7.6 Module Quiz

Date: 12/6/2025, 10:42:29 AM

Time Spent: 17:46

Score: 90%

Passing Score: 80%

Question 1 ✓ Correct

Company employees are accessing the same resources on the internet many times a day. As the network administrator, you configure a solution that forwards traffic to and from the internet and also caches content to improve performance and reduce bandwidth consumption.

What solution are you implementing?

● Proxy server ✓ Correct

○ Load balancer

○ NAT

○ UTM

Explanation

A proxy server takes a whole HTTP request from a client, checks it, and then forwards it to and from the destination server on the internet. It also caches content to improve performance.

In a port-based or overloaded network address translation (NAT), a NAT device translates between the private IP addresses used on the LAN and the public IP address on the router's WAN interface.

A unified threat management (UTM) appliance enforces a variety of security policies and controls, combining the work of multiple security functions.

A load balancer distributes client requests across server nodes in a farm or pool and can deploy in any situation where multiple servers are providing the same function.

Related Content

7.2.1 Proxy Servers

7.2.4 Load Balancers

resources\questions\q_proxy_servers_01.question.xml

Question 2 ✓ Correct

Your company is experiencing issues with data retrieval speed and efficiency. The current system relies heavily on spreadsheets for data storage, which has become cumbersome and limits the ability to generate complex reports.

As an IT specialist, you are tasked with recommending a solution to improve data management and retrieval.

Which of the following solutions would BEST address the company's needs?

● Transition to using a database server to store, organize, and manage data. ✓ Correct

○ Use a file/print server to manage data storage and facilitate easier access to shared resources.

○ Set up a mail server to handle data storage and improve communication efficiency.

○ Implement a web server to host the company's website and improve data retrieval speed.

Explanation

A database server is the appropriate solution for the scenario described. It is specifically designed to handle large volumes of structured and unstructured data, enabling efficient data retrieval, querying, and reporting, which addresses the company's needs for improved data management.

A web server is designed to host websites and handle HTTP requests. It is not suitable for improving data retrieval speed related to data management and reporting. The issue described is related to data storage and management, not web hosting.

A mail server is used for managing email communication and storage, not for general data management and retrieval. It would not address the issues related to data retrieval speed and efficiency described in the scenario.

While a file/print server can manage shared access to disk resources, it does not provide the querying and reporting capabilities needed to improve data retrieval speed and efficiency. A database server is better suited for these tasks.

Related Content

7.1.2 Database Servers

resources\questions\q_database_servers_02.question.xml

Question 3 ✓ Correct

What is a common cause of reduced network speed in a cabled link?

○ Outdated VoIP application

○ Weak wireless signal strength

● Mismatched duplex settings ✓ Correct

○ Incorrect network password

Explanation

Mismatched duplex settings on the network adapter and switch port can cause reduced network speed. Both the network adapter and switch port should be set to auto-negotiate to ensure proper communication.

An incorrect network password would prevent a device from connecting to the network entirely rather than causing reduced network speed. This issue is more relevant to wireless network troubleshooting, not cabled links.

Weak signal strength is a problem specific to wireless networks, not cabled links.

An outdated VoIP application would affect the quality of VoIP calls, not the overall network speed. This issue is related to troubleshooting VoIP, not general network speed issues in cabled links.

Related Content

7.3.2 Troubleshoot Network Speed Issues

resources\questions\q_troubleshoot_network_speed_issues_02.question.xml

Question 4 ✓ Correct

You are a network administrator tasked with configuring file sharing on a Windows network. You need to ensure that the file sharing protocol you use is secure and compatible with modern Windows systems.

Which of the following actions should you take to achieve this goal?

○ Disable SMB3 and enable NetBIOS over TCP/IP to enhance security and compatibility.

● Ensure that SMB3 is enabled and SMB1 is disabled on all networked devices. ✓ Correct

○ Enable SMB1 on all networked devices to ensure compatibility with older systems.

