Free Questions for N10-009 by certsinside

Shared by Livingston on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?

Options:

A- To encrypt sensitive data in transit

B- To secure the endpoint

C- To maintain contractual agreements

D- To comply with data retentin requirements

Answer:

A

Explanation:

The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user's device and the corporate network, ensuring that data is encrypted and protected

from interception.

Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks.

Data Protection: Essential for industries handling sensitive information, such as insurance brokerages, to protect customer data and comply with regulatory requirements.

Security: Enhances overall network security by providing secure remote access for employees.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses the role of VPNs in securing data in transit.

Cisco Networking Academy: Provides training on VPN technologies and their importance in data security.

Network+ Certification All-in-One Exam Guide: Explains VPN usage and its benefits in protecting sensitive information.

Question 2

Question Type: **MultipleChoice**

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?

Options:

A- SSE

B- ACL

C- Perimeter network

D- 802.1x

Answer:

D

Explanation:

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 Reference:

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 Exam Guide: Explains the benefits and configuration of 802.1x authentication in securing network access.

Question 3

Question Type: **MultipleChoice**

A storage network requires reduced overhead and increased efficiency for the amout of data being sent. Which of the following should an engineer likely configure to meet these requirements>?

Options:

A- Link speed

B- Jumbo frames

C- QoS

D- 802.1q tagging

Answer:

B

Explanation:

Jumbo frames are Ethernet frames with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes. Configuring jumbo frames can reduce overhead and increase efficiency in storage networks by allowing more data to be sent in each frame, thus reducing the number of frames needed to transmit the same amount of data.

Reduced Overhead: By sending larger frames, the relative overhead for headers and acknowledgments is reduced.

Increased Efficiency: Larger frames mean fewer packets to process, leading to better utilization of network bandwidth and improved performance in high-throughput environments like storage networks.

Configuration: Requires support from all devices in the network path, including switches and network interface cards (NICs).

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Explains jumbo frames and their benefits in reducing network overhead.

Cisco Networking Academy: Provides training on network optimization techniques, including the use of jumbo frames.

Network+ Certification All-in-One Exam Guide: Covers advanced Ethernet features, including jumbo frames and their configuration for improved network performance.

Question 4

Question Type: MultipleChoice

A newtwork administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?

Options:

A- A physical interface used for trunking logical ports

B- A physical interface used for management access

C- A logical interface used for the routing of VLANs

D- A logical interface used when the number of physical ports is insufficent.

Answer:

C

Explanation:

An SVI (Switched Virtual Interface) is a logical interface on a Layer 3-capable switch used to route traffic between VLANs. This is particularly useful in environments where voice and data traffic need to be separated, as each type of traffic can be assigned to different VLANs and routed accordingly.

SVI (Switched Virtual Interface): A virtual interface created on a switch for inter-VLAN routing.

VLAN Routing: Enables the routing of traffic between VLANs on a Layer 3 switch, allowing for logical separation of different types of traffic, such as voice and data.

Use Case: Commonly used in scenarios where efficient and segmented traffic management is required, such as in VoIP implementations.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses VLANs, SVIs, and their applications in network segmentation and routing.

Cisco Networking Academy: Provides training on VLAN configuration and inter-VLAN routing using SVIs.

Network+ Certification All-in-One Exam Guide: Covers network segmentation techniques, including the use of SVIs for VLAN routing.

Question 5

Question Type: MultipleChoice

Which of the following is an XML-based security concept that works by passing sensitve information about users, such as log-in information and attributes, to providers.

Options:

A- IAM

B- MFA

C- RADIUS

D- SAML

Answer:

D

Explanation:

Security Assertion Markup Language (SAML) is an XML-based standard used for exchanging authentication and authorization data between parties, particularly between an identity provider (IdP) and a service provider (SP). SAML is commonly used in Single Sign-On (SSO) solutions to pass sensitive user information, such as login credentials and attributes, securely between the identity provider and the service provider.

SAML (Security Assertion Markup Language): Facilitates web-based authentication and authorization, allowing users to access multiple services with a single set of credentials.

XML-based: Uses XML to encode the authentication and authorization data, ensuring secure transmission of user information.

Identity Federation: Enables secure sharing of identity information across different security domains, making it ideal for enterprise SSO solutions.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Covers authentication protocols, including SAML.

Cisco Networking Academy: Provides training on identity management and federation technologies.

Network+ Certification All-in-One Exam Guide: Explains SAML and its role in secure identity management and SSO.

Question 6

Question Type: **MultipleChoice**

Which of the following appliances provides users with an extended footprint that allows connections from multiple devices within a designated WLAN?

Options:

A- Router

B- Switch

C- Access point

D- Firewall

Answer:

C

Explanation:

An access point (AP) provides users with an extended footprint that allows connections from multiple devices within a designated Wireless Local Area Network (WLAN).

Router: Typically used to connect different networks, not specifically for extending wireless coverage.

Switch: Used to connect devices within a wired network, not for providing wireless access.

Access Point (AP): Extends wireless network coverage, allowing multiple wireless devices to connect to the network.

Firewall: Primarily used for network security, controlling incoming and outgoing traffic based on security rules, not for providing wireless connectivity.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Explains the roles and functions of network appliances, including access points.

Cisco Networking Academy: Provides training on deploying and managing wireless networks with access points.

Network+ Certification All-in-One Exam Guide: Covers network devices and their roles in creating and managing networks.

Question 7

Question Type: MultipleChoice

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?

Options:

A- 802.11ac

B- 802.11ax

C- 802.11g

D- 802.11n

Answer:

B

Explanation:

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 Reference:

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.

Question 8

Question Type: MultipleChoice

Which of the following ports is used for secure email?

Options:

A- 25

B- 110

C- 143

D- 587

Answer:

D

Explanation:

Port 587 is used for secure email submission. This port is designated for message submission by mail clients to mail servers using the SMTP protocol, typically with STARTTLS for encryption.

Port 25: Traditionally used for SMTP relay, but not secure and often blocked by ISPs for outgoing mail due to spam concerns.

Port 110: Used for POP3 (Post Office Protocol version 3), not typically secured.

Port 143: Used for IMAP (Internet Message Access Protocol), which can be secured with STARTTLS or SSL/TLS.

Port 587: Specifically used for authenticated email submission (SMTP) with encryption, ensuring secure transmission of email from clients to servers.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses email protocols and ports, including secure email transmission.

Cisco Networking Academy: Provides training on securing email communications and the use of appropriate ports.

Network+ Certification All-in-One Exam Guide: Explains email protocols, ports, and security considerations for email transmission.