CAS-005 Q&As

CompTIA SecurityX Exam

QUESTION 1

Asecuntv administrator is performing a gap assessment against a specific OS benchmark The benchmark requires the following configurations be applied to endpomts:

1.

Full disk encryption

2.

Host-based firewall

3.

Time synchronization

4.

Password policies

5.

Application allow listing

6.

Zero Trust application access

Which of the following solutions best addresses the requirements? (Select two).

A. CASB

B. SBoM

C. SCAP

D. SASE

E. HIDS

Correct Answer: CD

To address the specific OS benchmark configurations, the following solutions are most appropriate:

C. SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies. D. SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data. These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.

References:

CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures. NIST Special Publication 800-126, "The Technical Specification for the Security Content

Automation

Protocol (SCAP)": Details SCAP\\'s role in security automation. "Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth: Covers the principles of Zero Trust and how SASE can implement them.

By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintained effectively.

QUESTION 2

HOTSPOT

Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP address. The company uses the following internal IP address ranges: 192.10.1.0/24 for the corporate site and 192.10.2.0/24 for the remote

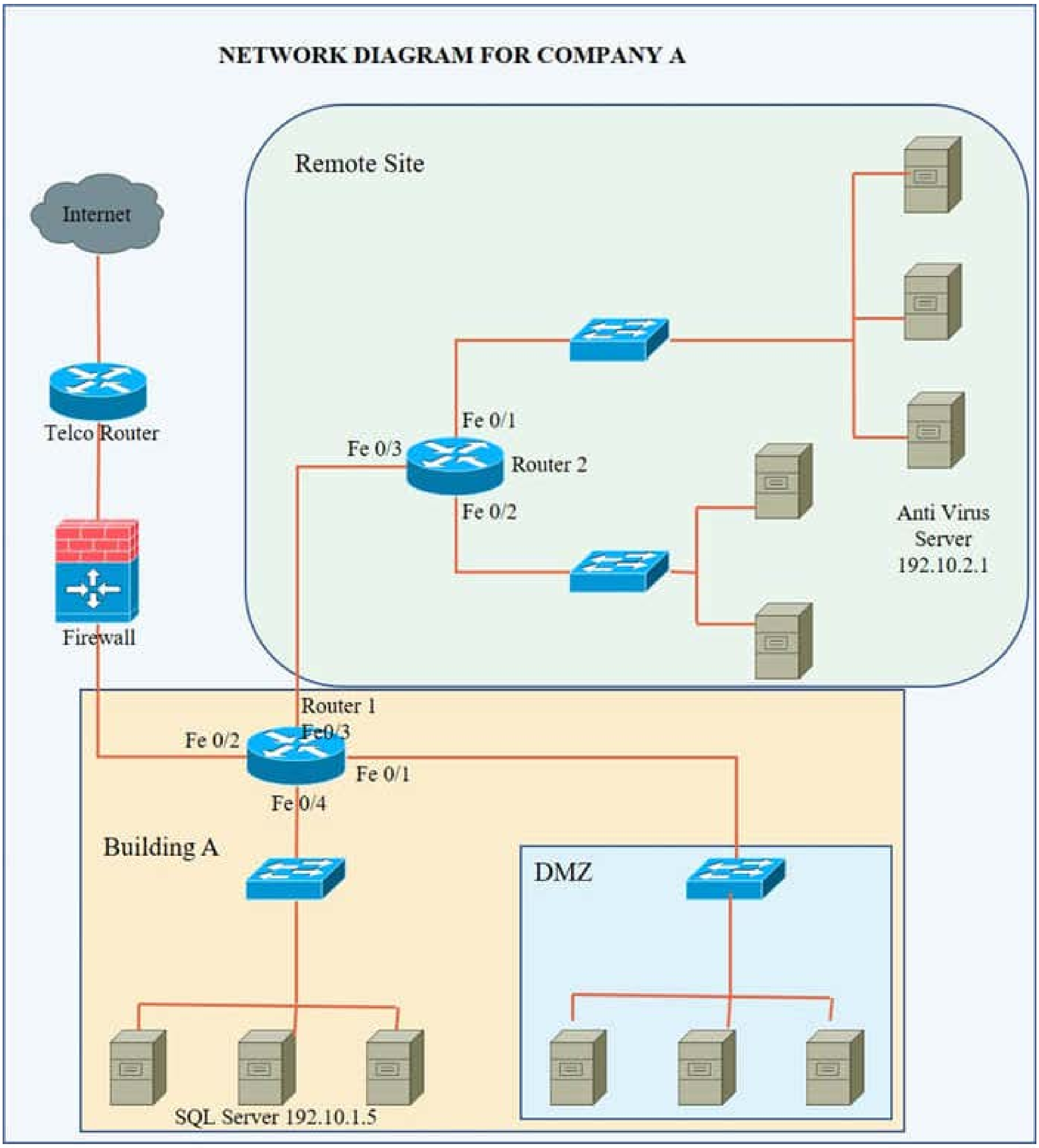
site. The Telco router interface uses the 192.10.5.0/30 IP range.

