

Fortinet

Exam Questions NSE7_EFW-6.4

Fortinet NSE 7 - Enterprise Firewall 6.4



NEW QUESTION 1

View the exhibit, which contains the output of diagnose sys session stat, and then answer the question below.

Which statements are correct regarding the output shown? (Choose two.)

- A. There are 0 ephemeral sessions.
- B. All the sessions in the session table are TCP sessions.
- C. No sessions have been deleted because of memory pages exhaustion.
- D. There are 166 TCP sessions waiting to complete the three-way handshake.

Answer: AC

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40578>

NEW QUESTION 2

Which statement about memory conserve mode is true?

- A. A FortiGate exits conserve mode when the configured memory use threshold reaches yellow.
- B. A FortiGate starts dropping all the new and old sessions when the configured memory use threshold reaches extreme.
- C. A FortiGate starts dropping new sessions when the configured memory use threshold reaches red
- D. A FortiGate enters conserve mode when the configured memory use threshold reaches red

Answer: C

NEW QUESTION 3

View the exhibit, which contains an entry in the session table, and then answer the question below.

Which one of the following statements is true regarding FortiGate's inspection of this session?

- A. FortiGate applied proxy-based inspection.
- B. FortiGate forwarded this session without any inspection.
- C. FortiGate applied flow-based inspection.
- D. FortiGate applied explicit proxy-based inspection.

Answer: A

Explanation:

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

NEW QUESTION 4

Examine the output of the 'get router info bgp summary' command shown in the exhibit; then answer the question below.

Which statement can explain why the state of the remote BGP peer 10.200.3.1 is Connect?

- A. The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.
- B. The TCP session for the BGP connection to 10.200.3.1 is down.
- C. The local peer has received the BGP prefixed from the remote peer.

D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Answer: B

Explanation:

<http://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=4>

NEW QUESTION 5

Which of the following statements are true regarding the SIP session helper and the SIP application layer gateway (ALG)? (Choose three.)

- A. SIP session helper runs in the kernel; SIP ALG runs as a user space process.
- B. SIP ALG supports SIP HA failover; SIP helper does not.
- C. SIP ALG supports SIP over IPv6; SIP helper does not.
- D. SIP ALG can create expected sessions for media traffic; SIP helper does not.
- E. SIP helper supports SIP over TCP and UDP; SIP ALG supports only SIP over UDP.

Answer: BCD

NEW QUESTION 6

What conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

- A. IP addresses are in the same subnet.
- B. Hello and dead intervals match.
- C. OSPF IP MTUs match.
- D. OSPF peer IDs match.
- E. OSPF costs match.

Answer: ABC

Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-advanced-routing-54/Routing_OSPF/OSPF_Bac

NEW QUESTION 7

What global configuration setting changes the behavior for content-inspected traffic while FortiGate is in system conserve mode?

- A. av-failopen
- B. mem-failopen
- C. utm-failopen
- D. ips-failopen

Answer: A

Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Other_Profile_Consideratio

NEW QUESTION 8

View the exhibit, which contains the output of a debug command, and then answer the question below.

Which of the following statements about the exhibit are true? (Choose two.)

- A. In the network on port4, two OSPF routers are down.
- B. Port4 is connected to the OSPF backbone area.
- C. The local FortiGate's OSPF router ID is 0.0.0.4
- D. The local FortiGate has been elected as the OSPF backup designated router.

Answer: BC

NEW QUESTION 9

Which two statements about an auxiliary session are true? (Choose two.)

- A. With the auxiliary session setting enabled, ECMP traffic is accelerated to the NP6 processor.
- B. With the auxiliary session setting enabled, two sessions will be created in case of routing change.
- C. With the auxiliary session setting disabled, for each traffic path, FortiGate will use the same auxiliary session.
- D. With the auxiliary session disabled, only auxiliary sessions will be offloaded.

Answer: CD

NEW QUESTION 10

Examine the IPsec configuration shown in the exhibit; then answer the question below.

An administrator wants to monitor the VPN by enabling the IKE real time debug using these commands: `diagnose vpn ike log-filter src-addr4 10.0.10.1`
`diagnose debug application ike -1`
`diagnose debug enable`

The VPN is currently up, there is no traffic crossing the tunnel and DPD packets are being interchanged between both IPsec gateways. However, the IKE real time debug does NOT show any output. Why isn't there any output?

- A. The IKE real time shows the phases 1 and 2 negotiations onl

- B. It does not show any more output once the tunnel is up.
- C. The log-filter setting is set incorrectl
- D. The VPN's traffic does not match this filter.
- E. The IKE real time debug shows the phase 1 negotiation onl
- F. For information after that, the administrator must use the IPsec real time debug instead: diagnose debug application ipsec -1.
- G. The IKE real time debug shows error messages onl
- H. If it does not provide any output, it indicates that the tunnel is operating normally.

