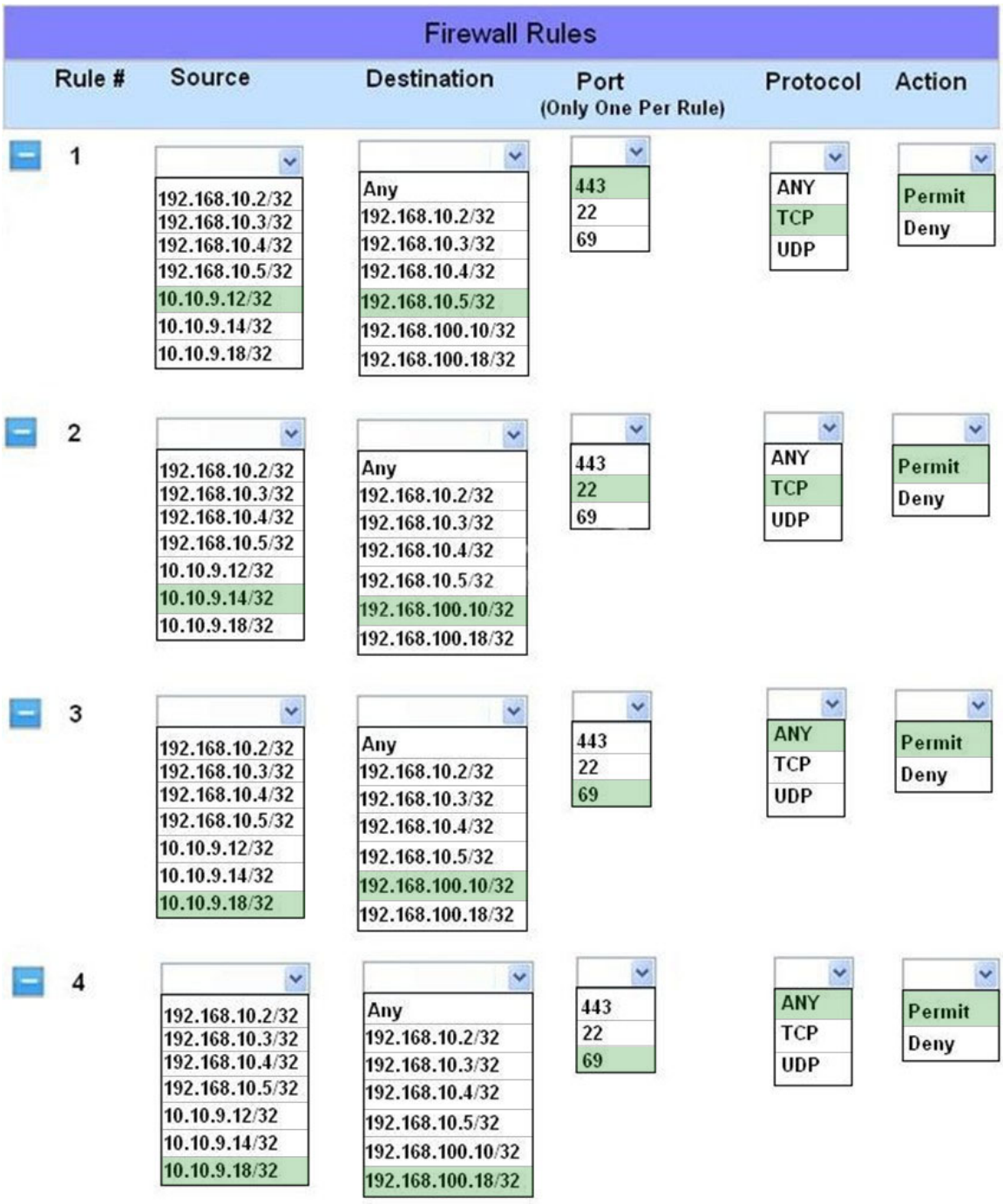
Firewall Rules
Rule #
Source
Destination
Port
(Only One Per Rule)
Protocol
Action
1
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
10.10.9.12/32
10.10.9.14/32
10.10.9.18/32
Any
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
192.168.100.10/32
192.168.100.18/32
443
22
69
ANY
TCP
UDP
Permit
Deny
2
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
10.10.9.12/32
10.10.9.14/32
10.10.9.18/32
Any
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
192.168.100.10/32
192.168.100.18/32
443
22
69
ANY
TCP
UDP
Permit
Deny
3
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
10.10.9.12/32
10.10.9.14/32
10.10.9.18/32
Any
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
192.168.100.10/32
192.168.100.18/32
443
22
69
ANY
TCP
UDP
Permit
Deny
4
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
10.10.9.12/32
10.10.9.14/32
10.10.9.18/32
Any
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
192.168.100.10/32
192.168.100.18/32
443
22
69
ANY
TCP
UDP
Permit
Deny

QUESTION 374
Which of the following would produce the closet experience of responding to an actual incident response scenario?

