



**Free Questions for NSE4\_FGT-7.2 by certsinside**

**Shared by Robinson on 12-12-2023**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

## Question Type: MultipleChoice

---

Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

What two conclusions can you make from the debug flow output? (Choose two.)

### Options:

---

- A- The debug flow is for ICMP traffic.
- B- The default route is required to receive a reply.
- C- A new traffic session was created.

**D-** A firewall policy allowed the connection.

### **Answer:**

---

A, C

### **Explanation:**

---

The debug flow output shows the result of a diagnose command that captures the traffic flow between the source and destination IP addresses<sup>1</sup>. The debug flow output reveals the following information about the traffic flow<sup>1</sup>:

The protocol is 1, which means that the traffic uses ICMP protocol<sup>2</sup>. ICMP is a protocol that is used to send error messages and test connectivity between devices<sup>2</sup>.

The session state is 0, which means that a new traffic session was created<sup>3</sup>. A session is a data structure that stores information about a connection between two devices<sup>3</sup>.

The policy ID is 1, which means that the traffic matched the firewall policy with ID 14. A firewall policy is a rule that defines how FortiGate processes traffic based on the source, destination, service, and action parameters<sup>4</sup>.

The action is 0, which means that the traffic was allowed by the firewall policy. An action is a parameter that specifies what FortiGate does with the traffic that matches a firewall policy.

Therefore, two conclusions that can be made from the debug flow output are:

The debug flow is for ICMP traffic.

A new traffic session was created.

## Question 2

---

**Question Type:** MultipleChoice

---

An administrator configures outgoing interface any in a firewall policy.

What is the result of the policy list view?

### Options:

---

- A- Search option is disabled.
- B- Policy lookup is disabled.
- C- By Sequence view is disabled.
- D- Interface Pair view is disabled.

### Answer:

---

D

### **Explanation:**

---

'If you use multiple source or destination interfaces, or the any interface in a firewall policy, you cannot separate policies into sections by interface pairs---some would be triplets or more. So instead, policies are then always displayed in a single list (By Sequence).'

## **Question 3**

---

### **Question Type: MultipleChoice**

---

What are two functions of the ZTNA rule? (Choose two.)

### **Options:**

---

- A-** It redirects the client request to the access proxy.
- B-** It applies security profiles to protect traffic.
- C-** It defines the access proxy.
- D-** It enforces access control.

## Answer:

---

B, D

## Explanation:

---

A ZTNA rule is a policy that enforces access control and applies security profiles to protect traffic between the client and the access proxy<sup>1</sup>. A ZTNA rule defines the following parameters<sup>1</sup>:

Incoming interface: The interface that receives the client request.

Source: The address and user group of the client.

ZTNA tag: The tag that identifies the domain that the client belongs to.

ZTNA server: The server that hosts the access proxy.

Destination: The address of the application that the client wants to access.

Action: The action to take for the traffic that matches the rule. It can be accept, deny, or redirect.

Security profiles: The security features to apply to the traffic, such as antivirus, web filter, application control, and so on.

A ZTNA rule does not redirect the client request to the access proxy. That is the function of a policy route that matches the ZTNA tag and sends the traffic to the ZTNA server<sup>2</sup>.

A ZTNA rule does not define the access proxy. That is done by creating a ZTNA server object that specifies the IP address, port, and certificate of the access proxy<sup>3</sup>.

FortiGate Infrastructure 7.2 Study Guide (p.177): 'A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. To create a rule, type a rule name, and add IP addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic.'

## Question 4

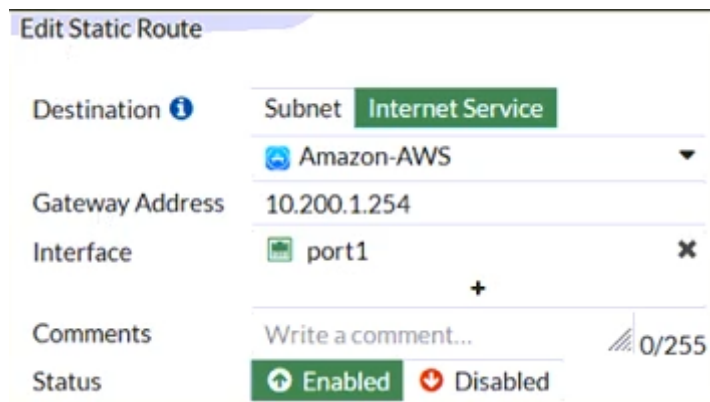
---

**Question Type:** MultipleChoice

---

Refer to the exhibit, which contains a static route configuration.

