

# NSE4\_FGT-7.2<sup>Q&As</sup>

Fortinet NSE 4 - FortiOS 7.2

## Pass Fortinet NSE4\_FGT-7.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

[https://www.pass2lead.com/nse4\\_fgt-7-2.html](https://www.pass2lead.com/nse4_fgt-7-2.html)

100% Passing Guarantee  
100% Money Back Assurance

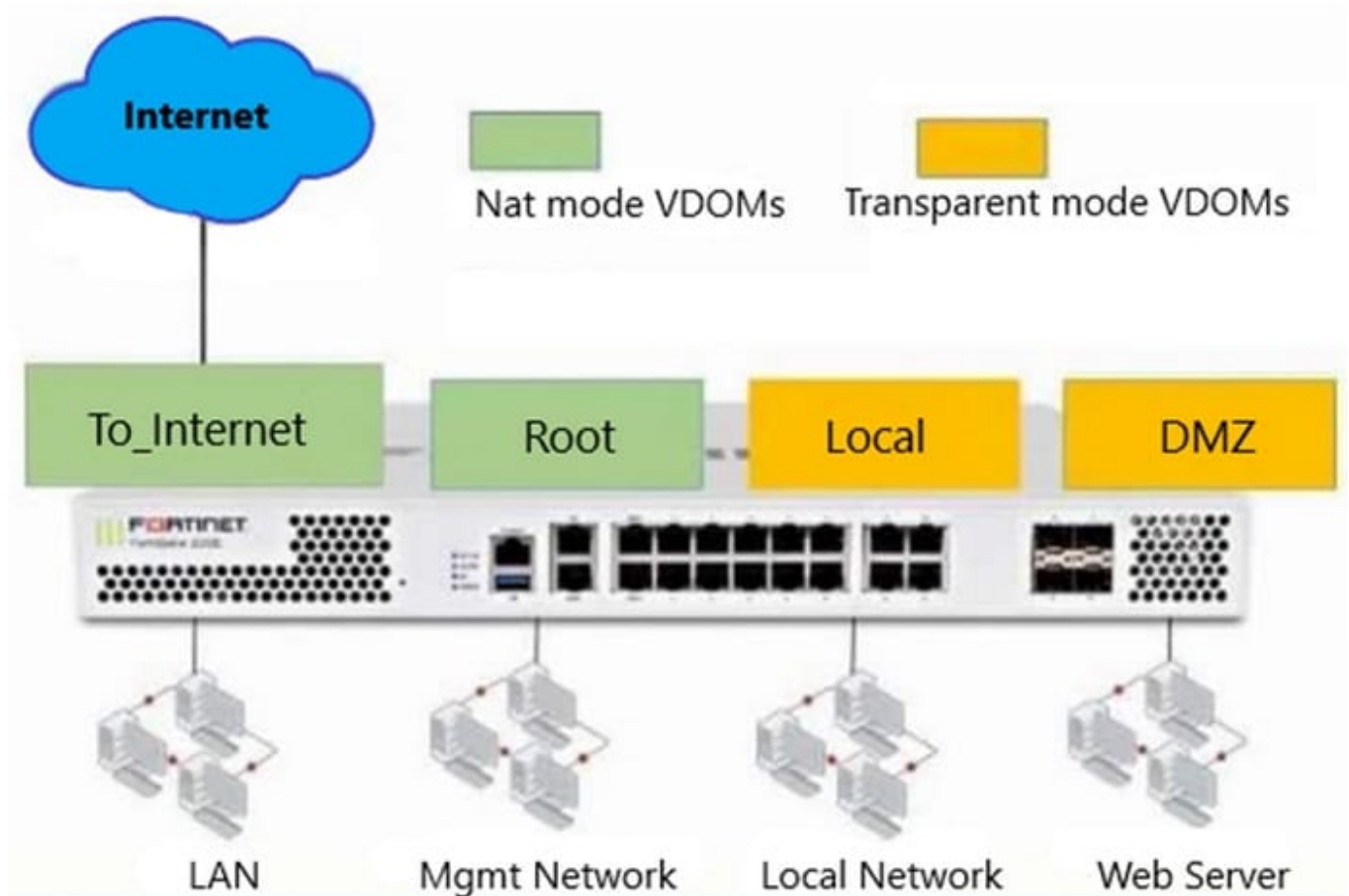
Following Questions and Answers are all new published by Fortinet Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

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 static route is 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.

