CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

NEW QUESTION 1
A security analyst needs to make a recommendation for restricting access to certain segments of the network using only data-link layer security. Which of the following controls will the analyst MOST likely recommend?

A. MAC
B. ACL
C. BPDU
D. ARP

Answer: A

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, andthen apply them to the production systems
C. Test the patches m 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
A cybersecurity department purchased o new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

A. Randomize the shared credentials
B. Use only guest accounts to connect.
C. Use SSH keys and remove generic passwords
D. Remove all user accounts.

Answer: C

NEW QUESTION 4
A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

A. perform attribution to specific APTs and nation-state actors.
B. anonymize any PII that is observed within the IoC data.
C. add metadata to track the utilization of threat intelligence reports.
D. assist companies with impact assessments based on the observed data.

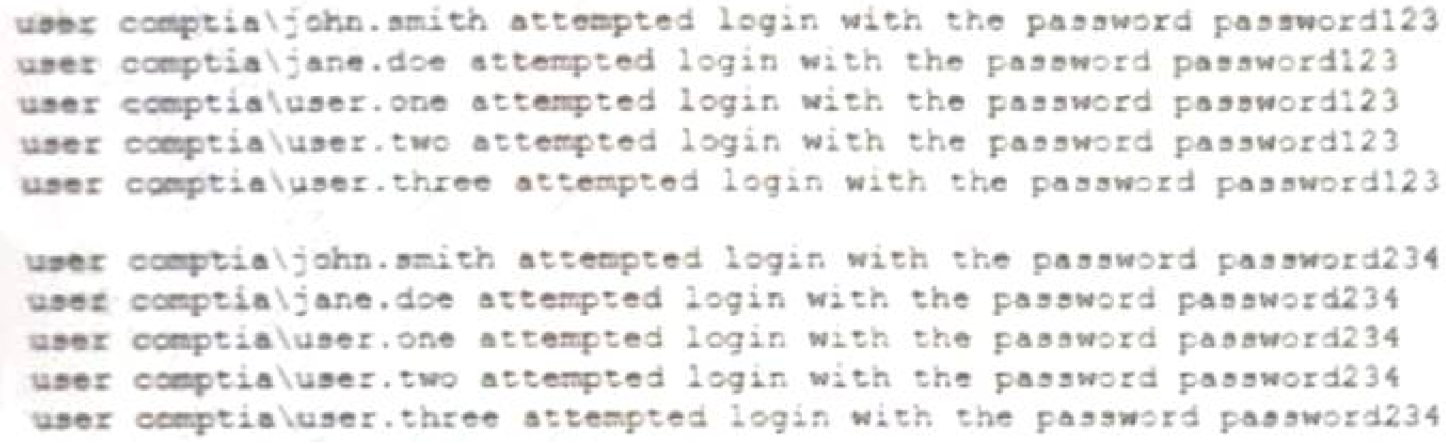
Answer: B

NEW QUESTION 5
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company’s final software releases? (Select TWO.)

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Answer: AD

NEW QUESTION 6
A security analyst is reviewing the following attack log output:



```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

A. Rainbow table
B. Brute-force

C. Password-spraying
D. Dictionary

Answer: C

NEW QUESTION 7
Which of the following relets to applications and systems that are used within an organization without consent or approval?

A. Shadow IT
B. OSINT
C. Dark web
D. Insider threats

Answer: A

NEW QUESTION 8
Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

A. The data owner
B. The data processor
C. The data steward
D. The data privacy officer.

Answer: C

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 malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

A. Security
B. Application
C. Dump
D. Syslog

Answer: C

NEW QUESTION 10
A security administrator currently spends a large amount of time on common security tasks, such aa report generation, phishing investigations, and user provisioning and deprovisioning This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

A. DAC
B. ABAC
C. SCAP
D. SOAR

Answer: D

NEW QUESTION 11
A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

A. Physical
B. Detective
C. Preventive
D. Compensating

Answer: D

NEW QUESTION 12
A security analyst has received an alert about being sent via email. The analyst's Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care From which of the following did the alert MOST likely originate?

A. S/MIME
B. DLP
C. IMAP
D. HIDS

Answer: B

NEW QUESTION 17
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 poising

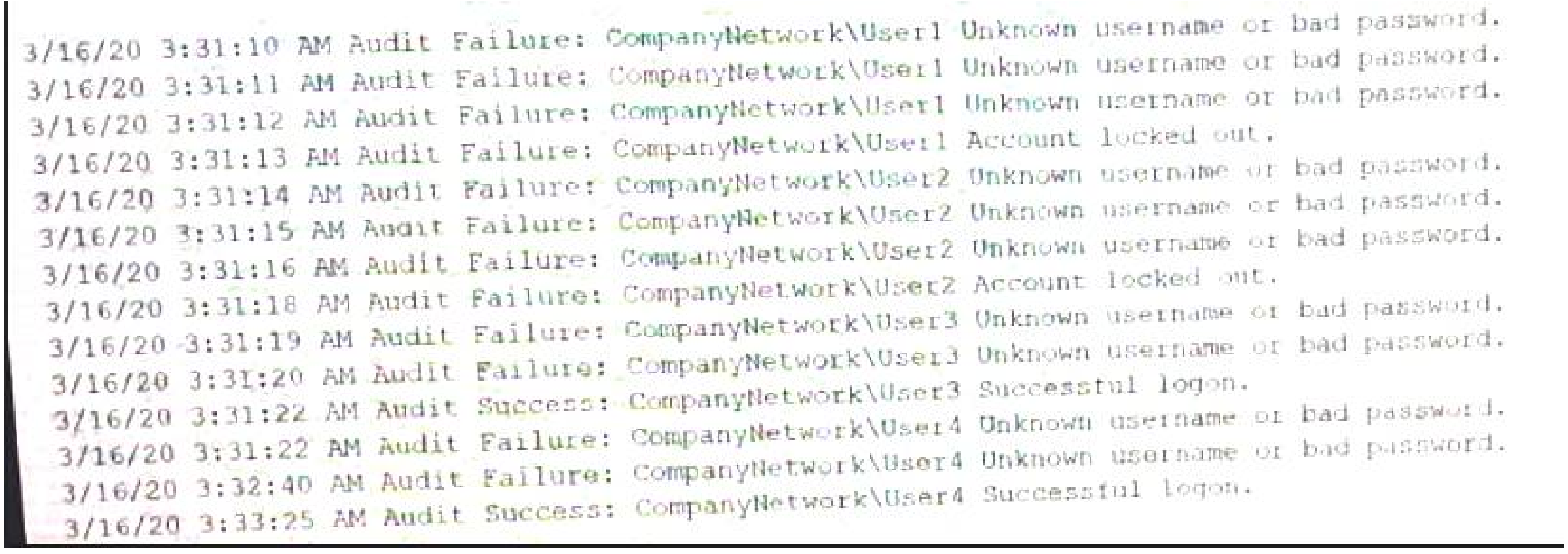
Answer: D

NEW QUESTION 19
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 22
A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:



```
3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.
3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User2 Account locked out.
3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:20 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful logon.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful logon.
```

Which of the following attacks MOST likely occurred?

A. Dictionary
B. Credential-stuffing
C. Password-spraying
D. Brute-force

Answer: D

NEW QUESTION 25
A symmetric encryption algorithm Is BEST suited for:

A. key-exchange scalability.
B. protecting large amounts of data.
C. providing hashing capabilities,
D. implementing non-repudiation.

Answer: D

NEW QUESTION 28
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 recent 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 32
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 36
The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the blowing would BEST address this security concern?

A. install a smart meter on the staff WiFi.
B. Place the environmental systems in the same DHCP scope as the staff WiFi.
C. Implement Zigbee on the staff WiFi access points.
D. Segment the staff WiFi network from the environmental systems network.

Answer: D

NEW QUESTION 39
A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

A. PCI DSS
B. ISO 22301
C. ISO 27001
D. NIST CSF

Answer: A

NEW QUESTION 43
To secure an application after a large data breach, an e-commerce site will be resetting all users’ credentials. Which of the following will BEST ensure the site’s users are not compromised after the reset?

A. A password reuse policy
B. Account lockout after three failed attempts
C. Encrypted credentials in transit
D. A geofencing policy based on login history

Answer: C

NEW QUESTION 45
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 46
A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?

A. Open the document on an air-gapped network
B. View the document's metadata for origin clues
C. Search for matching file hashes on malware websites
D. Detonate the document in an analysis sandbox

Answer: D

NEW QUESTION 51
A system administrator needs to implement an access control scheme that will allow an object’s access policy be determined by its owner. Which of the following access control schemes BEST fits the requirements?

A. Role-based access control
B. Discretionary access control

C. Mandatory access control
D. Attribute-based access control

Answer: B

NEW QUESTION 54
A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

A. Perform a site survey
B. Deploy an FTK Imager
C. Create a heat map
D. Scan for rogue access points
E. Upgrade the security protocols
F. Install a captive portal

Answer: AC

NEW QUESTION 59
A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization’s vulnerabilities. Which of the following would BEST meet this need?

A. CVE
B. SIEM
C. SOAR
D. CVSS

Answer: D

NEW QUESTION 63
A workwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

A. Network location
B. Impossible travel time
C. Geolocation
D. Geofencing

Answer: D

NEW QUESTION 67
A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

A. Dual power supply
B. Off-site backups
C. Automatic OS upgrades
D. NIC teaming
E. Scheduled penetration testing
F. Network-attached storage

Answer: AB

NEW QUESTION 68
Which of the following is a team of people dedicated testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

A. Red team
B. While team
C. Blue team
D. Purple team

Answer: A

NEW QUESTION 73
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 77
In which of the following situations would it be BEST to use a detective control type for mitigation?

A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
E. A company purchased liability insurance for flood protection on all capital assets.

Answer: D

NEW QUESTION 79
A security engineer needs to Implement the following requirements:
• All Layer 2 switches should leverage Active Directory tor authentication.
• All Layer 2 switches should use local fallback authentication If Active Directory Is offline.
• All Layer 2 switches are not the same and are manufactured by several vendors.
Which of the following actions should the engineer take to meet these requirements? (Select TWO).

A. Implement RADIUS.
B. Configure AAA on the switch with local login as secondary.
C. Configure port security on the switch with the secondary login method.
D. Implement TACACS+
E. Enable the local firewall on the Active Directory server.
F. Implement a DHCP server.

Answer: AB

NEW QUESTION 83
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 86
An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

A. An external security assessment
B. A bug bounty program
C. A tabletop exercise
D. A red-team engagement

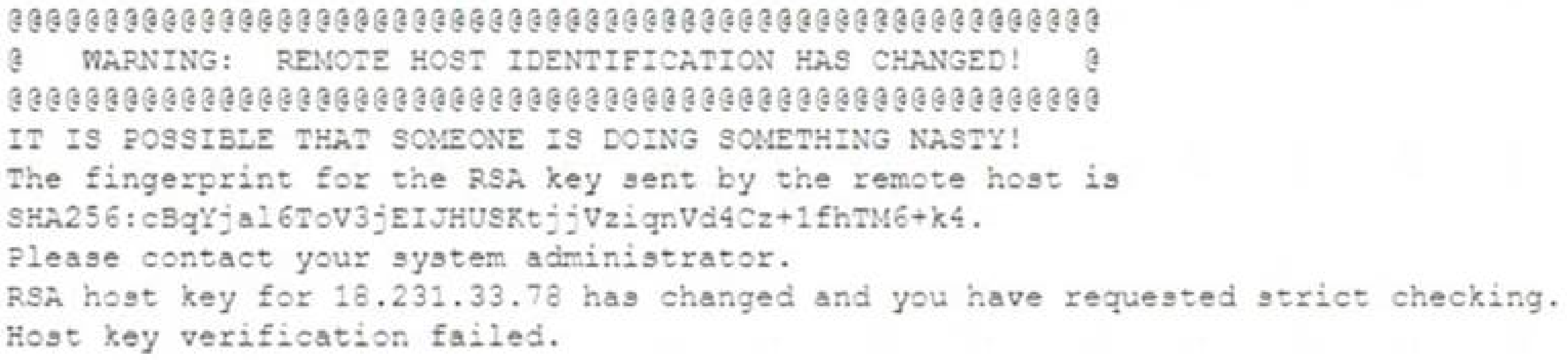
Answer: C

NEW QUESTION 91
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 95
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 99
Which of the following algorithms has the SMALLEST key size?

A. DES
B. Twofish
C. RSA
D. AES

Answer: B

NEW QUESTION 103
An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

A. SED
B. HSM
C. DLP
D. TPM

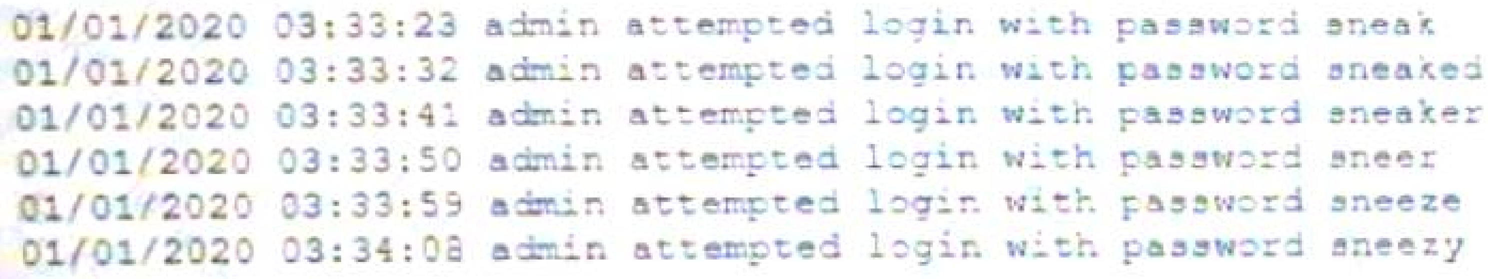
Answer: A

NEW QUESTION 106
A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

A. validate the vulnerability exists in the organization's network through penetration testing
B. research the appropriate mitigation techniques in a vulnerability database
C. find the software patches that are required to mitigate a vulnerability
D. prioritize remediation of vulnerabilities based on the possible impact.

Answer: D

NEW QUESTION 110
A security analyst is reviewing logs on a server and observes the following output:



```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

A. A rainbow table attack
B. A password-spraying attack
C. A dictionary attack
D. A keylogger attack

Answer: C

NEW QUESTION 112
A root cause analysis reveals that a web application outage was caused by one of the company’s developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

A. CASB
B. SWG
C. Containerization
D. Automated failover

Answer: C

NEW QUESTION 117
An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering it the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO’s concerns?

A. Disallow new hires from using mobile devices for six months
B. Select four devices for the sales department to use in a CYOD model
C. Implement BYOD for the sates department while leveraging the MDM

D. Deploy mobile devices using the COPE methodology

Answer: C

NEW QUESTION 120
Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe's identity before sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing
B. Whaling
C. Phishing
D. Vishing

Answer: C

NEW QUESTION 121
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 whiteboars 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 126
The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

A. A script kiddie
B. Shadow IT
C. Hacktivism
D. White-hat

Answer: B

NEW QUESTION 127
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 128
The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

A. data controller.
B. data owner
C. data custodian.
D. data processor

Answer: D

NEW QUESTION 133
An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load Which of the following are the BEST options to accomplish this objective'? (Select TWO)

A. Load balancing
B. Incremental backups
C. UPS
D. RAID
E. Dual power supply
F. NIC teaming

Answer: AD

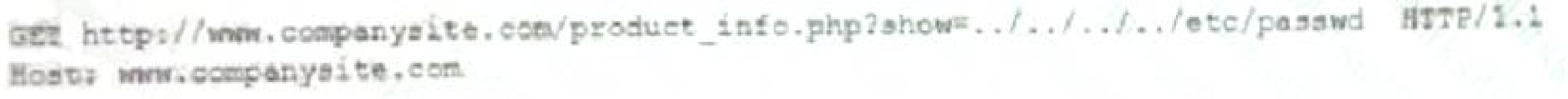
NEW QUESTION 137
A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts

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 138
During an incident response, a security analyst observes the following log entry on the web server.



```
GET http://www.companysite.com/product_info.php?show=../../../../etc/passwd  HTTP/1.1
Host: www.companysite.com
```

Which of the following BEST describes the type of attack the analyst is experience?