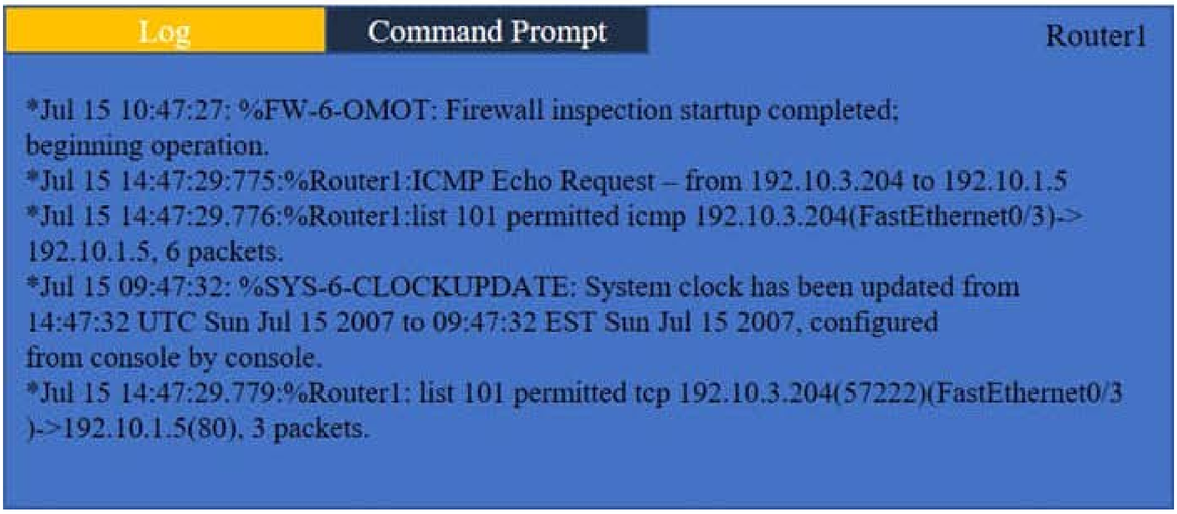
Instructions: Click on the simulation button to refer to the Network Diagram for Company A.

Click on Router 1, Router 2, and the Firewall to evaluate and configure each device.