Correct Answer: A

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46542>

## QUESTION 2

Which two statements are true about the FGCP protocol? (Choose two.)

- A. FGCP elects the primary FortiGate device.
- B. FGCP is not used when FortiGate is in transparent mode.
- C. FGCP runs only over the heartbeat links.
- D. FGCP is used to discover FortiGate devices in different HA groups.

Correct Answer: AC

The FGCP (FortiGate Clustering Protocol) is a protocol that is used to manage high availability (HA) clusters of FortiGate devices. It performs several functions, including the following:

**FGCP elects the primary FortiGate device:** In an HA cluster, FGCP is used to determine which FortiGate device will be the primary device, responsible for handling traffic and making decisions about what to allow or block. FGCP uses a variety of factors, such as the device's priority, to determine which device should be the primary.

**FGCP runs only over the heartbeat links:** FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between the devices.

FGCP does not run over other types of links, such as data links.

Reference:

<https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/564712/fgcp-fortigate-clustering-protocol>

FortiGate Infrastructure 7.2 Study Guide (p.292): "FortiGate HA uses the Fortinet- proprietary FortiGate Clustering Protocol (FGCP) to discover members, elect the primary FortiGate, synchronize data among members, and monitor the health

of members. To discover and monitor members, the members broadcast heartbeat packets over all configured heartbeat interfaces."

---

## QUESTION 3

Consider the topology:

Application on a Windows machine 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.

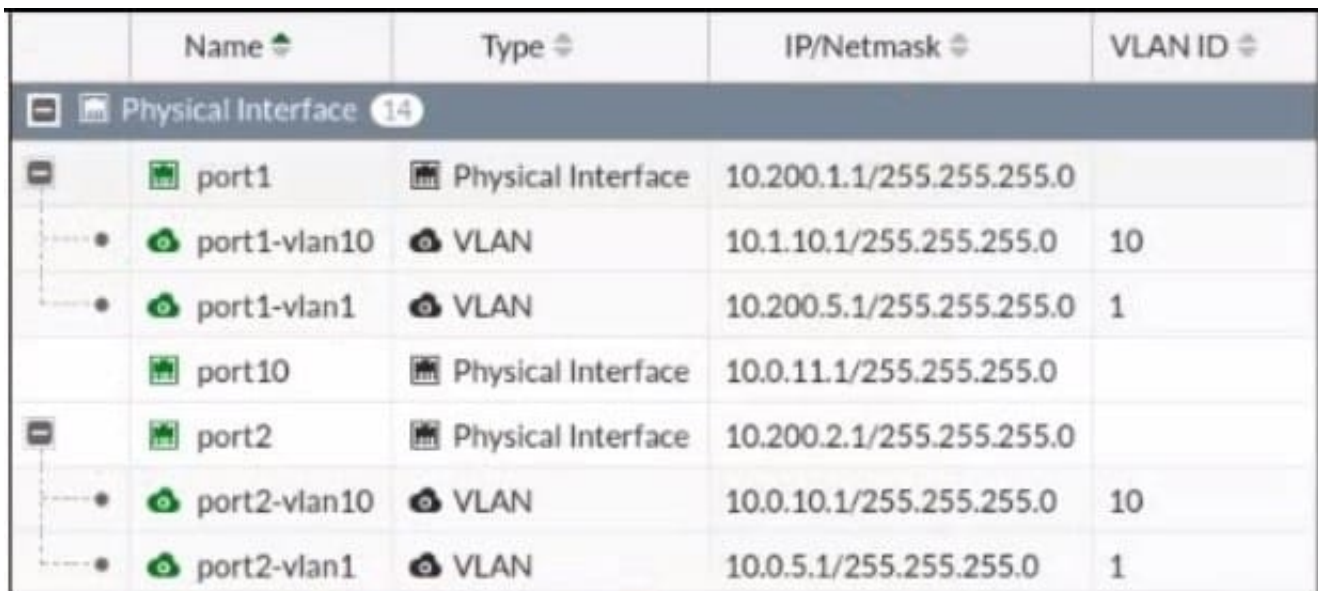
What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

- 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.

