

Fortinet

Exam Questions NSE7_EFW-6.4

Fortinet NSE 7 - Enterprise Firewall 6.4



NEW QUESTION 1

View the exhibit, which contains a partial routing table, and then answer the question below.

Assuming all the appropriate firewall policies are configured, which of the following pings will FortiGate route? (Choose two.)

- A. Source IP address 10.1.0.24, Destination IP address 10.72.3.20.
- B. Source IP address 10.72.3.27, Destination IP address 10.1.0.52.
- C. Source IP address 10.72.3.52, Destination IP address 10.1.0.254.
- D. Source IP address 10.73.9.10, Destination IP address 10.72.3.15.

Answer: BC

NEW QUESTION 2

What events are recorded in the crashlogs of a FortiGate device? (Choose two.)

- A. A process crash.
- B. Configuration changes.
- C. Changes in the status of any of the FortiGuard licenses.
- D. System entering to and leaving from the proxy conserve mode.

Answer: AD

Explanation:

diagnose debug crashlog read

275: 2014-08-05 13:03:53 proxy=acceptor service=imap session fail mode=activated276: 2014-08-05

13:03:53 proxy=acceptor service=ftp session fail mode=activated277: 2014-08-05 13:03:53 proxy=acceptor service=nnntp session fail mode=activated278:

2014-08-06 11:05:47 service=kernel conserve=on free="45034 pages" red="45874 pages" msg="Kernel279: 2014-08-06 11:05:47 enters conserve mode"280:

2014-08-06 13:07:16 service=kernel conserve=exit free="86704 pages" green="68811 pages"281: 2014-08-06 13:07:16 msg="Kernel leaves conserve

mode"282: 2014-08-06

13:07:16 proxy=imd sysconserve=exited total=1008 free=349 marginenter=201283: 2014-08-06 13:07:16 marginexit=302

NEW QUESTION 3

A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

- A. Firewall monitor.
- B. Policy monitor.
- C. Logs.
- D. Crashlogs.

Answer: CD

NEW QUESTION 4

Refer to the exhibit, which contains partial output from an IKE real-time debug.

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

- A. The remote gateway IP address is 10.0.0.1.

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

Answer: BC

NEW QUESTION 5

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

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

Answer: BD

Explanation:

CLI scripts can be run in three different ways: Device Database: By default, a script is executed on the device database. It is recommend you run the changes on the device database (default setting), as this allows you to check what configuration changes you will send to the managed device. Once scripts are run on the device database, you can install these changes to a managed device using the installation wizard.

Policy Package, ADOM database: If a script contains changes related to ADOM level objects and policies, you can change the default selection to run on Policy Package, ADOM database and can then be installed using the installation wizard.

Remote FortiGate directly (through CLI): A script can be executed directly on the device and you don't need to install these changes using the installation wizard. As the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.

NEW QUESTION 6

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

The administrator does not have access to the remote gateway. Based on the debug output, what configuration changes can the administrator make to the local gateway to resolve the phase 1 negotiation error?

- A. Change phase 1 encryption to AESCBC and authentication to SHA128.
- B. Change phase 1 encryption to 3DES and authentication to CBC.
- C. Change phase 1 encryption to AES128 and authentication to SHA512.
- D. Change phase 1 encryption to 3DES and authentication to SHA256.

Answer: B

NEW QUESTION 7

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

Which of the following statements is true regarding this output? (Choose two.)

- A. This web request was inspected using the root web filter profile.
- B. FortiGate found the requested URL in its local cache.
- C. The requested URL belongs to category ID 52.
- D. The web request was allowed by FortiGate.

Answer: BC

NEW QUESTION 8

View the exhibit, which contains a partial web filter profile configuration, and then answer the question below.

Which action will FortiGate take if a user attempts to access www.dropbox.com, which is categorized as File Sharing and Storage?

- A. FortiGate will exempt the connection based on the Web Content Filter configuration.
- B. FortiGate will block the connection based on the URL Filter configuration.
- C. FortiGate will allow the connection based on the FortiGuard category based filter configuration.
- D. FortiGate will block the connection as an invalid URL.

Answer: B

Explanation:

fortigate does it in order Static URL -> FortiGuard -> Content -> Advanced (java, cookie removal..)so block it in first step

NEW QUESTION 9

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 10

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

Which statements are true regarding the Weight value?

- A. Its initial value is calculated based on the round trip delay (RTT).
- B. Its initial value is statically set to 10.
- C. Its value is incremented with each packet lost.
- D. It determines which FortiGuard server is used for license validation.

Answer: C

NEW QUESTION 10

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 14

Refer to the exhibit, which contains the debug output of diagnose dvm device list.

Which two statements about the output shown in the exhibit are correct? (Choose two.)

- A. ADOMs are disabled on the FortiManager
- B. The FortiGate configuration is in sync with latest running revision history.
- C. There are pending device-level changes yet to be installed on Local-FortiGate.
- D. The policy package has been modified for Local-FortiGate.

Answer: BC

NEW QUESTION 15

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 16

A FortiGate device has the following LDAP configuration:

The administrator executed the 'dsquery' command in the Windows LDAP server 10.0.1.10, and got the following output:

```
>dsquery user -samid administrator
```

"CN=Administrator, CN=Users, DC=trainingAD, DC=training, DC=lab" Based on the output, what FortiGate LDAP setting is configured incorrectly?