○ Use FTP instead of SMB for file sharing, as it is inherently more secure and widely supported.

Explanation

Enabling SMB3 ensures the use of a secure and current version of the protocol while disabling SMB1 mitigates security risks.

Enabling SMB1 is not recommended as it has serious security vulnerabilities. SMB1 is disabled by default on current Windows versions due to these vulnerabilities.

Disabling SMB3 and enabling NetBIOS over TCP/IP would not enhance security. NetBIOS over TCP/IP is considered obsolete and poses a security risk.

FTP is not inherently more secure than SMB. In fact, plain FTP is unencrypted and poses a high-security risk. SMB3 is a more secure choice for file sharing on Windows networks.

Related Content

7.1.1 File/Print Servers

10.1.13 Scanner Configuration

resources\questions\q_file_print_servers_03.question.xml

Question 5 ✓ Correct

A user reports intermittent connectivity and slow transfer speeds on the office Wi-Fi network. Upon investigation, you find that the user's device is connected to the 2.4 GHz band, while other devices connected to the 5 GHz band are not experiencing any issues.

Additionally, the Wi-Fi analyzer shows that the 2.4 GHz band is heavily congested with multiple overlapping networks.

What is the BEST course of action to resolve the issue?

○ Replace the wireless access point with a newer model that supports higher speeds.

● Configure the user's device to connect to the 5 GHz band instead of the 2.4 GHz band. ✓ Correct

○ Adjust the channel settings on the wireless access point to a less congested channel in the 2.4 GHz band.

○ Move the user's device closer to the wireless access point to improve the signal strength.

Explanation

The 5 GHz band is less congested and offers better performance in terms of speed and reliability compared to the 2.4 GHz band, especially in environments with many overlapping networks. Configuring the user's device to connect to the 5 GHz band will resolve the issue of congestion and improve connectivity. This is the most effective solution based on the analysis of the problem.

While adjusting the channel settings can reduce interference in the 2.4 GHz band, it does not address the fundamental issue of congestion caused by multiple overlapping networks. Switching to the 5 GHz band is a more effective solution in this scenario.

Moving closer to the access point might improve signal strength, but it does not resolve the issue of congestion in the 2.4 GHz band. The problem is not related to signal strength but to interference and congestion.

Replacing the access point is unnecessary in this scenario because the issue is related to the user's device being connected to the congested 2.4 GHz band. The existing access point already supports the 5 GHz band, which is a viable solution. Replacing the hardware would be an excessive and costly approach.

Related Content

- 5.4.11 Long-Range Fixed Wireless
- 7.3.4 Troubleshoot Wireless Issues
- 7.3.6 Troubleshoot Limited Connectivity

resources\questions\q_troubleshoot_wireless_issues_04.question.xml

Question 6 ✓ Correct

Your organization uses a legacy system that is crucial for processing customer transactions.

Recently, an audit revealed that this system poses significant security vulnerabilities. You need to analyze the situation and decide on a strategic approach to address these vulnerabilities while ensuring business continuity.

Which of the following actions would BEST balance security and operational needs?

- ● Conduct a risk assessment to identify specific vulnerabilities and develop a targeted mitigation plan. ✓ Correct
- ○ Outsource the management of the legacy system to a third-party vendor specializing in legacy systems.
- ○ Ignore the audit findings, as the system has been operating without issues for years.
- ○ Immediately shut down the legacy system to prevent any potential security breaches.

Explanation

Conducting a risk assessment allows you to analyze the specific vulnerabilities of the legacy system and develop a targeted mitigation plan. This approach balances security needs with operational requirements by addressing vulnerabilities without disrupting business continuity.

Shutting down the legacy system immediately could disrupt business operations and is not a balanced approach. While it addresses security concerns, it fails to consider the operational impact and continuity of customer transactions.

Ignoring the audit findings is not a responsible approach. The security risks associated with legacy systems, and failing to address these vulnerabilities could lead to exploitation and potential breaches.