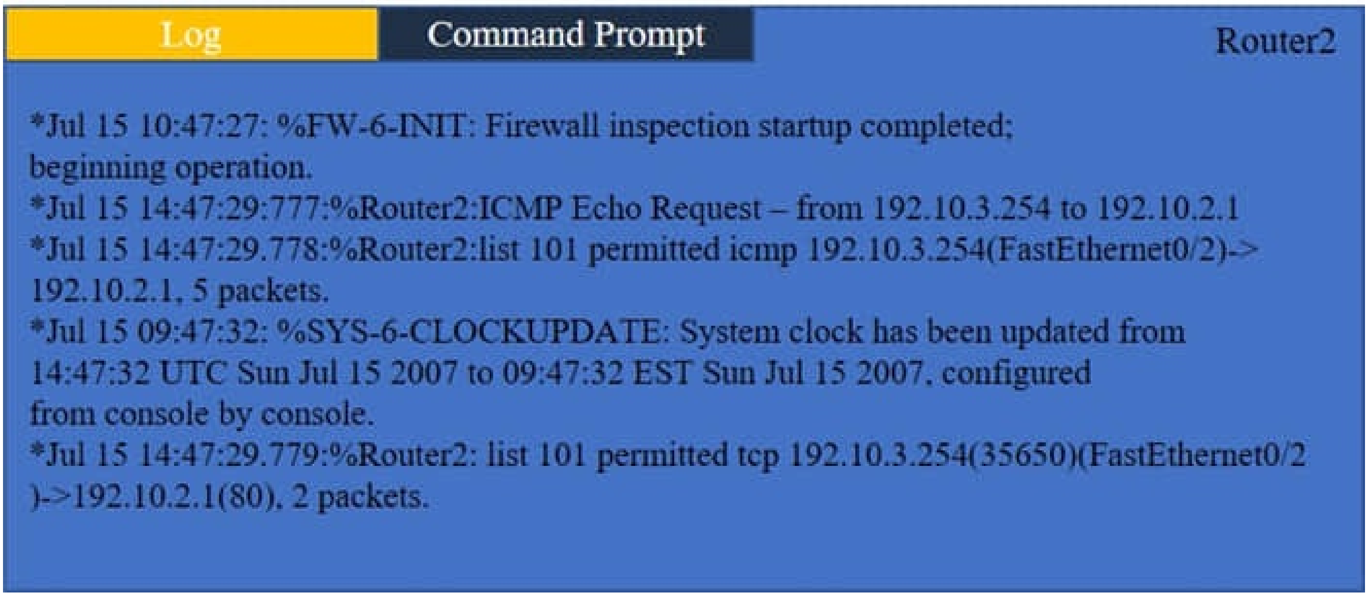
Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.

Task 2: Reconfigure the appropriate devices to prevent the attacks from continuing to target the SQL server and other servers on the corporate network.



