NSE8_812 Q&As

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

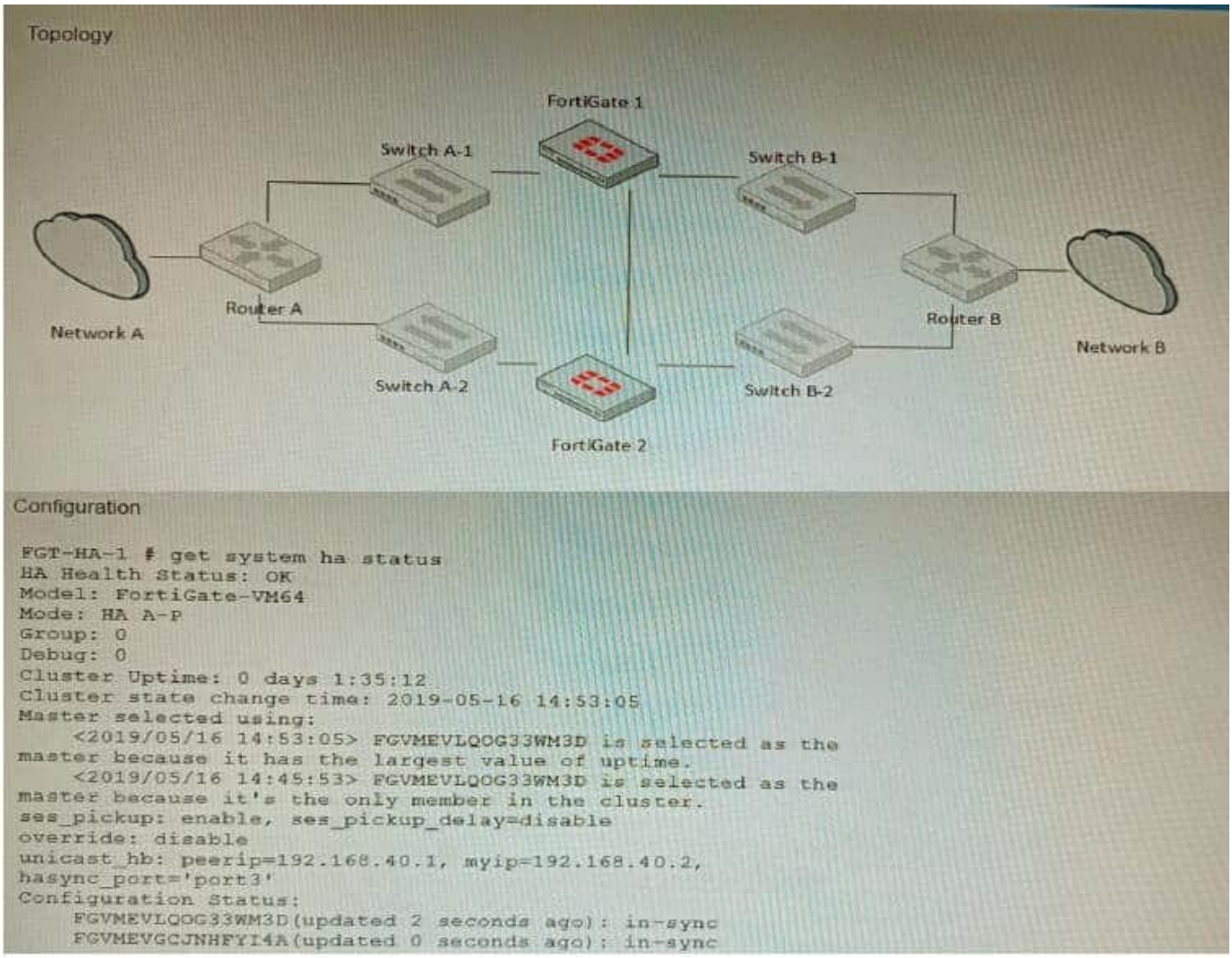
https://www.pass4itsure.com/nse8_812.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibits.



The exhibits show a FortiGate network topology and the output of the status of high availability on the FortiGate. Given this information, which statement is correct?