While outsourcing might provide some expertise in managing legacy systems, it does not directly address the specific vulnerabilities identified in the audit. A targeted mitigation plan based on a risk assessment would be more effective in balancing security and operational needs.

Related Content

resources\questions\q_legacy_systems_04.question.xml

Question 7 ✓ Correct

Which of the following all-in-one security appliance (UTM) functions detects intrusions and alerts the network but does not block traffic?

○ Intrusion protection

○ Anti-spam

○ VPN

● Intrusion detection ✓ Correct

Explanation

Intrusion detection detects intrusions and alerts the network. However, it does not block traffic.

Intrusion protection detects and blocks network traffic that is not recognized by its profile.

Anti-spam is designed to detect and block certain types of email.

A VPN encrypts traffic over a secure network. However, a VPN does not block traffic.

Related Content

resources\questions\q_spam_gateways_and_unified_threat_management_03.question.xml

Question 8 ✓ Correct

You are a network administrator tasked with securing your company's website to ensure that all data exchanged between your clients and the server is encrypted.

You need to implement a protocol that will provide this security by encrypting the data and verifying the server's identity.

Which of the following actions should you take to achieve this goal?

○ Set up the website to use FTP for data transmission and ensure that it operates over port 21.

○ Enable NetBIOS over TCP/IP on the web server to allow secure data transmission.

○ Configure the website to use HTTP and ensure all data is transmitted over port 80.

● Install a digital certificate from a trusted Certificate Authority (CA) on the web server and configure the website to use HTTPS. ✓ Correct

Explanation

By installing a digital certificate and configuring the website to use HTTPS, you ensure that data is encrypted and the server's identity is verified, providing the necessary security for data exchange.

HTTP does not encrypt data, leaving it vulnerable to interception. Port 80 is used for HTTP, which does not provide the security features required in the scenario.

FTP, especially when operating over port 21, does not inherently provide encryption for data transmission. The scenario requires encrypted data exchange, which FTP does not fulfill without additional security measures like FTPS or SFTP.

NetBIOS over TCP/IP is not related to securing web data transmission. It is an outdated protocol for network communication and does not provide the encryption and server identity verification required by the scenario.

Related Content

- 6.3.6 Well-Known Ports
- 7.1.4 Hypertext Transfer Protocol Secure

resources\questions\q_hypertext_transfer_protocol_secure_02.question.xml

Question 9 ✓ Correct

You are an IT technician troubleshooting a limited connectivity issue for a single user in an office environment. The user reports that they cannot access the internet but can still access local network resources.

You check the network adapter and see that it has an IP address in the range of 169.254.x.x.

What is the MOST likely cause of the issue, and what should you do to resolve it?

○ The user's computer has a faulty network adapter. Replace the network adapter.

○ The switch port is misconfigured. Reconfigure the switch port to the correct VLAN.

● The DHCP server is not assigning an IP address. Manually configure a valid IP address for the user. ✓ Correct

○ The network cable is damaged. Replace the cable with a known good one.

Explanation

When a device has an IP address in the range of 169.254.x.x, it indicates that the device has assigned itself an Automatic Private IP Addressing (APIPA) address because it could not obtain an IP address from a DHCP server. This is a common cause of limited connectivity issues. Manually configuring a valid IP address or troubleshooting the DHCP server to restore automatic IP assignment will resolve the issue.

While a damaged network cable can cause connectivity issues, it would typically result in no connectivity at all, not limited connectivity. The presence of an APIPA address indicates that the physical connection is intact, but the DHCP server is not reachable. Replacing the cable is unnecessary in this scenario.

A faulty network adapter would likely result in no connectivity or the inability to establish a link with the network. Since the user can access local network resources and has an APIPA address, the network adapter is functioning correctly. Replacing it would not resolve the issue.

