



# 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.geekcert.com/nse4\\_fgt-7-2.html](https://www.geekcert.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.

Name	Custom_Profile		
Comments	<div></div> 0/255		
Access Permissions			
Access Control	Permissions <span>Set All ▾</span>		
Security Fabric	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write
FortiView	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write
User & Device	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write
Firewall	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write <input type="radio"/> Custom
Log & Report	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write <input type="radio"/> Custom
Network	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write <input type="radio"/> Custom
System	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write <input type="radio"/> Custom
Security Profile	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write <input type="radio"/> Custom
VPN	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write
WAN Opt & Cache	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write
WiFi & Switch	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write

Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?



- A. Custom permission for Network
- B. Read/Write permission for Log and Report
- C. CLI diagnostics commands permission
- D. Read/Write permission for Firewall

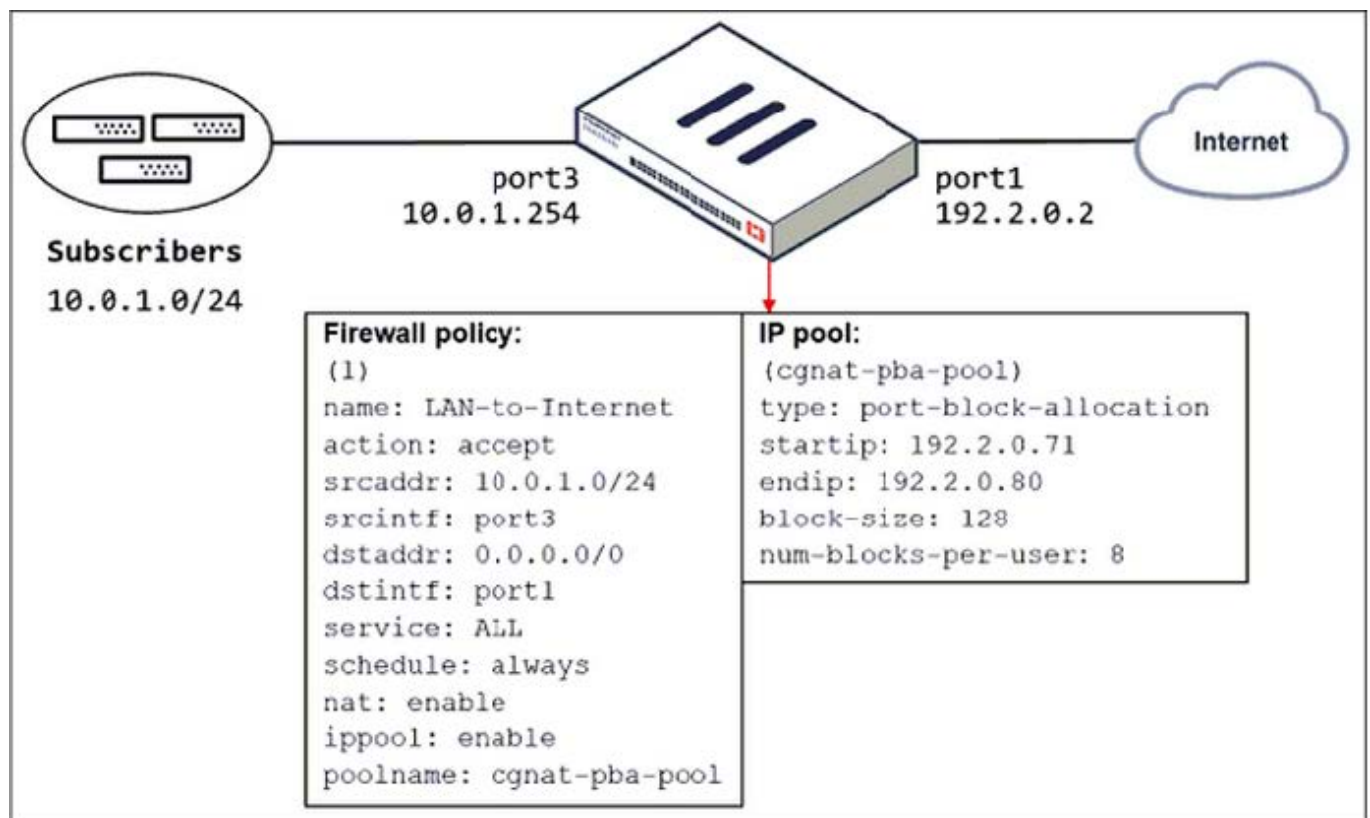
Correct Answer: C

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220>

## QUESTION 2

Refer to the exhibit.

The exhibit shows a diagram of a FortiGate device connected to the network and the firewall policy and IP pool configuration on the FortiGate device.



Which two actions does FortiGate take on internet traffic sourced from the subscribers? (Choose two.)

- A. FortiGate allocates port blocks per user, based on the configured range of internal IP addresses.
- B. FortiGate allocates port blocks on a first-come, first-served basis.
- C. FortiGate generates a system event log for every port block allocation made per user.
- D. FortiGate allocates 128 port blocks per user.



Correct Answer: BC

FortiGate Security 7.2 Study Guide (p.109): "FortiGate allocates port blocks on a first-come, first-served basis." "For logging purposes, when FortiGate allocates a port block to a host, it generates a system event log to inform the administrator."

### QUESTION 3

Refer to the exhibit.

An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option.

The screenshot shows the 'New RADIUS Server' configuration window in FortiGate. The 'Name' field is set to 'FortiAuthenticator-RADIUS'. Under 'Authentication method', the 'Default' tab is selected. The 'NAS IP' field is empty. The 'Include in every user group' checkbox is checked. Under 'Primary Server', the 'IP/Name' is set to '10.0.1.149' and the 'Secret' is masked with dots. At the bottom, there are buttons for 'Test Connectivity' and 'Test User Credentials'.

What is the impact of using the Include in every user group option in a RADIUS configuration?

- A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
- B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
- C. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.
- D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

Correct Answer: A

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/634373/authentication-servers>



#### QUESTION 4

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

**Exhibit A**

**Edit Policy**

Inspection Mode **Flow-based** Proxy-based

**Firewall / Network Options**

NAT ☒

IP Pool Configuration **Use Outgoing Interface Address**  
Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options **PRX** default

**Security Profiles**

AntiVirus ☒ **AV** default

Web Filter ☐

DNS Filter ☐

Application Control ☐

IPS ☐

SSL Inspection ☒ **SSL** deep-inspection

Decrypted Traffic Mirror ☐



**Exhibit B**

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

- A. The firewall policy performs the full content inspection on the file.
- B. The flow-based inspection is used, which resets the last packet to the user.
- C. The volume of traffic being inspected is too high for this model of FortiGate.
- D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Correct Answer: B



ONL"; If the virus is detected at the";STAR"; of the connection, the IPS engine sends the block replacement message immediately. When a virus is detected on a TCP session (FIRST TIME), but where";SOME PACKET"; have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again. In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

---

#### QUESTION 5

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

- A. The firmware image must be manually uploaded to each FortiGate.
- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.
- D. Traffic load balancing is temporally disabled while upgrading the firmware.

Correct Answer: CD

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

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

[NSE4\\_FGT-7.2 Exam Questions](#)