Chp 9 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/26/2022 11:17:41 am • Time spent: 12:02

Score: 100% Passing Score: 80%

Question 1: ✓ Correct

Network engineers have the option of using software to configure and control the network rather than relying on individual static configuration files that are located on each network device.

Which of the following is a relatively new technology that allows network and security professionals to use software to manage, control, and make changes to a network?

- ➡ ● Software-defined networking (SDN)
- ○ Control layer networking
- ○ Infrastructure software networking
- ○ Load balancing software

EXPLANATION

Software-defined networking (SDN) is a relatively new technology that allows network and security professionals to manage, control, and make changes to a network. Network engineers are able to use software to configure and control the network rather than relying on individual static configuration files that are located on each network device.

The Control layer is one of three layers that comprise software defined networking. The other layers are the Application layer and the Physical layer. Load balancers can be a component of the Application layer. The Physical layer can also be referred to as the Infrastructure layer.

REFERENCES

9.3.3 SDN Facts

q_sdn_software_secp7.question.fex

Question 2: ✓ Correct

Which of the following cloud storage access services acts as a gatekeeper, extending an organization's security policies into the cloud storage infrastructure?

○ A web service application programming interface

➡ ● A cloud-access security broker

○ A co-located cloud computer service

○ A cloud storage gateway

EXPLANATION

A cloud-access security broker (CASB) may act as a gatekeeper, extending an organization's security policies into the cloud storage infrastructure. A CASB focuses on the visibility of company data, regulation compliance, user access, and data security through encryption and loss prevention.

Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API), or by applications that utilize the API, such as cloud desktop storage (in other words, cloud storage gateways or web-based content management systems).

REFERENCES

▷ 9.4.3 Cloud Computing Security Issues

☰ 9.4.5 Cloud Storage Security Facts

☰ 9.5.5 Cloud Security Solutions Facts

q_cloud_stor_casb_secp7.question.fex

Question 3: ✓ Correct

Which of the following does the Application layer use to communicate with the Control layer?

○ Controllers

➡ ● Northbound APIs

○ These layers do not communicate

○ Southbound APIs

EXPLANATION

The Application layer communicates with the Control layer through what is called the northbound interface. These are sometimes called northbound APIs.

The controller is just a software platform that contains other applications. It can be thought of as the network's operating system.

The individual networking devices on the Physical layer use southbound APIs to communicate with the control plane and vice versa.

The Application and Control layers do communicate.

REFERENCES

9.3.3 SDN Facts

q_sdn_north_secp7.question.fex

Question 4: ✓ Correct

Which of the following Intune portals is used by end users to manage their own account and enroll devices?

- ○ Admin portal
- ➡ ● Company portal
- ○ Add Intune Users
- ○ Account portal

EXPLANATION

The Company portal is used by end users to manage their own account and enroll devices.

The Admin portal is used to manage enrolled devices and policies.

Add Intune Users is a configuration task that is completed in the Account portal.

The Account portal is used to manage subscriptions, users, groups, and domains.

REFERENCES

9.6.4 Enforcing Mobile Device Security Facts

q_mbl_dec_sec_portal_secp7.question.fex

Question 5: ✓ Correct

Which of the following is an advantage of a virtual browser?

- ○ Filters internet content based on ratings
- ○ Prevents adware and spyware that monitor your internet activity
- ➡ ◉ Protects the host operating system from malicious downloads
- ○ Prevents phishing and drive-by downloads

EXPLANATION

A virtual browser operates within a security sandbox that keeps activities within the browser from affecting the rest of the system. For example, malware downloaded by the virtual browser is limited to the security sandbox and cannot harm the operating system.

The virtual browser does not prevent adware, spyware, or phishing. These threats are still possible within the virtual browser. However, if malware is installed within the virtual session, the malware cannot harm the rest of the system, and the virtual browser can be easily restored to remove the malicious software.

REFERENCES

9.1.3 Virtualization Facts

q_virt_browser_02_secp7.question.fex

Question 6: ✓ Correct

The IT manager has tasked you with installing new physical machines. These computer systems are barebone systems that simply establish a remote connection to the data center to run the user's virtualized desktop.

Which type of deployment model is being used?

- ○ PaaS
- ○ Thick client
- ➡ ● Thin client
- ○ IaaS

EXPLANATION

This type of deployment is often referred to as a thin client deployment. This deployment utilizes virtual desktop infrastructure (VDI) to virtualize a user's desktop. The client machine is essentially only used to connect to the high-end machines in the data center.

IaaS delivers infrastructure to the client, such as processing, storage, networks, and virtualized environments.