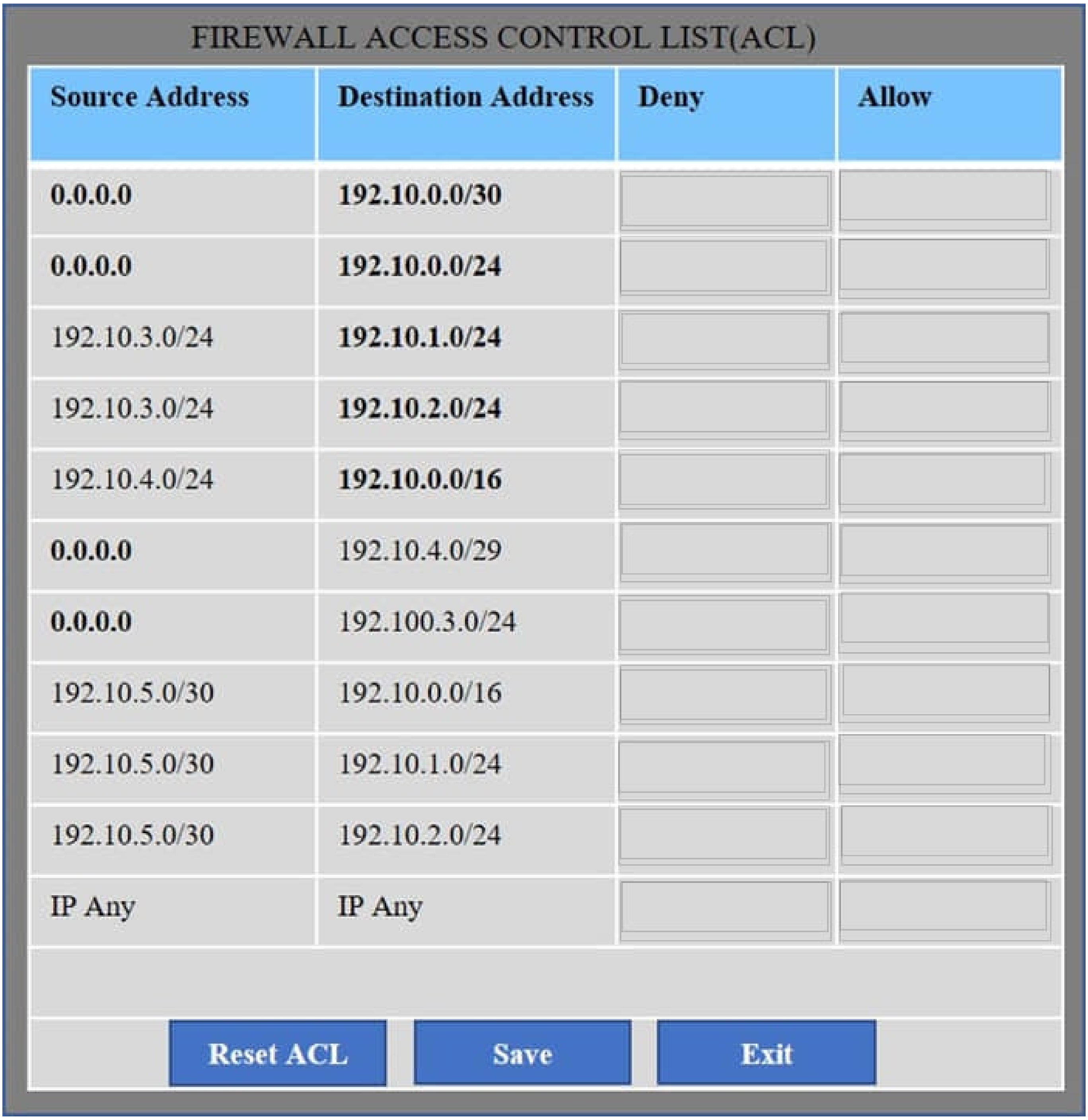


```
*Jul 15 10:47:27: %FW-6-OMOT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29:775:%Router1:ICMP Echo Request – from 192.10.3.204 to 192.10.1.5
*Jul 15 14:47:29.776:%Router1:list 101 permitted icmp 192.10.3.204(FastEthernet0/3)->
192.10.1.5, 6 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router1: list 101 permitted tcp 192.10.3.204(57222)(FastEthernet0/3
)->192.10.1.5(80), 3 packets.
```



```
*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29:777:%Router2:ICMP Echo Request – from 192.10.3.254 to 192.10.2.1
*Jul 15 14:47:29.778:%Router2:list 101 permitted icmp 192.10.3.254(FastEthernet0/2)->
192.10.2.1, 5 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router2: list 101 permitted tcp 192.10.3.254(35650)(FastEthernet0/2
)->192.10.2.1(80), 2 packets.
```