A. SQL injection
B. Cross-site scripting
C. Pass-the-hash
D. Directory traversal

Answer: B

NEW QUESTION 139
After entering a username and password, and administrator must gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

A. Multifactor authentication
B. Something you can do
C. Biometric
D. Two-factor authentication

Answer: D

NEW QUESTION 140
A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

A. The GPS location
B. When the file was deleted
C. The total number of print jobs
D. The number of copies made

Answer: A

NEW QUESTION 142
A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

A. Developing an incident response plan
B. Building a disaster recovery plan
C. Conducting a tabletop exercise
D. Running a simulation exercise

Answer: C

NEW QUESTION 146
A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO) A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
B. Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command m a live Linux environment to create a duplicate copy
C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
D. Refrain from completing a forensic analysts of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence

Answer: D

NEW QUESTION 151
A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

A. iPSec

B. Always On
C. Split tunneling
D. L2TP

Answer: B

NEW QUESTION 152
Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

A. DLP
B. HIDS
C. EDR
D. NIPS

Answer: C

NEW QUESTION 157
Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

A. Investigation
B. Containment
C. Recovery
D. Lessons learned

Answer: B

NEW QUESTION 162
A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:
http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us
The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:
http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us Which of the following application attacks is being tested?

A. Pass-the-hash
B. Session replay
C. Object deference
D. Cross-site request forgery

Answer: B

NEW QUESTION 165
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 166
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 169
In which of the following common use cases would steganography be employed?

A. Obfuscation
B. Integrity
C. Non-repudiation
D. Blockchain

Answer: A

NEW QUESTION 173
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 175
The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

A. Updating the playbooks with better decision points
B. Dividing the network into trusted and untrusted zones
C. Providing additional end-user training on acceptable use
D. Implementing manual quarantining of infected hosts

Answer: A

NEW QUESTION 177
The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.
B. Prevent data exposure queries.
C. Obfuscate the source code.
D. Submit the application to QA before releasing it.

Answer: D

NEW QUESTION 179
Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the read data?

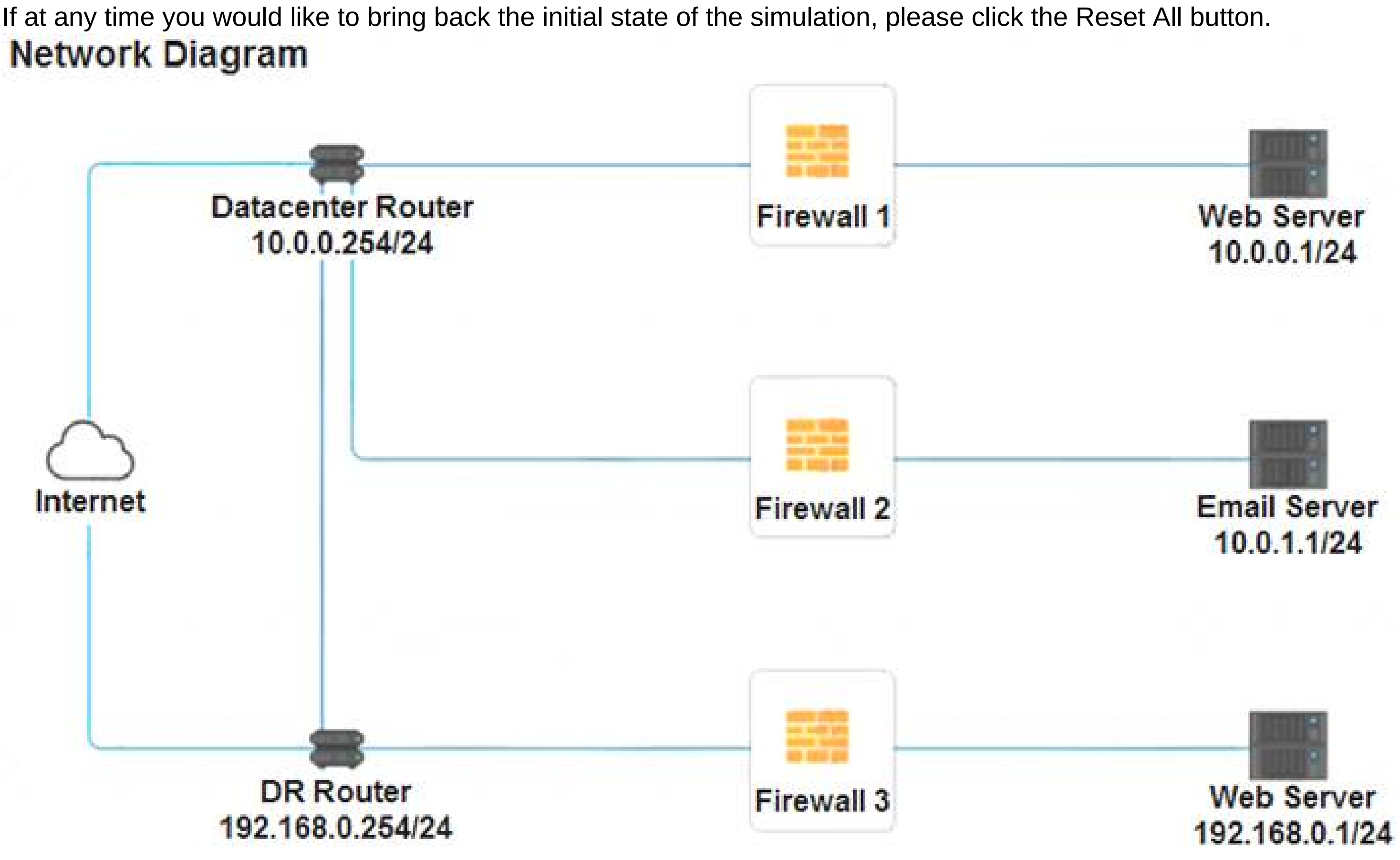
A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization

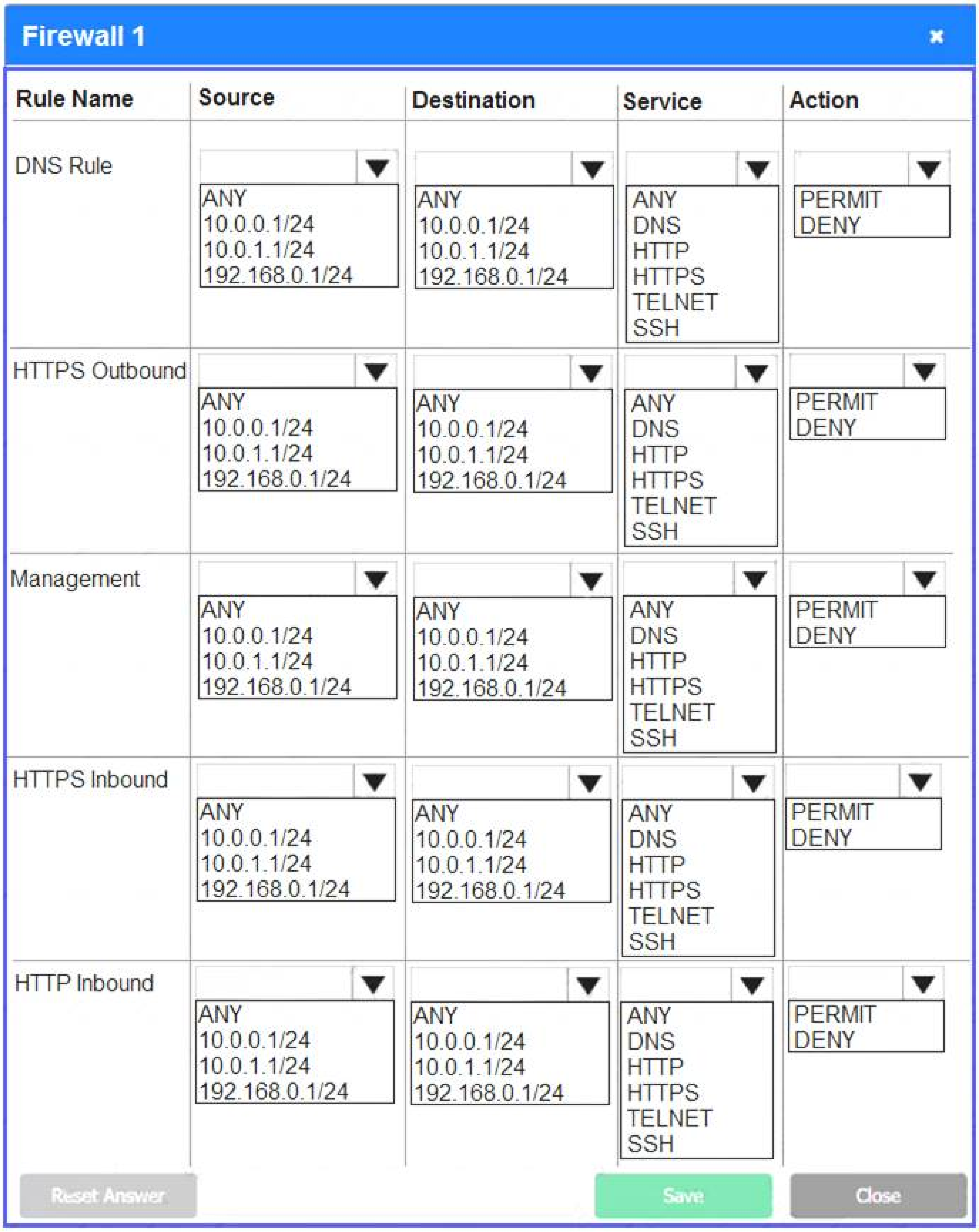
Answer: B

NEW QUESTION 184
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.

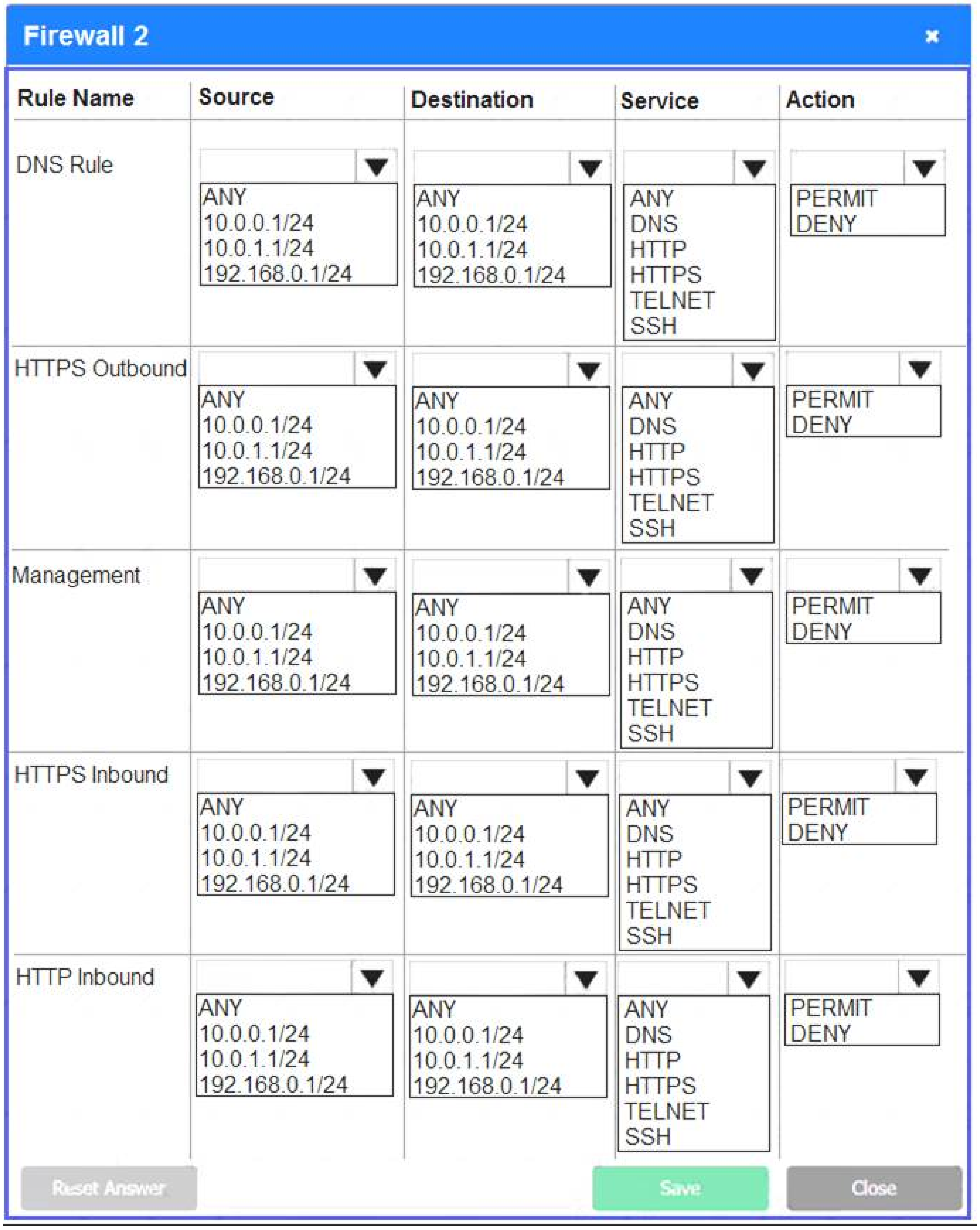
The ruleset order cannot be modified due to outside constraints.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