PaaS delivers everything a developer needs to build an application.

Traditional deployments, where most of the processing load is handled by the local workstation, are called thick client deployments.

REFERENCES

9.4.4 Cloud Computing Facts

q_cloud_comp_thin_secp7.question.fex

Question 7: ✓ Correct

Which of the following provides the network virtualization solution called XenServer?

○ VMWare

○ Microsoft

➡ ● Citrix

○ Cisco

EXPLANATION

Citrix provides the virtualization solution called XenServer, also referred to as Citrix Hypervisor.

Microsoft provides a virtualization solution called Hyper-V Network Virtualization.

VMWare provides a virtualization solution called ESXi.

Cisco does not provide a virtualization solution but does offer a vSwitch platform called Nexus 1000v.

REFERENCES

9.2.4 Virtualization Implementation Facts

q_virt_impl_citrix_secp7.question.fex

Question 8: ✓ Correct

Which of the following mobile device security considerations disables the ability to use the device after a short period of inactivity?

- ○ Remote wipe
- ○ GPS
- ○ TPM
- ➡ ● Screen lock

EXPLANATION

A lockout (or screen lock) disables the ability to use the device after a short period of inactivity. The correct password or personal identification number (PIN) unlocks the device.

Remote wipe, also known as sanitization, remotely clears specific, sensitive data on a mobile device. This task is also useful if you are assigning the device to another user or after multiple incorrect password or PIN entries. Data encryption also ensures data confidentiality on the device. Voice encryption (on mobile phones) ensures data confidentiality during transit. Global Positioning System (GPS) tracking can assist in a device's recovery by displaying its current location. Trusted Platform Module (TPM) is a hardware chip on the motherboard that can generate and store cryptographic keys to check the integrity of startup files and components.

REFERENCES

9.6.2 Mobile Device Connection Facts

q_mbl_dev_conn_lock_secp7.question.fex

Question 9: ✓ Correct

What is a virtual LAN that runs on top of a physical LAN called?

○ VMM

○ VFA

➡ ◉ VAN

○ VLAN

EXPLANATION

A virtual area network (VAN) is a virtual LAN running on top of a physical LAN. This configuration enables guest virtual machines on separate physical hosts to communicate.

VLANs allow several physical LANs to function as a single logical LAN.

A VFA is a virtual firewall appliance. This is software that functions as a network firewall device.

A virtual machine monitor is software, firmware, or hardware that creates and runs virtual machines. This is also known as a hypervisor.

REFERENCES

9.2.5 Virtual Networking Facts

q_virt_net_van_secp7.question.fex

Question 10: ✓ Correct

You have a development machine that contains sensitive information relative to your business. You are concerned that spyware and malware might be installed while users browse websites, which could compromise your system or pose a confidentiality risk.

Which of the following actions would BEST protect your system?

- ➡ ● Run the browser within a virtual environment.
- ○ Configure the browser to block all cookies and pop-ups.
- ○ Change the security level for the internet zone to High.
- ○ Run the browser in protected mode.

EXPLANATION

To best protect your system, run the browser in a virtual environment. Virtualization creates an environment that is logically separated from the main system. Any problems that occur within the virtual environment are contained within that environment and do not affect the rest of the system.

REFERENCES

9.1.3 Virtualization Facts

q_virt_browser_01_secp7.question.fex

Question 11: ✓ Correct

Cloud storage is a virtual service, so the infrastructure is the responsibility of the storage provider. Access control should be set as a local file system would be, with no need for the provider to have access to the stored data.

You are implementing the following measures to secure your cloud storage:

- Verify that security controls are the same as in a physical data center.
- Use data classification policies.
- Assign information into categories that determine storage, handling, and access requirements.
- Assign information classification based on information sensitivity and criticality.

Which of the following is another security measure you can implement?

➡ ● Dispose of data when it is no longer needed by using specialized tools.

○ Configure distributed resources to act as one in a federated architecture.

○ Configure redundancy and distribution of data.

○ Create versioned copies of your cloud data.

EXPLANATION

Disposing of data when it is no longer needed by using specialized tools is another security measure you can implement.

Creating versioned copies of your cloud data, configuring redundancy and distribution of data, and configuring distributed resources to act as one in a federated architecture are all measures that improve the fault tolerance and durability of your data.

REFERENCES

9.4.5 Cloud Storage Security Facts

q_cloud_stor_cloud_secp7.question.fex

Question 12: ✓ Correct

What is the limit of virtual machines that can be connected to a virtual network?