Answer: B

NEW QUESTION 10

Refer to the exhibit, which contains a TCL script configuration on FortiManager.

An administrator has configured the TCL script on FortiManager, but failed to apply any changes to the managed device after being executed. Why did the TCL script fail to make any changes to the managed device?

- A. Changes in an interface configuration can only be done by CLI script.
- B. The TCL script must start with #include <>.
- C. Incomplete commands are ignored in TCL scripts.
- D. The TCL command run_cmd has not been created.

Answer: D

NEW QUESTION 13

View the exhibit, which contains the output of get sys ha status, and then answer the question below.

Which statements are correct regarding the output? (Choose two.)

- A. The slave configuration is not synchronized with the master.
- B. The HA management IP is 169.254.0.2.
- C. Master is selected because it is the only device in the cluster.
- D. port 7 is used the HA heartbeat on all devices in the cluster.

Answer: AD

NEW QUESTION 17

View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

Why didn't the tunnel come up?

- A. The pre-shared keys do not match.
- B. The remote gateway's phase 2 configuration does not match the local gateway's phase 2 configuration.
- C. The remote gateway's phase 1 configuration does not match the local gateway's phase 1 configuration.
- D. The remote gateway is using aggressive mode and the local gateway is configured to use man mode.

Answer: C

NEW QUESTION 22

Examine the output from the 'diagnose debug authd fssso list' command; then answer the question below.

```
# diagnose debug authd fssso list —FSSO logons-IP: 192.168.3.1 User: STUDENT Groups: TRAININGAD/USERS Workstation: INTERNAL2. TRAINING. LAB The IP address 192.168.3.1 is
```

NOT the one used by the workstation INTERNAL2. TRAINING. LAB.

What should the administrator check?

- A. The IP address recorded in the logon event for the user STUDENT.
- B. The DNS name resolution for the workstation name INTERNAL2. TRAININ
- C. LAB.
- D. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2.TRAININ

- E. LAB.
- F. The reserve DNS lookup for the IP address 192.168.3.1.

Answer: C

NEW QUESTION 23

An administrator added the following IPsec VPN to a FortiGate configuration:

```
config vpn ipsec phase1 -interface edit "RemoteSite"
set type dynamic
set interface "port1" set mode main
set psksecret ENC LCVkCiK2E2PhVUzZe next
end
config vpn ipsec phase2-interface edit "RemoteSite"
set phase1 name "RemoteSite" set proposal 3des-sha256
next end
```

However, the phase 1 negotiation is failing. The administrator executed the IKF real time debug while attempting the IPsec connection. The output is shown in the exhibit.

What is causing the IPsec problem in the phase 1 ?

- A. The incoming IPsec connection is matching the wrong VPN configuration
- B. The phase-1 mode must be changed to aggressive
- C. The pre-shared key is wrong
- D. NAT-T settings do not match

Answer: C

NEW QUESTION 24

An administrator has configured a dial-up IPsec VPN with one phase 2, extended authentication (XAuth) and IKE mode configuration. The administrator has also enabled the IKE real time debug:

```
diagnose debug application ike-1 diagnose debug enable
```

In which order is each step and phase displayed in the debug output each time a new dial-up user is connecting to the VPN?

- A. Phase1; IKE mode configuration; XAuth; phase 2.
- B. Phase1; XAuth; IKE mode configuration; phase2.
- C. Phase1; XAuth; phase 2; IKE mode configuration.
- D. Phase1; IKE mode configuration; phase 2; XAuth.

Answer: B

Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/IKE_Packet

NEW QUESTION 28

Which two conditions must be met for a static route to be active in the routing table? (Choose two.)

- A. The link health monitor (if configured) is up.
- B. There is no other route, to the same destination, with a higher distance.
- C. The outgoing interface is up.
- D. The next-hop IP address is up.

Answer: AC

NEW QUESTION 31

Two independent FortiGate HA clusters are connected to the same broadcast domain. The administrator has reported that both clusters are using the same HA virtual MAC address. This creates a duplicated MAC address problem in the network. What HA setting must be changed in one of the HA clusters to fix the problem?

- A. Group ID.
- B. Group name.
- C. Session pickup.
- D. Gratuitous ARPs.

Answer: A

Explanation:

https://help.fortinet.com/fo50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverVMAC.htm

NEW QUESTION 34

View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

Which statements about this debug output are correct? (Choose two.)

- A. The remote gateway IP address is 10.0.0.1.
- B. It shows a phase 1 negotiation.
- C. The negotiation is using AES128 encryption with CBC hash.
- D. The initiator has provided remote as its IPsec peer ID.

