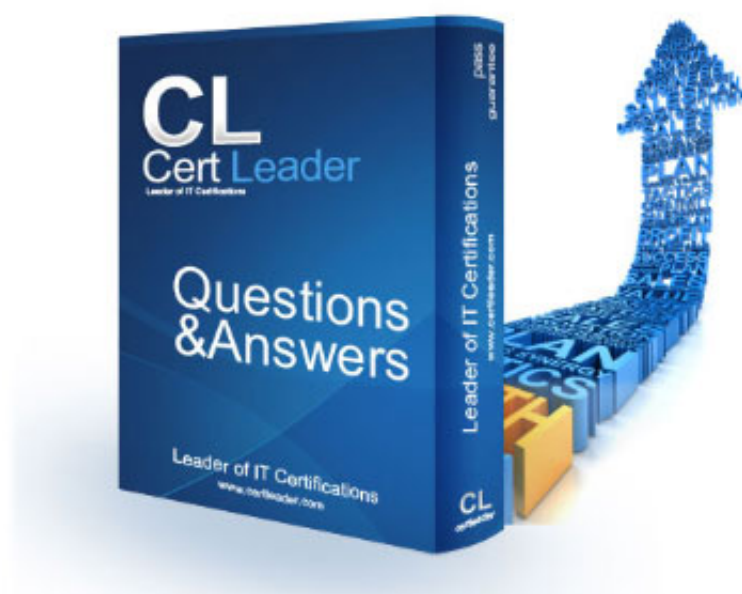


SY0-601 Dumps

CompTIA Security+ Exam

<https://www.certleader.com/SY0-601-dumps.html>



NEW QUESTION 1

A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

- A. SPIM
- B. Vishing
- C. Spear phishing
- D. Smishing

Answer: D

NEW QUESTION 2

Which of the following describes the BEST approach for deploying application patches?

- A. Apply the patches to systems in a testing environment then to systems in a staging environment, and finally to production systems.
- B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems
- C. Test the patches in a test environment apply them to the production systems and then apply them to a staging environment
- D. Apply the patches to the production systems apply them in a staging environment, and then test all of them in a testing environment

Answer: A

NEW QUESTION 3

An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

- A. business continuity plan
- B. communications plan.
- C. disaster recovery plan.
- D. continuity of operations plan

Answer: C

NEW QUESTION 4

A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the cause of the access issues?

- A. False rejection
- B. Cross-over error rate
- C. Efficacy rate
- D. Attestation

Answer: B

NEW QUESTION 5

A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?

- A. Hard token
- B. Retina scan
- C. SMS text
- D. Keypad PIN

Answer: B

NEW QUESTION 6

A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

- A. Configure the DLP policies to allow all PII
- B. Configure the firewall to allow all ports that are used by this application
- C. Configure the antivirus software to allow the application
- D. Configure the DLP policies to whitelist this application with the specific PII
- E. Configure the application to encrypt the PII

Answer: D

NEW QUESTION 7

A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

- A. A firewall
- B. A device pin
- C. A USB data blocker
- D. Biometrics

Answer:

C

NEW QUESTION 8

A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

- A. Implement open PSK on the APs
- B. Deploy a WAF
- C. Configure WIPS on the APs
- D. Install a captive portal

Answer: D

NEW QUESTION 9

After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?

- A. The public ledger
- B. The NetFlow data
- C. A checksum
- D. The event log

Answer: A

NEW QUESTION 10

A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?

- A. Due to foreign travel, the user's laptop was isolated from the network.
- B. The user's laptop was quarantined because it missed the latest path update.
- C. The VPN client was blacklisted.
- D. The user's account was put on a legal hold.

Answer: A

NEW QUESTION 10

A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string Which of the following would be BEST to use to accomplish the task? (Select TWO).

- A. head
- B. Tcpdump
- C. grep
- D. rail
- E. curl
- F. openssi
- G. dd

Answer: AB

NEW QUESTION 11

A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

- A. Man-in- the middle
- B. Spear-phishing
- C. Evil twin
- D. DNS poisoning

Answer: D

NEW QUESTION 16

Which of the following BEST explains the difference between a data owner and a data custodian?