A misconfigured switch port, such as one assigned to the wrong VLAN, could cause connectivity issues. However, this would typically prevent access to both local and internet resources. The fact that the user can access local resources suggests that the switch port is correctly configured. The issue lies with the DHCP server, not the switch port.

Related Content

- 7.3.1 Troubleshoot Wired Connectivity
- 7.3.6 Troubleshoot Limited Connectivity

resources\questions\q_troubleshoot_limited_connectivity_02.question.xml

Question 10 ✓ Correct

A company is experiencing poor VoIP call quality, including jitter and delays. You analyze the network and find that the issue occurs during peak usage times when multiple devices are streaming videos and downloading large files.

The company uses a SOHO router without advanced traffic management features.

What is the MOST likely cause of the VoIP issues?

○ The Internet Service Provider (ISP) is throttling VoIP traffic during peak hours.

○ The VoIP phones are outdated and cannot handle modern network traffic.

● The SOHO router lacks Quality of Service (QoS) configuration to prioritize VoIP traffic. ✓ Correct

○ The VoIP application is not compatible with the SOHO router.

Explanation

The lack of QoS on the SOHO router is the most likely cause of the VoIP issues. Without QoS, the router cannot prioritize VoIP traffic over other types of data, such as video streaming or file downloads. This results in jitter and delays during peak usage times, as VoIP packets are delayed or dropped due to network congestion.

VoIP applications are generally compatible with most routers, including SOHO models. The issue here is not compatibility but the router's inability to prioritize VoIP traffic during periods of high network usage.

The age of the VoIP phones is not the issue in this scenario. The problem lies in the network's inability to prioritize VoIP traffic, which is unrelated to the phones themselves.

While ISP throttling could theoretically cause issues, there is no evidence in this scenario to suggest that the ISP is specifically targeting VoIP traffic. The described problem is more likely due to the lack of QoS on the SOHO router.

Related Content

7.3.5 Troubleshoot VoIP Issues

resources\questions\q_troubleshoot_voip_issues_05.question.xml

Question 11 ✕ Incorrect

A company is experiencing slow network speeds, and the issue appears to affect multiple users connected to the same switch.

Upon reviewing the switch's configuration, you notice a high number of damaged frames being reported.

What is the MOST likely cause of the issue?

○ Malware infection on one of the connected hosts

● Mismatched duplex settings on the network adapter and switch port ✕ Incorrect

○ An outdated driver on a single user's network adapter

○ External interference affecting the cabling ✓ Correct

Explanation

External interference, such as from nearby power lines, fluorescent lighting, or motors, can cause issues like damaged frames in the cabling. This is the most likely cause when multiple users connected to the same switch are affected, and the switch reports damaged frames.

Mismatched duplex settings would typically affect the speed of a single connection rather than multiple users connected to the same switch. The issue described in the scenario is broader in scope.

While malware can cause network performance issues, it would not directly result in damaged frames being reported by the switch. Damaged frames are more indicative of physical or environmental issues with the cabling.

An outdated driver would only affect the performance of the specific user's connection. It would not cause network-wide issues or result in damaged frames being reported by the switch.

Related Content

7.3.2 Troubleshoot Network Speed Issues

resources\questions\q_troubleshoot_network_speed_issues_04.question.xml

Question 12 ✓ Correct

A security technician is installing a doorbell/video entry system for a customer so that the customer can see and communicate with people who come to their home when they aren't there.

What kind of device is the doorbell/video entry system?

● Smart device ✓ Correct

○ Zigbee

○ OT

○ Hub and control system

Explanation

The doorbell/video entry system is a smart device, which is a device or appliance that users can configure and monitor over an IoT network.

Zigbee is a wireless technology. While the control system is typically joined to the Wi-Fi network, smart devices may use other wireless technologies, such as Z-Wave or Zigbee, to exchange data via the hub.

A hub and control system are each required by IoT devices. The hub facilitates wireless networking while the control system operates the device.