Answer: BD

NEW QUESTION 36

Which two statements about bulk configuration changes made using FortiManager CLI scripts are correct? (Choose two.)

- A. When run on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate device.
- B. When run on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.
- C. When run on the All FortiGate in ADOM, changes are automatically installed without the creation of a new revision history.
- D. When run on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate device.

Answer: AB

NEW QUESTION 39

A FortiGate device has the following LDAP configuration:

The LDAP user student cannot authenticate. The exhibit shows the output of the authentication real time debug while testing the student account:

Based on the above output, what FortiGate LDAP settings must the administrator check? (Choose two.)

- A. cnid.
- B. username.
- C. password.
- D. dn.

Answer: BC

Explanation:

<https://kb.fortinet.com/kb/viewContent.do?externalId=13141>

NEW QUESTION 44

An administrator has configured a FortiGate device with two VDOMs: root and internal. The administrator has also created an inter-VDOM link that connects both VDOMs. The objective is to have each VDOM advertise some routes to the other VDOM via OSPF through the inter-VDOM link. What OSPF configuration settings must match in both VDOMs to have the OSPF adjacency successfully forming? (Choose three.)

- A. Router ID.
- B. OSPF interface area.
- C. OSPF interface cost.
- D. OSPF interface MTU.

E. Interface subnet mask.

Answer: BDE

NEW QUESTION 48

The logs in a FSSO collector agent (CA) are showing the following error: failed to connect to registry: PIKA1026 (192.168.12.232)
What can be the reason for this error?

- A. The CA cannot resolve the name of the workstation.
- B. The FortiGate cannot resolve the name of the workstation.
- C. The remote registry service is not running in the workstation 192.168.12.232.
- D. The CA cannot reach the FortiGate with the IP address 192.168.12.232.

Answer: C

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD30548>

NEW QUESTION 53

An administrator has configured the following CLI script on FortiManager, which failed to apply any changes to the managed device after being executed.

Why didn't the script make any changes to the managed device?

- A. Commands that start with the # sign are not executed.
- B. CLI scripts will add objects only if they are referenced by policies.
- C. Incomplete commands are ignored in CLI scripts.
- D. Static routes can only be added using TCL scripts.

Answer: A

Explanation:

https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/2400_Sc

A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.

NEW QUESTION 57

View the exhibit, which contains the output of a diagnose command, and then answer the question below.

What statements are correct regarding the output? (Choose two.)

- A. This is an expected session created by a session helper.
- B. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.0.1.10.
- C. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.200.1.1.
- D. This is an expected session created by an application control profile.

Answer: AC

NEW QUESTION 62

Examine the output of the 'get router info ospf neighbor' command shown in the exhibit; then answer the question below.

Which statements are true regarding the output in the exhibit? (Choose two.)

- A. The interface ToRemote is OSPF network type point-to-point.
- B. The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.
- C. The local FortiGate is the backup designated router for the wan1 network.
- D. The OSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the wan1 network.

Answer: AC

Explanation:

<https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html>

NEW QUESTION 63

A FortiGate's port1 is connected to a private network. Its port2 is connected to the Internet. Explicit web proxy is enabled in port1 and only explicit web proxy users can access the Internet. Web cache is NOT enabled. An internal web proxy user is downloading a file from the Internet via HTTP. Which statements are true regarding the two entries in the FortiGate session table related with this traffic? (Choose two.)

- A. Both session have the local flag on.
- B. The destination IP addresses of both sessions are IP addresses assigned to FortiGate's interfaces.
- C. One session has the proxy flag on, the other one does not.
- D. One of the sessions has the IP address of port2 as the source IP address.

Answer: AD

NEW QUESTION 65

Examine the output of the 'get router info bgp summary' command shown in the exhibit; then answer the question below.

Which statements are true regarding the output in the exhibit? (Choose two.)

- A. BGP state of the peer 10.125.0.60 is Established.
- B. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.
- C. Local BGP peer has not received an OpenConfirm from 10.200.3.1.
- D. The local BGP peer has received a total of 3 BGP prefixes.

Answer: AC

NEW QUESTION 70

Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below:

Which statements are true regarding the output in the exhibit? (Choose two.)

- A. BGP peers have successfully interchanged Open and Keepalive messages.
- B. Local BGP peer received a prefix for a default route.
- C. The state of the remote BGP peer is OpenConfirm.
- D. The state of the remote BGP peer will go to Connect after it confirms the received prefixes.

Answer: AB

NEW QUESTION 74

An administrator cannot connect to the GUI of a FortiGate unit with the IP address 10.0.1.254. The administrator runs the debug flow while attempting the connection using HTTP. The output of the debug flow is shown in the exhibit:

Based on the error displayed by the debug flow, which are valid reasons for this problem? (Choose two.)