- A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
- B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
- C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
- D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Answer: B

NEW QUESTION 18

A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an item, the password for the wireless network is printed on the receipt so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least

amount of overhead?

- A. WPA-EAP
- B. WEP-TKIP
- C. WPA-PSK
- D. WPS-PIN

Answer: A

NEW QUESTION 22

A security analyst needs to be proactive in understand the types of attacks that could potentially target the company's execute. Which of the following intelligence sources should to security analyst review?

- A. Vulnerability feeds
- B. Trusted automated exchange of indicator information
- C. Structured threat information expression
- D. Industry information-sharing and collaboration groups

Answer: D

NEW QUESTION 24

Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and It has continues to evade detection. Which of the following should administrator implement to protect the environment from this malware?

- A. Install a definition-based antivirus.
- B. Implement an IDS/IPS
- C. Implement a heuristic behavior-detection solution.
- D. Implement CASB to protect the network shares.

Answer: C

NEW QUESTION 26

To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?

- A. MaaS
- B. IaaS
- C. SaaS
- D. PaaS

Answer: D

NEW QUESTION 29

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

- A. SSAE SOC 2
- B. PCI DSS
- C. GDPR
- D. ISO 31000

Answer: C

NEW QUESTION 33

A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:

* Protection from power outages

* Always-available connectivity In case of an outage

The owner has decided to implement battery backups for the computer equipment Which of the following would BEST fulfill the owner's second need?

- A. Lease a point-to-point circuit to provide dedicated access.
- B. Connect the business router to its own dedicated UPS.
- C. Purchase services from a cloud provider for high availability
- D. Replace the business's wired network with a wireless network.

Answer: C

NEW QUESTION 36

An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

- A. Nmap
- B. cURL
- C. Netcat
- D. Wireshark

Answer: D

NEW QUESTION 38

A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this task?

- A. Netcat
- B. Netstat
- C. Nmap
- D. Nessus

Answer: B

NEW QUESTION 40

A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a projected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

- A. DNS sinkholding
- B. DLP rules on the terminal
- C. An IP blacklist
- D. Application whitelisting

Answer: D

NEW QUESTION 44

A company uses wireless for all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

- A. A BPDU guard
- B. WPA-EAP
- C. IP filtering
- D. A WIDS

Answer: B

NEW QUESTION 49

A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

- A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
- B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
- C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
- D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Answer: C

NEW QUESTION 53

An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

- A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
- B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
- C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
- D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

Answer: A

NEW QUESTION 58

A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

- A. A packet capture
- B. A user behavior analysis
- C. Threat hunting
- D. Credentialed vulnerability scanning

Answer: C

NEW QUESTION 63

A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:


```
#####
@  WARNING:  REMOTE HOST IDENTIFICATION HAS CHANGED!  @
#####
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVzignVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Which of the following network attacks is the researcher MOST likely experiencing?

- A. MAC cloning
- B. Evil twin
- C. Man-in-the-middle
- D. ARP poisoning

Answer: C

NEW QUESTION 65

An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

- A. Voice
- B. Gait
- C. Vein
- D. Facial
- E. Retina
- F. Fingerprint

Answer: BD

NEW QUESTION 70

A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

- A. Loss of proprietary information
- B. Damage to the company's reputation
- C. Social engineering
- D. Credential exposure

Answer: C

NEW QUESTION 72

A company has limited storage available and online presence that cannot for more than four hours. Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time In the event of a failure, which being maindful of the limited available storage space?

- A. Implement fulltape backup every Sunday at 8:00 p.m and perform nightly tape rotations.
- B. Implement different backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m
- C. Implement nightly full backups every Sunday at 8:00 p.m
- D. Implement full backups every Sunday at 8:00 p.m and nightly differential backups at 8:00

Answer: B

NEW QUESTION 73

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

- A. Nmap
- B. Wireshark
- C. Autopsy
- D. DNSEnum

Answer: A

NEW QUESTION 77

Which of the following would MOST likely support the integrity of a voting machine?

- A. Asymmetric encryption
- B. Blockchain
- C. Transport Layer Security
- D. Perfect forward secrecy

Answer: D

NEW QUESTION 80

A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

- A. FDE
- B. NIDS
- C. EDR
- D. DLP

Answer: C

NEW QUESTION 84

An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:

- A. MTBF
- B. RPO
- C. MTTR
- D. RTO

Answer: D

NEW QUESTION 87

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

- A. dd
- B. chmod
- C. dnsenum
- D. logger

Answer: A

NEW QUESTION 92

A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

- A. DDoS attack
- B. Memory leak
- C. Buffer overflow
- D. Resource exhaustion

Answer: D

NEW QUESTION 97

A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

A)

