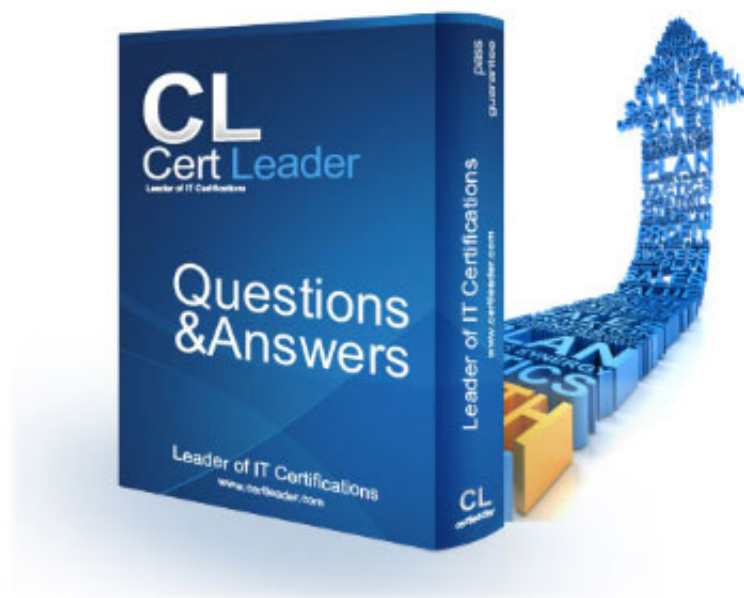


NSE7_EFW-6.4 Dumps

Fortinet NSE 7 - Enterprise Firewall 6.4

https://www.certleader.com/NSE7_EFW-6.4-dumps.html



NEW QUESTION 1

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 2

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 3

Which of the following statements are correct regarding application layer test commands? (Choose two.)

- A. They are used to filter real-time debugs.
- B. They display real-time application debugs.
- C. Some of them display statistics and configuration information about a feature or process.
- D. Some of them can be used to restart an application.

Answer: CD

Explanation:

Application layer test commands don't display info in real time, but they do show statistics and configuration info about a feature or process. You can also use some of these commands to restart a process or execute a change in its operation.

NEW QUESTION 4

Examine the following partial output from two system debug commands; then answer the question below.

Which of the following statements are true regarding the above outputs? (Choose two.)

- A. The unit is running a 32-bit FortiOS
- B. The unit is in kernel conserve mode
- C. The Cached value is always the Active value plus the Inactive value
- D. Kernel indirectly accesses the low memory (LowTotal) through memory paging

Answer: AC

NEW QUESTION 5

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

Which one of the following statements about this FortiGate is correct?

- A. It is currently in system conserve mode because of high CPU usage.
- B. It is currently in extreme conserve mode because of high memory usage.
- C. It is currently in proxy conserve mode because of high memory usage.
- D. It is currently in memory conserve mode because of high memory usage.

Answer: D

NEW QUESTION 6

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 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 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 9

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 10

Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

- A. Neighbor range
- B. Route reflector
- C. Next-hop-self
- D. Neighbor group

Answer: B

Explanation:

Route reflectors help to reduce the number of IBGP sessions inside an AS. A route reflector forwards the routes learned from one peer to the other peers. If you configure route reflectors, you don't need to create a full mesh IBGP network. All clients in a cluster only talk to route reflector to get sync routing updates. Route reflectors pass the routing updates to other route reflectors and border routers within the AS.

NEW QUESTION 10

View the IPS exit log, and then answer the question below.

diagnose test application ipsmonitor 3 ipseengine exit log"

pid = 93 (cfg), duration = 5605322 (s) at Wed Apr 19 09:57:26 2017 code = 11, reason: manual

What is the status of IPS on this FortiGate?

- A. IPS engine memory consumption has exceeded the model-specific predefined value.
- B. IPS daemon experienced a crash.
- C. There are communication problems between the IPS engine and the management database.
- D. All IPS-related features have been disabled in FortiGate's configuration.

Answer: D

Explanation:

The command diagnose test application ipsmonitor includes many options that are useful for troubleshooting purposes. Option 3 displays the log entries generated every time an IPS engine process stopped. There are various reasons why these logs are generated: Manual: Because of the configuration, IPS no longer needs to run (that is, all IPS-related features have been disabled)

NEW QUESTION 13

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

Which statement explains why the state of the 10.200.3.1 peer is Connect?

- A. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the OpenConfirm yet.
- B. The TCP session to 10.200.3.1 has not completed the 3-way handshake.
- C. The local router is receiving the BGP keepalives from the peer, but it has not received a BGP prefix yet.
- D. The local router has received the BGP prefixes from the remote peer.

Answer: B

Explanation:

BGP neighbor states and how they change:

- Idle: Initial state
- Connect: Waiting for a successful three-way TCP connection
- Active: Unable to establish the TCP session
- OpenSent: Waiting for an OPEN message from the peer
- OpenConfirm: Waiting for the keepalive message from the peer
- Established: Peers have successfully exchanged OPEN and keepalive messages

NEW QUESTION 17

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 20

A FortiGate is configured as an explicit web proxy. Clients using this web proxy are reposting DNS errors when accessing any website. The administrator executes the following debug commands and observes that the n-dns-timeout counter is increasing:

What should the administrator check to fix the problem?

- A. The connectivity between the FortiGate unit and the DNS server.
- B. The connectivity between the client workstations and the DNS server.
- C. That DNS traffic from client workstations is allowed by the explicit web proxy policies.
- D. That DNS service is enabled in the explicit web proxy interface.

Answer: A

NEW QUESTION 22

What is the diagnose test application ipsmonitor 99 command used for?