An administrator created a static route for Amazon Web Services.



The screenshot shows the 'Edit Static Route' configuration page in FortiGate. The configuration is as follows:

Field	Value
Destination	Subnet: Internet Service
	Gateway: Amazon-AWS
Gateway Address	10.200.1.254
Interface	port1
Comments	Write a comment... (0/255)
Status	Enabled

Which CLI command must the administrator use to view the route?

### Options:

---

- A- get router info routing-table database
- B- diagnose firewall proute list
- C- get internet-service route list
- D- get router info routing-table all

### Answer:

---

B

### Explanation:

---

ISDB static route will not create entry directly in routing-table. Reference: <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Creating-a-static-route-for-Predefined-Internet/ta-p/198756>

and here <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verify-the-matching-policy-route/ta-p/190640>

FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): 'Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table.' 'FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command.'



## Question 5

---

**Question Type:** MultipleChoice

---

Which statement is correct regarding the security fabric?

### Options:

---

- A- FortiManager is one of the required member devices.
- B- FortiGate devices must be operating in NAT mode.
- C- A minimum of two Fortinet devices is required.
- D- FortiGate Cloud cannot be used for logging purposes.

### Answer:

---

B

### Explanation:

---

FortiGate Security 7.2 Study Guide (p.428): 'You must have a minimum of two FortiGate devices at the core of the Security Fabric, plus one FortiAnalyzer or cloud logging solution. FortiAnalyzer Cloud or FortiGate Cloud can act as the cloud logging solution. The FortiGate devices must be running in NAT mode.'

## Question 6

---

**Question Type:** MultipleChoice

---

Refer to the exhibits.

Exhibit A shows the application sensor configuration. Exhibit B shows the Excessive-Bandwidth and Apple filter details.

### Edit Application Sensor

Categories

- All Categories
- Business (179, ☁ 6)
- Collaboration (293, ☁ 6)
- Game (124)
- Mobile (3)
- P2P (85)
- Remote.Access (91)
- Storage.Backup (296, ☁ 16)
- Video/Audio (206, ☁ 13)
- Web.Client (18)
- Cloud.IT (31)
- Email (87, ☁ 12)
- General.Interest (241, ☁ 9)
- Network.Service (332)
- Proxy (106)
- Social.Media (150, ☁ 31)
- Update (48)
- VoIP (31)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

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

Priority	Details	Type	Action
1	<b>BHVR</b> Excessive-Bandwidth	Filter	<input type="checkbox"/> Block
2	<b>VEND</b> Apple	Filter	<input type="checkbox"/> Monitor

Exhibit A Exhibit B

The image displays two screenshots of a network configuration interface, both titled "Edit Override".

**Top Screenshot:**

- Type: Application Filter
- Action: Block
- Filter: BHWR Excessive-Bandwidth
- Search: FaceTime
- Table Headers: Name, Category, Technology
- Table Content:
  - Application Signature 1/1262
  - FaceTime (VoIP) Client-Server

**Bottom Screenshot:**

- Type: Application Filter
- Action: Monitor
- Filter: VENDOR Apple
- Search: FaceTime
- Table Headers: Name, Category, Technology
- Table Content:
  - Application Signature 1/33
  - FaceTime (VoIP) Client-Server

Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

### Options:

---

- A- Apple FaceTime will be allowed, based on the Categories configuration.
- B- Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.
- C- Apple FaceTime will be allowed, based on the Apple filter configuration.
- D- Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.

### Answer:

---

B

### Explanation:

---

FortiGate Security 7.2 Study Guide (p.310): 'Then, FortiGate scans packets for matches, in this order, for the application control profile:  
1. Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies. 2. Categories: Finally, the application control profile applies the action that you've configured for applications in your selected categories.'

## Question 7

---

**Question Type:** MultipleChoice

---

Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?

**Options:**

---

- A-** VDOMs without ports with connected devices are not displayed in the topology.
- B-** Downstream devices can connect to the upstream device from any of their VDOMs.
- C-** Security rating reports can be run individually for each configured VDOM.
- D-** Each VDOM in the environment can be part of a different Security Fabric.