➡ ● Unlimited

○ 54

○ 16,777,214

○ 65,534

EXPLANATION

An unlimited number of virtual machines can be connected to a virtual network.

254 is the maximum hosts in a Class C network.

65,534 is the maximum hosts in a Class B network.

16,777,214 is the maximum hosts in a Class A network.

REFERENCES

9.2.4 Virtualization Implementation Facts

q_virt_impl_unlimited_secp7.question.fex

Question 13: ✓ Correct

Which type of firewall operates at Layer 7 of the OSI model?

- ○ Packet-filtering
- ○ Stateful
- ○ Circuit-level gateway
- ➡ ● Application layer

EXPLANATION

Application layer firewalls work on Layer 7 of the OSI model. They are considered third-generation firewalls.

Transport layer (Layer 4) firewalls are considered to be stateful firewalls. They are referred to as second-generation firewalls.

A circuit-level gateway firewall operates at the Session layer of the OSI model.

Packet-filtering firewalls work on Layer 3. They are considered first-generation firewalls.

REFERENCES

9.5.5 Cloud Security Solutions Facts

q_cloud_sec_sol_app_secp7.question.fex

Question 14: ✓ Correct

Your organization recently purchased 20 Android tablets for use by the organization's management team.

To increase the security of these devices, you want to ensure that only specific apps can be installed. Which of the following would you implement?

- ○ App blacklisting
- ➡ ● App whitelisting
- ○ Application Control
- ○ Credential Manager

EXPLANATION

App whitelisting is the process of defining specific apps that users can have on their mobile devices. Apps not on the whitelist are not allowed to be installed.

Blacklisting apps is the process of defining specific apps that users cannot have on their mobile devices.

The Credential Manager function that is implemented in most mobile operating systems can store usernames and passwords for the end user.

Application Control is implemented by each mobile operating system. It determines how apps are installed and where they come from.

REFERENCES

9.6.2 Mobile Device Connection Facts

q_mbl_dev_conn_white_secp7.question.fex

Question 15: ✓ Correct

Which device deployment model gives businesses significant control over device security while allowing employees to use their devices to access both corporate and personal data?

- ➡ ● COPE
- ○ CYOD
- ○ VDI
- ○ BYOD

EXPLANATION

The Corporate-Owned, Personally Enabled (COPE) model gives businesses significant control over device security while allowing employees to use their devices to access both corporate and personal data. Because the company owns the device, it can be secured more easily and wiped clean if lost or stolen. One disadvantage of this model is that employees who are not free to choose their own devices may end up bringing their own anyway.

The Bring Your Own Device (BYOD) model has users bringing in their personal devices and using them for business use.

The Choose Your Own Device (CYOD) model provides slightly more flexibility in giving users a limited selection of devices to choose from.

A virtual desktop interface (VDI) can be used with any device deployment model. A VDI allows mobile devices to establish a remote connection to a virtualized desktop.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_cope_secp7.question.fex

Question 16: ✓ Correct

Which of the following tools allows the user to set security rules for an instance of an application that interacts with one organization and different security rules for an instance of the application when interacting with another organization?

○ Replication

➡ ● Instance awareness

○ Integration

○ Encryption

EXPLANATION

Instance awareness is the ability to apply cloud security within an application that has rules specific to an instance. This tool allows the user to set security rules for an instance of an app interacting with one organization and different security rules for an instance of the app when it interacts with another.

Cloud integration is the system that connects application repositories, systems, and IT environments in a way that allows access and exchange of data over a network by multiple devices and locations.

Encryption is one method that a cloud provider can use to protect a customer's data.

Cloud service providers replicate data in multiple zones and within zones to provide high availability.

REFERENCES

9.5.3 Cloud Security Controls Facts

q_cloud_sec_ctrls_awareness_secp7.question.fex

Question 17: ✓ Correct

Your organization allows employees to bring their own devices into work, but management is concerned that a malicious internal user could use a mobile device to conduct an insider attack.

Which of the following should be implemented to help mitigate this threat?

○ Implement an AUP that specifies which apps are allowed for use with organizational data.

○ Implement a Network Access Control (NAC) solution.

○ Implement a guest wireless network that is isolated from your organization's production network.

➡ ● Implement an AUP that specifies where and when mobile devices can be possessed within the organization.

EXPLANATION

To mitigate the threat of an insider attack, you should consider implementing an AUP that:

- Specifies where and when mobile devices can be possessed within the organization. For example, the possession of mobile devices may be prohibited in high-security areas.
- Notifies users that personally owned devices are subject to random searches if brought on site.

