N10-009$^{\text{Q\&As}}$

CompTIA Network+ Exam

Pass CompTIA N10-009 Exam with 100% Guarantee

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

QUESTION 1

An administrator is configuring a switch that will be placed in an area of the office that is accessible to customers. Which of the following is the best way for the administrator to mitigate unknown devices from connecting to the network?

A. SSE

B. ACL

C. Perimeter network

D. 802.1x

Correct Answer: D

802.1x is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. This ensures that only authorized devices can access the network, making it ideal for mitigating the risk of

unknown devices connecting to the network, especially in accessible areas. 802.1x Authentication: Requires devices to authenticate using credentials (e.g., username and password, certificates) before gaining network access. Access

Control: Prevents unauthorized devices from connecting to the network, enhancing security in public or semi-public areas. Implementation: Typically used in conjunction with a RADIUS server to manage authentication requests.

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Covers 802.1x and its role in network security.

Cisco Networking Academy: Provides training on implementing 802.1x for secure network access control.

Network+ Certification All-in-One uide: Explains the benefits and configuration of 802.1x authentication in securing network access.

QUESTION 2

A client wants to increase overall security after a recent breach. Which of the following would be best to implement? (Select two.)

A. Least privilege network access

B. Dynamic inventeries

C. Central policy management

D. Zero-touch provisioning

E. Configuration drift prevention

F. Subnet range limits

Correct Answer: AC

To increase overall security after a recent breach, implementing least privilege network access and central policy management are effective strategies. Least Privilege Network Access: This principle ensures that users and devices are

granted only the access necessary to perform their functions, minimizing the potential for unauthorized access or breaches. By limiting permissions, the risk of an attacker gaining access to critical parts of the network is reduced. Central

Policy Management: Centralized management of security policies allows for consistent and streamlined implementation of security measures across the entire network. This helps in quickly responding to security incidents, ensuring

compliance with security protocols, and reducing the chances of misconfigurations.

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Discusses network security principles, including least privilege and policy management. Cisco Networking Academy: Provides training on implementing security policies and access

controls.

Network+ Certification All-in-One uide: Covers strategies for enhancing network security and managing policies effectively.

QUESTION 3

A network administrator is connecting two Layer 2 switches in a network. These switches must transfer data in multiple networks.

Which of the following would fulfill this requirement?

A. Jumbo frames

B. 802.1Q tagging

C. Native VLAN

D. Link aggregation

Correct Answer: B

802.1Q tagging, also known as VLAN tagging, is used to identify VLANs on a trunk link between switches. This allows the switches to transfer data for multiple VLANs (or networks) over a single physical connection. This method ensures that

traffic from different VLANs is properly separated and managed across the network.References:

CompTIA Network+ study materials.

QUESTION 4

A company is implementing a wireless solution in a high-density environment.

Which of the following 802.11 standards is used when a company is concerned about device saturation and converage?

A. 802.11ac

B. 802.11ax

C. 802.11g

D. 802.11n

Correct Answer: B

802.11ax, also known as Wi-Fi 6, is designed for high-density environments and improves device saturation and coverage compared to previous standards. 802.11ac: While it offers high throughput, it is not optimized for high-density

environments as effectively as 802.11ax.

802.11ax (Wi-Fi 6): Introduces features like OFDMA, MU-MIMO, and BSS Coloring, which enhance performance in crowded environments, reduce latency, and increase the number of devices that can be connected simultaneously. 802.11g

and 802.11n: Older standards that do not offer the same level of efficiency or support for high device density as 802.11ax.

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Covers the 802.11 standards and their capabilities.

Cisco Networking Academy: Provides training on Wi-Fi technologies and best practices for high-density deployments.

Network+ Certification All-in-One uide: Discusses the various 802.11 standards and their applications in different environments.

QUESTION 5

An administrator wants to host services on the internet using an internal server. The server is configured with an RFC1918 address, and the administrator wants to make the services that are hosted on the server available on one of the company\\'s public IP addresses. Which of the following should the administrator configure to allow this access?

A. IPv6 tunneling

B. Virtual IP

C. Dual stack

D. EUI-64

Correct Answer: B

References

What is a Virtual IP Address (VIP)? - Definition from Techopedia IPv6 Tunneling - an overview | ScienceDirect Topics Dual Stack Definition [EUI-64 - an overview | ScienceDirect Topics]