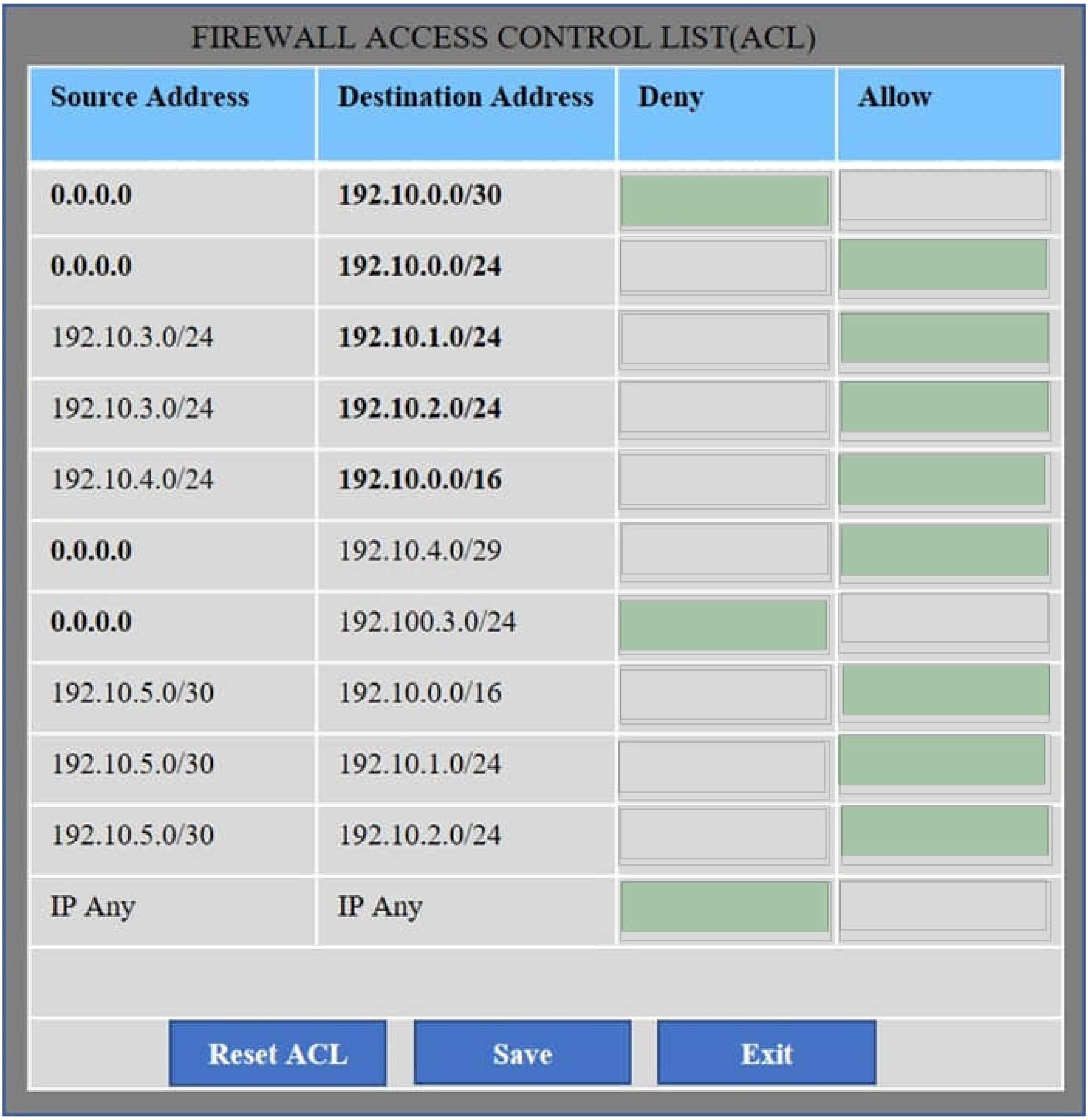
Hot Area:



FIREWALL ACCESS CONTROL LIST(ACL)

Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30		
0.0.0.0	192.10.0.0/24		
192.10.3.0/24	192.10.1.0/24		
192.10.3.0/24	192.10.2.0/24		
192.10.4.0/24	192.10.0.0/16		
0.0.0.0	192.10.4.0/29		
0.0.0.0	192.100.3.0/24		
192.10.5.0/30	192.10.0.0/16		
192.10.5.0/30	192.10.1.0/24		
192.10.5.0/30	192.10.2.0/24		
IP Any	IP Any		

