

Vendor: Fortinet

# Exam Code: NSE7\_EFW-7.0

**Exam Name:** Fortinet NSE 7 - Enterprise Firewall 7.0

Version: DEMO

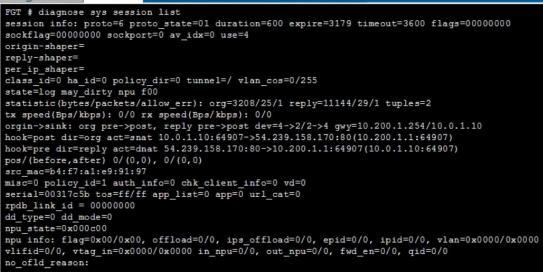


# **QUESTION 1**

Refer to the exhibits, which show the configuration on FortiGate and partial session information for internet traffic from a user on the internal network.

Configuration Session config system global set snat-route-change disable end config router static edit 1 set gateway 10.200.1.254 set priority 5 set device "port1" next edit 2 set gateway 10.200.2.254 set priority 10 set device "port2" next end

#### Configuration Session



If the priority on route ID 2 were changed from 10 to 0, what would happen to traffic matching that user session?

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

#### Answer: D

#### **Explanation:**

With snat-route-change disable, sessions using SNAT keep using the same outbound interface, as long as the old route is still active.



# **QUESTION 2**

Which two conditions would prevent a static route from being added to the routing table? (Choose two.)

- A. There is another other route to the same destination, with a lower distance.
- B. The route has a lower priority value than another route to the same destination.
- C. The next-hop IP address is unreachable.
- D. The interface specified in the route configuration is down.

# Answer: AD

#### Explanation:

Route with lower distance is preferred and it is inserted to RIB.

#### **QUESTION 3**

An administrator wants to capture encrypted phase 2 traffic between two FortiGate devices using the built-in sniffer.

If the administrator knows that there is no NAT device located between both FortiGate devices, which command should the administrator run?

- A. diagnose sniffer packet any 'ah'
- B. diagnose sniffer packet any 'ip proto 50'
- C. diagnose sniffer packet any 'udp port 4500'
- D. diagnose sniffer packet any 'udp port 500'

# Answer: B

#### **Explanation:**

#Diagnose sniffer packet any 'host <remote-gateway> and esp' >> ESP traffic uses "IP Protocol 50"

#### **QUESTION 4**

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

- A. Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer.
- B. Only the root FortiGate sends logs to FortiAnalyzer.
- C. Only FortiGate devices with fabric-object-unification set to default will receive and synchronize global CMDB objects sent by the root FortiGate.
- D. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.

# Answer: AC

**Explanation:** 

Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer.

# **QUESTION 5**

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



the 0.252000.27. assessed as and and tot assess
ike 0:253000:27: responder: main mode get 1st message
ike 0:253000:27: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:253000:27: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:253000:27: VID FRAGMENTATION 404887D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:253000:27: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:253000:27: incoming proposal:
ike 0:253000:27: proposal id = 0:
<pre>ike 0:253000:27: protocol id = ISAKMP:</pre>
ike 0:253000:27: trans_id = KEY_IKE.
<pre>ike 0:253000:27: encapsulation = IKE/none</pre>
<pre>ike 0:253000:27: type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256</pre>
<pre>ike 0:253000:27: type=OAKLEY_HASH_ALG, val=SHA2_256.</pre>
<pre>ike 0:253000:27: type=AUTH_METHOD, val=PRESHARED_KEY.</pre>
<pre>ike 0:253000:27: type=OAKLEY_GROUP, val=MODP1536.</pre>
ike 0:253000:27: ISAKMP SA lifetime=86400
ike 0:253000:27: my proposal, gw Remotesite:
ike 0:253000:27: proposal id = 1:
<pre>ike 0:253000:27: protocol id = ISAKMP:</pre>
ike 0:253000:27: trans_id = KEY_IKE.
<pre>ike 0:253000:27: encapsulation = IKE/none</pre>
ike 0:253000:27: type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
<pre>ike 0:253000:27: type=OAKLEY_HASH_ALG, val=SHA.</pre>
<pre>ike 0:253000:27: type=AUTH_METHOD, val=PRESHARED_KEY.</pre>
<pre>ike 0:253000:27: type=OAKLEY_GROUP, val=MODP1536.</pre>
ike 0:253000:27: ISAKMP SA lifetime=86400
ike 0:253000:27: negotiation failure
ike Negot:253a8cbe6335e6fd/000000000000000000000000000000000000

Why did the tunnel not come up?

- A. The local gateway has configured less secure encryption and hashing algorithms compared to the remote gateway.
- B. The Diffie-Hellman group does not match on the local and remote gateways.
- C. The proposal ID does not match between local and remote gateways.
- D. The encapsulation method for phase 2 is set to none on local and remote gateways.

# Answer: A

#### Explanation:

local gateway: encryption AES-128, hash SHA remote gateway: encryption AES-256, hash SHA-256 So local gateway has less secure settings

# **QUESTION 6**

An administrator has created a VPN community within VPN Manager on FortiManager. They also added gateways to the VPN community and are now trying to create firewall policies to permit traffic over the tunnel; however, the VPN interfaces are not listed as available options. What step must the administrator take to resolve this issue?

