

## Exam Questions NSE7\_EFW-6.4

Fortinet NSE 7 - Enterprise Firewall 6.4

[https://www.2passeasy.com/dumps/NSE7\\_EFW-6.4/](https://www.2passeasy.com/dumps/NSE7_EFW-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 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 3

Examine the following traffic log; then answer the question below.

```
date=20xx-02-01 time=19:52:01 devname=master device_id="xxxxxxx" log_id=0100020007 type=event subtype=system pri critical vd=root service=kemel status=failure msg="NAT port is exhausted."
```

What does the log mean?

- A. There is not enough available memory in the system to create a new entry in the NAT port table.
- B. The limit for the maximum number of simultaneous sessions sharing the same NAT port has been reached.
- C. FortiGate does not have any available NAT port for a new connection.
- D. The limit for the maximum number of entries in the NAT port table has been reached.

**Answer:** B

#### NEW QUESTION 4

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

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

**Answer: D**

#### NEW QUESTION 5

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 6

The CLI command set intelligent-mode <enable | disable> controls the IPS engine's adaptive scanning behavior. Which of the following statements describes IPS adaptive scanning?

- A. Determines the optimal number of IPS engines required based on system load.
- B. Downloads signatures on demand from FDS based on scanning requirements.
- C. Determines when it is secure enough to stop scanning session traffic.
- D. Choose a matching algorithm based on available memory and the type of inspection being performed.

**Answer: C**

#### Explanation:

Configuring IPS intelligenceStarting with FortiOS 5.2, intelligent-mode is a new adaptive detection method. This command is enabled the default and it means that the IPS engine will perform adaptive scanning so that, for some traffic, the FortiGate can quickly finish scanning and offload the traffic to NPU or kernel. It is a balanced method which could cover all known exploits. When disabled, the IPS engine scans every single byte. config ips globalset intelligent-mode {enable|disable}end

#### NEW QUESTION 7

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 8

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 9

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 10

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 10

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 15

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

```
# diagnose debug authd fssolist —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. TRAINING.
- C. LAB.
- D. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2. TRAINING.
- E. LAB.
- F. The reverse DNS lookup for the IP address 192.168.3.1.

**Answer: C**

#### NEW QUESTION 16

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 IKE 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 phrase-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 20

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 24

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 25

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](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 29

View the following FortiGate configuration.

All traffic to the Internet currently egresses from port1. The exhibit shows partial session information for Internet traffic from a user on the internal network:

If the priority on route ID 1 were changed from 5 to 20, what would happen to traffic matching that user's session?

- A. The session would remain in the session table, and its traffic would still egress from port1.
- B. The session would remain in the session table, but its traffic would now egress from both port1 and port2.
- C. The session would remain in the session table, and its traffic would start to egress from port2.
- D. The session would be deleted, so the client would need to start a new session.

**Answer:** A

**Explanation:**

<http://kb.fortinet.com/kb/documentLink.do?externalID=FD40943>

#### NEW QUESTION 31

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

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

**Answer:** B

#### NEW QUESTION 35

Refer to the exhibit, which contains the output of diagnose sys session list.

If the HA ID for the primary unit is zero (0), which statement about the output is true?

- A. This session cannot be synced with the slave unit.
- B. The inspection of this session has been offloaded to the slave unit.
- C. The master unit is processing this traffic.
- D. This session is for HA heartbeat traffic.

**Answer:** C

#### NEW QUESTION 39

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](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 41**

How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

- A. FortiManager can download and maintain local copies of FortiGuard databases.
- B. FortiManager supports only FortiGuard push to managed devices.
- C. FortiManager will respond to update requests only if they originate from a managed device.
- D. FortiManager does not support rating requests.

**Answer:** A

**NEW QUESTION 44**

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 47**

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 51**

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 54**

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 56**

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 57**

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 61**

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

Based on the debug output, which phase-1 setting is enabled in the configuration of this VPN?

- A. auto-discovery-sender
- B. auto-discovery-forwarder
- C. auto-discovery-shortcut
- D. auto-discovery-receiver

**Answer: B**

#### NEW QUESTION 64

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 65

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 68**

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 70**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7\_EFW-6.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7\_EFW-6.4 Product From:

[https://www.2passeasy.com/dumps/NSE7\\_EFW-6.4/](https://www.2passeasy.com/dumps/NSE7_EFW-6.4/)

## Money Back Guarantee

### **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 First Try
- \* NSE7\_EFW-6.4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year