7.2.8 Lesson Review

Date: 11/30/2025, 2:58:40 PM

Time Spent: 11:05

Score: 90%

Passing Score: 80%

Question 1 ✓ Correct

A company has recently experienced performance issues with its web application during peak usage times. The application is hosted on multiple servers, but users report slow response times and occasional timeouts.

As a network administrator, you are tasked with resolving these issues.

Which solution would BEST address the company's performance problems?

- ○ Set up a spam gateway to filter out unwanted email traffic.
- ○ Deploy an intrusion detection system to monitor and alert on suspicious activities.
- ◉ Implement a load balancer to distribute incoming requests evenly across all servers. ✓ Correct
- ○ Install a firewall to block unnecessary traffic and reduce server load.

Explanation

Implementing a load balancer will distribute incoming client requests evenly across all available servers. This helps to manage the load more effectively, preventing any single server from becoming overwhelmed and improving overall application performance during peak usage times.

While a firewall can block unnecessary traffic, it does not address the distribution of legitimate client requests across multiple servers. The primary issue is related to load distribution, which is best handled by a load balancer.

An intrusion detection system (IDS) focuses on monitoring and alerting for suspicious activities, not on improving performance or distributing client requests. The performance issue is not related to security threats but to load management.

A spam gateway is designed to filter email traffic, which is unrelated to the performance issues of a web application. The problem lies in managing web application requests, not email traffic.

Related Content

7.2.1 Proxy Servers

7.2.4 Load Balancers

resources\questions\q_load_balancers_04.question.xml

Question 2 Correct

What is a key characteristic of a legacy system?

- A legacy system is typically used for modern applications and services.
- A legacy system is always supported by its vendor with regular updates.
- A legacy system is designed to integrate seamlessly with new technologies.
- A legacy system is no longer directly supported by its vendor. ✓ Correct

Explanation

A legacy system is one that is no longer directly supported by its vendor. This lack of support is a defining characteristic of legacy systems and poses security risks.

A legacy system is defined by the fact that it is no longer directly supported by its vendor. This means that regular updates and support are not provided, which is a significant risk factor for such systems.

Legacy systems are generally used for older applications and services that are too complex or costly to migrate to modern platforms. They are not typically associated with modern applications.

Legacy systems often do not integrate well with new technologies. They are typically retained because they perform specific functions that are difficult to replace, not because they work well with modern systems.

Related Content

resources\questions\q_legacy_systems_02.question.xml

Question 3 ✓ 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 4 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 5 ✓ Correct

You are setting up a smart home system that includes smart lightbulbs, a smart thermostat, and a video doorbell. You want to control all these devices remotely using your smartphone.

Which component is essential for integrating these devices into a cohesive Internet of Things (IoT) network?

- (●) A hub/control system to facilitate communication and control of the devices ✓ Correct
- ( ) A high-capacity data storage server to save all device settings and logs
- ( ) A powerful router to provide high-speed internet to each device
- ( ) A backup power supply to ensure devices remain operational during power outages

Explanation

A hub/control system is essential for integrating IoT devices into a cohesive network. It facilitates communication between devices and allows you to control them remotely using your smartphone.

While data storage can be useful for logging and settings, it is not essential for integrating and controlling IoT devices. The primary need is for communication and control, not storage.

Although a router is important for internet connectivity, the key component for integrating and controlling IoT devices is a hub/control system, not just internet access.

While a backup power supply can be beneficial for maintaining operation during outages, it is not essential for the integration and control of IoT devices in a network. The focus is on communication and control.

Related Content

7.2.7 Internet of Things Devices

resources\questions\q_internet_of_things_devices_03.question.xml

Question 6 ✕ Incorrect

How do embedded systems within a Supervisory Control and Data Acquisition (SCADA) system typically communicate with field devices?

