DUMPSBOSS.

Fortinet NSE 4 - FortiOS 7.2

Fortinet NSE4_FGT-7.2

Version Demo

Total Demo Questions: 10

Total Premium Questions: 155

Buy Premium PDF

https://dumpsboss.co

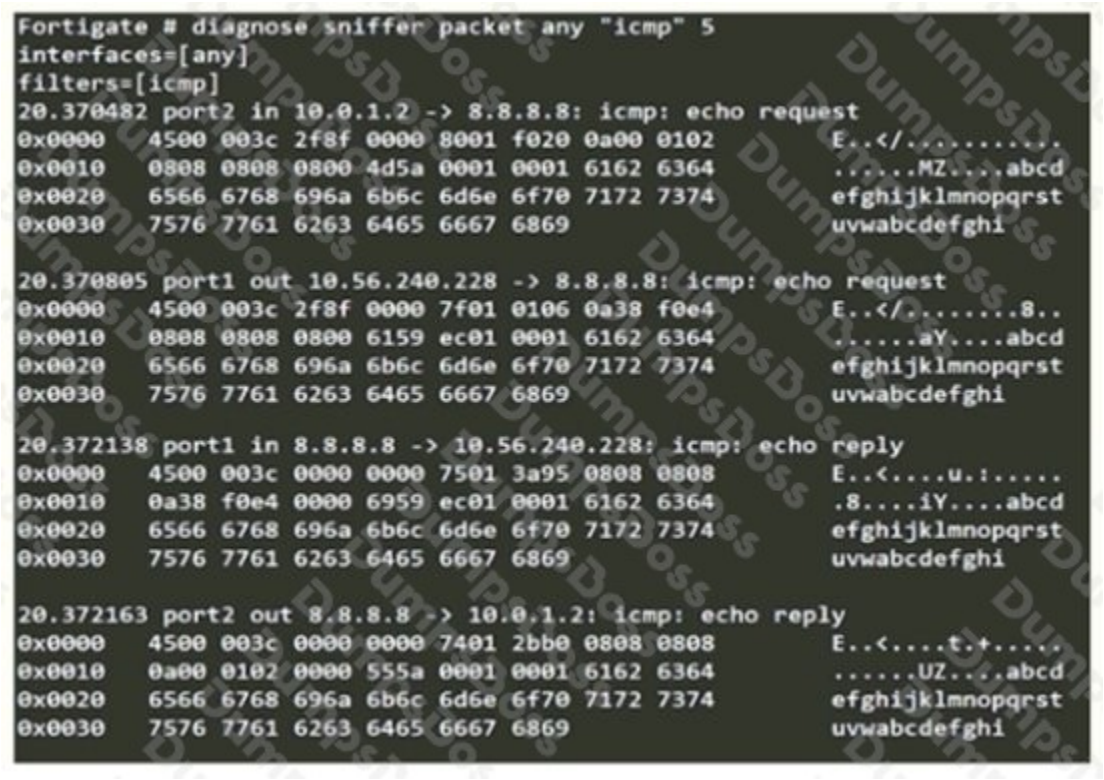
support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

58

Refer to the exhibit.



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

ANSWER: A C E

Explanation:

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.

QUESTION NO: 2

44

Which statement about the policy ID number of a firewall policy is true?

A. It is required to modify a firewall policy using the CLI.

B. It represents the number of objects used in the firewall policy.

C. It changes when firewall policies are reordered.

D. It defines the order in which rules are processed.

ANSWER: A

QUESTION NO: 3

17

In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

A. The IP version of the sources and destinations in a firewall policy must be different.

B. The Incoming Interface. Outgoing Interface. Schedule, and Service fields can be shared with both IPv4 and IPv6.

C. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.

D. The IP version of the sources and destinations in a policy must match.

E. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

ANSWER: B D E

QUESTION NO: 4

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

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

B. To finish any inspection operations

C. To remove the NAT operation

D. To generate logs

ANSWER: A

Explanation:

TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an entry in the firewall session table.

QUESTION NO: 5

View the exhibit.

Which of the following statements are correct? (Choose two.)

A. This setup requires at least two firewall policies with the action set to IPsec.

B. Dead peer detection must be disabled to support this type of IPsec setup.

C. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.

D. This is a redundant IPsec setup.

ANSWER: C D

Explanation:

https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/632796/ospf-with-ipsec-vpn-for-network-redundancy

QUESTION NO: 6

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser

does not report errors.

What is the reason for the certificate warning errors?

A. The browser requires a software update.

B. FortiGate does not support full SSL inspection when web filtering is enabled.

C. The CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.

D. There are network connectivity issues.

ANSWER: C

Explanation:

Reference: https://kb.fortinet.com/kb/documentLink .do?externalID=FD41394

QUESTION NO: 7

109

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.

ANSWER: D

QUESTION NO: 8

94

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

A. The interface has been configured for one-arm sniffer.

B. The interface is a member of a virtual wire pair.

C. The operation mode is transparent.

D. The interface is a member of a zone.

E. Captive portal is enabled in the interface.

ANSWER: A B C

Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

QUESTION NO: 9

Refer to the exhibit.

Based on the raw log, which two statements are correct? (Choose two.)

A. Traffic is blocked because Action is set to DENY in the firewall policy.

B. Traffic belongs to the root VDOM.

C. This is a security log.

D. Log severity is set to error on FortiGate.

ANSWER: A C

QUESTION NO: 10

59

An organization's employee needs to connect to the office through a high-latency internet connection.

Which SSL VPN setting should the administrator adjust to prevent the SSL VPN negotiation failure?

A. Change the session-ttl.

B. Change the login timeout.

C. Change the idle-timeout.

D. Change the udp idle timer.

ANSWER: B