Correct Answer: CD

**QUESTION 4**

Refer to the exhibit.



Name	Type	IP/Netmask	VLAN ID
<b>Physical Interface 14</b>			
port1	Physical Interface	10.200.1.1/255.255.255.0	
port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
port10	Physical Interface	10.0.11.1/255.255.255.0	
port2	Physical Interface	10.200.2.1/255.255.255.0	
port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

- A. Traffic between port2 and port2-vlan1 is allowed by default.
- B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
- C. port1 is a native VLAN.
- D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Correct Answer: CD

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf>  
<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883>

**QUESTION 5**

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

- A. Configure Source IP Pools.
- B. Configure split tunneling in tunnel mode.
- C. Configure different SSL VPN realms.
- D. Configure host check .

Correct Answer: D

---

**QUESTION 6**

Which statement about video filtering on FortiGate is true?

- A. Full SSL Inspection is not required.
- B. It is available only on a proxy-based firewall policy.
- C. It inspects video files hosted on file sharing services.
- D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Correct Answer: B

Reference: <https://docs.fortinet.com/document/fortigate/7.0.0/new-features/190873/video-filtering>

---

**QUESTION 7**

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.

Exhibit A Exhibit B

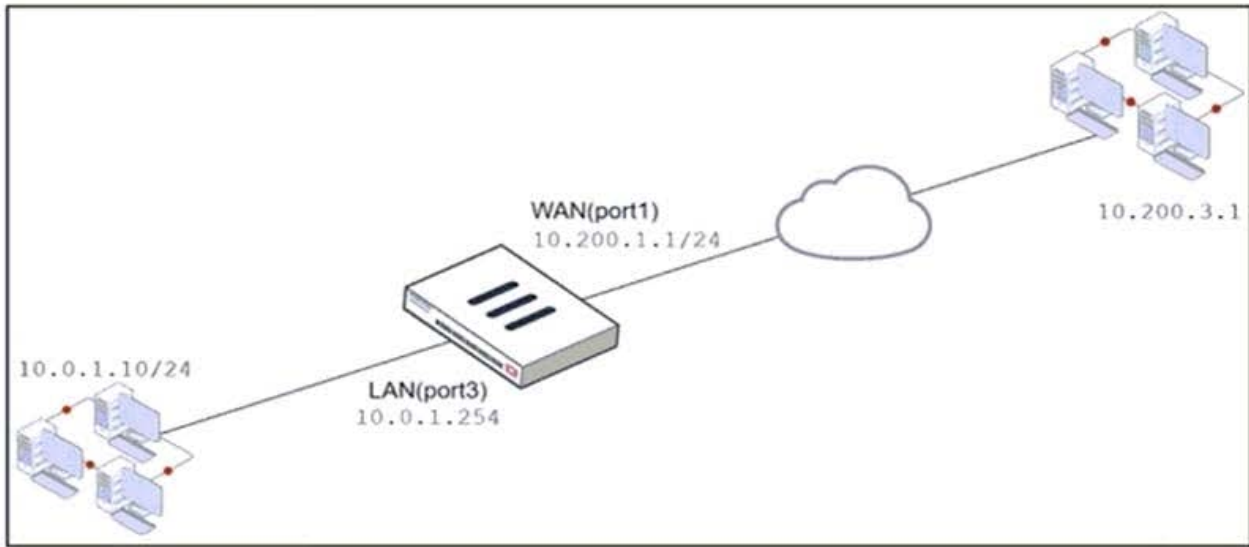


Exhibit A Exhibit B

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

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	
Protocol	TCP UDP SCTP ICMP
Port Mapping Type	One to one Many to many
External service port	10443
Map to IPv4 port	443

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination

address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

- A. 10.0.1.254, 10.0.1.10, and 443, respectively
- B. 10.0.1.254, 10.200.1.10, and 443, respectively
- C. 10.200.3.1, 10.0.1.10, and 443, respectively
- D. 10.0.1.254, 10.0.1.10, and 10443, respectively

Correct Answer: A

Translations:

10.200.3.1 --> 10.0.1.254 because NAT enable in firewall policy

10.200.1.10 --> 10.0.1.10 because VIP as Destination 10443 --> 443 because Port Forwarding enabled on VIP

Reference and download study guide: <https://ebin.pub/fortinet-fortigate-security-study-guide-for-fortios-72.html>

---

#### QUESTION 8

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

- A. Source defined as Internet Services in the firewall policy.
- B. Destination defined as Internet Services in the firewall policy.
- C. Highest to lowest priority defined in the firewall policy.
- D. Services defined in the firewall policy.
- E. Lowest to highest policy ID number.

