



# NSE4\_FGT-6.0<sup>Q&As</sup>

Fortinet NSE 4 - FortiOS 6.0

## Pass Fortinet NSE4\_FGT-6.0 Exam with 100% Guarantee

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

[https://www.passapply.com/nse4\\_fgt-6-0.html](https://www.passapply.com/nse4_fgt-6-0.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

Which configuration objects can be selected for the Source field of a firewall policy? (Choose two.)

- A. Firewall service
- B. User or user group
- C. IP Pool
- D. FQDN address

Correct Answer: BC

### QUESTION 2

Examine the exhibit, which shows the partial output of an IKE real-time debug.

```
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=4497f0b077c742b5/0000000000000000 len=296
ike 0:4497f0b077c742b5/0000000000000000:8: responder: main mode get 1st message...
...
ike 0:4497f0b077c742b5/0000000000000000:8: SA proposal chosen, matched gateway Remote
ike 0: found Remote 172.20.186.222 2 -> 172.20.187.114:500
...
ike 0:Remote:8: sent IKE msg (ident_r1send): 172.20.186.222:500->172.20.187.114:500, len=160
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder:main mode get 2nd message...
....
ike 0:Remote:8: sent IKE msg (ident_r2send): 172.20.186.222:500->172.20.187.114:500, len=292
ike 0:Remote:8: ISAKMP SA 4497f0b077c742b5/fbbb59b259a0fc3e key 24:DCD18FBE7CFA138E27B06F
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder: main mode get 3rd message...
...
ike 0:Remote:8: PSK authentication succeeded
ike 0:Remote:8: authentication OK
ike 0:Remote:8: established IKE SA 4497f0b077c742b5/fbbb59b259a0fc3e
```

Which of the following statement about the output is true?

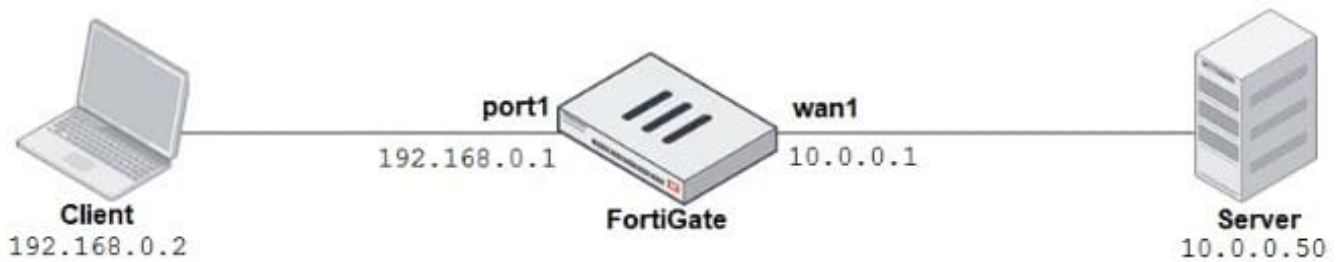
- A. The VPN is configured to use pre-shared key authentication.
- B. Extended authentication (XAuth) was successful.
- C. Remote is the host name of the remote IPsec peer.
- D. Phase 1 went down.

Correct Answer: A

### QUESTION 3



Examine this network diagram:



Examine this explicit web proxy configuration:

**Explicit Proxy**

☒ Explicit Web Proxy

Listen on Interfaces

port1

+

x

HTTP port

8080

HTTPS port

Use HTTP Port

Specify

FTP over HTTP

☐

Proxy auto-config (PAC)

☐

Proxy FQDN

default.fqdn

Max HTTP request length

4

KB

Max HTTP message length

32

KB

Unknown HTTP version

Best Effort

Reject

Realm

default

Default Firewall Policy Action

Accept

Deny

What filter can be used in the command diagnose sniffer packet to capture the traffic between the client and the explicit web proxy?

- A. `host 10.0.0.50 and port 8080\`
- B. `host 10.0.0.50 and port 80\`
- C. `host 192.168.0.2 and port 8080\`
- D. `host 192.168.0.1 and port 80\`

Correct Answer: C



#### QUESTION 4

A company needs to provide SSL VPN access to two user groups. The company also needs to display different welcome messages on the SSL VPN login screen for both user groups.

What is required in the SSL VPN configuration to meet these requirements?

- A. Different SSL VPN realms for each group.
- B. Two separate SSL VPNs in different interfaces mapping the same ssl.root.
- C. Two firewall policies with different captive portals.
- D. Different virtual SSL VPN IP addresses for each group.

Correct Answer: A

#### QUESTION 5

Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.

Name: **WINDOWS\_SERVERS** [View IPS Signatures]

Comments: 0 / 255

IPS Signatures

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
A32S.Botnet	0	000000	Server.Client	TCP	All	Monitor	✓

IPS Filters

Filter Details	Action	Packet Logging
Location:server OS:Windows	Block	✓

Apply

What are the expected actions if traffic matches this IPS sensor? (Choose two.)

- A. The sensor will gather a packet log for all matched traffic.
- B. The sensor will not block attackers matching the A32S.Botnet signature.
- C. The sensor will block all attacks for Windows servers.



D. The sensor will reset all connections that match these signatures.

Correct Answer: AC

[NSE4\\_FGT-6.0 VCE Dumps](#)

[NSE4\\_FGT-6.0 Practice  
Test](#)

[NSE4\\_FGT-6.0 Braindumps](#)