An embedded system network is known as an operational technology (OT) network, to distinguish it from an IT network.

Related Content

7.2.7 Internet of Things Devices

resources\questions\q_internet_of_things_devices_01.question.xml

Question 13 — Partial

Which of the following functions are performed by proxy servers? (Select two.)

- ☑ Block unwanted packets from entering your private network. ✗ Incorrect
- □ Filter unwanted email.
- □ Store client files.
- □ Cache web pages. ✓ Correct
- ☑ Block employees from accessing certain websites. ✓ Correct

Explanation

A proxy, or proxy server, stands between client computers and web servers. You can use a proxy server to prevent access to specific websites or to cache (save) frequently used web pages.

When a proxy receives a request from the client, the proxy checks to verify that the client is allowed access to the website. If they are, the proxy then checks its cache to see if the requested page is there. If the page is already cached, the proxy server fulfills the request by displaying the requested page from the cache rather than retrieving it from the internet. Receiving a web page from a local proxy server is much faster than downloading the page from the internet.

Related Content

7.2.1 Proxy Servers

7.2.4 Load Balancers

resources\questions\q_proxy_servers_05.question.xml

Question 14 ✓ Correct

Your organization is currently using flat file spreadsheets to manage customer data, but as the business grows, the limitations of this system are becoming apparent. The data is becoming increasingly difficult to manage, and generating meaningful reports is time-consuming and error-prone.

You are asked to analyze the situation and recommend a solution that will address these challenges.

Which of the following options would BEST resolve the issues with data management and reporting?

- ○ Set up a mail server to centralize communication and improve the accuracy of customer data management.
- ● Implement a relational database server to enable structured data storage and efficient querying. ✓ Correct
- ○ Use a file/print server to organize customer data into shared folders, making it easier to access and report on.
- ○ Deploy a web server to host the company's internal applications, which will streamline data management and reporting processes.

Explanation

A relational database server allows for structured data storage, which facilitates efficient querying and complex reporting. It addresses the limitations of flat file spreadsheets by enabling better data organization and management.

A web server is primarily used for hosting web applications and does not inherently improve data management or reporting capabilities. It does not address the core issue of managing and querying customer data efficiently.

A mail server is designed for managing email communication, not for data storage or reporting. It would not resolve the issues related to data management and reporting described in the scenario.

While a file/print server can facilitate shared access to data, it does not provide the structured data storage and querying capabilities needed for efficient reporting. A relational database server is better suited for these tasks.

Related Content

7.1.2 Database Servers

resources\questions\q_database_servers_03.question.xml

Question 15 ✓ Correct

You are an IT administrator setting up email access for remote employees who need to download their emails to their local devices and read them offline.

Which protocol would you apply to configure their email clients to meet this requirement?

○ Simple Mail Transfer Protocol (SMTP)

○ Internet Message Access Protocol (IMAP)

● Post Office Protocol (POP3) ✓ Correct

○ Hypertext Transfer Protocol Secure (HTTPS)

Explanation

POP3 is designed to download emails from the server to a local device, allowing users to read their emails offline. This protocol is ideal for remote employees who need to access their emails without a continuous internet connection, as it downloads the emails to their local devices.

SMTP is primarily used for sending emails from a client to a server or between servers. It is not used for downloading emails to a local device for offline access. Therefore, it does not meet the requirement of allowing remote employees to download and read emails offline.

IMAP allows users to access and manage their emails directly on the email server, providing synchronization across multiple devices. While it supports offline access to some extent, it is not primarily designed for downloading emails to a local device for offline reading. IMAP keeps emails on the server, which is not the primary requirement in this scenario.

HTTPS is used for secure web browsing and is not related to email retrieval or management. It does not apply to configuring email clients for downloading emails, making it irrelevant to the scenario described.

Related Content

7.1.5 Mail Servers

7.1.6 Mailbox Servers

resources\questions\q_mailbox_servers_03.question.xml