- A. To enable IPS bypass mode
- B. To provide information regarding IPS sessions
- C. To disable the IPS engine
- D. To restart all IPS engines and monitors

Answer: D

NEW QUESTION 25

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 27

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 32

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 33

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 37

View these partial outputs from two routing debug commands:

Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

- A. Both port1 and port2
- B. port3
- C. port1
- D. port2

Answer: C

NEW QUESTION 39

When using the SSL certificate inspection method for HTTPS traffic, how does FortiGate filter web requests when the browser client does not provide the server name indication (SNI) extension?

- A. FortiGate uses CN information from the Subject field in the server's certificate.
- B. FortiGate switches to the full SSL inspection method to decrypt the data.
- C. FortiGate blocks the request without any further inspection.
- D. FortiGate uses the requested URL from the user's web browser.

Answer: A

NEW QUESTION 42

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 43

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 44

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 provides VM license validation services.

Answer: AD

NEW QUESTION 48

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 49

Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below.

Why didn't the tunnel come up?

- A. IKE mode configuration is not enabled in the remote IPsec gateway.
- 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. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mode.

Answer: C

NEW QUESTION 52

What configuration changes can reduce the memory utilization in a FortiGate? (Choose two.)

- A. Reduce the session time to live.
- B. Increase the TCP session timers.
- C. Increase the FortiGuard cache time to live.
- D. Reduce the maximum file size to inspect.

Answer: AD

NEW QUESTION 56

Which two tasks are automated using the Install Wizard on FortiManager? (Choose two.)

- A. Preview pending configuration changes for managed devices.
- B. Add devices to FortiManager.
- C. Import policy packages from managed devices.
- D. Install configuration changes to managed devices.
- E. Import interface mappings from managed devices.

Answer: AD

Explanation:

https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/1200_ins

There are 4 main wizards: Add Device: is used to add devices to central management and import their configurations.
Install: is used to install configuration changes from Device Manager or Policies & Objects to the managed devices. It allows you to preview the changes and, if the administrator doesn't agree with the changes, cancel and modify them.
Import policy: is used to import interface mapping, policy database, and objects associated with the managed devices into a policy package under the Policy & Object tab. It runs with the Add Device wizard by default and may be run at any time from the managed device list.
Re-install policy: is used to perform a quick install of the policy package. It doesn't give the ability to preview the changes that will be installed to the managed device.

NEW QUESTION 60

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 61

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

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

- A. The port4 interface is connected to the OSPF backbone area.
- B. The local FortiGate has been elected as the OSPF backup designated router.
- C. There are at least 5 OSPF routers connected to the port4 network.
- D. Two OSPF routers are down in the port4 network.

Answer: AC

Explanation:

on BROADCAST network there are 4 neighbors, among which 1*DR +1*BDR. So our FG has 4 neighbors, but create adjacency only with 2 (with DR and BDR). 2 neighbors DRouter (not down).

NEW QUESTION 64

Which statement is true regarding File description (FD) conserve mode?

- A. IPS inspection is affected when FortiGate enters FD conserve mode.
- B. A FortiGate enters FD conserve mode when the amount of available description is less than 5%.
- C. FD conserve mode affects all daemons running on the device.
- D. Restarting the WAD process is required to leave FD conserve mode.

Answer: B

NEW QUESTION 67

Which two tasks are automated using the Install Wizard on FortiManager? (Choose two.)

- A. Installing configuration changes to managed devices
- B. Importing interface mappings from managed devices
- C. Adding devices to FortiManager
- D. Previewing pending configuration changes for managed devices

Answer: AD

NEW QUESTION 70

An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer. If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

- A. diagnose sniffer packet any 'udp port 500'
- B. diagnose sniffer packet any 'udp port 4500'
- C. diagnose sniffer packet any 'esp'
- D. diagnose sniffer packet any 'udp port 500 or udp port 4500'

Answer: C

Explanation:

Capture IKE Traffic without NAT:diagnose sniffer packet 'host and udp port 500'

-----Capture ESP

Traffic without NAT:diagnose sniffer packet any 'host and esp'

-----Capture IKE

and ESP with NAT-T:diagnose sniffer packet any 'host and (udp port 500 or udp port 4500)'

NEW QUESTION 73

Which real time debug should an administrator enable to troubleshoot RADIUS authentication problems?

- A. Diagnose debug application radius -1.
- B. Diagnose debug application fnbamd -1.
- C. Diagnose authd console –log enable.
- D. Diagnose radius console –log enable.

Answer: B

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD32838>

NEW QUESTION 75

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 79

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

TheBGP 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 81

Which 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 86

Examine the output of the 'diagnose sys session list expectation' command shown in the exhibit; than 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 89

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 90

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 94

Examine the following partial outputs from two routing debug commands; then answer the question below.

```
# get router info kernel
```

```
tab=254 vf=0 scope=0type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.1.254 dev=2(port1)
```

```
tab=254 vf=0 scope=0type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.2.254 dev=3(port2)
```

```
tab=254 vf=0 scope=253type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/.->10.0.1.0/24 pref=10.0.1.254 gwy=0.0.0.0 dev=4(port3)
```

```
# get router info routing-table all s*0.0.0.0/0 [10/0] via 10.200.1.254, port1 [10/0] via 10.200.2.254, port2, [10/0] dO.0.1.0/24 is directly connected, port3  
dO.200.1.0/24 is directly connected, port1 dO.200.2.0/24 is directly connected, port2
```

Which outbound interface or interfaces will be used by this FortiGate to route web traffic from internal users to the Internet?

- A. port1
- B. port2.
- C. Both port1 and port2.
- D. port3.

Answer: B

NEW QUESTION 97

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 102

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 107

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE7_EFW-6.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE7_EFW-6.4-dumps.html