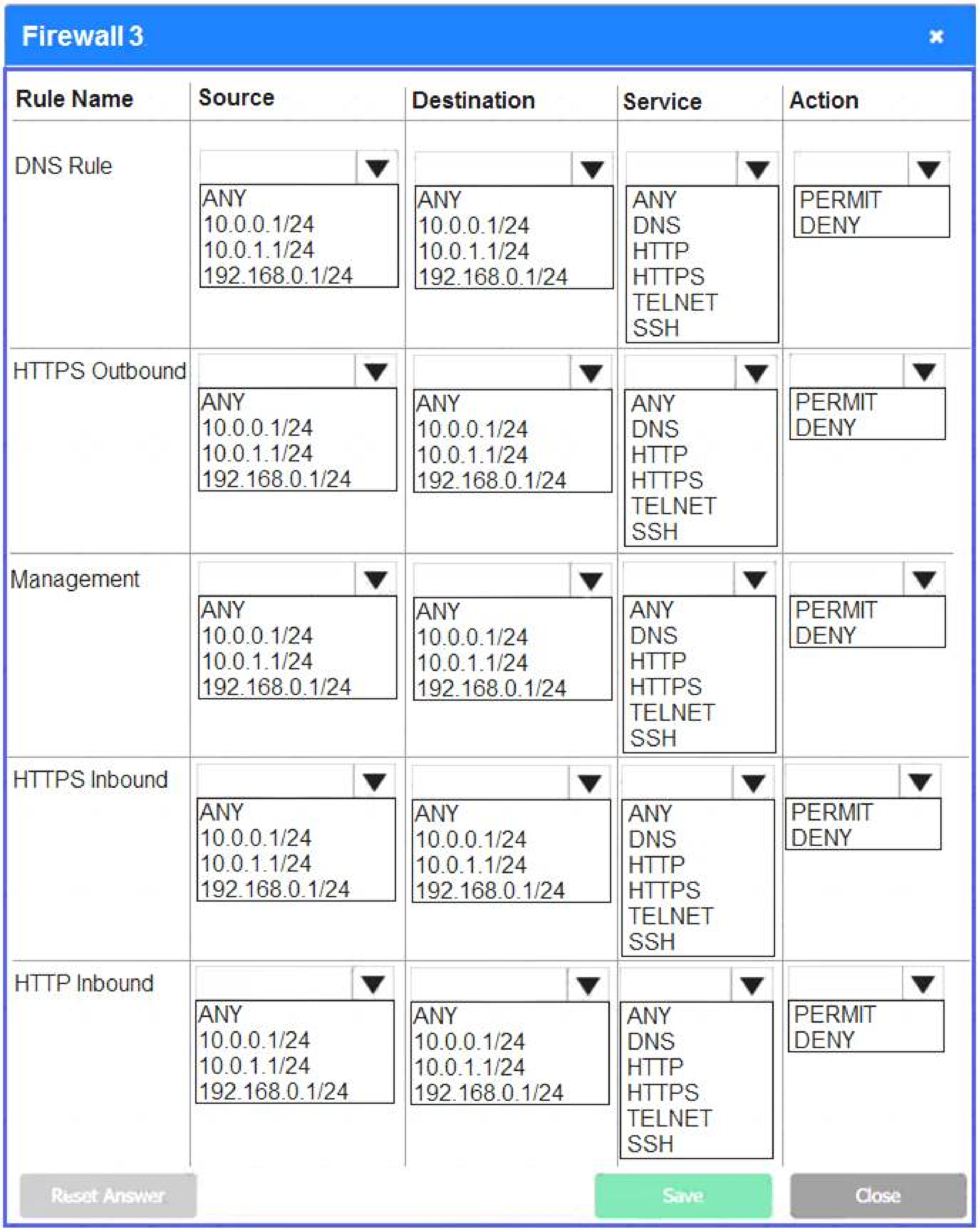
Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY



Firewall 2 ✖

Rule Name	Source	Destination	Service	Action
DNS Rule	▼ ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	▼ ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	▼ ANY DNS HTTP HTTPS TELNET SSH	▼ PERMIT DENY
HTTPS Outbound	▼ ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	▼ ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	▼ ANY DNS HTTP HTTPS TELNET SSH	▼ PERMIT DENY
Management	▼ ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	▼ ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	▼ ANY DNS HTTP HTTPS TELNET SSH	▼ PERMIT DENY
HTTPS Inbound	▼ ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	▼ ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	▼ ANY DNS HTTP HTTPS TELNET SSH	▼ PERMIT DENY
HTTP Inbound	▼ ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	▼ ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	▼ ANY DNS HTTP HTTPS TELNET SSH	▼ PERMIT DENY



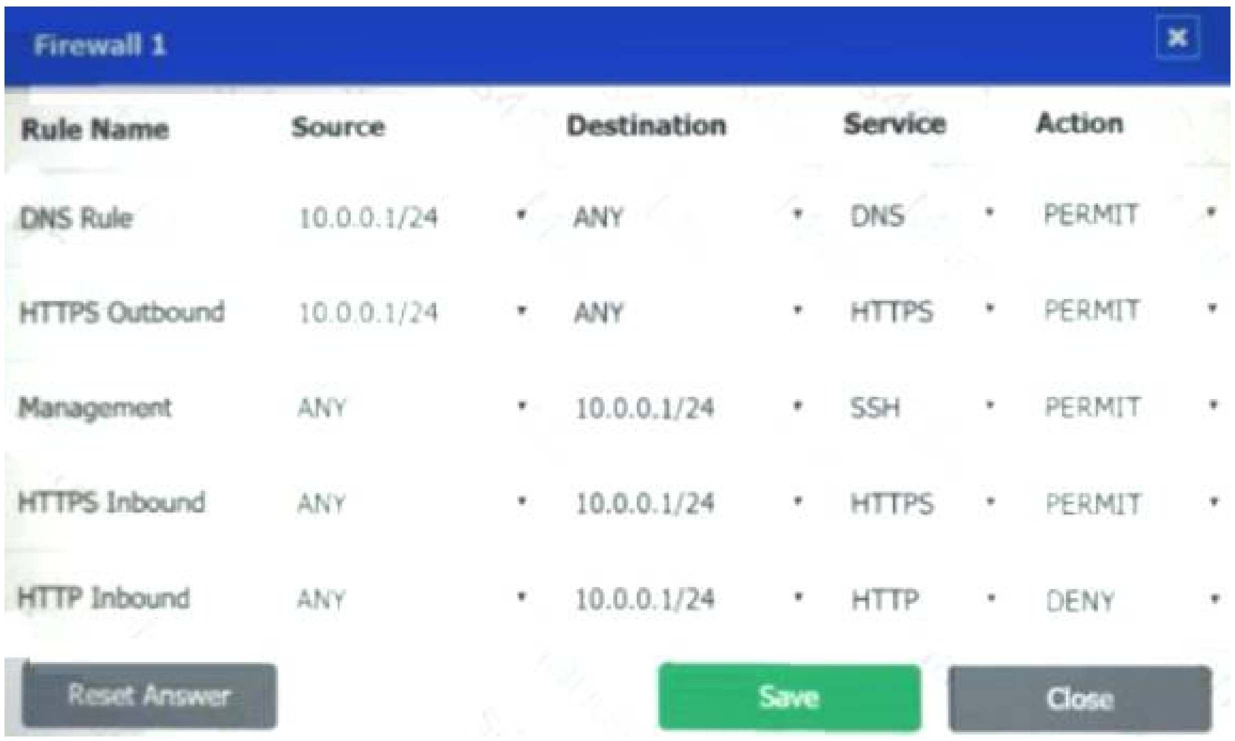
Firewall 3

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY

A.

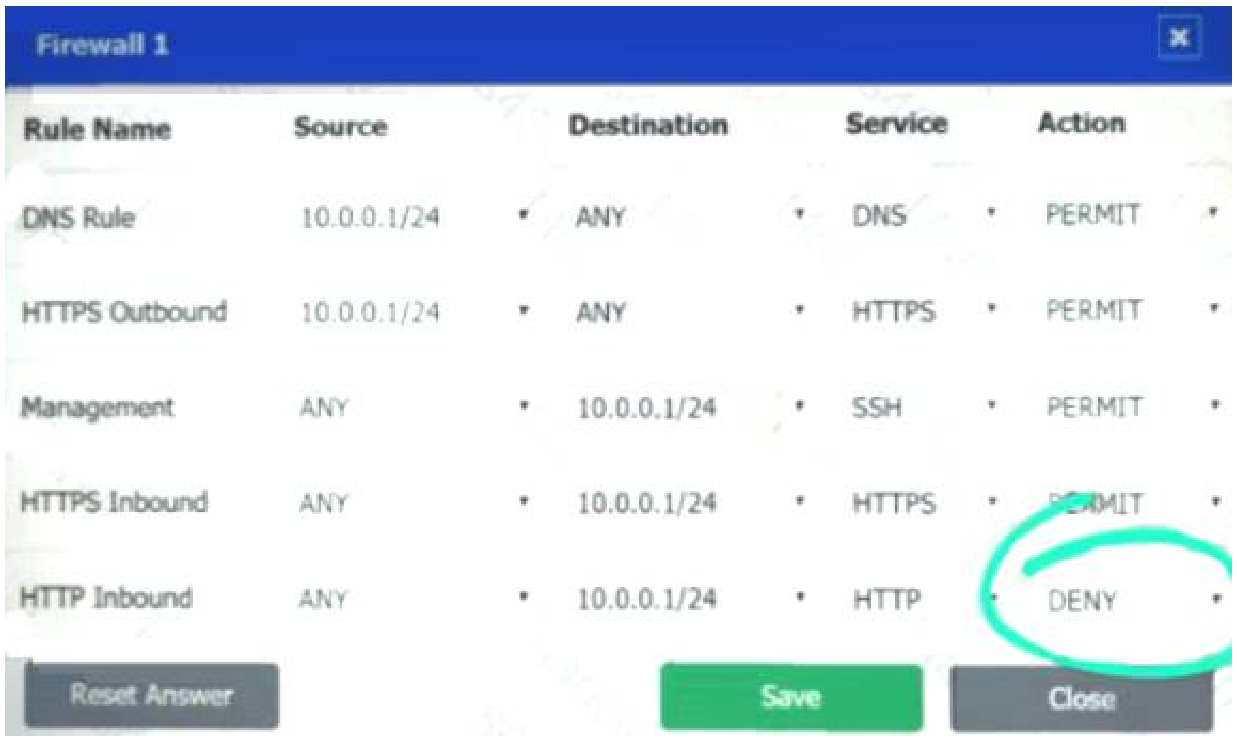
Answer: A

Explanation:
See explanation below.
Explanation
Firewall 1:



Firewall 1

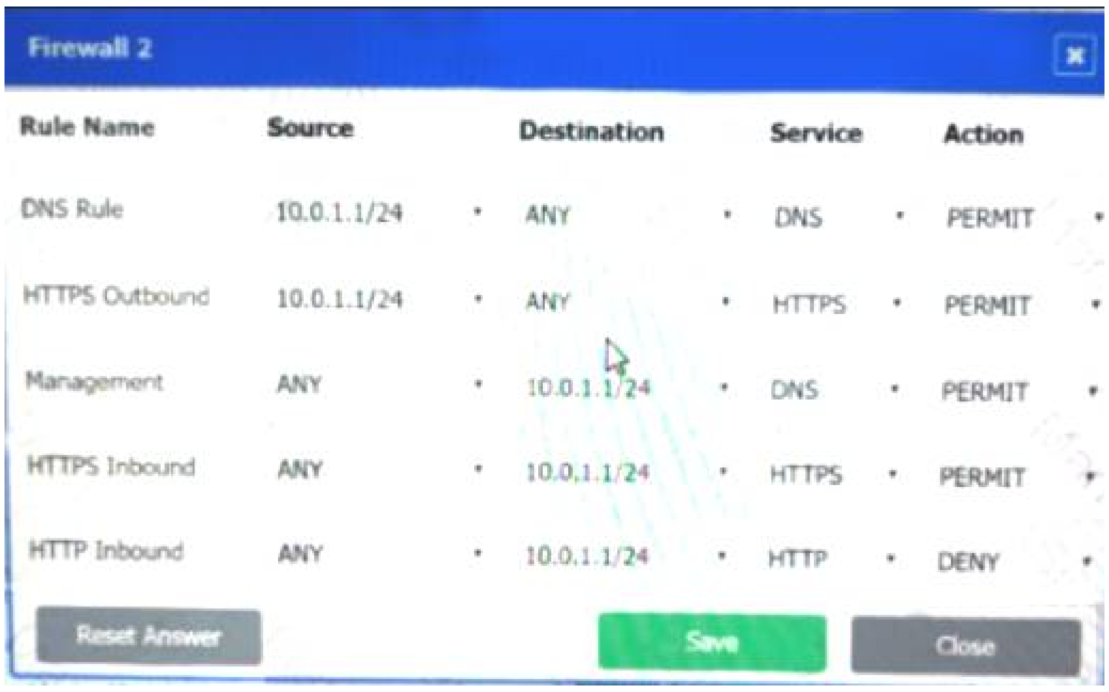
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY



Firewall 1

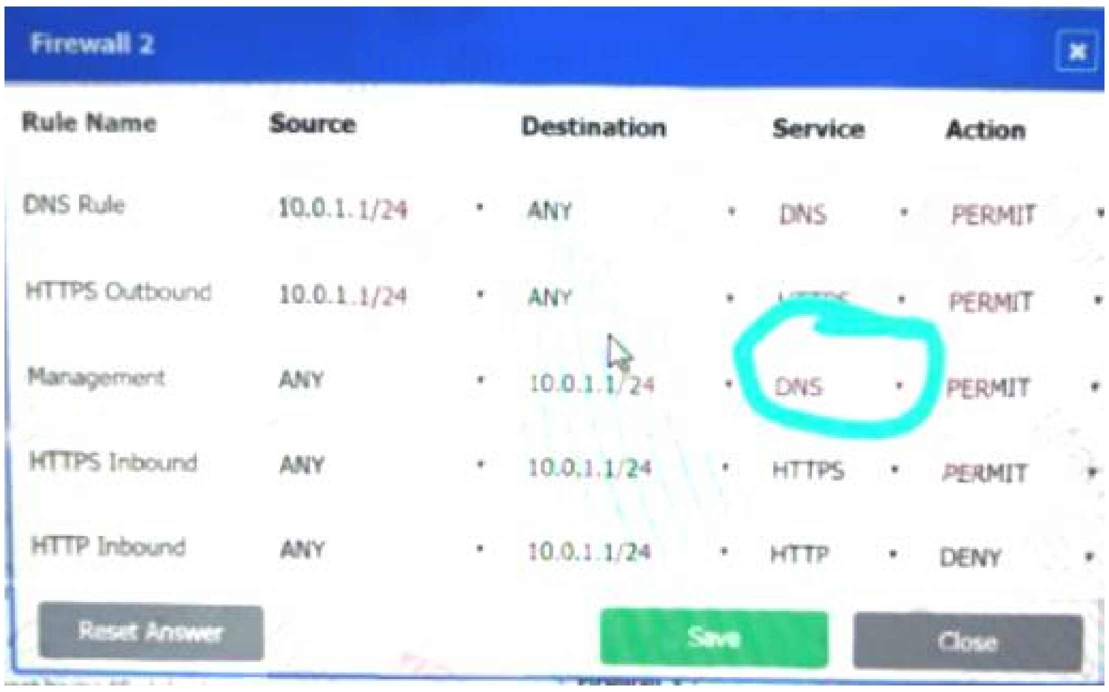
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY

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:



