

NSE4_FGT-7.0^{Q&As}

Fortinet NSE 4 - FortiOS 7.0

Pass Fortinet NSE4_FGT-7.0 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse4_fgt-7-0.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 two statements about IPsec authentication on FortiGate are correct? (Choose two.)

- A. For a stronger authentication, you can also enable extended authentication (XAuth) to request the remote peer to provide a username and password
- B. FortiGate supports pre-shared key and signature as authentication methods.
- C. Enabling XAuth results in a faster authentication because fewer packets are exchanged.
- D. A certificate is not required on the remote peer when you set the signature as the authentication method.

Correct Answer: AB

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/913287/ipsec-vpn-authenticatingaremote-fortigate-peer-with-a-pre-shared-key>

QUESTION 2

Refer to the exhibit.



Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

- A. The signature setting uses a custom rating threshold.
- B. The signature setting includes a group of other signatures.
- C. Traffic matching the signature will be allowed and logged.
- D. Traffic matching the signature will be silently dropped and logged.

Correct Answer: D

Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

QUESTION 3

Refer to the exhibit.

Authentication rule

Edit Rule	Authentication rule
Name	WebproxyRule
Source Address	<input type="text" value="LOCAL_SUBNET"/> <input type="button" value="x"/> +
Protocol	<input type="text" value="HTTP"/>
Authentication Scheme	<input checked="" type="checkbox"/> <input type="text" value="Web-Proxy-Scheme"/>
IP-based Authentication	<input checked="" type="button" value="Enable"/> <input type="button" value="Disable"/>
SSO Authentication Scheme	<input type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/1023
Enable This Rule	<input checked="" type="button" value="Enable"/> <input type="button" value="Disable"/>

Users

+ Create New	✎ Edit	🗑 Delete	<input type="text" value="Search"/>
Name	Type		
👤 User-A	👤 LOCAL		
👤 User-B	👤 LOCAL		
👤 User-C	👤 LOCAL		

Authentication scheme

Edit Authentication Scheme

Name:

Method: ✕

User database: Local Other

Two-factor authentication:

Firewall address

Edit Address

Category: Address Proxy Address

Name:

Color:

Type:

IP/Netmask:

Interface:

Static route configuration:

Comments: 0/255

Proxy address

Edit Address

Category: Address Proxy Address

Name:

Color:

Type:

Host:

User Agent: ✕
 ✕
 ✕

Comments: 0/255

Proxy address

Edit Address

Category: Address **Proxy Address**

Name: Browser-CAT-2

Color:

Type: User Agent

Host: LOCAL_SUBNET

User Agent: Mozilla Firefox

Comments: Write a comment. 0/255

Web proxy address

ID	Source	Destination	Schedule	Action
explicit-web proxy → port1 3				
1	Browser-CAT-2 LOCAL_SUBNET User-B	all	always	DENY
2	LOCAL_SUBNET Browser-CAT-1 User-A	all	always	ACCEPT
3	LOCAL_SUBNET	all	always	ACCEPT

The exhibit shows proxy policies and proxy addresses, the authentication rule and authentication scheme, users, and firewall address.

An explicit web proxy is configured for subnet range 10.0.1.0/24 with three explicit web proxy policies. The authentication rule is configured to authenticate HTTP requests for subnet range 10.0.1.0/24 with a form-based authentication scheme for the FortiGate local user database.

Users will be prompted for authentication.

How will FortiGate process the traffic when the HTTP request comes from a machine with the source IP

10.0.1.10 to the destination http://www.fortinet.com? (Choose two.)

- A. If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.
- B. If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.
- C. If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.
- D. If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.

Correct Answer: BD

QUESTION 4

Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

- A. Antivirus engine
- B. Intrusion prevention system engine
- C. Flow engine
- D. Detection engine

Correct Answer: B

Reference: <http://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control>

QUESTION 5

Refer to the exhibit.

```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000 4500 003c 2f8f 0000 8001 f020 0a00 0102 E.</.....
0x0010 0808 0808 0800 4d5a 0001 0001 6162 6364 .....MZ....abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwbcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000 4500 003c 2f8f 0000 7f01 0106 0a38 f0e4 E.</.....8..
0x0010 0808 0808 0800 6159 ec01 0001 6162 6364 .....aY....abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwbcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000 4500 003c 0000 0000 7501 3a95 0808 0808 E.<.....u:.....
0x0010 0a38 f0e4 0000 6959 ec01 0001 6162 6364 .8....iY....abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwbcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000 4500 003c 0000 0000 7401 2bb0 0808 0808 E.<....t.+.....
0x0010 0a00 0102 0000 555a 0001 0001 6162 6364 .....UZ....abcd
0x0020 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869 uvwbcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.

Which three pieces of information are included in the sniffer output? (Choose three.)

- A. Interface name
- B. Ethernet header
- C. IP header
- D. Application header

E. Packet payload

Correct Answer: ACE

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=11186>

[Latest NSE4_FGT-7.0 Dumps](#)

[NSE4_FGT-7.0 PDF Dumps](#) [NSE4_FGT-7.0 Braindumps](#)