A. Lessons learned
B. Simulation
C. Walk-through
D. Tabletop

Correct Answer: B

QUESTION 375
A security analyst is hardening a network infrastructure. The analyst is given the following requirements.

- Preserve the use of public IP addresses assigned to equipment on the core router.
- Enable "in transport `encryption protection to the web server with the strongest ciphers.

Which of the following should the analyst implement to meet these requirements? (Select TWO).

A. Configure VLANs on the core router
B. Configure NAT on the core router
C. Configure BGP on the core router
D. Configure AES encryption on the web server
E. Enable 3DES encryption on the web server
F. Enable TLSv2 encryption on the web server

Correct Answer: BF

QUESTION 376
Entering a secure area requires passing through two doors, both of which require someone who is already inside to initiate access. Which of the following types of physical security controls does this describe?

A. Cameras
B. Faraday cage
C. Access control vestibule
D. Sensors
E. Guards

Correct Answer: C

QUESTION 377
Users reported several suspicious activities within the last two weeks that resulted in several unauthorized transactions. Upon investigation, the security analyst found the following:

- Multiple reports of breached credentials within that time period
- Traffic being redirected in certain parts of the network
- Fraudulent emails being sent by various internal users without their consent

Which of the following types of attacks was MOST likely used?

A. Replay attack

B. Race condition
C. Cross site scripting
D. Request forgeries

Correct Answer: C

QUESTION 378
A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following

- The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.
- One of the websites the manager used recently experienced a data breach.
- The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country.

Which of the following attacks has MOST likely been used to compromise the manager's corporate account?

A. Remote access Trojan
B. Brute-force
C. Dictionary
D. Credential stuffing
E. Password spraying

Correct Answer: D

QUESTION 379
An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account. Which of the following would be BEST to minimize this risk?

A. Require a complex, eight-character password that is updated every 90 days.
B. Perform only non-intrusive scans of workstations.
C. Use non-credentialed scans against high-risk servers.
D. Log and alert on unusual scanner account logon times.

Correct Answer: D

QUESTION 380
A SOC is currently being outsourced. Which of the following is being used?

A. Microservices
B. SaaS
C. MSSP
D. PaaS
Correct Answer: C
Explanation:
https://www.datashieldprotect.com/blog/pros-and-cons-of-an-outsourced-soc

QUESTION 381

An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations
B. It provides insurance in case of a data breach
C. It provides complimentary training and certification resources to IT security staff.
D. It certifies the organization can work with foreign entities that require a security clearance
E. It assures customers that the organization meets security standards

Correct Answer: E
Explanation:
According to the ISO https://www.iso.org/standard/54534.html

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

QUESTION 382
Which of the following BEST helps to demonstrate integrity during a forensic investigation?

A. Event logs
B. Encryption
C. Hashing
D. Snapshots

Correct Answer: C
Explanation:
Digital evidence integrity is ensured by calculating MD5 and SHA1 hashes of the extracted content and storing it in a report along with other details related to the drive. It also offers an encryption feature to ensure the confidentiality of the digital evidence.

QUESTION 383
A malware attack has corrupted 30TB of company data across all file servers A systems administrator Identifies the malware and contains the Issue, but the data Is unrecoverable. The administrator Is not concerned about the data loss because the company has a system in place that will allow users to access the data that was backed up last night. Which of the following resiliency techniques did the administrator MOST likely use to prevent impacts to business operations after an attack?

A. Tape backups
B. Replication
C. RAID
D. Cloud storage
Correct Answer: C

QUESTION 384
A financial institution would like to stare is customer data a could but still allow the data to be accessed and manipulated while encrypted. Doing se would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concern about computational overheads and slow speeds. Which of the following cryptographic

techniques would BEST meet the requirement?

A. Asymmetric
B. Symmetric
C. Homeomorphic
D. Ephemeral

Correct Answer: C
Explanation:
"In a nutshell, homomorphic encryption is a method of encryption that allows any data to remain encrypted while it's being processed and manipulated. It enables you or a third party (such as a cloud provider) to apply functions on encrypted data without needing to reveal the values of the data."

https://www.thesslstore.com/blog/what-is-homomorphic-encryption/
https://en.wikipedia.org/wiki/Homomorphic_encryption

QUESTION 385
A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

A. Establish chain of custody.
B. Inspect the file metadata.
C. Reference the data retention policy.
D. Review the email event logs

Correct Answer: B

QUESTION 386
A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

A. RAT
B. Ransomware
C. Logic bomb
D. A worm

Correct Answer: C

QUESTION 387
An external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

A. Perform a vulnerability scan to identity the weak spots.
B. Use a packet analyzer to Investigate the NetFlow traffic.
C. Check the SIEM to review the correlated logs.
D. Require access to the routers to view current sessions.