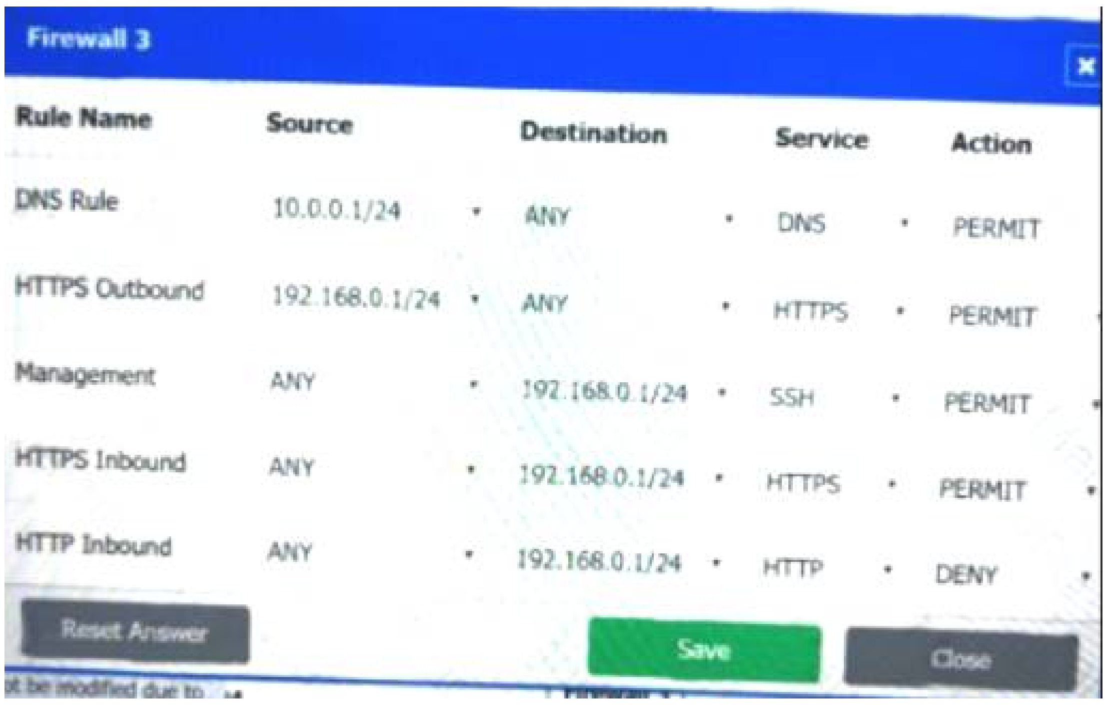
Firewall 2

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

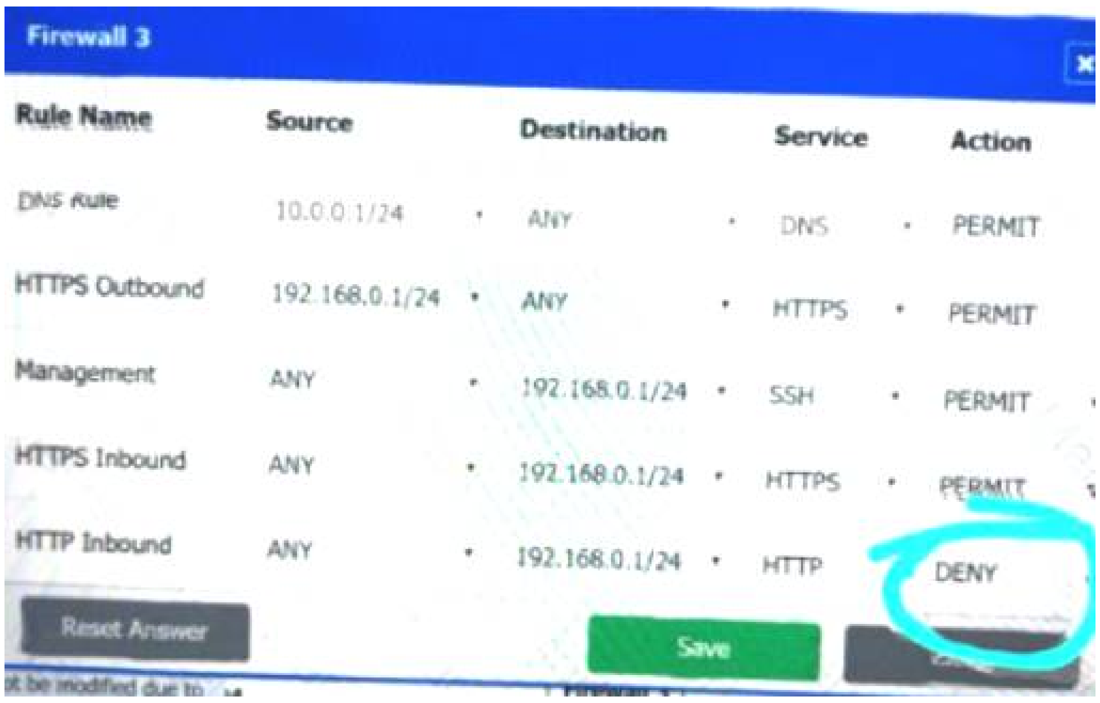


Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Firewall 3:



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



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 187

An organization has decided to host its web application and database in the cloud Which of the following BEST describes the security concerns for this decision?

A. Access to the organization's servers could be exposed to other cloud-provider clients
B. The cloud vendor is a new attack vector within the supply chain
C. Outsourcing the code development adds risk to the cloud provider
D. Vendor support will cease when the hosting platforms reach EOL.

Answer: B

NEW QUESTION 191

The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO’s concerns?

A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.

B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
C. SSO would reduce the password complexity for frontline staff.
D. SSO would reduce the resilience and availability of system if the provider goes offline.

Answer: D

NEW QUESTION 192
An organization just experienced a major cyberattack modem. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?

A. Shadow IT
B. An insider threat
C. A hacktivist
D. An advanced persistent threat

Answer: D

NEW QUESTION 196
When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

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

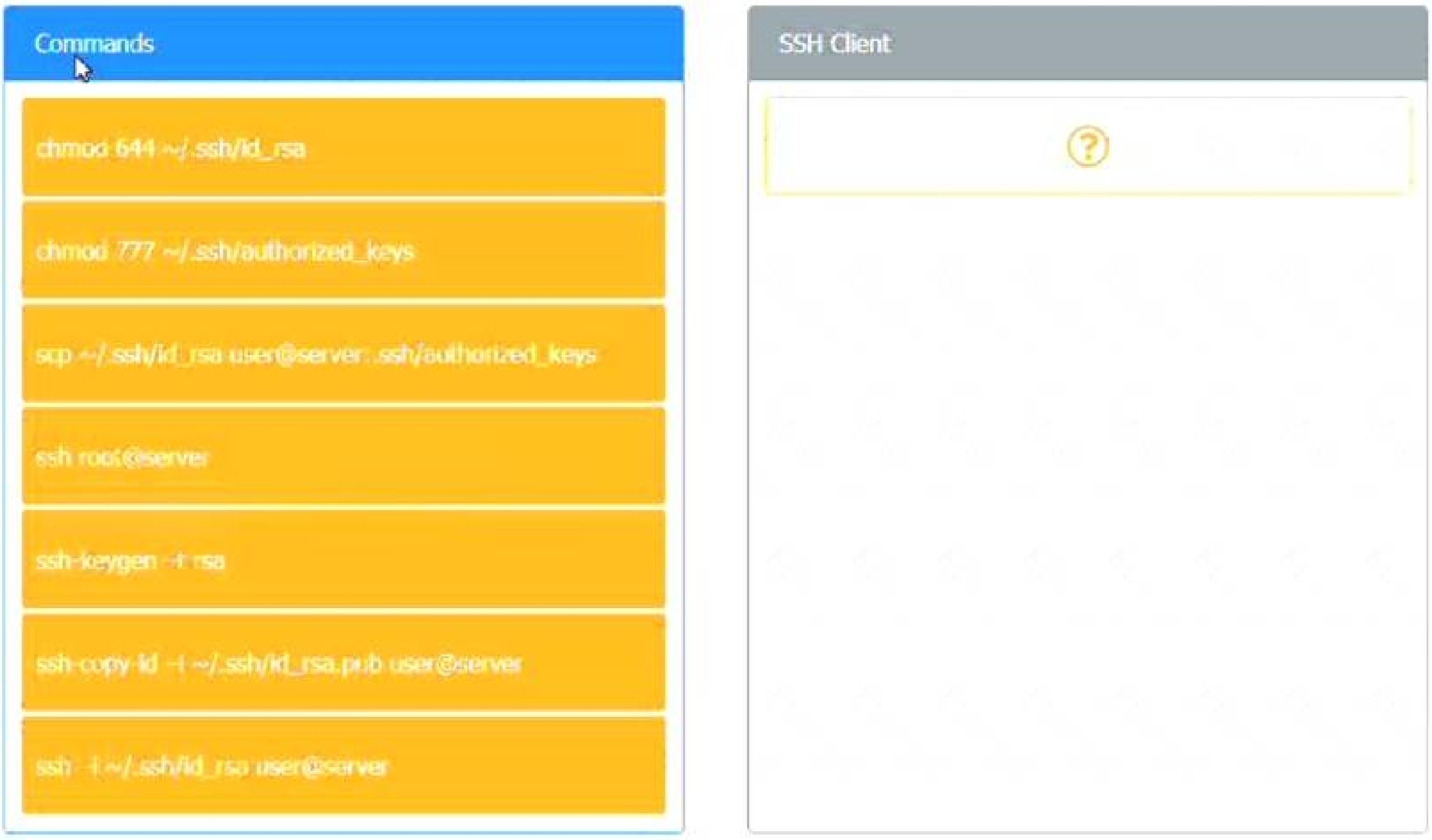
Answer: D

NEW QUESTION 197
A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB
D. SWG

Answer: C

NEW QUESTION 198
A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS
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.

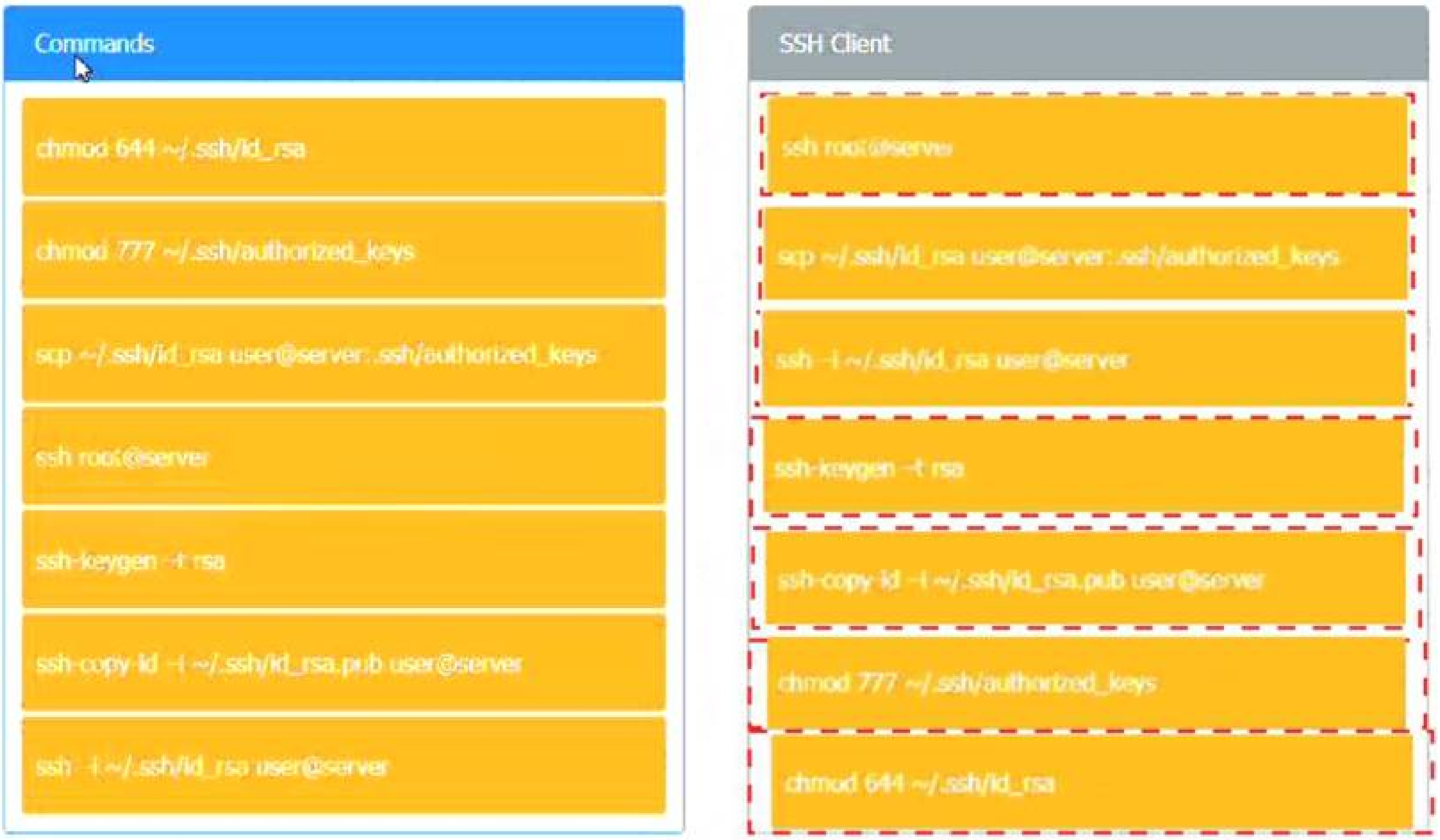


```
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Commands

```
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
```

SSH Client

```
ssh root@server
scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys
ssh -i ~/.ssh/id_rsa user@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
chmod 777 ~/.ssh/authorized_keys
chmod 644 ~/.ssh/id_rsa
```

NEW QUESTION 201
Users at organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function property. Which of the following should the security administrator consider implementing to address this issue?

A. Application code signing
B. Application whitellsting
C. Data loss prevention
D. Web application firewalls

Answer: B

NEW QUESTION 204
The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of $10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

A. Phishing
B. Whaling
C. Typo squatting
D. Pharming

Answer: B

NEW QUESTION 205
While checking logs, a security engineer notices a number of end users suddenly downloading files with the .t ar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.
B. The workstations are beaconing to a command-and-control server.
C. A logic bomb was executed and is responsible for the data transfers.
D. A fireless virus is spreading in the local network environment.

Answer: A

NEW QUESTION 206
A security administrator needs to create a RAIS configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the following RAID configurations should the administration use?

A. RA1D 0
B. RAID1
C. RAID 5
D. RAID 10

Answer: C

NEW QUESTION 210
A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

A. Predictability
B. Key stretching
C. Salting
D. Hashing

Answer: C

NEW QUESTION 213
Which of the following types of controls is a turnstile?

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

Answer: A

NEW QUESTION 214
A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

A. Mobile device management
B. Full-device encryption
C. Remote wipe
D. Biometrics

Answer: A

NEW QUESTION 215
A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money that 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 219
An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?

A. Incident response
B. Communications
C. Disaster recovery
D. Data retention

Answer: C

NEW QUESTION 223
Which of the following would be the BEST resource lor a software developer who is looking to improve secure coding practices for web applications?

A. OWASP
B. Vulnerability scan results
C. NIST CSF
D. Third-party libraries

Answer: A

NEW QUESTION 226
Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

A. The data protection officer
B. The data processor
C. The data owner
D. The data controller

Answer: C

NEW QUESTION 231

A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

A. A captive portal
B. PSK
C. 802.1X
D. WPS

Answer: C

NEW QUESTION 236
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 238
A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis
B. Restrict administrative privileges and patch ail systems and applications.
C. Rebuild all workstations and install new antivirus software
D. Implement application whitelisting and perform user application hardening

Answer: A

NEW QUESTION 239
A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?

A. Set up an air gap for the switch.
B. Change the default password for the switch.
C. Place the switch In a Faraday cage.
D. Install a cable lock on the switch

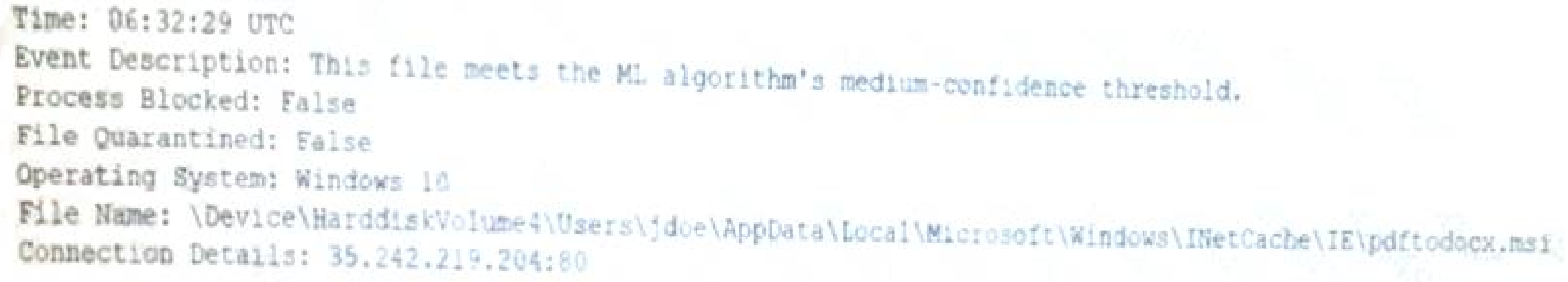
Answer: B

NEW QUESTION 243
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 248
An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:



```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\IE\pdftodocx.msi
Connection Details: 35.242.219.204:80
```

Which of the following is the MOST likely cause of the issue?

A. The end user purchased and installed a PUP from a web browser
B. A bot on the computer is brute forcing passwords against a website
C. A hacker is attempting to exfiltrate sensitive data
D. Ransomware is communicating with a command-and-control server.

Answer: A

NEW QUESTION 253

......

NEW QUESTION 1
A security analyst needs to make a recommendation for restricting access to certain segments of the network using only data-link layer security. Which of the following controls will the analyst MOST likely recommend?

A. MAC
B. ACL
C. BPDU
D. ARP

Answer: A

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, andthen apply them to the production systems
C. Test the patches m 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
A cybersecurity department purchased o new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

A. Randomize the shared credentials
B. Use only guest accounts to connect.
C. Use SSH keys and remove generic passwords
D. Remove all user accounts.

Answer: C

NEW QUESTION 4
A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

A. perform attribution to specific APTs and nation-state actors.
B. anonymize any PII that is observed within the IoC data.
C. add metadata to track the utilization of threat intelligence reports.
D. assist companies with impact assessments based on the observed data.

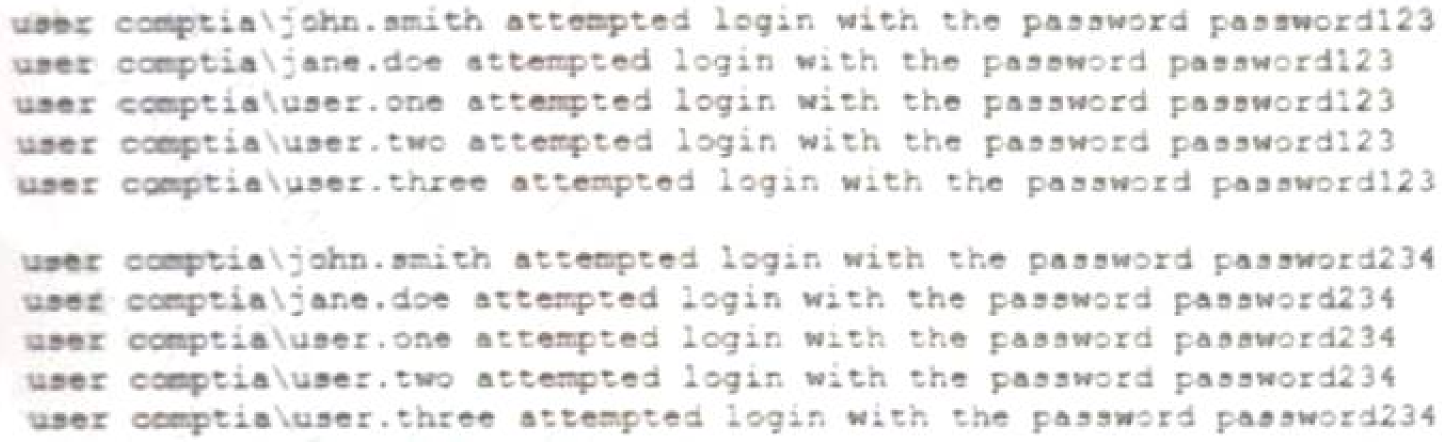
Answer: B

NEW QUESTION 5
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Answer: AD

NEW QUESTION 6
A security analyst is reviewing the following attack log output:



```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

A. Rainbow table
B. Brute-force

C. Password-spraying
D. Dictionary

Answer: C

NEW QUESTION 7
Which of the following relets to applications and systems that are used within an organization without consent or approval?

A. Shadow IT
B. OSINT
C. Dark web
D. Insider threats

Answer: A

NEW QUESTION 8
Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

A. The data owner
B. The data processor
C. The data steward
D. The data privacy officer.

Answer: C

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 malicious actor recently penetration a company’s network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

A. Security
B. Application
C. Dump
D. Syslog

Answer: C

NEW QUESTION 10
A security administrator currently spends a large amount of time on common security tasks, such aa report generation, phishing investigations, and user provisioning and deprovisioning This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

A. DAC
B. ABAC
C. SCAP
D. SOAR

Answer: D

NEW QUESTION 11
A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

A. Physical
B. Detective
C. Preventive
D. Compensating

Answer: D

NEW QUESTION 12
A security analyst has received an alert about being sent via email. The analyst’s Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care From which of the following did the alert MOST likely originate?

A. S/MIME
B. DLP
C. IMAP
D. HIDS

Answer: B

NEW QUESTION 17
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 poising

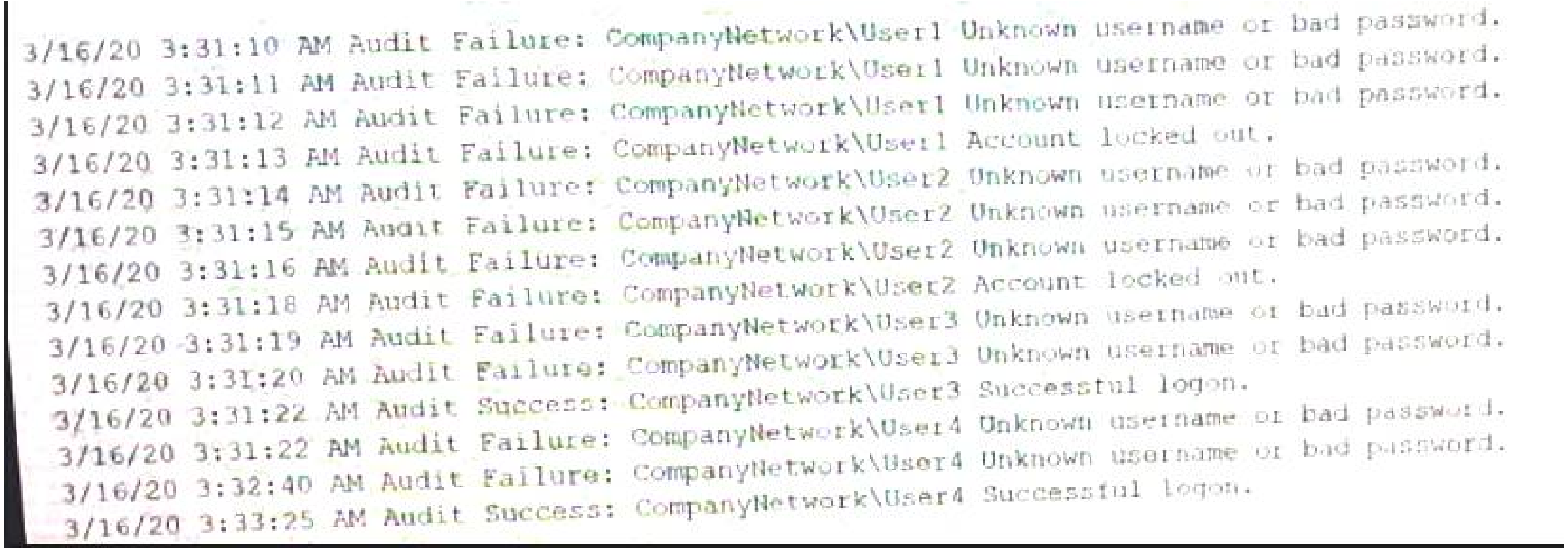
Answer: D

NEW QUESTION 19
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 22
A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:



```
3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.
3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User2 Account locked out.
3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:20 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful logon.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful logon.
```

Which of the following attacks MOST likely occurred?

A. Dictionary
B. Credential-stuffing
C. Password-spraying
D. Brute-force

Answer: D

NEW QUESTION 25
A symmetric encryption algorithm Is BEST suited for:

A. key-exchange scalability.
B. protecting large amounts of data.
C. providing hashing capabilities,
D. implementing non-repudiation.

Answer: D

NEW QUESTION 28
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 recent 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 32
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 36
The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the blowing would BEST address this security concern?

A. install a smart meter on the staff WiFi.
B. Place the environmental systems in the same DHCP scope as the staff WiFi.
C. Implement Zigbee on the staff WiFi access points.
D. Segment the staff WiFi network from the environmental systems network.

Answer: D

NEW QUESTION 39
A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

A. PCI DSS
B. ISO 22301
C. ISO 27001
D. NIST CSF

Answer: A

NEW QUESTION 43
To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

A. A password reuse policy
B. Account lockout after three failed attempts
C. Encrypted credentials in transit
D. A geofencing policy based on login history

Answer: C

NEW QUESTION 45
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 46
A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?

A. Open the document on an air-gapped network
B. View the document's metadata for origin clues
C. Search for matching file hashes on malware websites
D. Detonate the document in an analysis sandbox

Answer: D

NEW QUESTION 51
A system administrator needs to implement an access control scheme that will allow an object's access policy be determined by its owner. Which of the following access control schemes BEST fits the requirements?

A. Role-based access control
B. Discretionary access control

C. Mandatory access control
D. Attribute-based access control

Answer: B

NEW QUESTION 54
A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

A. Perform a site survey
B. Deploy an FTK Imager
C. Create a heat map
D. Scan for rogue access points
E. Upgrade the security protocols
F. Install a captive portal

Answer: AC

NEW QUESTION 59
A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

A. CVE
B. SIEM
C. SOAR
D. CVSS

Answer: D

NEW QUESTION 63
A workwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

A. Network location
B. Impossible travel time
C. Geolocation
D. Geofencing

Answer: D

NEW QUESTION 67
A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

A. Dual power supply
B. Off-site backups
C. Automatic OS upgrades
D. NIC teaming
E. Scheduled penetration testing
F. Network-attached storage

Answer: AB

NEW QUESTION 68
Which of the following is a team of people dedicated testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

A. Red team
B. While team
C. Blue team
D. Purple team

Answer: A

NEW QUESTION 73
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 77
In which of the following situations would it be BEST to use a detective control type for mitigation?

A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
E. A company purchased liability insurance for flood protection on all capital assets.

Answer: D

NEW QUESTION 79
A security engineer needs to Implement the following requirements:
• All Layer 2 switches should leverage Active Directory tor authentication.
• All Layer 2 switches should use local fallback authentication If Active Directory Is offline.
• All Layer 2 switches are not the same and are manufactured by several vendors.
Which of the following actions should the engineer take to meet these requirements? (Select TWO).

A. Implement RADIUS.
B. Configure AAA on the switch with local login as secondary.
C. Configure port security on the switch with the secondary login method.
D. Implement TACACS+
E. Enable the local firewall on the Active Directory server.
F. Implement a DHCP server.

Answer: AB

NEW QUESTION 83
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 86
An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

A. An external security assessment
B. A bug bounty program
C. A tabletop exercise
D. A red-team engagement

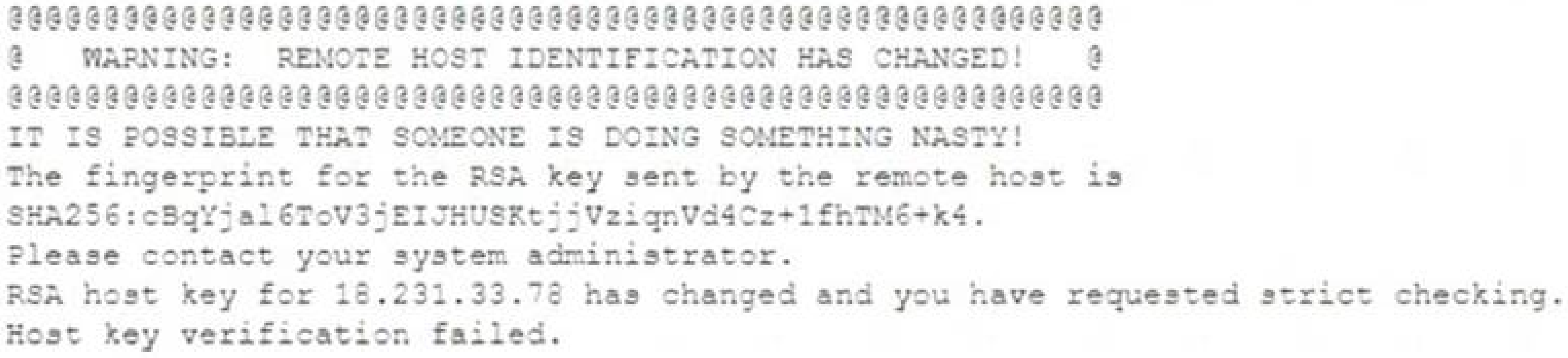
Answer: C

NEW QUESTION 91
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 95
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 99
Which of the following algorithms has the SMALLEST key size?

A. DES
B. Twofish
C. RSA
D. AES

Answer: B

NEW QUESTION 103
An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

A. SED
B. HSM
C. DLP
D. TPM

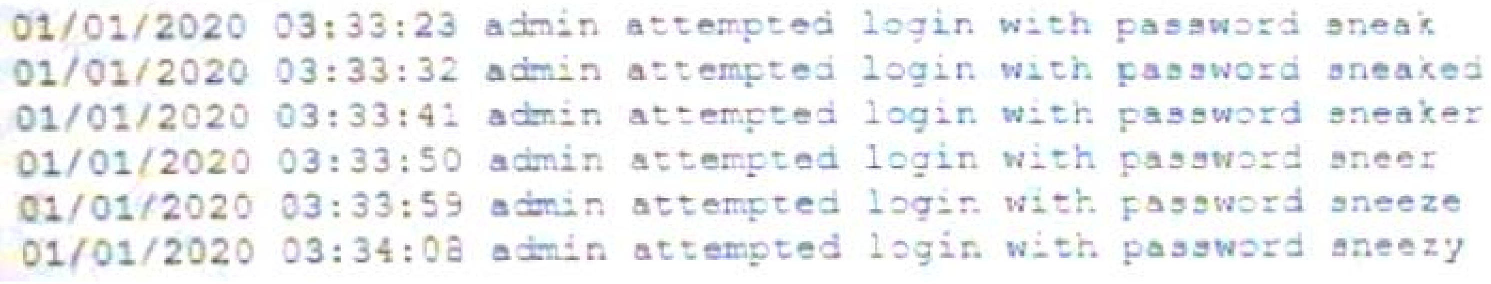
Answer: A

NEW QUESTION 106
A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

A. validate the vulnerability exists in the organization's network through penetration testing
B. research the appropriate mitigation techniques in a vulnerability database
C. find the software patches that are required to mitigate a vulnerability
D. prioritize remediation of vulnerabilities based on the possible impact.

Answer: D

NEW QUESTION 110
A security analyst is reviewing logs on a server and observes the following output:



```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

A. A rainbow table attack
B. A password-spraying attack
C. A dictionary attack
D. A keylogger attack

Answer: C

NEW QUESTION 112
A root cause analysis reveals that a web application outage was caused by one of the company’s developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

A. CASB
B. SWG
C. Containerization
D. Automated failover

Answer: C

NEW QUESTION 117
An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering it the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO’s concerns?

A. Disallow new hires from using mobile devices for six months
B. Select four devices for the sales department to use in a CYOD model
C. Implement BYOD for the sates department while leveraging the MDM

D. Deploy mobile devices using the COPE methodology

Answer: C

NEW QUESTION 120
Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe’s identity before sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing
B. Whaling
C. Phishing
D. Vishing

Answer: C

NEW QUESTION 121
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 whiteboars 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 126
The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

A. A script kiddie
B. Shadow IT
C. Hacktivism
D. White-hat

Answer: B

NEW QUESTION 127
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 128
The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

A. data controller.
B. data owner
C. data custodian.
D. data processor

Answer: D

NEW QUESTION 133
An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load Which of the following are the BEST options to accomplish this objective'? (Select TWO)

A. Load balancing
B. Incremental backups
C. UPS
D. RAID
E. Dual power supply
F. NIC teaming

Answer: AD

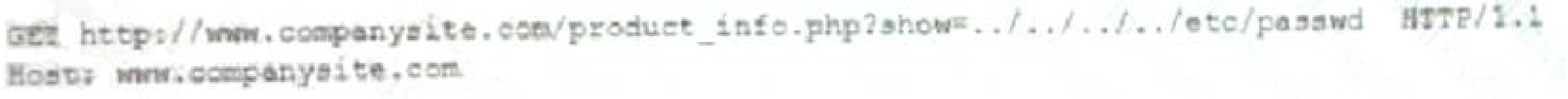
NEW QUESTION 137
A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts

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 138
During an incident response, a security analyst observes the following log entry on the web server.



