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

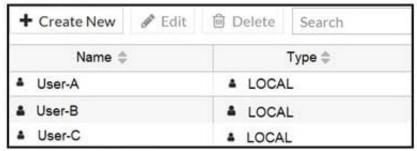
Refer to the exhibit.

Authentication rule

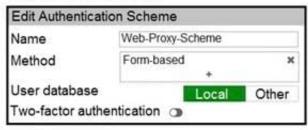




Users



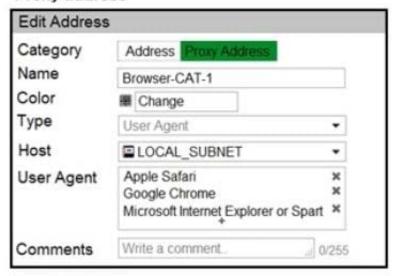
Authentication scheme



Firewall address



Proxy address

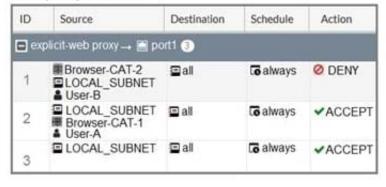




Proxy address



Web proxy address



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.../......
        0808 0808 0800 4d5a 0001 0001 6162 6364
0x0010
                                                       .....MZ....abcd
0x0020
        6566 6768 696a 6b6c 6d6e 6f70 7172 7374
                                                       efghijklmnopqrst
0x0030
        7576 7761 6263 6465 6667 6869
                                                       uvwabcdefghi
20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
       4500 003c 2f8f 0000 7f01 0106 0a38 f0e4
                                                       0x0010
        0808 0808 0800 6159 ec01 0001 6162 6364
                                                       ....aY....abcd
        6566 6768 696a 6b6c 6d6e 6f70 7172 7374
0x0020
                                                       efghijklmnopqrst
0x0030 7576 7761 6263 6465 6667 6869
                                                       uvwabcdefghi
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
                                                       uvwabcdefghi
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.+....
        0a00 0102 0000 555a 0001 0001 6162 6364
0x0010
                                                       .....UZ....abcd
                                                       efghijklmnopqrst
0x0020
        6566 6768 696a 6b6c 6d6e 6f70 7172 7374
        7576 7761 6263 6465 6667 6869
                                                       uvwabcdefghi
0x0030
```

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



https://www.leads4pass.com/nse4_fgt-7-0.html 2024 Latest leads4pass NSE4_FGT-7.0 PDF and VCE dumps Download

E. Packet payload

Correct Answer: ACE

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

<u>Latest NSE4 FGT-7.0</u> <u>Dumps</u> NSE4 FGT-7.0 PDF Dumps NSE4 FGT-7.0 Braindumps