- A. HTTP administrative access is disabled in the FortiGate interface with the IP address 10.0.1.254.
- B. Redirection of HTTP to HTTPS administrative access is disabled.
- C. HTTP administrative access is configured with a port number different than 80.
- D. The packet is denied because of reverse path forwarding check.

Answer: AC

NEW QUESTION 79

Examine the following routing table and BGP configuration; then answer the question below.

The BGP connection is up, but the local peer is NOT advertising the prefix 192.168.1.0/24. Which configuration change will make the local peer advertise this prefix?

- A. Enable the redistribution of connected routers into BGP.
- B. Enable the redistribution of static routers into BGP.
- C. Disable the setting network-import-check.
- D. Enable the setting ebgp-multipath.

Answer: C

NEW QUESTION 84

An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link-failed-signal to fix the problem. Which statement is correct regarding this command?

- A. Forces the former primary device to shut down all its non-heartbeat interfaces for one second while the failover occurs.
- B. Sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.
- C. Sends a link failed signal to all connected devices.
- D. Disables all the non-heartbeat interfaces in all the HA members for two seconds after a failover.

Answer: A

NEW QUESTION 86

An administrator is running the following sniffer in a FortiGate: diagnose sniffer packet any "host 10.0.2.10" 2
What information is included in the output of the sniffer? (Choose two.)

- A. Ethernet headers.
- B. IP payload.
- C. IP headers.
- D. Port names.

Answer: BC

Explanation:

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

NEW QUESTION 89

Which two statements about OCVPN are true? (Choose two.)

- A. Only root vdom supports OCVPN.
- B. OCVPN supports static and dynamic IPs in WAN interface.
- C. OCVPN offers only Hub-Spoke VPNs.
- D. FortiGate devices under different FortiCare accounts can be used to form OCVPN.

Answer: AB

NEW QUESTION 94

Examine the output of the 'diagnose sys session list expectation' command shown in the exhibit; then answer the question below.

Which statement is true regarding the session in the exhibit?

- A. It was created by the FortiGate kernel to allow push updates from FortiGuard.
- B. It is for management traffic terminating at the FortiGate.
- C. It is for traffic originated from the FortiGate.
- D. It was created by a session helper or ALG.

Answer: D

NEW QUESTION 99

Refer to the exhibit, which contains the partial output of a diagnose command.

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

- A. Anti-replay is enabled.
- B. DPD is disabled.
- C. Remote gateway IP is 10.200.4.1.
- D. Quick mode selectors are disabled.

Answer: AC

NEW QUESTION 101

View the central management configuration shown in the exhibit, and then answer the question below.

Which server will FortiGate choose for antivirus and IPS updates if 10.0.1.243 is experiencing an outage?

- A. 10.0.1.240
- B. One of the public FortiGuard distribution servers
- C. 10.0.1.244
- D. 10.0.1.242

Answer: B

NEW QUESTION 103

View the exhibit, which contains a screenshot of some phase-1 settings, and then answer the question below.

The VPN is up, and DPD packets are being exchanged between both IPsec gateways; however, traffic cannot pass through the tunnel. To diagnose, the administrator enters these CLI commands:

However, the IKE real time debug does not show any output. Why?

- A. The debug output shows phases 1 and 2 negotiations only
- B. Once the tunnel is up, it does not show any more output.
- C. The log-filter setting was set incorrectly
- D. The VPN's traffic does not match this filter.
- E. The debug shows only error message
- F. If there is no output, then the tunnel is operating normally.
- G. The debug output shows phase 1 negotiation only
- H. After that, the administrator must enable the following real time debug: diagnose debug application ipsec -1.

Answer: B

NEW QUESTION 105

Which two statements about the Security Fabric are true? (Choose two.)

- A. Only the root FortiGate collects network information and forwards it to FortiAnalyzer.
- B. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.
- C. All FortiGate devices in the Security Fabric must have bidirectional FortiTelemetry connectivity.
- D. Branch FortiGate devices must be configured first.

Answer: BC

NEW QUESTION 106

Refer to the exhibit, which shows a FortiGate configuration.

An administrator is troubleshooting a web filter issue on FortiGate. The administrator has configured a web filter profile and applied it to a policy; however, the web filter is not inspecting any traffic that is passing through the policy.

What must the administrator change to fix the issue?

- A. The administrator must increase webfilter-timeout.
- B. The administrator must disable webfilter-force-off.
- C. The administrator must change protocol to TCP.
- D. The administrator must enable fortiguard-anycast.

Answer: D

NEW QUESTION 107

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE7_EFW-6.4 Practice Exam Features:

- * NSE7_EFW-6.4 Questions and Answers Updated Frequently
- * NSE7_EFW-6.4 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_EFW-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_EFW-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_EFW-6.4 Practice Test Here](#)