# 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.pass2lead.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**

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 2**

You are responsible for recommending an adapter type for NICs on a FortiGate VM that will run on an ESXi Hypervisor. Your recommendation must consider performance as the main concern, cost is not a factor. Which adapter type for the NICs will you recommend?

A. Native ESXi Networking with E1000

B. Virtual Function (VF) PCI Passthrough

C. Native ESXi Networking with VMXNET3

D. Physical Function (PF) PCI Passthrough

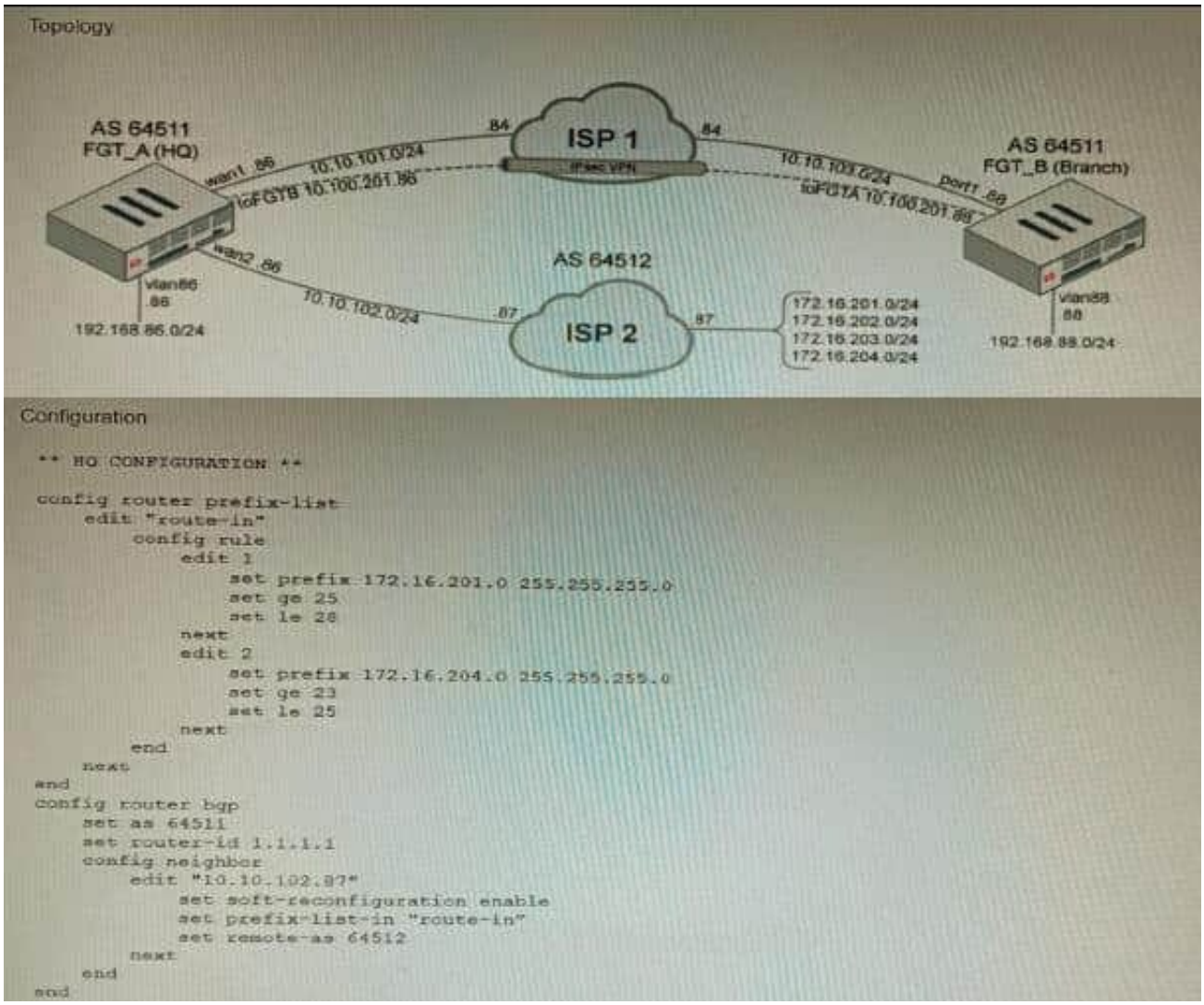
Correct Answer: C

Explanation: The FortiGate VM is a virtual firewall appliance that can run on various hypervisors, such as ESXi, Hyper-V, KVM, etc. The adapter type for NICs on a FortiGate VM determines the performance and compatibility of the network interface cards with the hypervisor and the physical network. There are different adapter types available for NICs on a FortiGate VM, such as E1000, VMXNET3, SR-IOV, etc. If performance is the main concern and cost is not a factor, one option is to use native ESXi networking with VMXNET3 adapter type for NICs on a FortiGate VM that will run on an ESXi hypervisor. VMXNET3 is a paravirtualized network interface card that is optimized for performance in virtual machines and supports features such as multiqueue support, Receive Side Scaling (RSS), Large Receive Offload (LRO), IPv6 offloads, and MSI/MSI-X interrupt delivery. Native ESXi networking means that the FortiGate VM uses the