A Network Access Control (NAC) solution would not help mitigate an insider attack with mobile devices.

Implementing an Acceptable Use Policy (AUP) that specifies which apps are allowed for use with organizational data would not help mitigate an insider attack with mobile devices.

Implementing a guest wireless network that is isolated from your organization's production network would not help mitigate an insider attack with mobile devices.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_aup_03_secp7.question.fex

Question 18: ✓ Correct

Which type of firewall protects against packets coming from certain IP addresses?

- ○ Circuit-level
- ➡ ● Packet-filtering
- ○ Application layer
- ○ Stateful

EXPLANATION

Packet-filtering firewalls work on Layer 3. They are considered to be first-generation firewalls. These firewalls check a packet's source and destination address, protocol, and destination ports. They can protect against packets coming from certain IP addresses.

Transport layer (Layer 4) firewalls are considered to be stateful firewalls. They are referred to as second-generation firewalls.

A circuit-level gateway firewall operates at the Session layer of the OSI model.

Application layer firewalls work on Layer 7 of the OSI model. They are considered third-generation firewalls.

REFERENCES

9.5.5 Cloud Security Solutions Facts

q_cloud_sec_sol_packet_secp7.question.fex

Question 19: ✓ Correct

Which APIs do individual networking devices use to communicate with the control plane from the Physical layer?

➡ ● Southbound

○ Northbound

○ Northbound and Southbound

○ None

EXPLANATION

Individual networking devices on the Physical layer use southbound APIs to communicate with the control plane and vice versa.

The Application layer communicates with the Control layer through what is called the northbound interface.

REFERENCES

☰ 9.3.3 SDN Facts

q_sdn_south_secp7.question.fex

Question 20: ✓ Correct

Which of the following cloud computing solutions delivers software applications to a client either over the internet or on a local area network?

○ PaaS

○ IaaS

○ DaaS

➡ ● SaaS

EXPLANATION

Software as a Service (SaaS) delivers software applications to the client either over the internet or on a local area network (LAN).

Infrastructure as a Service (IaaS) delivers infrastructure to the client, such as processing, storage, networks, and virtualized environments. The client deploys and runs software without purchasing servers, data center space, or network equipment. Platform as a Service (PaaS) delivers everything a developer needs to build an application on the cloud infrastructure. The deployment comes without the cost and complexity of buying and managing the underlying hardware and software layers. Data as a Service (DaaS) stores and provides data from a centralized location without the need for local collection and storage.

REFERENCES

9.4.4 Cloud Computing Facts

q_cloud_comp_saas_secp7.question.fex

Question 21: ✓ Correct

Which of the following serves real-time applications without buffer delays?

○ SCADA

○ SoC

○ FPGA

➡ ● RTOS

EXPLANATION

A real-time operating system (RTOS) is an operating system that serves real-time applications without buffer delays. They are generally used in systems that require a response within a strict time constraint.

Supervisory control and data acquisition (SCADA) devices are special computer systems that gather, analyze, and manage automated factory equipment.

A system on a chip (SoC) is an integrated circuit that includes all components of a typical computer system, including digital, analog, mixed-signal, and radio frequency functions.

A Field-Programmable Gate Array (FPGA) is an integrated circuit manufactured and then later configured by the customer.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_rtos_secp7.question.fex

Question 22: ✓ Correct

Which of the following is used as a secure tunnel to connect two networks?

○ VLAN

○ VFA

➡ ● VPN

○ VAN

EXPLANATION

A virtual private network (VPN) is usually used as a secure tunnel over another network, connecting multiple remote endpoints (such as routers). A multipoint VPN is a VPN connecting more than two endpoints.

VLANs allow several physical LANs to function as a single logical LAN.

A virtual area network (VAN) is a virtual LAN running on top of a physical LAN.

A VFA is a virtual firewall appliance. This is software that functions as a network firewall device.

REFERENCES

9.2.5 Virtual Networking Facts

q_virt_net_vpn_secp7.question.fex

Question 23: ✓ Correct

Which of the following is a policy that defines appropriate and inappropriate usage of company resources, assets, and communications?

○ Disaster recovery plan (DRP)

○ Business continuity plan (BCP)

○ Business impact analysis (BIA)

➡ ● Acceptable use policy (AUP)

EXPLANATION

An acceptable use policy (AUP) is a policy that defines appropriate and inappropriate usage of company resources, assets, and communications.

A business impact analysis (BIA) identifies critical processes and assets and the effect of their loss on the company.

A disaster recovery plan (DRP) addresses how a corporation should respond to a disaster.