- ◯ Through wireless communication using Wi-Fi technology
- ◯ Through direct physical connections using USB cables
- ◯ By utilizing WAN communications such as cellular or satellite links ✓ Correct
- ◉ Via local area network (LAN) connections using Ethernet cables ✕ Incorrect

Explanation

SCADA systems typically use WAN communications, such as cellular or satellite, to link the SCADA server to field devices. This allows for communication over large distances, which is typical for SCADA systems managing multiple-site industrial control systems.

SCADA systems typically manage large-scale operations where direct physical connections like USB cables are impractical due to distance and scale.

SCADA systems often require communication over long distances, which LAN connections using Ethernet cables are not suited for. WAN communications are more appropriate for such scenarios.

Wi-Fi technology is generally used for shorter-range communication and is not typically employed for the long-distance communication required by SCADA systems, which instead use WAN communications like cellular or satellite links.

Related Content

7.2.6 Embedded Systems and SCADA
resources\questions\q_embedded_systems_and_scada_03.question.xml

Question 7 ✓ 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 8 Correct

An energy company is upgrading its systems across multiple sites. The company would like to control the systems with software that communicates with the current programmable logic controllers (PLCs) and new RTUs.

What kind of system is the company upgrading to?

- (●) SCADA ✓ Correct
- ( ) OT
- ( ) Embedded system
- ( ) ICS

Explanation

The company is upgrading to a supervisory control and data acquisition (SCADA) system, which will take the place of a control server in large-scale, multiple-site ICSs.

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

An embedded system is an electronic device that performs a specific, dedicated function. Embedded systems might typically have operated within a closed network.

An industrial control system (ICS) provides mechanisms for workflow and process automation. An ICS controls machinery used in critical infrastructures, such as power and water suppliers.

Related Content

7.2.6 Embedded Systems and SCADA

resources\questions\q_embedded_systems_and_scada_01.question.xml

Question 9 ✓ Correct

A local dentist has contracted with you to implement a network in her new office. Because of security concerns related to patient privacy laws, she has asked that the new network meet the following criteria and be cost-effective:

- No one from the internet should be able to access her internal network.
- Email messages should be scanned for spam, phishing attacks, and malware before they reach users' workstations.
- Employees' access to non-work-related websites, especially sites that contain inappropriate content, should be blocked.
- A system should be put in place to detect and prevent external attacks on her network.

Which of the following would BEST meet your client's criteria?

- ○ Implement an email security appliance.
- ○ Implement a content filter.
- ○ Implement an intrusion prevention system (IPS).
- ◉ Implement an all-in-one UTM security appliance. ✓ Correct
- ○ Implement a firewall.

Explanation

The network criteria specified by your client require several different network devices to be implemented, including a firewall, an email scanner, a content filter, and an intrusion prevention system. The most cost-effective way to best meet your client's criteria would be an all-in-one UTM security appliance.

While you could purchase each device separately, the cost of doing so would probably be quite high. Because you are working with a small business, an all-in-one security appliance that includes all of these functions in a single device would be more cost-effective and easier for you to manage.

Related Content

resources\questions\q_spam_gateways_and_unified_threat_management_02.question.xml

Question 10 ✓ Correct

As a network administrator for your company, you want to set up a network device that manages traffic leaving and entering your network from the outside.

Which of the following proxy server configurations would BEST meet your requirements?

- ○ Transparent proxy
- ◉ Non-transparent proxy ✓ Correct
- ○ VPN
- ○ Content filter

Explanation

A proxy server can operate as a non-transparent service, in which the client must be configured with the IP address and service port (often 8080 by convention) of the proxy server.

A content filter is a role of a proxy server that is designed to block traffic by regulating incoming and outgoing connection requests. This prevents users from accessing websites they should not have access to.

A proxy server can operate as a transparent service, in which the client requires no special configuration.

A VPN allows users to connect to the internet anonymously. All data is encrypted, and not even the ISP can see the contents of the traffic.

Related Content

7.2.1 Proxy Servers

7.2.4 Load Balancers

resources\questions\q_proxy_servers_04.question.xml