A. Install the VPN community and gateway configuration to the FortiGate devices, in order for the interfaces to be displayed within Policy & Objects on FortiManager



- B. Set up all of the phase 1 settings in the VPN community that they neglected to set up initially. The interfaces will be automatically generated after the administrator configures all of the required settings.
- C. Refresh the device status from the Device Manager so that FortiGate will populate the IPsec interfaces.
- D. Create interface mappings for the IPsec VPN interfaces, before they can be used in a policy.

# Answer: A

#### **Explanation:**

We need to install the configuration before doing the policies.

- 1- Create a VPN Community
- 2- Install VPN Configuration
- 3- Add IPsec Firewall Policies
- 4- Install the Policies

# **QUESTION 7**

Which action will FortiGate take when using the default settings for SSL certificate inspection, where the server name indication (SNI) does not match either the common name (CN) or any of the subject alternative names (SAN) in the server certificate?

- A. FortiGate uses the CN information from the Subject field in the server certificate.
- B. FortiGate uses the first entry listed in the SAN field in the server certificate.
- C. FortiGate uses the SNI from the user's web browser.
- D. FortiGate closes the connection because this represents an invalid SSL/TLS configuration.

# Answer: A

#### **Explanation:**

By default, mode enable, it will use the CN value in Strict mode, it will close the connection.

# **QUESTION 8**

Which two configuration commands change the default behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

- A. set av-failopen off
- B. set av-failopen pass
- C. set fail-open enable
- D. set ips fail-open disable

# Answer: AC

Explanation: config ips global set fail-open {enable | disable} end When disabled (default), the IPS engine drops all new sessions that require flow-based inspection. config system global set av-failopen {pass | off | one-shot} end pass This is the default settings.



# QUESTION 9

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.

What can the administrator do to fix this problem?

- A. Configure remote link monitoring to detect an issue in the forwarding path.
- B. Configure set send-garp-on-failover enable under config system ha on both cluster members.
- C. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports.
- D. Configure set link-failed-signal enable under config system ha on both cluster members.

# Answer: D

#### **Explanation:**

link-failed-signal - Enable to shut down all interfaces for 1 sec after a failover. Use if gratuitous ARPs do not update network.

# **QUESTION 10**

What is the diagnose test application ipsmenitor 5 command used for?

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

# Answer: A

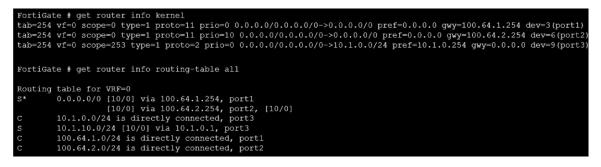
#### Explanation:

# diagnose test application ipsmonitor

- 5: Toggle bypass status
- 13: IPS session list
- 98: Stop all IPS engines
- 99: Restart all IPS engines and monitor

# **QUESTION 11**

Refer to the exhibit, which shows partial outputs from two routing debug commands.



Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

- A. Set the priority of the static default route using port1 to 10.
- B. Set the priority of the static default route using port2 to 1.



- C. Set preserve-session-route to enable.
- D. Set snat-route-change to enable.

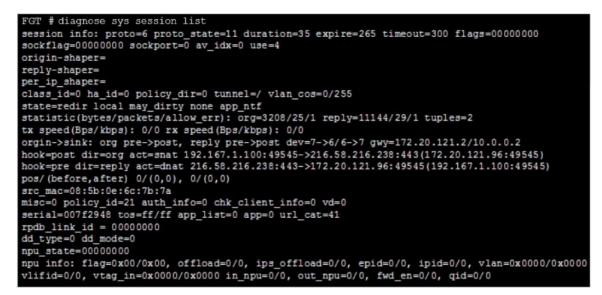
# Answer: A

#### **Explanation:**

ECMP pre-requisite is "routes must have the same destination and costs. In the case of static routes, costs include distance and priority". In this case traffic is routed through port 1 because of the lower priority. If we raise priority on port 1 to the value of 10 the traffic should be routed through both ports 1 and 2.

#### **QUESTION 12**

Refer to the exhibit, which shows a session table entry.



Which statement about FortiGate behavior relating to this session is true?

- A. FortiGate redirected the client to the captive portal to authenticate, so that a correct policy match could be made.
- B. FortiGate forwarded this session without any inspection.
- C. FortiGate is performing security profile inspection using the CPU.
- D. FortiGate applied only IPS inspection to this session.

# Answer: C

#### **Explanation:**

url\_cat=41 suggests that it has webfilter applied. On the other hand, all npu flag suggests that no offload is applied, being then inspected by the CPU.



# Thank You for Trying Our Product

# Lead2pass Certification Exam Features:

- ★ More than 99,900 Satisfied Customers Worldwide.
- ★ Average 99.9% Success Rate.
- ★ Free Update to match latest and real exam scenarios.
- ★ Instant Download Access! No Setup required.
- ★ Questions & Answers are downloadable in PDF format and VCE test engine format.



- ★ Multi-Platform capabilities Windows, Laptop, Mac, Android, iPhone, iPod, iPad.
- ★ 100% Guaranteed Success or 100% Money Back Guarantee.
- ★ Fast, helpful support 24x7.

View list of all certification exams: <u>http://www.lead2pass.com/all-products.html</u>



10% Discount Coupon Code: ASTR14