```
GET http://www.companysite.com/product_info.php?show=../../../../etc/passwd  HTTP/1.1
Host: www.companysite.com
```

Which of the following BEST describes the type of attack the analyst is experience?

A. SQL injection
B. Cross-site scripting
C. Pass-the-hash
D. Directory traversal

Answer: B

NEW QUESTION 139
After entering a username and password, and administrator must gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

A. Multifactor authentication
B. Something you can do
C. Biometric
D. Two-factor authentication

Answer: D

NEW QUESTION 140
A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

A. The GPS location
B. When the file was deleted
C. The total number of print jobs
D. The number of copies made

Answer: A

NEW QUESTION 142
A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

A. Developing an incident response plan
B. Building a disaster recovery plan
C. Conducting a tabletop exercise
D. Running a simulation exercise

Answer: C

NEW QUESTION 146
A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO) A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
B. Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command m a live Linux environment to create a duplicate copy
C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
D. Refrain from completing a forensic analysts of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence

Answer: D

NEW QUESTION 151
A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

A. iPSec

B. Always On
C. Split tunneling
D. L2TP

Answer: B

NEW QUESTION 152
Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

A. DLP
B. HIDS
C. EDR
D. NIPS

Answer: C

NEW QUESTION 157
Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

A. Investigation
B. Containment
C. Recovery
D. Lessons learned

Answer: B

NEW QUESTION 162
A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:
http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us
The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:
http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us Which of the following application attacks is being tested?

A. Pass-the-hash
B. Session replay
C. Object deference
D. Cross-site request forgery

Answer: B

NEW QUESTION 165
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 166
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 169
In which of the following common use cases would steganography be employed?

A. Obfuscation
B. Integrity
C. Non-repudiation
D. Blockchain

Answer: A

NEW QUESTION 173
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 175
The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

A. Updating the playbooks with better decision points
B. Dividing the network into trusted and untrusted zones
C. Providing additional end-user training on acceptable use
D. Implementing manual quarantining of infected hosts

Answer: A

NEW QUESTION 177
The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.
B. Prevent data exposure queries.
C. Obfuscate the source code.