A business continuity plan (BCP) addresses how a corporation responds to the disruption of critical systems.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_aup_01_secp7.question.fex

Question 24: ✓ Correct

Which of the following is a network device that is deployed in the cloud to protect against unwanted access to a private network?

- ○ Cloud native controls
- ○ Virtual area network
- ○ Cloud-access security broker
- ➡ ● Cloud-based firewall

EXPLANATION

A cloud-based firewall is a software network device that is deployed in the cloud. It protects against unwanted access to a private network.

Cloud native controls refer to the security controls that are native to the cloud provider.

A virtual area network (VAN) is a virtual LAN running on top of a physical LAN. This configuration enables guest virtual machines on separate physical hosts to communicate.

A cloud-access security broker (CASB) is an on-premises, cloud-based software tool or service that sits between an organization and a cloud service provider.

REFERENCES

9.5.5 Cloud Security Solutions Facts

q_cloud_sec_sol_firewall_secp7.question.fex

Question 25: ✓ Correct

You notice that a growing number of devices, such as environmental control systems and wearable devices, are connecting to your network. These devices, known as smart devices, are sending and receiving data via wireless network connections.

Which of the following labels applies to this growing ecosystem of smart devices?

➡ ● Internet of Things (IoT)

○ The smartnet

○ Dynamic environment

○ Internet of smart devices

EXPLANATION

These smart devices are part of a growing ecosystem known as the Internet of Things (IoT). Environments that contain these types of devices are known as static environments. A static environment is one that never changes (or changes very infrequently) and that a network administrator has very little control over. For example, a smart television in an office has embedded technology that might never be updated, which creates a security hole in the company's network.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_smart_01_secp7.question.fex

Question 26: ✓ Correct

Recently, a serious security breach occurred in your organization. An attacker was able to log in to the internal network and steal data through a VPN connection using the credentials assigned to a vice president in your organization.

For security reasons, all individuals in upper management in your organization have unlisted home phone numbers and addresses. However, security camera footage from the vice president's home recorded someone rummaging through her garbage cans prior to the attack. The vice president admitted to writing her VPN login credentials on a sticky note that she subsequently threw away in her household trash. You suspect the attacker found the sticky note in the trash and used the credentials to log in to the network.

You've reviewed the vice president's social media pages. You found pictures of her home posted, but you didn't notice anything in the photos that would give away her home address. She assured you that her smartphone was never misplaced prior to the attack.

Which security weakness is the MOST likely cause of the security breach?

- ○ Weak passwords were used on her smartphone.
- ○ Sideloaded apps were installed on her smartphone.
- ➡ ● Geotagging was enabled on her smartphone.
- ○ A Christmas tree attack was executed on her smartphone.

EXPLANATION

Geotagging embeds GPS coordinates within mobile device files (such as image or video files) created with the device's camera. While this feature can be useful in some circumstances, it can also create security concerns. In this scenario, the vice president probably posted geotagged images to her social media accounts. The attacker likely analyzed the images to discover where she lived and then conducted a dumpster dive attack that yielded the sticky note with the vice president's VPN credentials. The best way to remedy this weakness is to simply disable this functionality in the mobile devices you manage.

Sideloaded apps can only be installed if the device administrator has specifically configured the device to allow them, so this is an unlikely cause. A weak smartphone password is a concern, but this would not be the cause of the exploit if the device were always in the vice president's possession. A Christmas tree attack is used to fingerprint network devices, not to gather personally identifiable information.

REFERENCES

9.6.2 Mobile Device Connection Facts

q_mbl_dev_conn_geo_tag_secp7.question.fex

Question 27: ✓ Correct

Which of the following methods can cloud providers implement to provide high availability?

➡ ● Replication

○ Integration

○ Encryption

○ Instance awareness

EXPLANATION

Cloud service providers replicate data in multiple zones and within zones to provide high availability. Replication:

- Helps eliminate downtime (the time your data is unavailable).
- Redirects to another availability zone when a zone fails.

Cloud integration is the system that connects application repositories, systems, and IT environments in a way that allows access and exchange of data over a network by multiple devices and locations.

Encryption is one method that a cloud provider can use to protect a customer's data.

Instance awareness is the ability to apply cloud security within an application that has rules specific to an instance.

REFERENCES

9.5.3 Cloud Security Controls Facts

q_cloud_sec_ctrls_replication_secp7.question.fex

Question 28: ✓ Correct

Mobile device management (MDM) provides the ability to do which of the following?

○ Control data access.

○ Update apps as needed.

➡ ● Track the device.

○ Remotely install apps.

