



NSE4_FGT-7.2^{Q&As}

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.pass4itsure.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.

```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

- A. The IPS engine was inspecting high volume of traffic.
- B. The IPS engine was unable to prevent an intrusion attack .
- C. The IPS engine was blocking all traffic.
- D. The IPS engine will continue to run in a normal state.

Correct Answer: A

fortinet-fortigate-security-study-guide-for-fortios-72 page 417 If there are high-CPU use problems caused by the IPS, you can use the diagnose test application ipsmonitor command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

Reference: <https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/232929/troubleshooting-high-cpu-usage>

QUESTION 2

Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

- A. FortiGate points the collector agent to use a remote LDAP server.
- B. FortiGate uses the AD server as the collector agent.
- C. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- D. FortiGate queries AD by using the LDAP to retrieve user group information.

Correct Answer: CD

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>



QUESTION 3

If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source field of a firewall policy?

- A. IP address
- B. Once Internet Service is selected, no other object can be added
- C. User or User Group
- D. FQDN address

Correct Answer: B

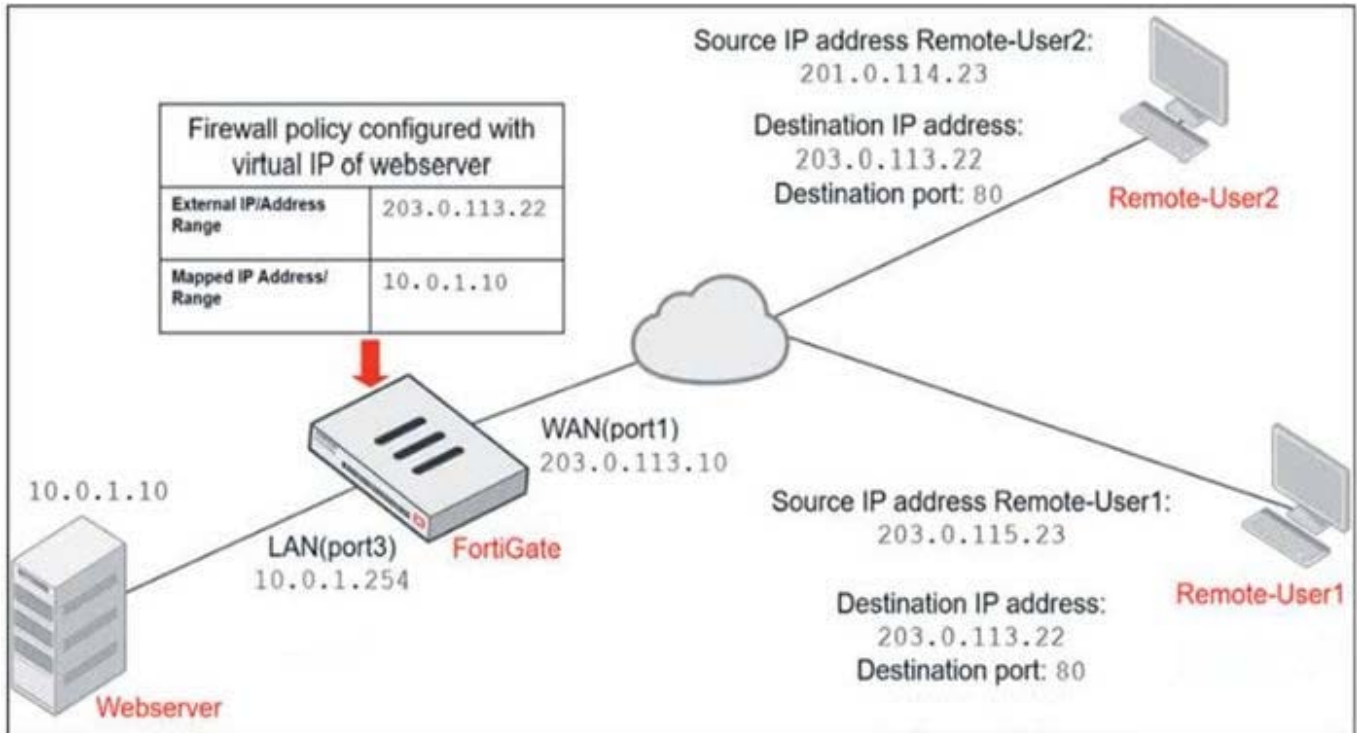
Reference: <https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-in-policy>

QUESTION 4

Refer to the exhibits.

The exhibits show a network diagram and firewall configurations.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver. Remote-User2 must not be able to access the Webserver.



Edit Address

Name	Deny_IP
Color	Change
Type	Subnet
IP/Netmask	201.0.114.23/32
Interface	WAN (port1)
Static route configuration	<input type="checkbox"/>
Comments	Deny web server access. 23/255

Firewall address object

Firewall policies

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) -> LAN (port3) 2						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Webserver	always	ALL	ACCEPT

In this scenario, which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

- A. Disable match-vip in the Deny policy.
- B. Set the Destination address as Deny_IP in the Allow-access policy.
- C. Enable match vip in the Deny policy.
- D. Set the Destination address as Web_server in the Deny policy.



Correct Answer: BC

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta-p/189641>

The exhibits show a network diagram and firewall configurations for a FortiGate unit that has two policies: Allow_access and Deny. The Allow_access policy allows traffic from the WAN (port1) interface to the LAN (port3) interface with the destination address of VIP and the service of HTTPS. The VIP object maps the external IP address 10.200.1.10 and port 10443 to the internal IP address 10.0.1.10 and port 443 of the Webserver. The Deny policy denies traffic from the WAN (port1) interface to the LAN (port3) interface with the source address of Deny_IP and the destination address of All. In this scenario, the administrator wants to deny Webserver access for Remote-User2, who has the IP address 10.200.3.2, which is included in the Deny_IP address object. Remote-User1, who has the IP address 10.200.3.1, must be able to access the Webserver. To achieve this goal, the administrator can make two changes to deny Webserver access for Remote-User2: Set the Destination address as Webserver in the Deny policy. This will make the Deny policy more specific and match only the traffic that is destined for the Webserver's internal IP address, instead of any destination address. Enable matchvip in the Deny policy. This will make the Deny policy apply to traffic that matches a VIP object, instead of ignoring it. This way, the Deny policy will block Remote-User2's traffic that uses the VIP object's external IP address and port.

QUESTION 5

An administrator has a requirement to keep an application session from timing out on port 80.

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

- A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
- B. Create a new service object for HTTP service and set the session TTL to never
- C. Set the TTL value to never under config system-ttl
- D. Set the session TTL on the HTTP policy to maximum

Correct Answer: BC

[NSE4_FGT-7.2 PDF Dumps](#) [NSE4_FGT-7.2 VCE Dumps](#)

[NSE4_FGT-7.2 Exam Questions](#)