```
http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
```

B)

```
http://sample.url.com/someotherpageonsite/../../../../etc/shadow
```

C)

```
http://sample.url.com/select-from-database-where-password-null
```

D)

```
http://redirect.sample.url.sampleurl.com/malicious-dns-redirect
```

A. Option A

- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 101

A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

- A. Security information and event management
- B. A web application firewall
- C. A vulnerability scanner
- D. A next-generation firewall

Answer: A

NEW QUESTION 103

Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?

- A. DDoS
- B. Man-in-the-middle
- C. MAC flooding
- D. Domain hijacking

Answer: A

NEW QUESTION 104

A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two- drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

- A. 1
- B. 5
- C. 6

Answer: B

NEW QUESTION 105

Which of the following disaster recovery tests is The LEAST time-consuming for the disaster recovery team?

- A. Tabletop
- B. Parallel
- C. Full interruption
- D. Simulation

Answer: D

NEW QUESTION 109

A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

- A. Corrective
- B. Physical
- C. Detective
- D. Administrative

Answer: C

NEW QUESTION 110

Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hot-spots?

- A. Footprinting
- B. White-box testing
- C. A drone/UAV
- D. Pivoting

Answer: A

NEW QUESTION 113

Local guidelines require that all information systems meet a minimum-security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the baseline?

- A. SOAR playbook
- B. Security control matrix

- C. Risk management framework
- D. Benchmarks

Answer: D

NEW QUESTION 115

In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

- A. Identification
- B. Preparation
- C. Eradiction
- D. Recovery
- E. Containment

Answer: E

NEW QUESTION 120

Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).

- A. Testing security systems and processes regularly
- B. Installing and maintaining a web proxy to protect cardholder data
- C. Assigning a unique ID to each person with computer access
- D. Encrypting transmission of cardholder data across private networks
- E. Benchmarking security awareness training for contractors
- F. Using vendor-supplied default passwords for system passwords

Answer: BD

NEW QUESTION 125

Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

- A. Cross-site scripting
- B. Data exfiltration
- C. Poor system logging
- D. Weak encryption
- E. SQL injection
- F. Server-side request forgery

Answer: DF

NEW QUESTION 128

Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

- A. SaaS
- B. PaaS
- C. IaaS
- D. DaaS

Answer: C

NEW QUESTION 129

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites. INSTRUCTIONS

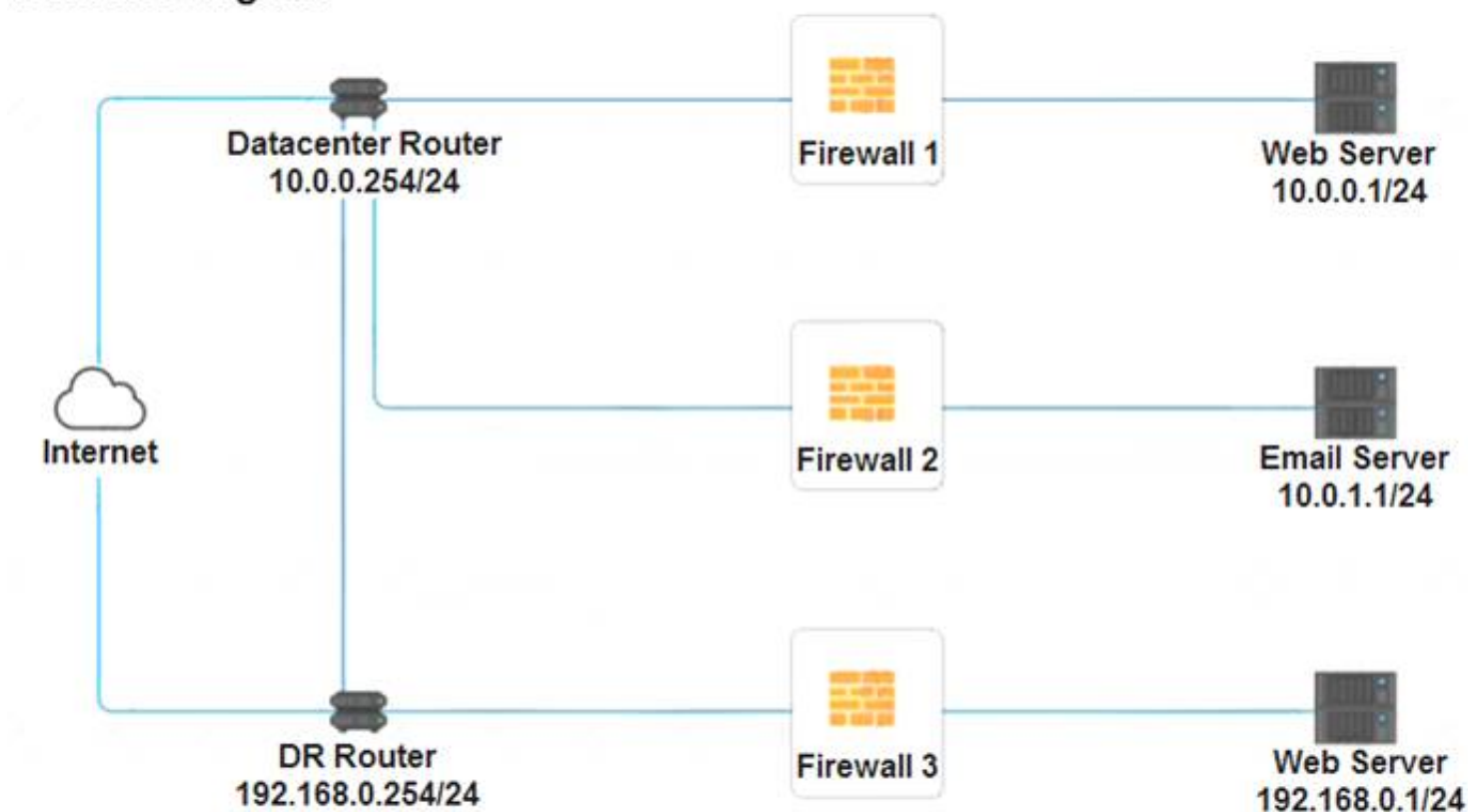
Click on each firewall to do the following:

- Deny cleartext web traffic.