EXPLANATION

Mobile device management (MDM) solutions allow IT administrators to remotely manage a mobile device even if it's a personally owned device being used for work-related purposes.

Mobile device management provides the ability to:

- Track the device.
- Push apps and updates (this is also known as provisioning the device).
- Manage security settings, such as lock screens, passwords, etc.
- Remotely wipe the device in case it is lost or stolen.

Mobile application management provides the ability to remotely install and uninstall apps.

Microsoft Intune allows the system administrator to:

- Manage mobile devices
- Manage mobile apps
- Control data access
- Comply with security policies

REFERENCES

9.7.2 Mobile Device Management Facts

q_mdm_mdm_secp7.question.fex

Question 29: ✓ Correct

Which SDN layer would a load balancer that stops and starts VMs as resource use increases reside on?

➡ ● Application

○ Session

○ Control

○ Physical

EXPLANATION

Applications reside on the Application layer. A load balancer that stops and starts VMs as resource use increases is an example of an application that would reside on this layer.

The Physical layer is where both physical and virtual network devices sit.

The Session layer is the fifth layer of the OSI model.

The Control layer is the middle layer. This is where the controller resides.

REFERENCES

9.3.3 SDN Facts

q_sdn_app_02_secp7.question.fex

Question 30: ✓ Correct

Which of the following is an example of protocol-based network virtualization?

○ vSwitch

➡ ◉ VLAN

○ VFA

○ VMM

EXPLANATION

VLANs and VPNs are two examples of protocol-based network virtualization.

A vSwitch is software that facilitates the communication between virtual machines by checking data packets before moving them to a destination.

A VFA is a virtual firewall appliance. This is software that functions as a network firewall device.

A virtual machine monitor is software, firmware, or hardware that creates and runs virtual machines. This is also known as a hypervisor.

REFERENCES

9.2.5 Virtual Networking Facts

q_virt_net_vlan_secp7.question.fex

Question 31: ✓ Correct

Which of the following lets you make phone calls over a packet-switched network?

○ RTOS

○ FPGA

○ SCADA

➡ ● VoIP

EXPLANATION

Voice over IP (VoIP) is a protocol optimized for the transmission of voice data (telephone calls) through a packet-switched IP network. VoIP routes phone calls through an IP network, including the internet. VoIP solutions can integrate with a public-switched telephone network (PSTN) to allow VoIP customers to make and receive external calls.

A Field-Programmable Gate Array (FPGA) is an integrated circuit configured by the customer.

A real-time operating system (RTOS) is an operating system that serves real-time applications without buffer delays. They are generally used in systems that require a response within a strict time constraint.

Supervisory control and data acquisition (SCADA) devices are special computer systems that gather, analyze, and manage automated factory equipment.

REFERENCES

5.12.2 VLAN Facts

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_voip_secp7.question.fex

Question 32: ✓ Correct

Which of the following app deployment and update methods allows updates to be uploaded onto Intune where they can be pushed out to users within 24 hours?

○ BYOD

➡ ● Remote management

○ Self-service portal

○ App catalog

EXPLANATION

With remote management, all app types (except for line-of-business apps) automatically update as needed. Updates can be uploaded onto Intune where they can be pushed out to users within 24 hours.

A company can create a self-service portal using Intune. This makes the distribution of apps easier for everyone.

Bring Your Own Device (BYOD) is a policy that allows a user to use their personal device for business purposes.

An app catalog allows an organization to define the apps that a user can and cannot use.

REFERENCES

9.7.6 Mobile Application Management Facts

q_mam_remote_01_secp7.question.fex

Question 33: ✓ Correct

Which of the following is a technique that disperses a workload between two or more computers or resources to achieve optimal resource utilization, throughput, or response time?

○ Hypervisor

○ Virtualization

○ Bottleneck

➡ ● Load balancing

EXPLANATION

Load balancing is a technique that disperses a workload between two or more computers or resources to achieve optimal resource utilization, throughput, or response time. The primary goal of load balancing is to improve performance and create high availability by configuring multiple devices to respond as one.

A hypervisor is a thin layer of software that resides between the guest operating system and the hardware.

Virtualization refers to installing and running multiple operating systems concurrently on a single physical machine.

A bottleneck is an area (software, hardware component, etc.) that all traffic slows down at.

REFERENCES

9.1.3 Virtualization Facts

q_virt_load_balance_secp7.question.fex

Question 34: ✓ Correct

Which of the following is the recommend Intune configuration?

