Vendor: CompTIA

Exam Code:CAS-002

Exam Name: CompTIA Advanced Security Practitioner Exam

Version: Demo

QUESTION 1

A large organization that builds and configures every data center against distinct requirements loses efficiency, which results in slow response time to resolve issues. However, total uniformity presents other problems. Which of the following presents the GREATEST risk when consolidating to a single vendor or design solution?

A. Competitors gain an advantage by increasing their service offerings.

B. Vendor lock in may prevent negotiation of lower rates or prices.

C. Design constraints violate the principle of open design.

D. Lack of diversity increases the impact of specific events or attacks.

Correct Answer: D

QUESTION 2

A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

A. Background checks

B. Job rotation

C. Least privilege

D. Employee termination procedures

Correct Answer: B

QUESTION 3

CORRECT TEXT

Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several Internal networks. The intent of this firewall is to make traffic more

restrictive. Given the following information answer the questions below:

User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet:192.168.3.0/24

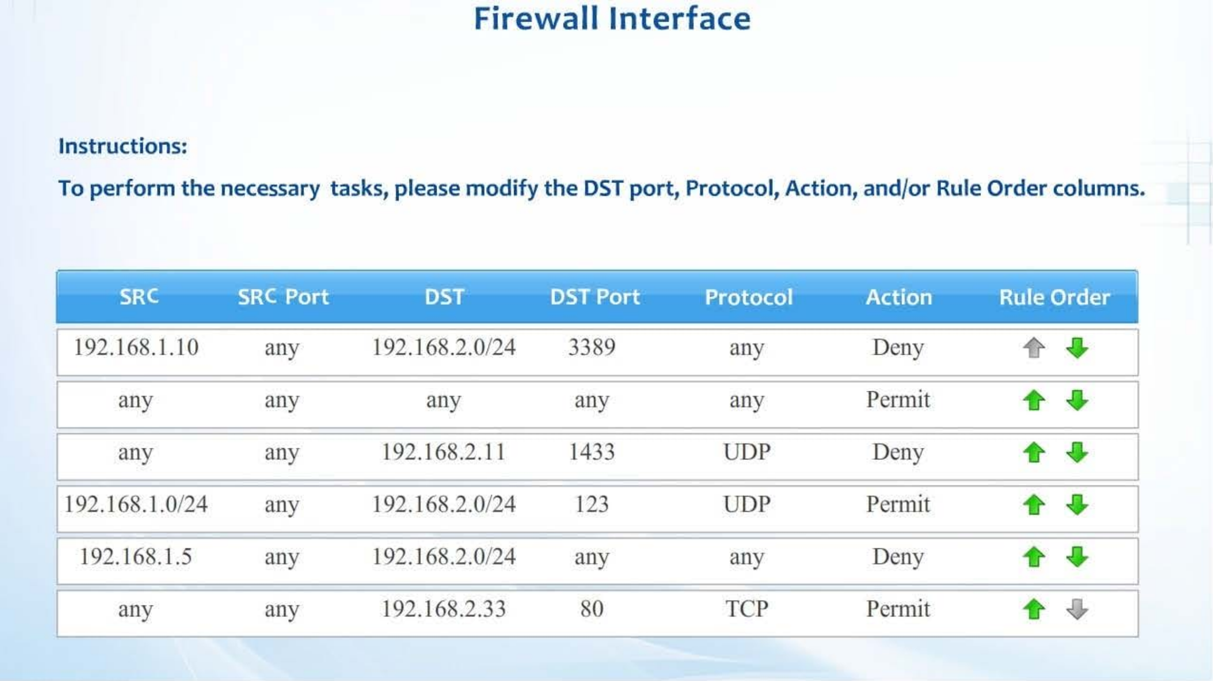
Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down

Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.

Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.

Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.