A. The ethertype values of the HA packets are 0x8890, 0x8891, and 0x8892

B. The cluster mode can support a maximum of four (4) FortiGate VMs

C. The cluster members are on the same network and the IP addresses were statically assigned.

D. FGVMEVLQOG33WM3D and FGVMEVGCJNHFYI4A share a virtual MAC address.

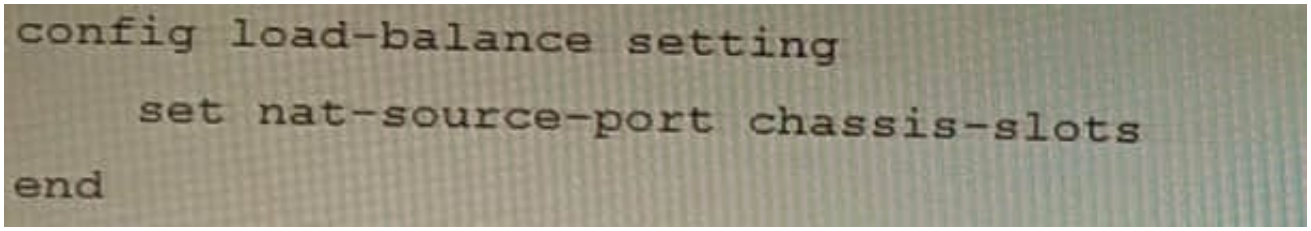
Correct Answer: D

Explanation: The output of the status of high availability on the FortiGate shows that the cluster mode is active-passive, which means that only one FortiGate unit is active at a time, while the other unit is in standby mode. The active unit handles all traffic and also sends HA heartbeat packets to monitor the standby unit. The standby unit becomes active if it stops receiving heartbeat packets from the active unit, or if it receives a higher priority from another cluster unit. In

active-passive mode, all cluster units share a virtual MAC address for each interface, which is used as the source MAC address for all packets forwarded by the cluster.
References:https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103439/high- availability-with-two-fortigates

QUESTION 2

Review the following FortiGate-6000 configuration excerpt:



Based on the configuration, which statement is correct regarding SNAT source port partitioning behavior?

A. It dynamically distributes SNAT source ports to operating FPCs or FPMs.

B. It is the default SNAT configuration and preserves active sessions when an FPC or FPM goes down.

C. It statically distributes SNAT source ports to operating FPCs or FPMs

D. It equally distributes SNAT source ports across chassis slots.

Correct Answer: A

Explanation: The configuration excerpt shows that the SNAT source port partitioning behavior is set to dynamic. This means that the FortiGate will dynamically distribute SNAT source ports to operating FPCs or FPMs. This ensures that active

sessions are not interrupted if an FPC or FPM goes down.

The other options are incorrect. Option B is incorrect because the default SNAT configuration is static. Option C is incorrect because the configuration excerpt does not specify that SNAT source ports are statically distributed. Option D is

incorrect because the SNAT source ports are not evenly distributed across chassis slots. Here are some additional details about SNAT source port partitioning behavior:

SNAT source port partitioning behavior can be set to dynamic or static.

The default SNAT configuration is static.

Dynamic SNAT source port partitioning ensures that active sessions are not interrupted if an FPC or FPM goes down.

Static SNAT source port partitioning can improve performance by reducing the number of SNAT lookups.

QUESTION 3

You must configure an environment with dual-homed servers connected to a pair of FortiSwitch units using an MCLAG.

Multicast traffic is expected in this environment, and you should ensure unnecessary traffic is pruned from links that do not have a multicast listener.

In which two ways must you configure the igmps-f lood-traffic and igmps-flood-report settings? (Choose two.)