➡ ● Intune Standalone

○ Company portal

○ Hybrid MDM

○ Account portal

EXPLANATION

Intune Standalone is the recommended deployment method. Intune Standalone is a cloud-only solution that is managed using a web console that can be accessed from anywhere with internet access.

Hybrid MDM with Configuration Manager is a solution that combines Intune's mobile device management capabilities into Configuration Manager.

The Account portal is used to manage subscriptions, users, groups, and domains.

The Company portal is used by end users to manage their own account and enroll devices.

REFERENCES

9.6.4 Enforcing Mobile Device Security Facts

q_mbl_dec_sec_config_secp7.question.fex

Question 35: ✓ Correct

A group of small local businesses have joined together to share access to a cloud-based payment system.

Which type of cloud is MOST likely being implemented?

○ Hybrid

○ Private

➡ ● Community

○ Public

EXPLANATION

A community cloud is designed to be shared by several organizations. Access is restricted to users within the organizations who are sharing the community cloud infrastructure.

A hybrid cloud is composed of a combination of public, private, and community cloud resources from different service providers.

A public cloud can be accessed by anyone.

A private cloud provides resources to a single organization.

REFERENCES

9.4.4 Cloud Computing Facts

q_cloud_comp_community_secp7.question.fex

Question 36: ✓ Correct

Which of the following can provide the most specific protection and monitoring capabilities?

➡ ● Cloud-access security broker

○ Secure web gateway

○ Cloud-based firewall

○ Cloud native controls

EXPLANATION

A cloud-access security broker (CASB) is an on-premises, cloud-based software tool or service that sits between an organization and a cloud service provider. A CASB can offer malware protection and encryption and can also give more specific protection and monitoring capabilities than secure web gateways (SWGs) and enterprise firewalls.

A cloud-based firewall is a software network device that is deployed in the cloud. It protects against unwanted access to a private network.

Cloud native controls refer to the security controls that are native to the cloud provider.

Secure web gateways (SWGs) detect malicious traffic and work at the Application layer in the cloud.

REFERENCES

▷ 9.4.3 Cloud Computing Security Issues

☰ 9.4.5 Cloud Storage Security Facts

☰ 9.5.5 Cloud Security Solutions Facts

q_cloud_sec_sol_casb_01_secp7.question.fex

Question 37: ✓ Correct

Mobile application management (MAM) provides the ability to do which of the following?

➡ ● Remotely install and uninstall apps.

○ Manage mobile devices.

○ Comply with security policies.

○ Control data access.

EXPLANATION

Mobile application management (MAM) solutions focus on managing the applications on a mobile device but not the device itself. Licensed applications or custom-designed apps fall under MAM policies.

Mobile application management provides the ability to:

- Remotely install and uninstall apps.
- Update apps as needed.
- Limit functionality in an app as needed.

Microsoft Intune allows the system administrator to:

- Manage mobile devices
- Manage mobile apps
- Control data access
- Comply with security policies

REFERENCES

9.7.2 Mobile Device Management Facts

q_mdm_mam_secp7.question.fex

Question 38: ✓ Correct

Which of the following is the first phase of the Microsoft Intune application life cycle?

- ○ Deploy
- ○ Configure
- ➡ ● Add
- ○ Protect

EXPLANATION

The first phase of the Microsoft Intune application life cycle is to add the apps that are to be managed and assigned in Intune.

Deploy is the second phase.

Configure is the third phase.

Protect is the fourth phase.

REFERENCES

☰ 9.7.6 Mobile Application Management Facts

q_mam_add_secp7.question.fex

Question 39: ✓ Correct

What is isolating a virtual machine from the physical network to allow testing to be performed without impacting the production environment called?

○ Workload balancing

➡ ● Sandboxing

○ Testing

○ Resource pooling

EXPLANATION

Isolating a virtual machine from the physical network to allow testing to be performed without impacting the production environment is known as sandboxing.

Resource pooling creates shared logical pools of CPU and memory resources from many physical machines within the hypervisor. This guarantees a level of resources for specific virtual machines.

Virtual machines can be configured in a lab environment that mirrors a production network to provide a testing environment.

Workload balancing distributes a workload (the total requests made by users and applications of a system) across multiple computers or a computer cluster to achieve optimal resource utilization, maximum throughput, minimal response time, and less overload.

REFERENCES

4.2.1 Operating System Hardening

4.2.2 Hardening Facts

4.2.3 Hardening an Operating System

4.2.4 Managing Automatic Updates

4.2.6 Configuring Microsoft Defender Firewall

4.2.8 Configuring Windows Defender with Firewall Advanced Security

9.1.3 Virtualization Facts

q_virt_sandbox_secp7.question.fex

Question 40: ✓ Correct

Which of the following do Raspberry Pi systems make use of?