Correct Answer: ABD

When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:

1.

Incoming Interface

2.

Outgoing Interface

3.

Source: IP address, user, internet services

4.

Destination: IP address or internet services

5.

Service: IP protocol and port number

6.

Schedule: Applies during configured times

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47435>

---

### QUESTION 9

Which two statements are true when FortiGate is in transparent mode? (Choose two.)

- A. By default, all interfaces are part of the same broadcast domain.
- B. The existing network IP schema must be changed when installing a transparent mode.
- C. Static routes are required to allow traffic to the next hop.
- D. FortiGate forwards frames without changing the MAC address.

Correct Answer: AD

Reference: [https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate\\_Transparent\\_Mode\\_Technical\\_Guide\\_FortiOS\\_4\\_0\\_version1.2.pdf&documentID=FD33113](https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113)

---

### QUESTION 10

Examine this FortiGate configuration: How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

```
config authentication setting
    set active-auth-scheme SCHEME1
end
config authentication rule
    edit WebProxyRule
        set srcaddr 10.0.1.0/24
        set active-auth-method SCHEME2
    next
end
```

- A. It always authorizes the traffic without requiring authentication.
- B. It drops the traffic.
- C. It authenticates the traffic using the authentication scheme SCHEME2.



D. It authenticates the traffic using the authentication scheme SCHEME1.

Correct Answer: D

"What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting"

---

#### QUESTION 11

In an explicit proxy setup, where is the authentication method and database configured?

- A. Proxy Policy
- B. Authentication Rule
- C. Firewall Policy
- D. Authentication scheme

Correct Answer: D

---

#### QUESTION 12

Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

- A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
- B. ADVPN is only supported with IKEv2.
- C. Tunnels are negotiated dynamically between spokes.
- D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Correct Answer: AC

---

#### QUESTION 13

Which statement about video filtering on FortiGate is true?

- A. Video filtering FortiGuard categories are based on web filter FortiGuard categories.
- B. It does not require a separate FortiGuard license.
- C. Full SSL inspection is not required.
- D. its available only on a proxy-based firewall policy.

Correct Answer: D

FortiGate Security 7.2 Study Guide (p.279): "To apply the video filter profile, proxy-based firewall polices currently allow

you to enable the video filter profile. You must enable full SSL inspection on the firewall policy."

<https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/860867/filtering-based-on-fortiguard-categories>

#### QUESTION 14

Refer to the exhibits.

```
# 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
```

Exhibit A | Exhibit B

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

Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds. Based on the system performance output, which two statements are correct? (Choose two.)

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

Correct Answer: BD

Reference: <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Conserve-mode-changes/ta-p/198502>

configurable thresholds

Though it is recommended to keep the default memory threshold, a new CLI command has been added to allow administrators to adjust the thresholds.

Default values are :

-red : 88% of total memory is considered "used memory"

-extreme : 95% of total memory is considered "used memory"

-green : 82% of total memory is considered "used memory"

---

#### QUESTION 15

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.

Which two other security profiles can you apply to the security policy? (Choose two.)

- A. Antivirus scanning
- B. File filter
- C. DNS filter
- D. Intrusion prevention

Correct Answer: AD

Security policy: If the traffic is allowed as per the consolidated policy, FortiGate will then process it based on the security policy to analyze additional criteria, such as URL categories for web filtering and application control. Also, if enabled, the security policy further inspects traffic using security profiles such as IPS and AV.

[Latest NSE4\\_FGT-7.2 Dumps](#)

[NSE4\\_FGT-7.2 PDF Dumps](#)

[NSE4\\_FGT-7.2 Practice Test](#)