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

Answer: B

Explanation:

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD37516>

NEW QUESTION 17

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

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

- A. The local router's BGP state is Established with the 10.125.0.60 peer.
- B. Since the counters were last reset; the 10.200.3.1 peer has never been down.
- C. The local router has received a total of three BGP prefixes from all peers.
- D. The local router has not established a TCP session with 100.64.3.1.

Answer: AD

NEW QUESTION 21

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 26

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

```
# diagnose debug authd fsso 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 forthe IP address 192.168.3.1.

Answer: C

NEW QUESTION 31

Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

- A. FortiGate limits the number of simultaneous sessions per explicit web proxy use
- B. This limit CANNOT be modified by the administrator.
- C. FortiGate limits the total number of simultaneous explicit web proxy users.
- D. FortiGate limits the number of simultaneous sessions per explicit web proxy user The limit CAN bmodified by the administrator
- E. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials.This limit CANNOT be modified by the administrator.

Answer: B

Explanation:

https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-WAN-opt-52/web_proxy.htm#Explicit2

The explicit proxy does not limit the number of active sessions for each user. As a result the actual explicit proxy session count is usually much higher than the number of explicit web proxy users. If an excessive number of explicit web proxy sessions is compromising system performance you can limit the amount of users if the FortiGate unit is operating with multiple VDOMs.

NEW QUESTION 36

Refer to the exhibit, which contains the output of a BGP debug command.

Which statement about the exhibit is true?

- A. The local router has received a total of three BGP prefixes from all peers.
- B. The local router has not established a TCP session with 100.64.3.1.
- C. Since the counters were last reset, the 10.200.3.1 peer has never been down.
- D. The local router BGP state is OpenConfirm with the 10.127.0.75 peer.

Answer: B

NEW QUESTION 39

Which two statements about FortiManager is true when it is deployed as a local FDS? (Choose two.)

- A. It caches available firmware updates for unmanaged devices.
- B. It can be configured as an update server, or a rating server, but not both.
- C. It supports rating requests from both managed and unmanaged devices.
- D. It provide VM license validation services.

Answer: AD

NEW QUESTION 40

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/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverVMAC.htm

NEW QUESTION 43

What does the dirty flag mean in a FortiGate session?

- A. Traffic has been blocked by the antivirus inspection.
- B. The next packet must be re-evaluated against the firewall policies.
- C. The session must be removed from the former primary unit after an HA failover.
- D. Traffic has been identified as from an application that is not allowed.

Answer: B

Explanation:

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD40119&sliceId=1>

NEW QUESTION 48

Examine the partial output from two web filter debug commands; then answer the question below:

Based on the above outputs, which is the FortiGuard web filter category for the web site www.fgt99.com?

- A. Finance and banking
- B. General organization.
- C. Business.
- D. Information technology.

Answer: C

NEW QUESTION 51

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 administer 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 52

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. The remote gateway IP is 10.200.4.1.
- C. DPD is disabled.
- D. Quick mode selectors are disabled.

Answer: AB

NEW QUESTION 56

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 BGP debug command, and then answer the question below.

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

- A. For the peer 10.125.0.60, the BGP state of is Established.
- B. The local BGP peer has received a total of three BGP prefixes.
- C. Since the BGP counters were last reset, the BGP peer 10.200.3.1 has never been down.
- D. The local BGP peer has not established a TCP session to the BGP peer 10.200.3.1.

Answer: AD

NEW QUESTION 59

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 61

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

View the exhibit, which contains a session entry, and then answer the question below.

Which statement is correct regarding this session?

- A. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
- B. It is an ICMP session from 10.1.10.10 to 10.200.5.1.
- C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.
- D. It is a TCP session in CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.

Answer: B

NEW QUESTION 66

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 71

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

Based on the output, which of the following statements is correct?

- A. Anti-reply is enabled.
- B. DPD is disabled.
- C. Quick mode selectors are disabled.
- D. Remote gateway IP is 10.200.5.1.

Answer: A

NEW QUESTION 73

Which of the following events can trigger the election of a new primary unit in a HA cluster? (Choose two.)

- A. Primary unit stops sending HA heartbeat keepalives.
- B. The FortiGuard license for the primary unit is updated.
- C. One of the monitored interfaces in the primary unit is disconnected.
- D. A secondary unit is removed from the HA cluster.

Answer: AC

NEW QUESTION 78

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 79

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 onl
- B. Once the tunnel is up, it does not show any more output.
- C. The log-filter setting was set incorrectl
- 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 onl
- H. After that, the administrator must enable the following real time debug: diagnose debug application ipsec -1.

Answer: B

NEW QUESTION 80

Refer to the exhibit, which contains the output of get system ha status.

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

- A. The slave configuration is synchronized with the master.
- B. port7 is used as the HA heartbeat on all devices in the cluster.
- C. Master is selected based on the priority configured under config system ha.
- D. The HA management IP is 169.254.0.2.

Answer: BC

NEW QUESTION 81

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 84

Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command.

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

- A. Phase 2 authentication is set to sha1 on both sides.
- B. Anti-replay is disabled.

- C. Hub2Spoke1 is a policy-based VPN.
- D. Hub2Spoke1 is configured on interface wan2.

Answer: AD

NEW QUESTION 85

.....

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](#)