- Ensure secure management protocols are used.
- Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram



Firewall 1
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>PERMIT DENY</div> </div>
HTTPS Outbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>PERMIT DENY</div> </div>
Management	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>PERMIT DENY</div> </div>
HTTPS Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>PERMIT DENY</div> </div>
HTTP Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>ANY DNS HTTP HTTPS TELNET SSH</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div>PERMIT DENY</div> </div>

Reset Answer
Save
Close

Firewall 2
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> PERMIT DENY </div>
HTTPS Outbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> PERMIT DENY </div>
Management	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> PERMIT DENY </div>
HTTPS Inbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> PERMIT DENY </div>
HTTP Inbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> PERMIT DENY </div>

Reset Answer
Save
Close

Firewall 3
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> PERMIT DENY </div>
HTTPS Outbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> PERMIT DENY </div>
Management	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> PERMIT DENY </div>
HTTPS Inbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> PERMIT DENY </div>
HTTP Inbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;"> PERMIT DENY </div>

Reset Answer
Save
Close

A.

Answer: A

Explanation:

See explanation below.

Explanation

Firewall 1:

Firewall 1					
Rule Name	Source	Destination	Service	Action	
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT	•
HTTPS Outbound	10.0.0.1/24	• ANY	• HTTPS	• PERMIT	•
Management	ANY	• 10.0.0.1/24	• SSH	• PERMIT	•
HTTPS Inbound	ANY	• 10.0.0.1/24	• HTTPS	• PERMIT	•
HTTP Inbound	ANY	• 10.0.0.1/24	• HTTP	• DENY	•
<div>Reset Answer</div> <div>Save</div> <div>Close</div>					

Firewall 1					
Rule Name	Source	Destination	Service	Action	
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT	•
HTTPS Outbound	10.0.0.1/24	• ANY	• HTTPS	• PERMIT	•
Management	ANY	• 10.0.0.1/24	• SSH	• PERMIT	•
HTTPS Inbound	ANY	• 10.0.0.1/24	• HTTPS	• PERMIT	•
HTTP Inbound	ANY	• 10.0.0.1/24	• HTTP	• DENY	•
<div>Reset Answer</div> <div>Save</div> <div>Close</div>					

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Firewall 2:

Firewall 2					
Rule Name	Source	Destination	Service	Action	
DNS Rule	10.0.1.1/24	• ANY	• DNS	• PERMIT	•
HTTPS Outbound	10.0.1.1/24	• ANY	• HTTPS	• PERMIT	•
Management	ANY	• 10.0.1.1/24	• DNS	• PERMIT	•
HTTPS Inbound	ANY	• 10.0.1.1/24	• HTTPS	• PERMIT	•
HTTP Inbound	ANY	• 10.0.1.1/24	• HTTP	• DENY	•
<div>Reset Answer</div> <div>Save</div> <div>Close</div>					

Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	10.0.1.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 10.0.1.1/24	• DNS	• PERMIT
