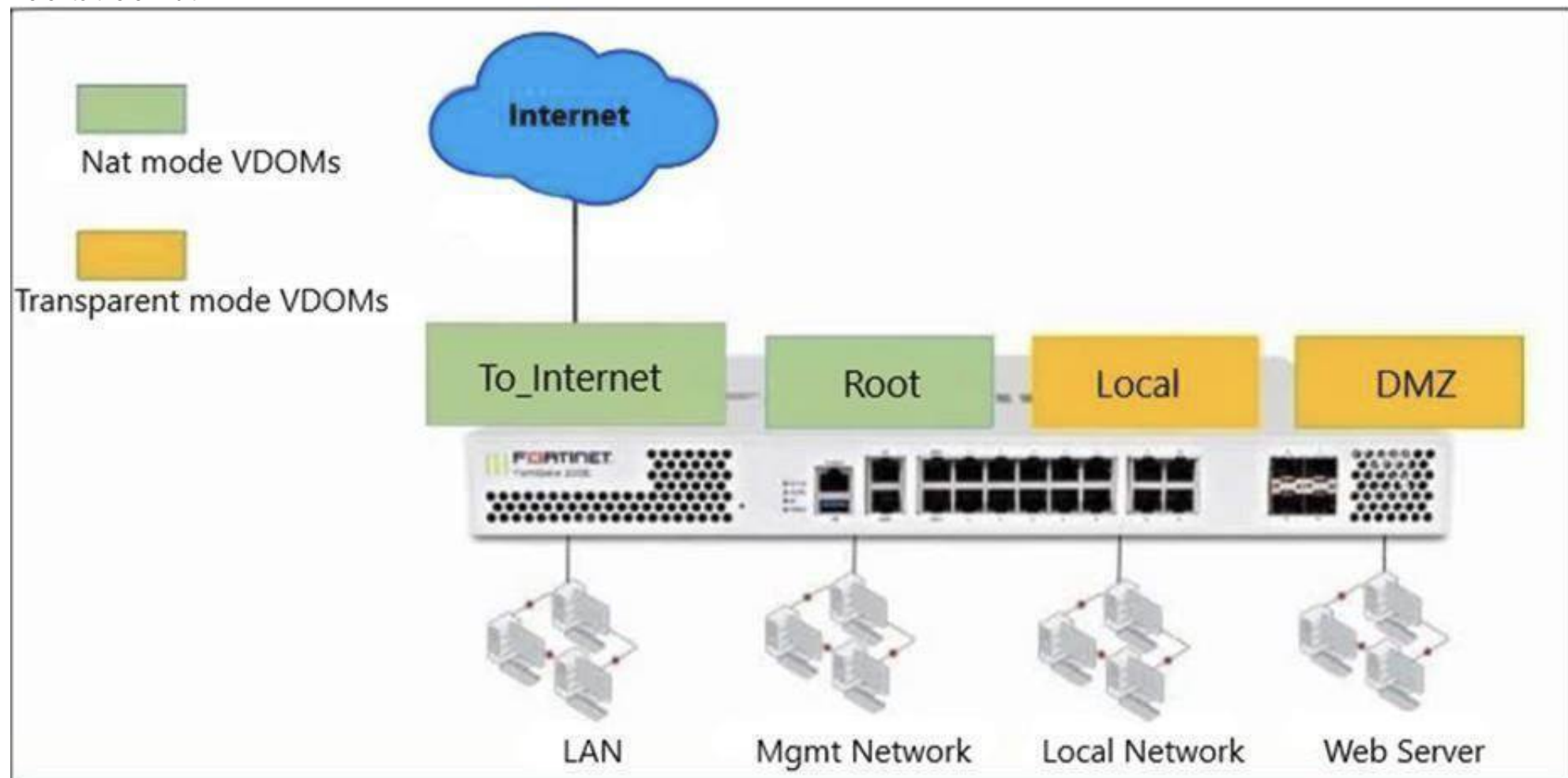
- A. Port block allocation: This type of IP pool allocates a block of ports from a single public IP to multiple clients. It allows efficient use of a limited number of public IPs by distributing port ranges among users, which is crucial for carrier-grade NAT environments where a large number of users 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 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 18

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

FCP_FGT_AD-7.4 Practice Exam Features:

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

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