A. disable on ICL trunks

B. enable on ICL trunks

C. disable on the ISL and FortiLink trunks

D. enable on the ISL and FortiLink trunks

Correct Answer: AD

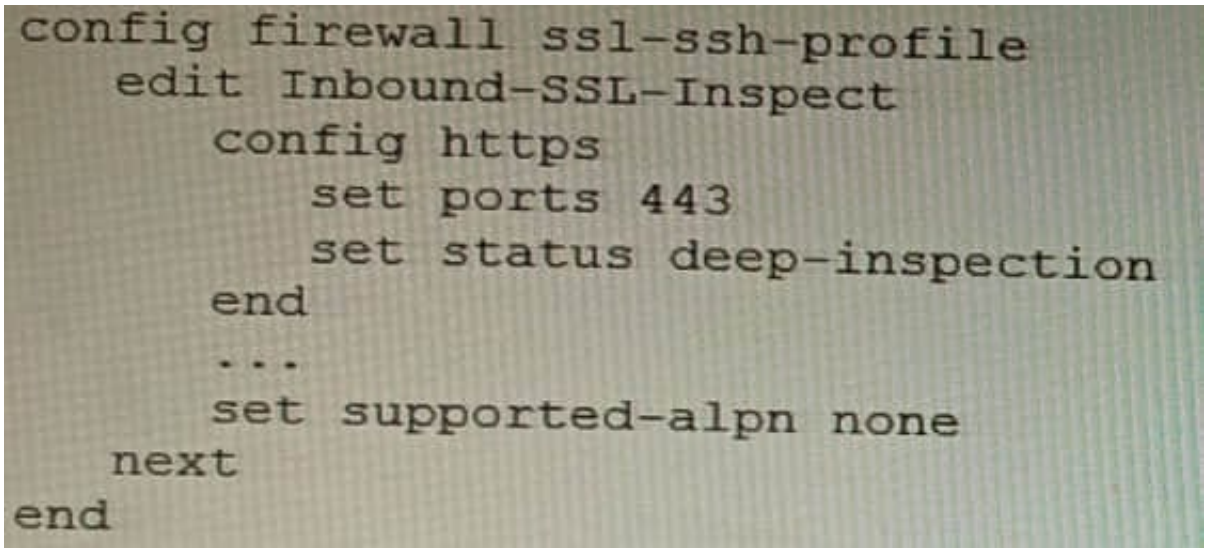
Explanation: To ensure that unnecessary multicast traffic is pruned from links that do not have a multicast listener, you must disable IGMP flood traffic on the ICL trunks and enable IGMP flood reports on the ISL and FortiLink trunks. Disabling

IGMP flood traffic will prevent the FortiSwitch units from flooding multicast traffic to all ports on the ICL trunks. This will help to reduce unnecessary multicast traffic on the network.

Enabling IGMP flood reports will allow the FortiSwitch units to learn which ports are interested in receiving multicast traffic. This will help the FortiSwitch units to prune multicast traffic from links that do not have a multicast listener.

QUESTION 4

Refer to the CLI configuration of an SSL inspection profile from a FortiGate device configured to protect a web server:



Based on the information shown, what is the expected behavior when an HTTP/2 request comes in?

A. FortiGate will reject all HTTP/2 ALPN headers.

B. FortiGate will strip the ALPN header and forward the traffic.

C. FortiGate will rewrite the ALPN header to request HTTP/1.

D. FortiGate will forward the traffic without modifying the ALPN header.

Correct Answer: A

Explanation: Thesupported-alpnparameter is set tohttp1.1in the SSL inspection profile. This means that the FortiGate will only accept HTTP/1.1 traffic. Any HTTP/2 traffic will be rejected.

The following is the relevant documentation from Fortinet:

Thesupported-alpnparameter specifies the list of ALPN protocols that the FortiGate will accept. If the client requests a protocol that is not in this list, the FortiGate will reject the connection.

The default value for thesupported-alpnparameter isall. This means that the FortiGate will accept any ALPN protocol that the client requests. To reject all HTTP/2 traffic, set thesupported-alpnparameter tohttp1.1. Source: https://

docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2- support-in-proxy-mode-ssl-inspection

QUESTION 5

A remote IT Team is in the process of deploying a FortiGate in their lab. The closed environment has been configured to support zero-touch provisioning from the FortiManager, on the same network, via DHCP options. After waiting 15 minutes, they are reporting that the FortiGate received an IP address, but the zero-touch process failed.

The exhibit below shows what the IT Team provided while troubleshooting this issue:

```
FGT # diagnose fdsm fmg-auto-discovery-status
dhcp: fmg-ip=172.18.60.115, fmg-domain-name='', config-touched=1(/bin/dhcpcd)
```

Which statement explains why the FortiGate did not install its configuration from the FortiManager?

A. The FortiGate was not configured with the correct pre-shared key to connect to the FortiManager

B. The DHCP server was not configured with the FQDN of the FortiManager

C. The DHCP server used the incorrect option type for the FortiManager IP address.

D. The configuration was modified on the FortiGate prior to connecting to the FortiManager

Correct Answer: C

Explanation: C is correct because the DHCP server used the incorrect option type for the FortiManager IP address. The option type should be 43 instead of 15, as shown in the FortiManager Administration Guide under Zero-Touch Provisioning > Configuring DHCP options for ZTP. References: https://docs.fortinet.com/document/fortimanager/7.4.0/administration-guide/568591/high-availabilityhttps://docs.fortinet.com/document/fortimanager/7.4.0/administration- guide/568591/high-availability/568592/configuring-ha-options