**Answer:**

---

A

**Explanation:**

---

FortiGate Security 7.2 Study Guide (p.436): 'When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. Only the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable Device Detection on ports you want to have displayed in the Security Fabric. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single Security Fabric.'

## Question 8

---

**Question Type:** MultipleChoice

---

Refer to the exhibit.

The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.

An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.

**Edit Web Filter Profile**

Name Corporate

Comments Write a comment... 0/255

Feature set **Flow-based** Proxy-based

FortiGuard Category Based Filter

Allow
  Monitor
  Block
  Warning
  Authenticate

Name	Action
<b>Bandwidth Consuming 6</b>	
Freeware and Software Downloads	<input checked="" type="checkbox"/> Allow
File Sharing and Storage	<input checked="" type="checkbox"/> Allow
Streaming Media and Download	<input checked="" type="checkbox"/> Allow
Peer-to-peer File Sharing	<input checked="" type="checkbox"/> Allow
Internet Radio and TV	<input checked="" type="checkbox"/> Allow
Internet Telephony	<input checked="" type="checkbox"/> Allow
<b>Security Risk 6</b>	
Malicious Websites	<input type="checkbox"/> Block

35% 91

What are two solutions for satisfying the requirement? (Choose two.)

**Options:**

---



- A-** Configure a separate firewall policy with action Deny and an FQDN address object for \*.download.com as destination address.
- B-** Configure a web override rating for download.com and select Malicious Websites as the subcategory.
- C-** Set the Freeware and Software Downloads category Action to Warning.
- D-** Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

### **Answer:**

---

B, D

### **Explanation:**

---

FortiGate Security 7.2 Study Guide (p.268-269): 'If you want to make an exception, for example, rather than unblock access to a potentially unwanted category, change the website to an allowed category. You can also do the reverse. You can block a website that belongs to an allowed category.' 'Static URL filtering is another web filter feature. Configured URLs in the URL filter are checked against the visited websites. If a match is found, the configured action is taken. URL filtering has the same patterns as static domain filtering: simple, regular expressions, and wildcard.'

B) Configure a web override rating for download.com and select Malicious Websites as the subcategory.

This is true because a web override rating is a feature that allows the administrator to change the FortiGuard category of a specific website or domain, and apply a different action to it based on the web filter profile. By configuring a web override rating for download.com and selecting Malicious Websites as the subcategory, the administrator can block access to download.com, which belongs to the Freeware and Software Downloads category by default, without affecting other websites in the same category. The Malicious Websites category has the action Block in the web filter profile shown in the exhibit.

D) Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

This is true because a static URL filter entry is a feature that allows the administrator to define custom rules for filtering specific URLs or domains, and apply an action to them based on the web filter profile. By configuring a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively, the administrator can block access to download.com and any subdomains or paths under it, without affecting other websites in the Freeware and Software Downloads category. The static URL filter entries have higher priority than the FortiGuard category based filter entries in the web filter profile.

## Question 9

---

**Question Type: MultipleChoice**

---

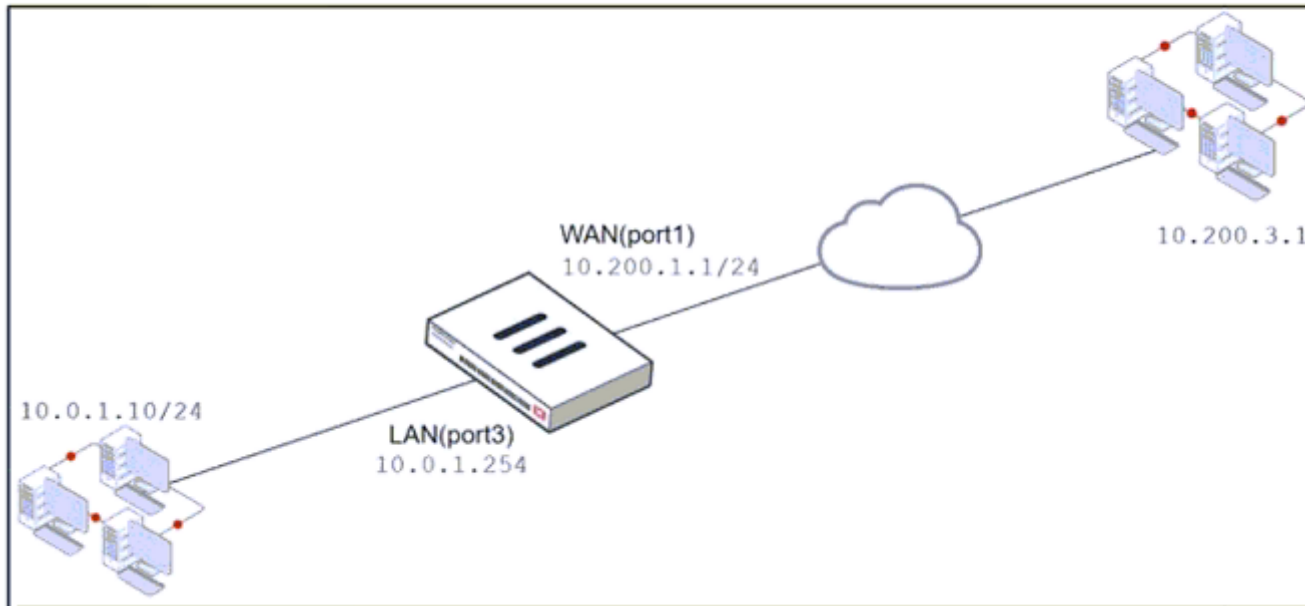
Refer to the exhibits.

Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.

The WAN (port1) interface has the IP address 10.200.1.1/24.

The LAN (port3) interface has the IP address 10.0.1.254/24.

The administrator disabled the WebServer firewall policy.



Name	From	To	Source	Destination	Schedule	Service	Action	NAT
Full_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	ACCEPT	Enabled
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Disabled

**Edit Virtual IP**

VIP type IPv4

Name VIP

Comments Write a comment... 0/255

Color Change

Network

Interface WAN (port1)

Type Static NAT

External IP address/range 10.200.1.10

Map to

IPv4 address/range 10.0.1.10

Optional Filters

Port Forwarding

Which IP address will be used to source NAT the traffic, if a user with address 10.0.1.10 connects over SSH to the host with address 10.200.3.1?

### Options:

---

A- 10.200.1.10

B- 10.0.1.254

C- 10.200.1.1

D- 10.200.3.1

### Answer:

---

C

### Explanation:

---

Traffic is coming from LAN to WAN, matches policy Full\_Access which has NAT enable, so traffic uses source IP address of outgoing interface. Simple SNAT.

## Question 10

---

**Question Type:** MultipleChoice

---

What are two characteristics of FortiGate HA cluster virtual IP addresses? (Choose two.)

## Options:

---

- A- Virtual IP addresses are used to distinguish between cluster members.
- B- Heartbeat interfaces have virtual IP addresses that are manually assigned.
- C- The primary device in the cluster is always assigned IP address 169.254.0.1.
- D- A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.

## Answer:

---

A, D

## Explanation:

---

Fortigate Infrastructure 7.2 Study Guide page 301

FortiGate Infrastructure 7.2 Study Guide (p.301):

'FGCP automatically assigns the heartbeat IP addresses based on the serial number of each device. The IP address 169.254.0.1 is assigned to the device with the highest serial number.'

'A change in the heartbeat IP addresses may happen when a FortiGate device joins or leaves the cluster.'

'The HA cluster uses the heartbeat IP addresses to distinguish the cluster members and synchronize data.'

## Question 11

---

**Question Type:** MultipleChoice

---

An administrator wants to simplify remote access without asking users to provide user credentials.

Which access control method provides this solution?

**Options:**

---

**A-** ZTNA IP/MAC filtering mode

**B-** ZTNA access proxy

**C-** SSL VPN

**D-** L2TP

**Answer:**

---

B

## **Explanation:**

---

FortiGate Infrastructure 7.2 Study Guide (p.165): 'ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs.'

This is true because ZTNA access proxy is a feature that allows remote users to access internal applications without requiring VPN or user credentials. ZTNA access proxy uses a secure tunnel between the user's device and the FortiGate, and authenticates the user based on device identity and context. The user only needs to install a lightweight agent on their device, and the FortiGate will automatically assign them to the appropriate application group based on their device profile. This simplifies remote access and enhances security by reducing the attack surface<sup>12</sup>



**To Get Premium Files for NSE4\_FGT-7.2 Visit**

[https://www.p2pexams.com/products/nse4\\_fgt-7.2](https://www.p2pexams.com/products/nse4_fgt-7.2)

**For More Free Questions Visit**

<https://www.p2pexams.com/fortinet/pdf/nse4-fgt-7.2>

