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.passapply.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

QUESTION 1

Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides (client and server) have terminated the session?

A. To remove the NAT operation.

B. To generate logs

C. To finish any inspection operations.

D. To allow for out-of-order packets that could arrive after the FIN/ACK packets.

Correct Answer: D

QUESTION 2

What are two characteristics of FortiGate HA cluster virtual IP addresses? (Choose two.)

A. Virtual IP addresses are used to distinguish between cluster members.

B. Heartbeat interfaces have virtual IP addresses that are manually assigned.

C. The primary device in the cluster is always assigned IP address 169.254.0.1.

D. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.

Correct Answer: AD

"FGCP automatically assigns the heartbeat IP addresses based on the serial number of each device. The IP address 169.254.0.1 is assigned to the device with the highest serial number."

"A change in the heartbeat IP addresses may happen when a FortiGate device joins or leaves the cluster."

"The HA cluster uses the heartbeat IP addresses to distinguish the cluster members and synchronize data."

https://networkinterview.com/fortigate-ha-high-availability/

QUESTION 3

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 4

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

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                  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.+.....
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                  uvwabcdefghi
```

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

Study Guide Routing Diagnostics Packet Capture Verbosity Level.

diagnose sniffer packet `\\'

In the example, verbosity is 5.

The verbosity level specifies how much info you want to display.

1 (default): IP Headers.

2: IP Headers, Packet Payload.

3. IP Headers, Packet Payload, Ethernet Headers.

4: IP Headers, Interface Name.

5: IP Headers, Packet Payload, Interface Name.

6: IP Headers, Packet Payload, Ethernet Headers, Interface Name.

Latest NSE4_FGT-7.2 Dumps

NSE4_FGT-7.2 Study Guide

NSE4_FGT-7.2 Exam Questions