- ○ RTOS
- ➡ ● SoC
- ○ FPGA
- ○ SCADA

EXPLANATION

A system on a chip (SoC) is an integrated circuit that includes all components of a typical computer system, including digital, analog, mixed-signal, and radio frequency functions. Raspberry Pi is a common device that uses an SoC. Because of their relatively low cost, SoCs are often used by hobbyists.

A real-time operating system (RTOS) is an operating system that serves real-time applications without buffer delays. They are generally used in systems that require a response within a strict time constraint.

Supervisory control and data acquisition (SCADA) devices are special computer systems that gather, analyze, and manage automated factory equipment.

A Field-Programmable Gate Array (FPGA) is an integrated circuit configured by the customer.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_soc_secp7.question.fex

Question 41: ✓ Correct

Which of the following are disadvantages of server virtualization?

○ A compromised guest system might affect multiple servers.

○ Systems are isolated from each other and cannot interact with other systems.

○ It increases hardware costs.

➡ ◉ A compromised host system might affect multiple servers.

EXPLANATION

Virtualization allows a single physical machine (known as the host operating system) to run multiple virtual machines (known as guest operating systems). The virtual machines appear to be self-contained and autonomous systems. Disadvantages of virtualization include:

- An attack on the host machine could compromise all guest machines operating on that host.
- A bottleneck or failure of any hardware component that is shared between multiple guests, such as a failure in a disk subsystem, could affect multiple virtual machines.
- While administration is centralized, virtualization is a newer technology and requires new skills, so managing virtual servers could add complexity.

A compromise of a guest system is typically limited to that system only because each virtual machine is kept partitioned from other guest machines. System isolation, if configured, is an advantage of virtualization. Isolation is typically used for testing purposes and prevents unreliable applications from interfering with other systems. Virtual systems do not need to be isolated. They can be configured to have full network access to other virtual machines or other network devices.

An advantage of virtualization is reduced hardware costs.

REFERENCES

9.1.3 Virtualization Facts

q_virt_server_secp7.question.fex

Question 42: ✓ Correct

Which of the following is an exploit in which malware allows the virtual OS to interact directly with the hypervisor?

- ○ Bottleneck
- ○ Jump
- ➡ ● Escape
- ○ Load balancing

EXPLANATION

Virtual machine escape is an exploit in which malware allows the operating system within a virtual machine to break out and interact directly with the hypervisor.

Jump is not a type of VM exploit.

Load balancing is a technique that disperses a workload between two or more computers or resources to achieve optimal resource utilization, throughput, or response time.

A bottleneck is an area (software, hardware component, etc.) that all traffic slows down at.

REFERENCES

9.1.3 Virtualization Facts

q_virt_escape_secp7.question.fex

Question 43: ✓ Correct

Which of the following devices facilitates communication between different virtual machines by checking data packets before moving them to a destination?

- ○ Virtual router
- ○ Hypervisor
- ○ Virtual firewall
- ➡ ● Virtual switch

EXPLANATION

A virtual switch is software that facilitates the communication between different virtual machines. It does so by checking data packets before moving them to a destination. They may already be a part of software installed in the virtual machine, or they may be part of the server firmware.

REFERENCES

9.2.5 Virtual Networking Facts

q_virt_net_switch_secp7.question.fex

Question 44: ✓ Correct

If a user's BYOD device (such as a tablet or phone) is infected with malware, that malware can be spread if that user connects to your organization's network. One way to prevent this event is to use a Network Access Control (NAC) system.

How does an NAC protect your network from being infected by a BYOD device?

➡ ● The NAC remediates devices before allowing them to connect to your network.

○ The NAC notifies users that personally owned devices are subject to random searches if brought on site.

○ The NAC specifies which apps can be used while the BYOD device is connected to the organization's network.

○ The NAC forces BYOD devices to connect to a guest network that is isolated from your production network.

EXPLANATION

The NAC remediates devices before allowing them to connect to your network. This means that the NAC performs the following types of device management tasks before allowing a device to connect to the network:

- Operating system updates
- App updates
- Anti-malware installation
- Anti-malware definition updates

An alternative to using an NAC solution is to force BYOD devices to connect to a guest network that is isolated from your production network. An Acceptable Use Policy (AUP) specifies which apps can be used while the BYOD device is connected to the organization's network. An AUP also notifies users that personally owned devices are subject to random searches if brought on site.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_nac_01_secp7.question.fex