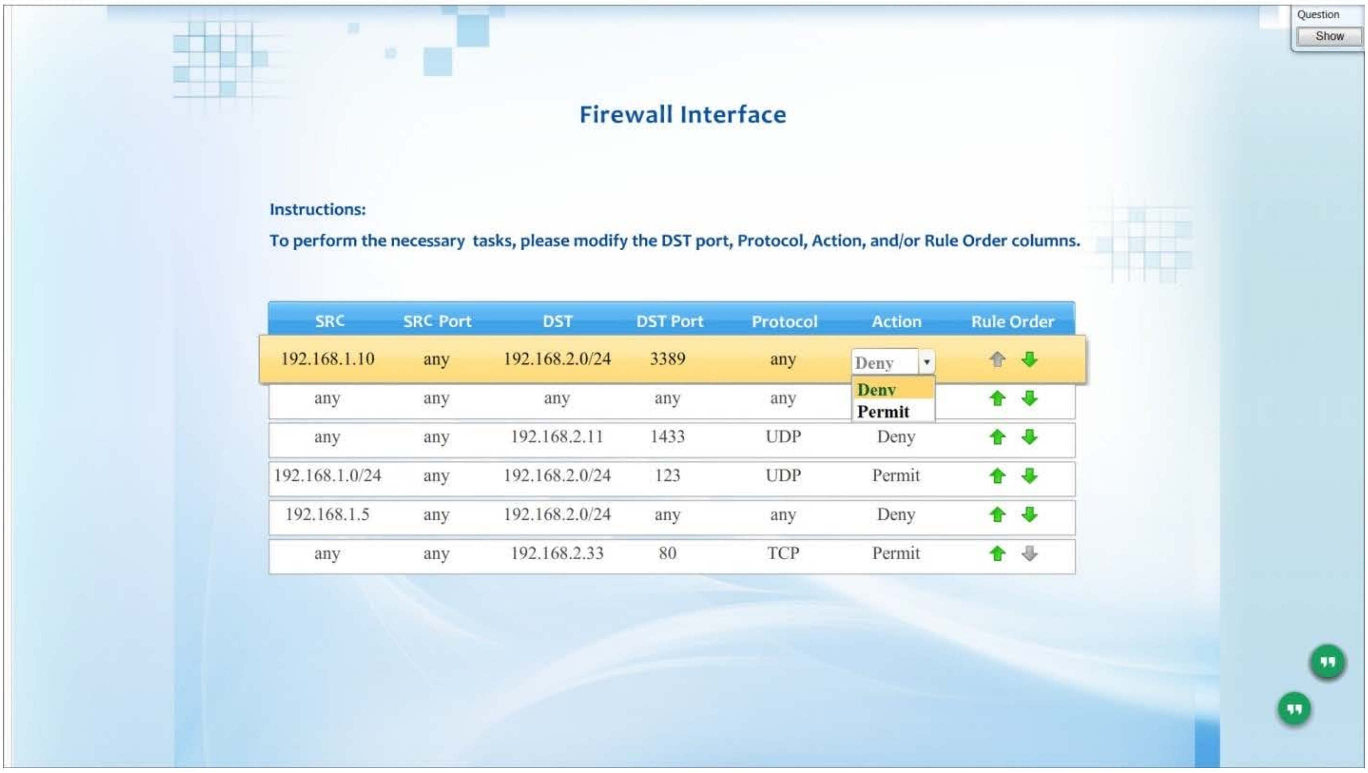


Firewall Interface

Instructions:

To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns.

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Deny	↑ ↓
any	any	any	any	any	Permit	↑ ↓
any	any	192.168.2.11	1433	UDP	Deny	↑ ↓
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	↑ ↓
192.168.1.5	any	192.168.2.0/24	any	any	Deny	↑ ↓
any	any	192.168.2.33	80	TCP	Permit	↑ ↓



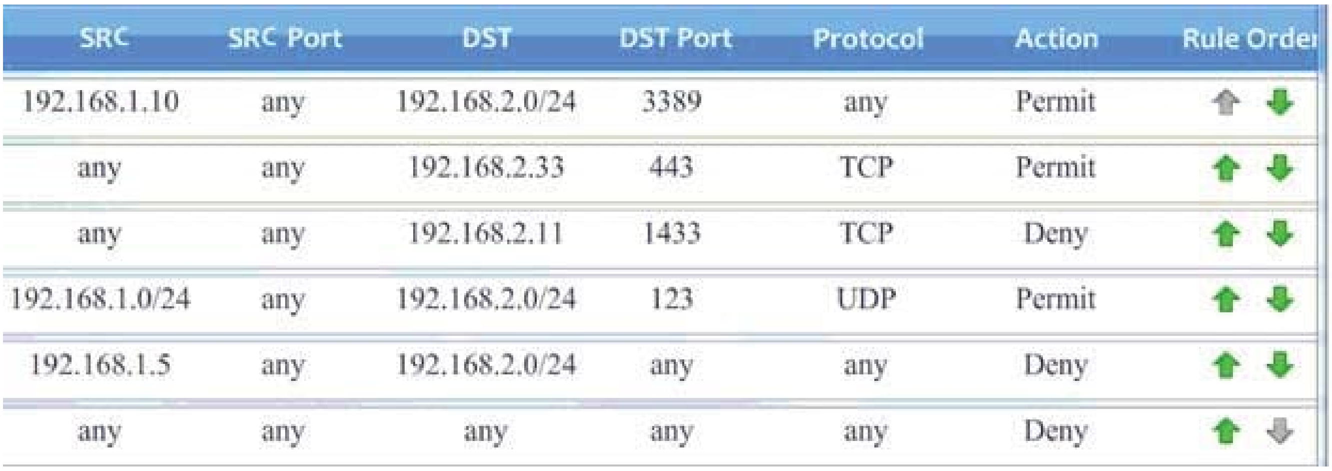
Firewall Interface

Instructions:

To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns.

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Deny ▾	↑ ↓
any	any	any	any	any		↑ ↓
any	any	192.168.2.11	1433	UDP	Deny	↑ ↓
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	↑ ↓
192.168.1.5	any	192.168.2.0/24	any	any	Deny	↑ ↓
any	any	192.168.2.33	80	TCP	Permit	↑ ↓

Correct Answer: Answer: Please look into the explanation for the solution to this question.



SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	↑ ↓
any	any	192.168.2.33	443	TCP	Permit	↑ ↓
any	any	192.168.2.11	1433	TCP	Deny	↑ ↓
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	↑ ↓
192.168.1.5	any	192.168.2.0/24	any	any	Deny	↑ ↓
any	any	any	any	any	Deny	↑ ↓

QUESTION 4

A human resources manager at a software development company has been tasked with recruiting personnel for a new cyber defense division in the company. This division will require personnel to have high technology skills and industry certifications. Which of the following is the BEST method for this manager to gain insight into this industry to execute the task?

A. Interview candidates, attend training, and hire a staffing company that specializes in technology jobs

B. Interview employees and managers to discover the industry hot topics and trends

C. Attend meetings with staff, internal training, and become certified in software management

D. Attend conferences, webinars, and training to remain current with the industry and job requirements

Correct Answer: D

QUESTION 5

An organization has several production critical SCADA supervisory systems that cannot follow the normal 30-day patching policy. Which of the following BEST maximizes the protection of these systems from malicious software?

A. Configure a firewall with deep packet inspection that restricts traffic to the systems

B. Configure a separate zone for the systems and restrict access to known ports

C. Configure the systems to ensure only necessary applications are able to run

D. Configure the host firewall to ensure only the necessary applications have listening ports

Correct Answer: C

QUESTION 6

A company is evaluating a new marketing strategy involving the use of social networking sites to reach its customers. The marketing director wants to be able to report important company news, product updates, and special promotions on the social websites.

After an initial and successful pilot period, other departments want to use the social websites to post their updates as well.

The Chief Information Officer (CIO) has asked the company security administrator to document three negative security impacts of allowing IT staff to post work related information on such websites.

Which of the following are the major risks the security administrator should report back to the CIO? (Select THREE).

A. Brute force attacks

B. Malware infection

C. DDOS attacks

D. Phishing attacks

E. SQL injection attacks

F. Social engineering attacks

Correct Answer: BDF

QUESTION 7

A network administrator with a company\\'s NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company\\'s physical security, which of the following can the network administrator use to scan and detect the presence of a malicious actor physically accessing the company\\'s network or information systems from within? (Select TWO).

A. RAS

B. Vulnerability scanner

C. HTTP intercept

D. HIDS

E. Port scanner

F. Protocol analyzer

Correct Answer: DE

QUESTION 8

The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer data. The Chief Risk Officer (CRO) is concerned about the outsourcing plans. Which of the following risks are MOST likely to occur if adequate controls are not implemented?

A. Geographical regulation issues, loss of intellectual property and interoperability agreement issues

B. Improper handling of client data, interoperability agreement issues and regulatory issues

C. Cultural differences, increased cost of doing business and divestiture issues

D. Improper handling of customer data, loss of intellectual property and reputation damage

Correct Answer: D

QUESTION 9

An IT administrator wants to restrict DNS zone transfers between two geographically dispersed, external company DNS name servers, and has decided to use TSIG. Which of the following are critical when using TSIG? (Select TWO).

A. Periodic key changes once the initial keys are established between the DNS name servers.

B. Secure exchange of the key values between the two DNS name servers.

C. A secure NTP source used by both DNS name servers to avoid message rejection.

D. DNS configuration files on both DNS name servers must be identically encrypted.

E. AES encryption with a SHA1 hash must be used to encrypt the configuration files on both DNS name servers.

Correct Answer: BC

QUESTION 10

New zero-day attacks are announced on a regular basis against a broad range of technology systems. Which of the following best practices should a security manager do to manage the risks of these attack vectors? (Select TWO).

A. Establish an emergency response call tree.

B. Create an inventory of applications.

C. Backup the router and firewall configurations.

D. Maintain a list of critical systems.

E. Update all network diagrams.

Correct Answer: BD

QUESTION 11

Customer Need:

"We need the system to produce a series of numbers with no discernible mathematical progression for use by our Java based, PKI-enabled, customer facing website."

Which of the following BEST restates the customer need?

A. The system shall use a pseudo-random number generator seeded the same every time.

B. The system shall generate a pseudo-random number upon invocation by the existing Java program.

C. The system shall generate a truly random number based upon user PKI certificates.

D. The system shall implement a pseudo-random number generator for use by corporate customers.

Correct Answer: B

QUESTION 12

Which of the following is the MOST secure way to ensure third party applications and introduce only acceptable risk?

A. Line by line code review and simu-lation; uncovers hidden vulnerabilities and allows for behavior to be observed with minimal risk.

B. Technical exchange meetings with the application\\'s vendor; vendors have more in depth knowledge of the product.

C. Pilot trial; minimizes the impact to the enterprise while still providing services to enterprise users.

D. Full deployment with crippled features; allows for large scale testing and observation of the applications security profile.

Correct Answer: A