D. Submit the application to QA before releasing it.

Answer: D

NEW QUESTION 179
Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the read data?

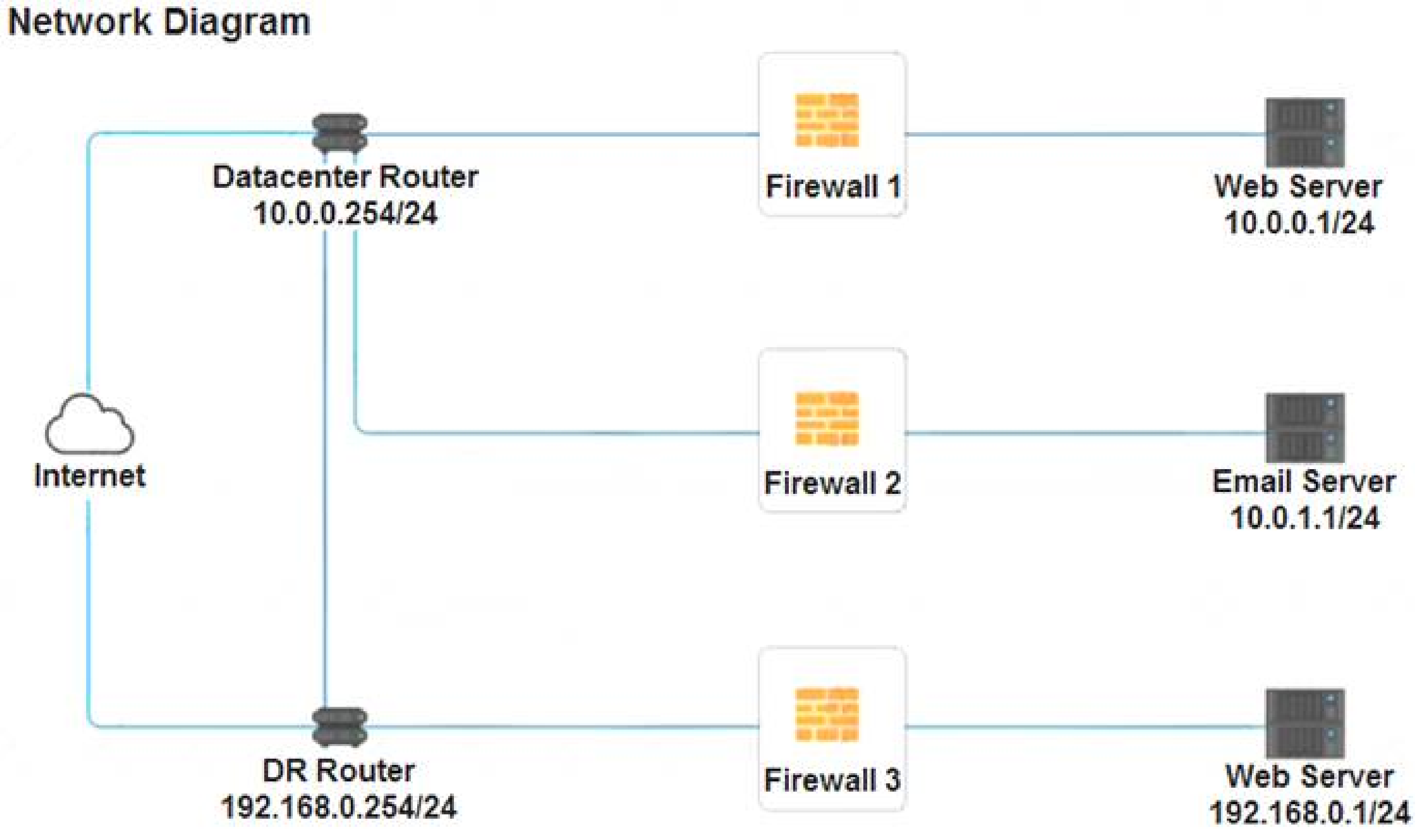
A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization

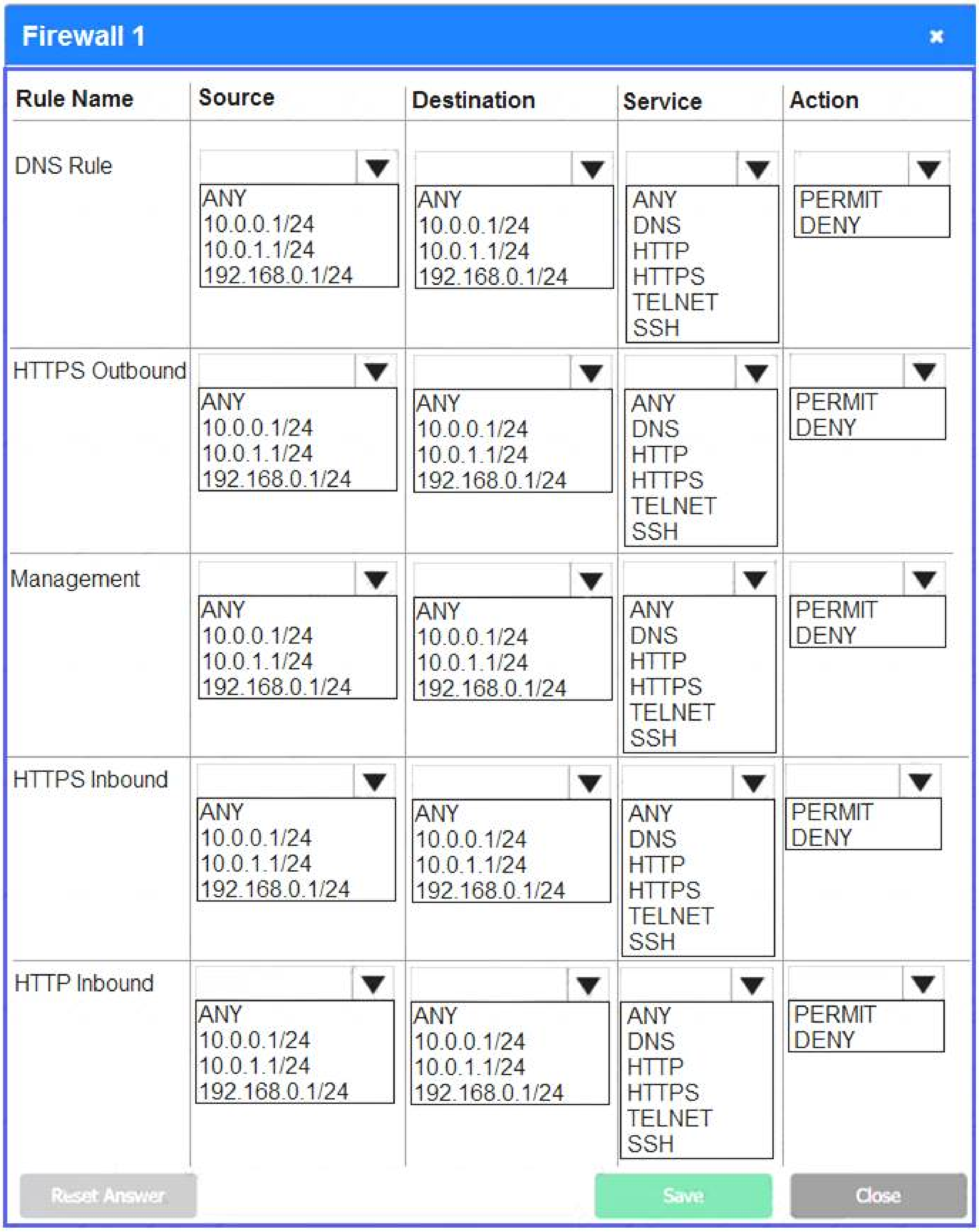
Answer: B

NEW QUESTION 184
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.

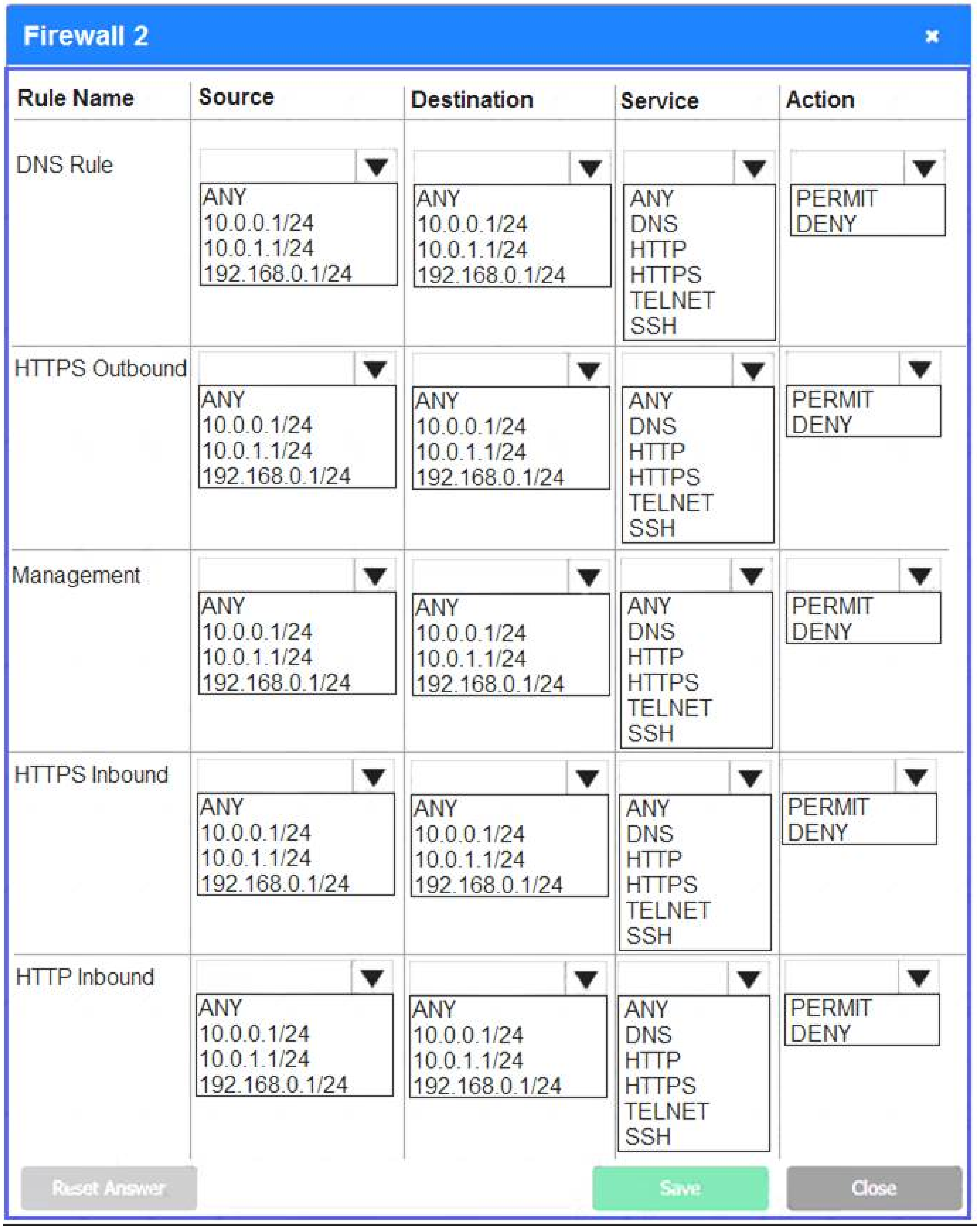
The ruleset order cannot be modified due to outside constraints.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





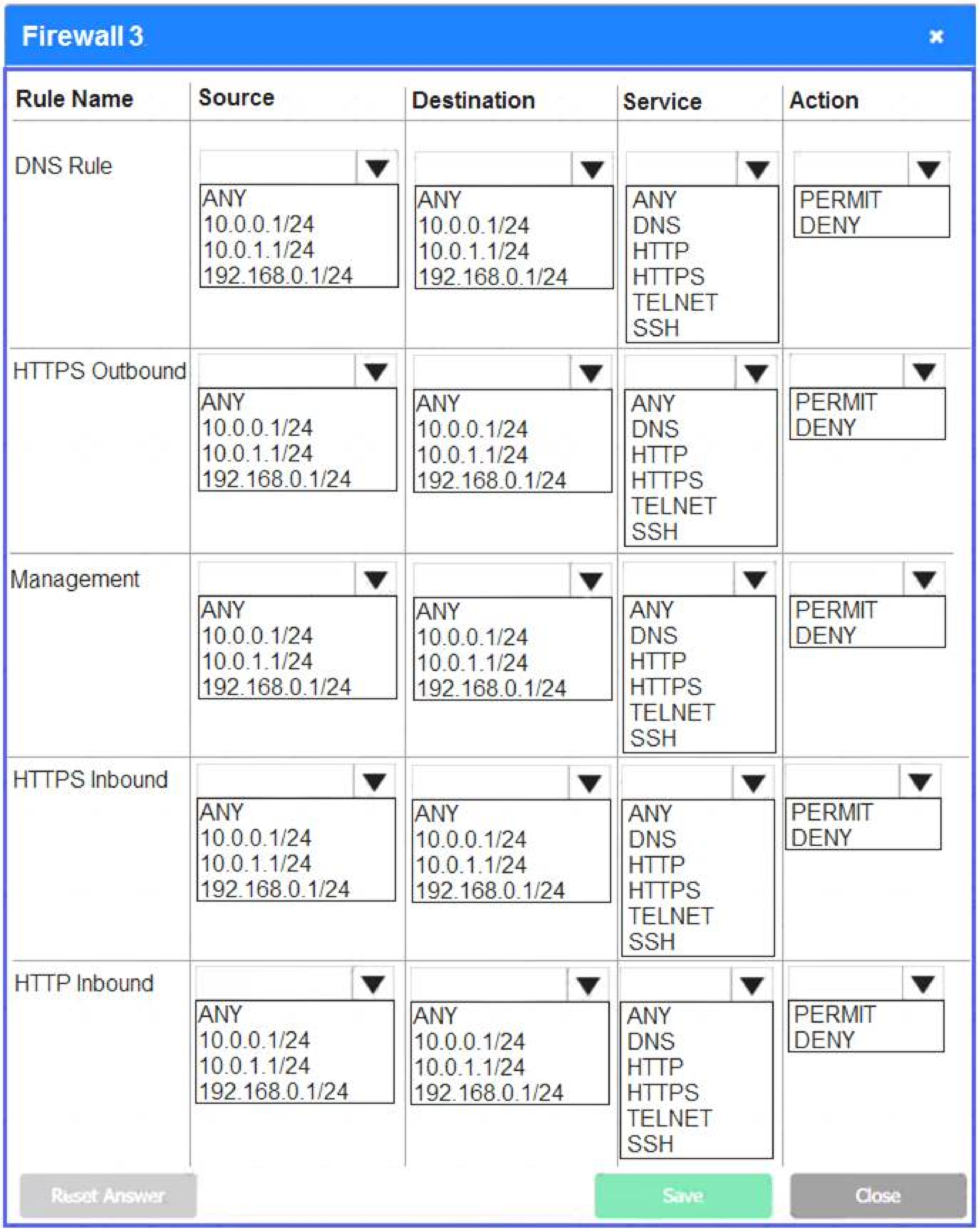
Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY



Firewall 2

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY



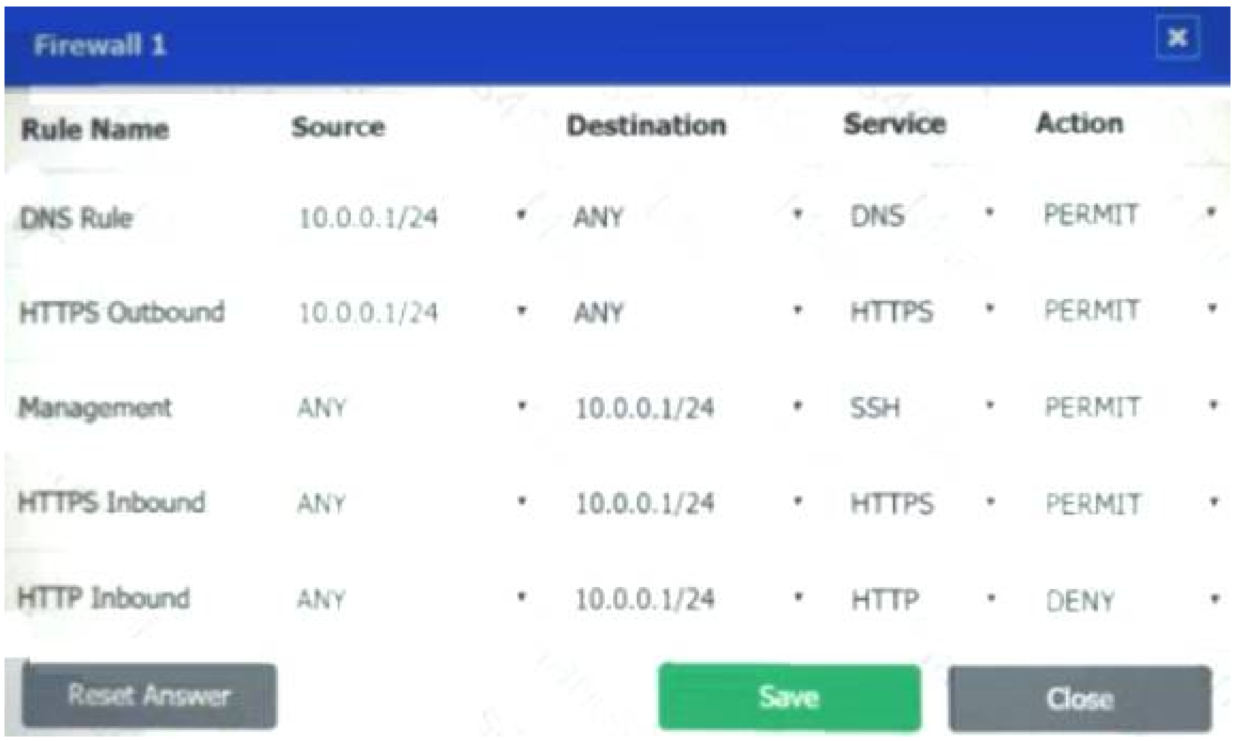
Firewall 3

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY

A.

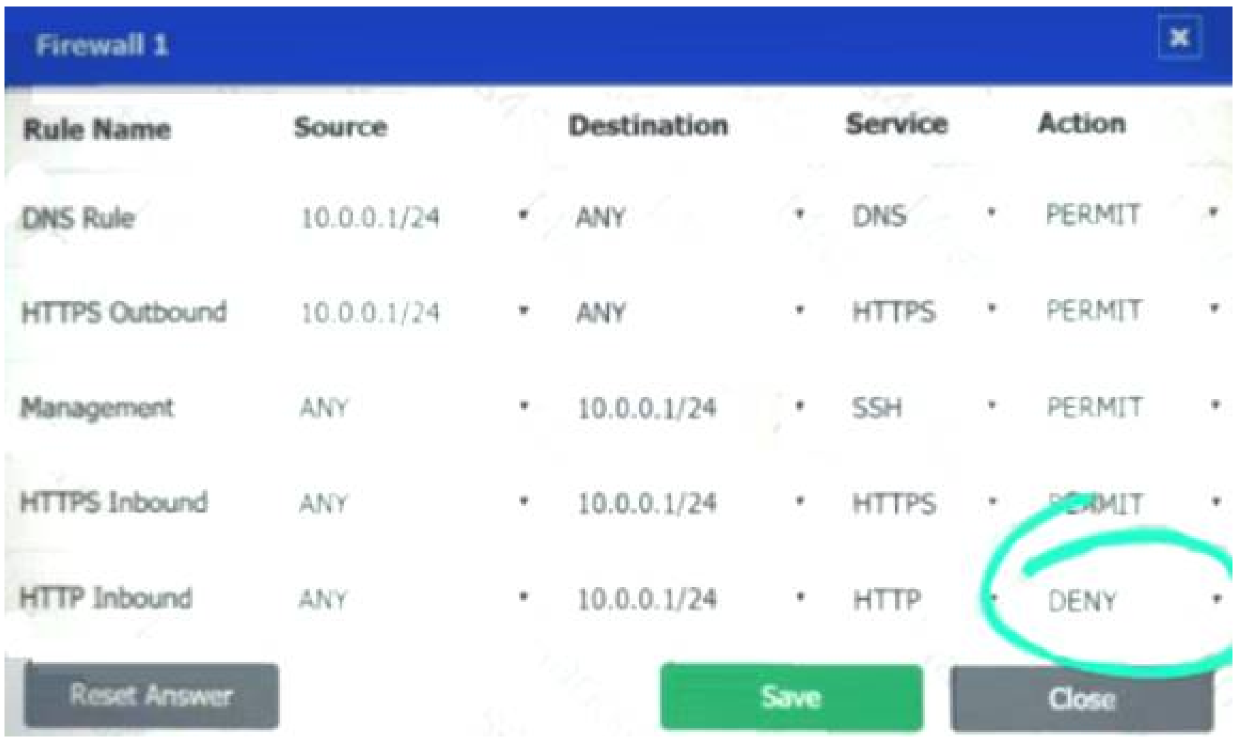
Answer: A

Explanation:
See explanation below.
Explanation
Firewall 1:



Firewall 1

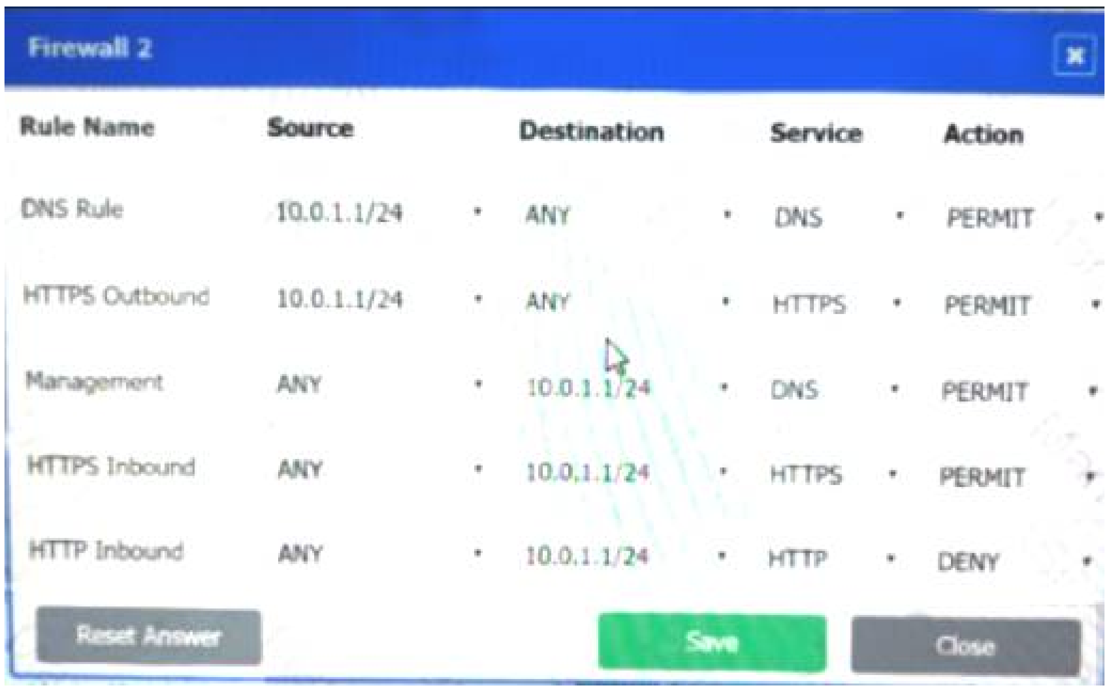
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY



Firewall 1

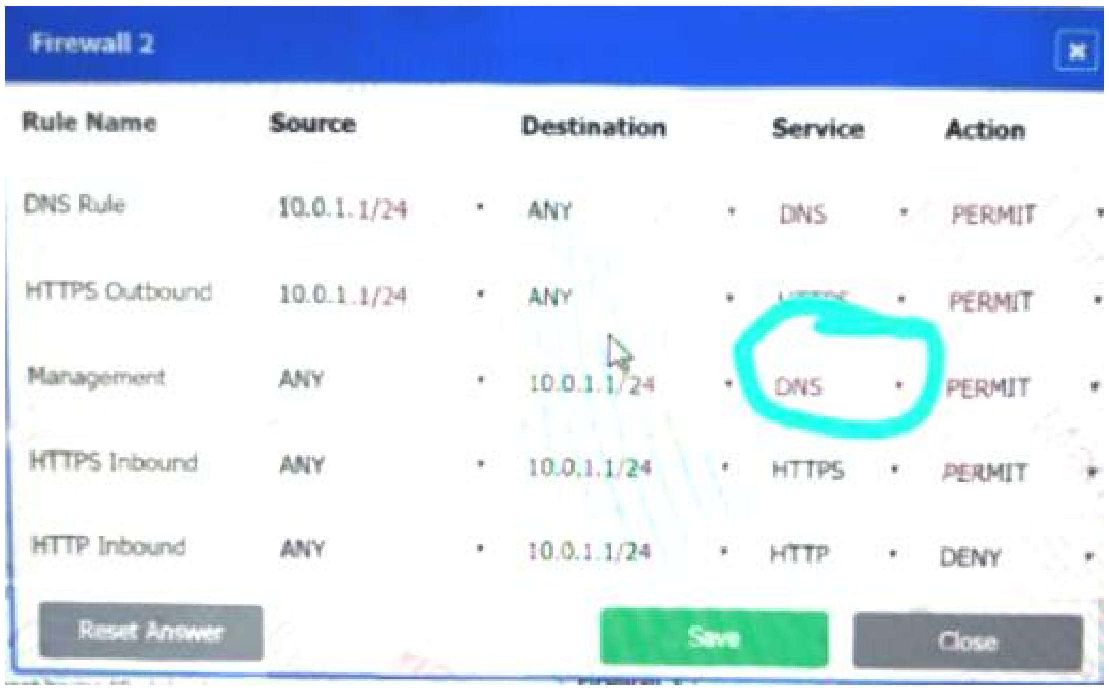
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY

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

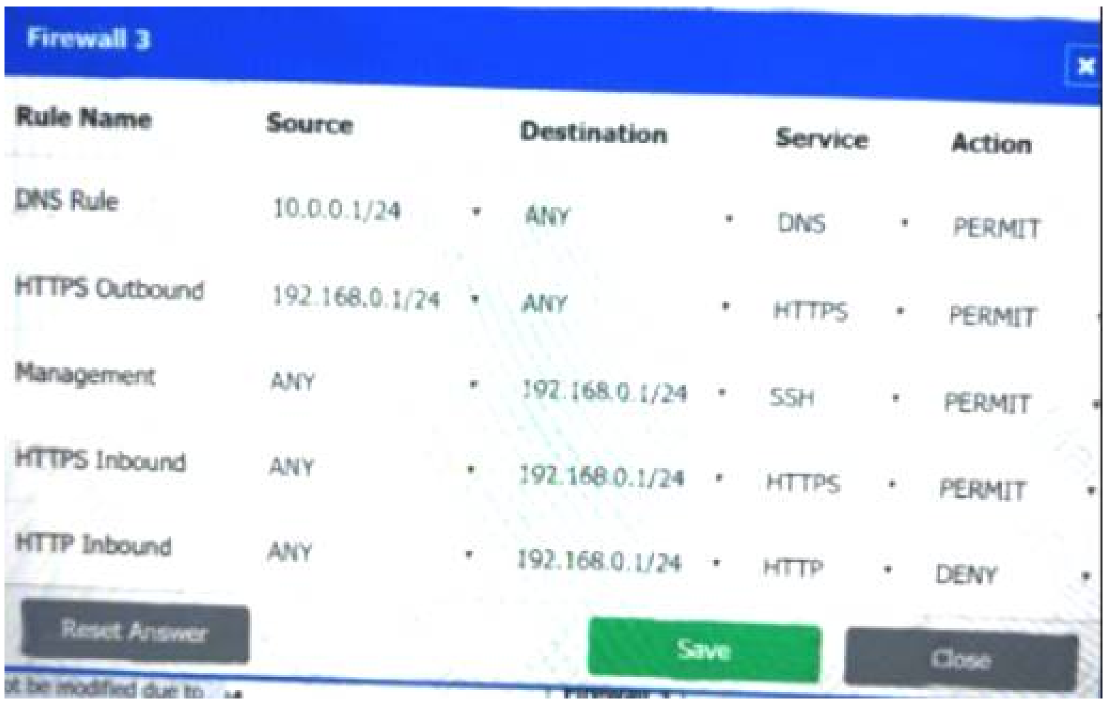
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY



Firewall 2

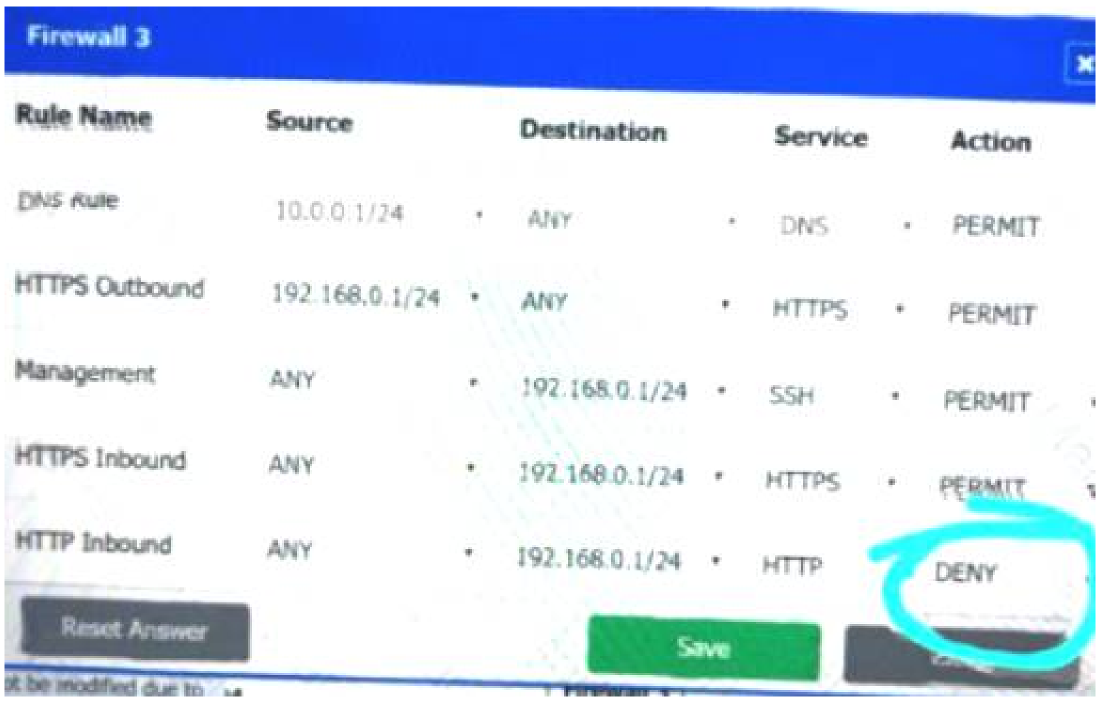
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

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 187
An organization has decided to host its web application and database in the cloud Which of the following BEST describes the security concerns for this decision?

A. Access to the organization's servers could be exposed to other cloud-provider clients
B. The cloud vendor is a new attack vector within the supply chain
C. Outsourcing the code development adds risk to the cloud provider
D. Vendor support will cease when the hosting platforms reach EOL.

Answer: B

NEW QUESTION 191
The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO’s concerns?

A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.

B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
C. SSO would reduce the password complexity for frontline staff.
D. SSO would reduce the resilience and availability of system if the provider goes offline.

Answer: D

NEW QUESTION 192
An organization just experienced a major cyberattack modem. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?

A. Shadow IT
B. An insider threat
C. A hacktivist
D. An advanced persistent threat

Answer: D

NEW QUESTION 196
When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

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

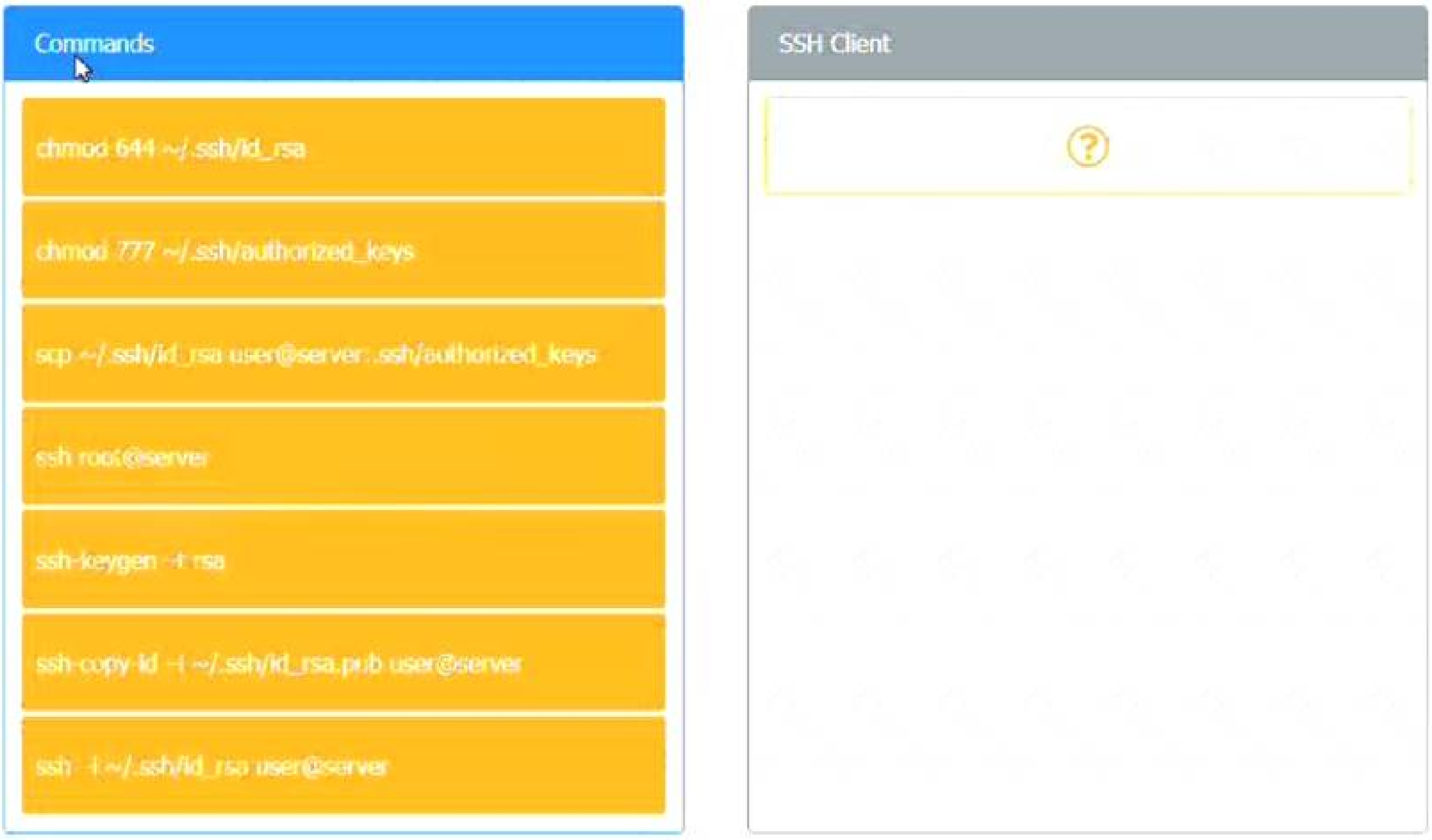
Answer: D

NEW QUESTION 197
A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB
D. SWG

Answer: C

NEW QUESTION 198
A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS
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.

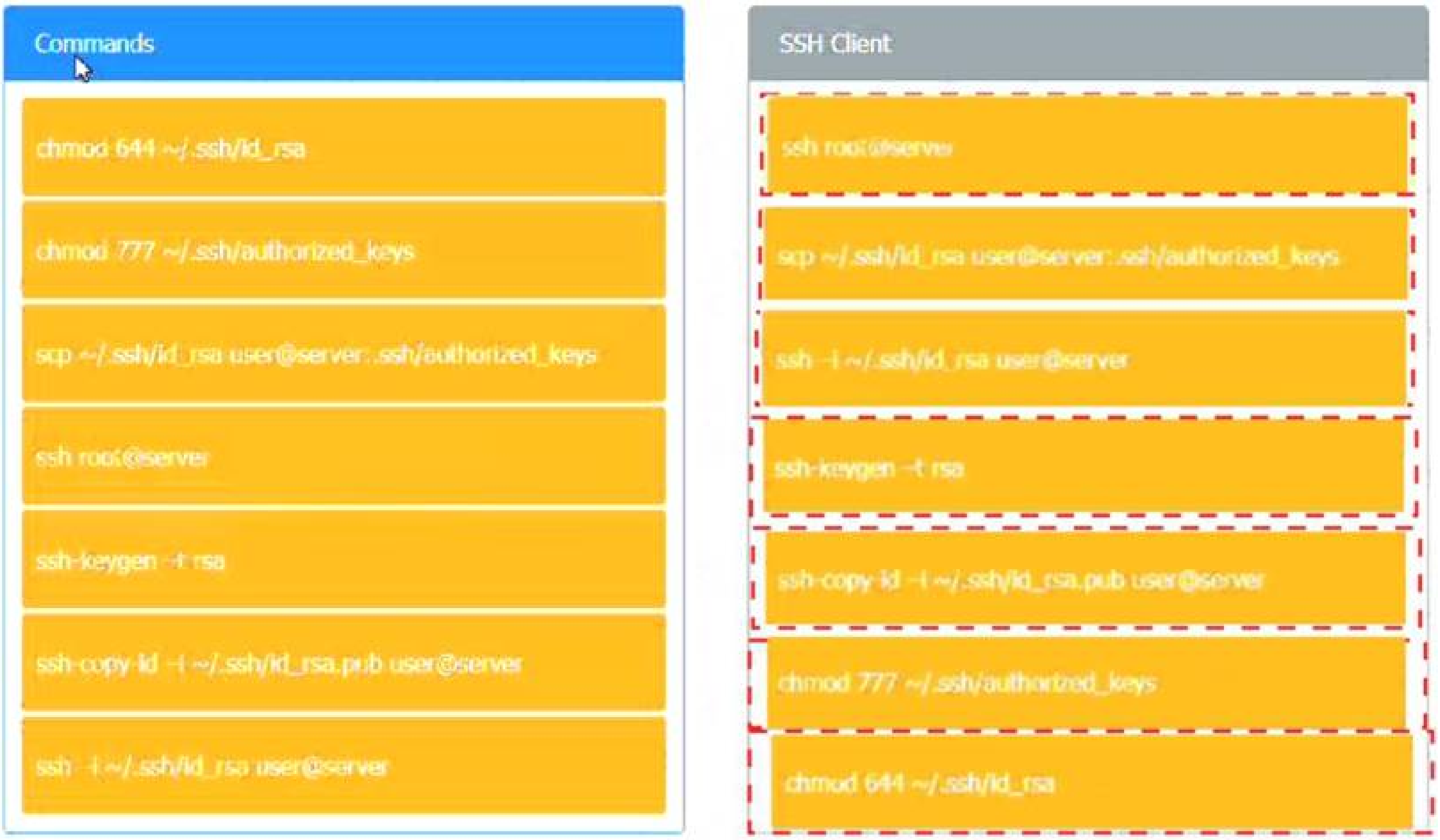