HTTPS Inbound	ANY	• 10.0.1.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 10.0.1.1/24	• HTTP	• DENY

Firewall 3:

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	192.168.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 192.168.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 192.168.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 192.168.0.1/24	• HTTP	• DENY

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	192.168.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 192.168.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 192.168.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 192.168.0.1/24	• HTTP	• DENY

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

NEW QUESTION 131

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO).

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

Answer: AE

NEW QUESTION 135

- A. Transference
- B. Avoidance
- C. Acceptance
- D. Mitigation

NEW QUESTION 138

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

A. Mastered
B. Not Mastered

Explanation:

visit - <https://www.certleader.com>

NEW QUESTION 140

Which of the following types of controls is a turnstile?

- A. Physical
- B. Detective
- C. Corrective
- D. Technical

Answer: A

NEW QUESTION 143

A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money than it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

- A. MTBF
- B. RPO
- C. RTO
- D. MTTR

Answer: C

NEW QUESTION 145

A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the MOST likely cause of the issue?

- A. The S/MIME plug-in is not enabled.
- B. The SLL certificate has expired.
- C. Secure IMAP was not implemented
- D. POP3S is not supported.

Answer: A

NEW QUESTION 148

The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

- A. Install a NIDS device at the boundary.
- B. Segment the network with firewalls.
- C. Update all antivirus signatures daily.
- D. Implement application blacklisting.

Answer: B

NEW QUESTION 152

A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

- A. Monitoring large data transfer transactions in the firewall logs
- B. Developing mandatory training to educate employees about the removable media policy
- C. Implementing a group policy to block user access to system files
- D. Blocking removable-media devices and write capabilities using a host-based security tool

Answer: D

NEW QUESTION 154

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

- A. VPN
- B. Drive encryption
- C. Network firewall
- D. File level encryption
- E. USB blocker
- F. MFA

Answer: BE

NEW QUESTION 157

An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

- A. Screen locks
- B. Application management
- C. Geofencing
- D. Containerization

Answer:

D

NEW QUESTION 160

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SY0-601 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SY0-601-dumps.html>