standard virtual switch (vSwitch) or distributed virtual switch (dvSwitch) provided by the ESXi hypervisor to connect to the physical network. This option can provide high performance and compatibility for NICs on a FortiGate VM without requiring additional hardware or software components. References: https://docs.fortinet.com/document/fortigate/7.0.0/vm-installation- for-vmware-esxi/19662/installing-fortigate-vm-on-vmware- esxihttps://docs.fortinet.com/document/fortigate/7.0.0/vm-installationfor-vmware- esxi/19662/networking

**QUESTION 3**

Refer to the exhibits.




A customer has deployed a FortiGate with iBGP and eBGP routing enabled. HQ is receiving routes over eBGP from ISP 2; however, only certain routes are showing up in the routing table-Assume that BGP is working perfectly and that the only possible modifications to the routing table are solely due to the prefix list that is applied on HQ.

Given the exhibits, which two routes will be active in the routing table on the HQ firewall? (Choose two.)

A. 172.16.204.128/25

B. 172.16.201.96/29

C. 172,620,64,27

D. 172.16.204.64/27

Correct Answer: AD

Explanation: The prefix list in the exhibit is configured to match prefixes that are either in the 172.16.204.0/24 subnet or in the 172.62.0.0/16 subnet. The routes that match these prefixes will be active in the routing table on the HQ firewall. The

routes that match the following prefixes will not be active in the routing table:

172.16.201.96/29

These routes do not match the criteria set by the prefix list.

References:

Prefix lists | FortiGate / FortiOS 7.4.0 - Fortinet Document Library Configuring BGP | FortiGate / FortiOS 7.4.0 - Fortinet Document Library

**QUESTION 4**

You want to use the MTA adapter feature on FortiSandbox in an HA-Cluster. Which statement about this solution is true?

A. The configuration of the MTA Adapter Local Interface is different than on port1.

B. The MTA adapter is only available in the primary node.

C. The MTA adapter mode is only detection mode.

D. The configuration is different than on a standalone device.

Correct Answer: B

Explanation: The MTA adapter feature on FortiSandbox is a feature that allows FortiSandbox to act as a mail transfer agent (MTA) that can receive, inspect, and forward email messages from externalsources. The MTA adapter feature can be used to integrate FortiSandbox with third-party email security solutions that do not support direct integration with FortiSandbox, such as Microsoft Exchange Server or Cisco Email Security Appliance (ESA). The MTA adapter feature can also be used to enhance email security by adding an additional layer of inspection and filtering before delivering email messages to the final destination. The MTA adapter feature can be enabled on FortiSandbox in an HA-Cluster, which is a configuration that allows two FortiSandbox units to synchronize their settings and data and provide high availability and load balancing for sandboxing services. However, one statement about this solution that is true is that the MTA adapter is only available in the primary node. This means that only one FortiSandbox unit in the HA- Cluster can act as an MTA and receive email messages from external sources, while the other unit acts as a backup node that can take over the MTA role if the primary node fails or loses connectivity. This also means that only one IP address or FQDN can be used to configure the external sources to send email messages to the FortiSandbox MTA, which is the IP address or FQDN of the primary node. References: https://docs.fortinet.com/document/fortisandbox/3.2.0/administration-guide/19662/mail- transfer-agent-mtahttps://docs.fortinet.com/document/fortisandbox/3.2.0/administration-guide/19662/high-availability-ha

**QUESTION 5**

Which two statements are correct on a FortiGate using the FortiGuard Outbreak Protection Service (VOS)? (Choose two.)

A. The FortiGuard VOS can be used only with proxy-base policy inspections.

B. If third-party AV database returns a match the scanned file is deemed to be malicious.

C. The antivirus database queries FortiGuard with the hash of a scanned file

D. The AV engine scan must be enabled to use the FortiGuard VOS feature

E. The hash signatures are obtained from the FortiGuard Global Threat Intelligence database.

Correct Answer: CE

C. The antivirus database queries FortiGuard with the hash of a scanned file. This is how the FortiGuard VOS service works. The FortiGate queries FortiGuard with the hash of a scanned file, and FortiGuard returns a list of known malware signatures that match the hash.

E. The hash signatures are obtained from the FortiGuard Global Threat Intelligence database. This is where the FortiGuard VOS service gets its hash signatures from. The FortiGuard Global Threat Intelligence database is updated regularly with new malware signatures.