Free Questions for NSE6_FSW-7.2 by dumpssheet

Shared by Serrano on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which feature should you enable to reduce the number or unwanted IGMP reports processed by the IGMP querier?

Options:

A- Enable the IGMP flood setting on the static port for all multicast groups.

B- Enable the IGMP flood reports setting on the mRouter port.

C- Enable IGMP snooping proxy.

D- Enable IGMP flood unknown multicast traffic on the global setting.

Answer:

C

Question 2

Question Type: MultipleChoice

Which statement about the IGMP snooping querier when enabled on a VLAN is true?

Options:

A- Active multicast receiver entries are aging on each IGMP query sent on the VLAN

B- IGMP reports on the VLAN are forwarded to all switch ports.

C- The setting can only be enabled using the FortiSwitch CLI.

D- All other indirectly connected switches will be unable to get IGMP multicast traffic.

Answer:

D

Question 3

Question Type: MultipleChoice

Which statement about the configuration of VLANs on a managed FortiSwitch port is true?

Options:

A- Untagged VLANs must be part of the allowed VLANs: ingress and egress.

B- FortiSwitch VLAN interfaces are created only when FortiSwitch is managed by Forti-Gate.

C- The native VLAN is implicitly part of the allowed VLAN on the port.

D- Allowed VLANS expand the collision domain to the port.

Answer:

C

Question 4

Question Type: **MultipleChoice**

Which statement about using MAC, IP, and protocol-based VLANs on FortiSwitch is true?

Options:

A- It is a scalable and secure solution in comparison to other Layer 2 security measures.

B- FortiSwitch uses only the Ethernet type to assign traffic to VLANs.

C- It provides benefits that can be obtained when using 802.1X authentication.

D- Endpoints are required to use the same FortiSwitch port to remain members of the VLAN.

Answer:

C

Question 5

Question Type: **MultipleChoice**

To enhance service in emergency situations, to which LLDP-MED Type-Length-Values does Forti-Switch advertise to IP phones?

Options:

A- Network policy

B- Inventory management

C- Location

D- Power management

Answer:

B

Question 6

Question Type: MultipleChoice

Which two statements about DHCP snooping enabled on a FortiSwitch VLAN are true? (Choose two.)

Options:

A- Enabling DHCP snooping on a FortiSwitch VLAN ensures requests and replies are seen by all DHCP servers.

B- switch-controller-dhcp-snooping-verify-mac verifies the destination MAC address to protect against DHCP exhaustion attacks.

C- By default, all FortiSwitch ports are set to forward client DHCP requests to untrusted ports.

D- Settings related to DHCP option 82 are only configurable through the CLI

Answer:

C, D

Question 7

Question Type: MultipleChoice

What is the role of a device that is simultaneously functioning as both the distribution and core in the hierarchy network model?

Options:

A- POE with high density FortiSwitch

B- FortiGate managing FortiSwitch

C- FortiSwitch functioning as standalone

D- HA backup FortiGate managing FortiSwitch

Answer:

B

Question 8

Question Type: MultipleChoice

Which statement about the use of the switch port analyzer (SPAN) packet capture method is true?

Options:

A- Mirrored traffic can be sent across multiple switches.

B- SPAN can be configured only on a standalone FortiSwitch.

C- Traffic on the management interface can be mirrored and captured by the monitoring device.

D- The monitoring device must be connected to the same switch where the traffic is being mirrored

Answer:

C

Question 9

Question Type: **MultipleChoice**

In which two ways can you assign a FortiSwitch port to a VDOM using multi-tenancy setup? (Choose two.)

Options:

A- Switch the FortiLink interface to the target VDOM.

B- Remove the managed FortiSwitch and allocate ports directly on FortiSwitch.

C- Create a virtual port pool on the FortiGate CLI.

D- Assign a port to a VDOM directly on the managed FortiSwitch.

Answer:

C, D

Question 10

Question Type: **MultipleChoice**

How are the 'by VLAN redirect MAC address quarantine' mode and the 'by redirect MAC address quarantine' mode on FortiGate similar?

Options:

A- Both modes move quarantined devices to the quarantine VLAN.

B- Both modes require firewall policies to block inter-VLAN traffic.

C- Both modes add quarantined device MAC addresses to the blocked firewall address group.

D- Both modes block intra-VLAN traffic by FortiGate automatically.

Answer:

D

Question 11

Question Type: **MultipleChoice**

An administrator needs to deploy managed FortiSwitch devices in a remote location where multiple VLANs must be utilized to segment devices. No Layer 3 switch or router is present. The the only WAN connectivity is the router provided by the ISP connected to the public internet.

Which two items will the administrator need to use? (Choose two.)

Options:

A- A FortiSwitch interface connected to the ISP router configured with fortilink-13-mode enabled.

B- FortiSwitch and FortiGate devices configured with VXLAN interfaces.

C- FortiSwitch devices configured with NAT disabled.

D- FortiSwitch devices that have the required internal hardware for this configuration.

E- FortiSwitch and FortiGate devices configured with IPsec interfaces.

Answer:

B, C

Question 12

Question Type: MultipleChoice

How does FortiSwitch perform actions on ingress and egress traffic using the access control list (ACL)?

Options:

A- Only high-end FortiSwitch models support ACL.

B- ACL can be used only at the prelookup stage in the traffic processing pipeline.

C- Classifiers enable matching traffic based only on the VLAN ID.

D- FortiSwitch checks ACL policies only from top to bottom.

Answer:

D