```
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Commands

```
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
```

SSH Client

```
ssh root@server
scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys
ssh -i ~/.ssh/id_rsa user@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
chmod 777 ~/.ssh/authorized_keys
chmod 644 ~/.ssh/id_rsa
```

NEW QUESTION 201

Users at organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function property. Which of the following should the security administrator consider implementing to address this issue?

A. Application code signing
B. Application whitellsting
C. Data loss prevention
D. Web application firewalls

Answer: B

NEW QUESTION 204

The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of $10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

A. Phishing
B. Whaling
C. Typo squatting
D. Pharming

Answer: B

NEW QUESTION 205

While checking logs, a security engineer notices a number of end users suddenly downloading files with the .t ar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.
B. The workstations are beaconing to a command-and-control server.
C. A logic bomb was executed and is responsible for the data transfers.
D. A fireless virus is spreading in the local network environment.

Answer: A

NEW QUESTION 206

A security administrator needs to create a RAIS configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the following RAID configurations should the administration use?

A. RA1D 0
B. RAID1
C. RAID 5
D. RAID 10

Answer: C

NEW QUESTION 210
A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

A. Predictability
B. Key stretching
C. Salting
D. Hashing

Answer: C

NEW QUESTION 213
Which of the following types of controls is a turnstile?

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

Answer: A

NEW QUESTION 214
A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

A. Mobile device management
B. Full-device encryption
C. Remote wipe
D. Biometrics

Answer: A

NEW QUESTION 215
A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money that 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 219
An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?

A. Incident response
B. Communications
C. Disaster recovery
D. Data retention

Answer: C

NEW QUESTION 223
Which of the following would be the BEST resource lor a software developer who is looking to improve secure coding practices for web applications?

A. OWASP
B. Vulnerability scan results
C. NIST CSF
D. Third-party libraries

Answer: A

NEW QUESTION 226
Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

A. The data protection officer
B. The data processor
C. The data owner
D. The data controller

Answer: C

NEW QUESTION 231

A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

A. A captive portal
B. PSK
C. 802.1X
D. WPS

Answer: C

NEW QUESTION 236
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 238
A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis
B. Restrict administrative privileges and patch ail systems and applications.
C. Rebuild all workstations and install new antivirus software
D. Implement application whitelisting and perform user application hardening

Answer: A

NEW QUESTION 239
A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?

A. Set up an air gap for the switch.
B. Change the default password for the switch.
C. Place the switch In a Faraday cage.
D. Install a cable lock on the switch

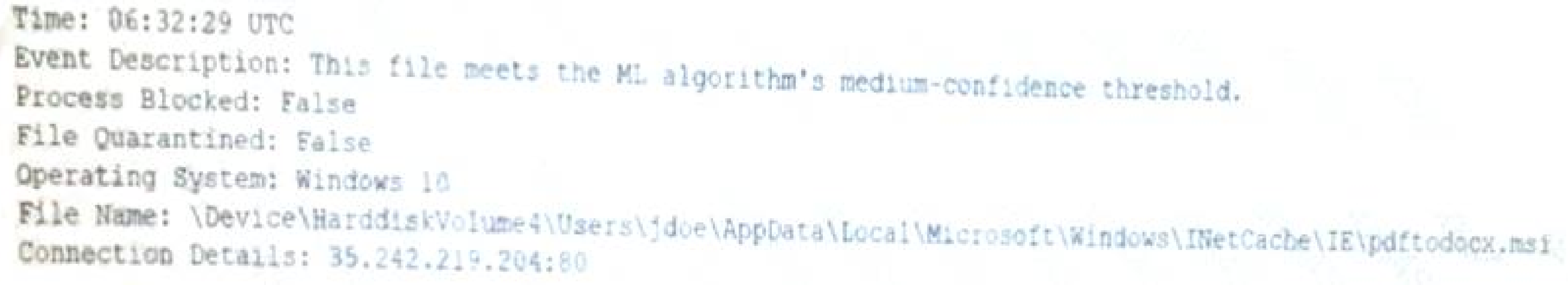
Answer: B

NEW QUESTION 243
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 248
An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:



```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\IE\pdftodocx.msi
Connection Details: 35.242.219.204:80
```

Which of the following is the MOST likely cause of the issue?

A. The end user purchased and installed a PUP from a web browser
B. A bot on the computer is brute forcing passwords against a website
C. A hacker is attempting to exfiltrate sensitive data
D. Ransomware is communicating with a command-and-control server.

Answer: A

NEW QUESTION 253

......

Relate Links

100% Pass Your SY0-601 Exam with Exambible Prep Materials

https://www.exambible.com/SY0-601-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/