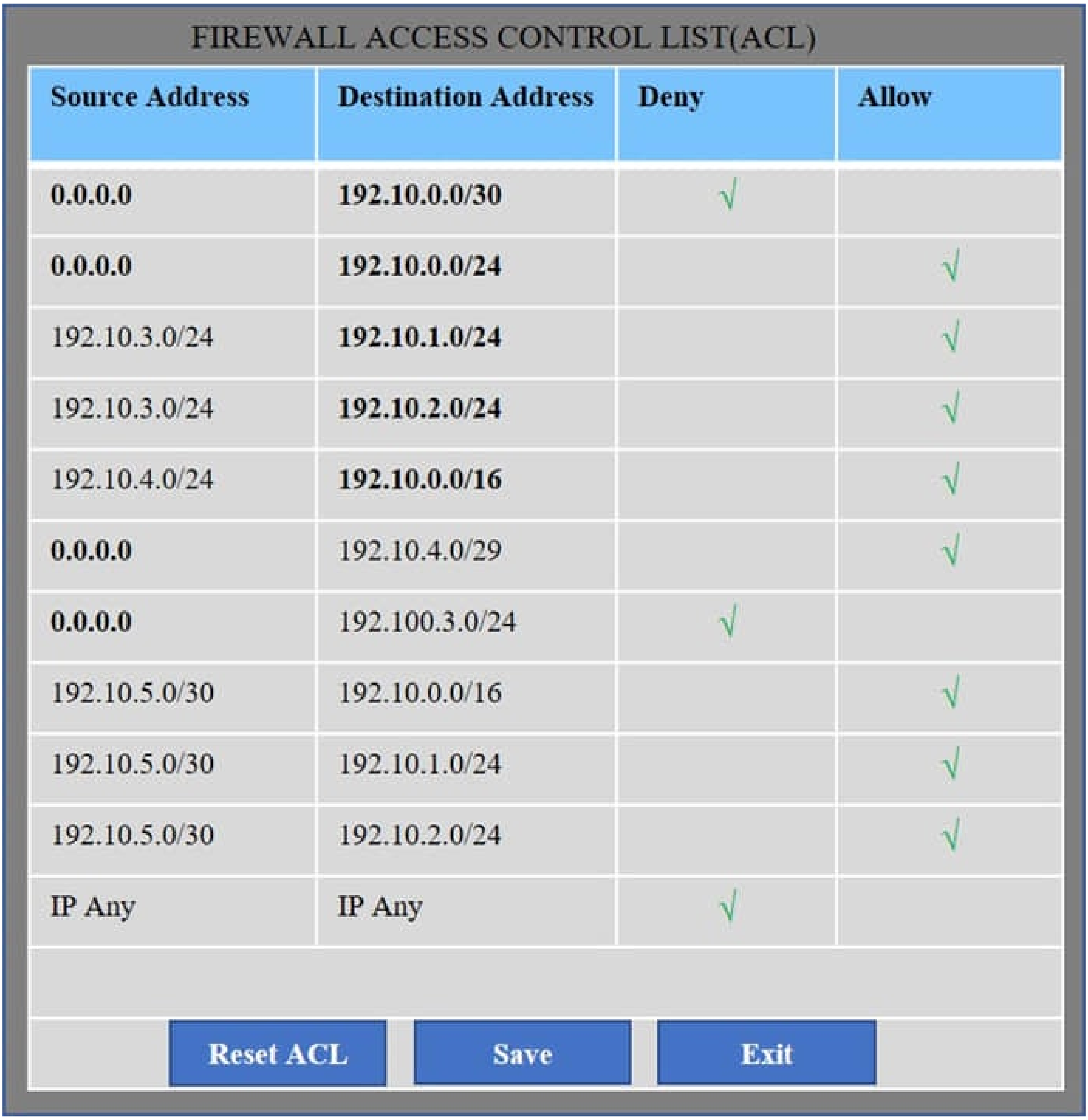
Correct Answer:



FIREWALL ACCESS CONTROL LIST(ACL)

Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	🟩	□
0.0.0.0	192.10.0.0/24	□	🟩
192.10.3.0/24	192.10.1.0/24	□	🟩
192.10.3.0/24	192.10.2.0/24	□	🟩
192.10.4.0/24	192.10.0.0/16	□	🟩
0.0.0.0	192.10.4.0/29	□	🟩
0.0.0.0	192.100.3.0/24	🟩	□
192.10.5.0/30	192.10.0.0/16	□	🟩
192.10.5.0/30	192.10.1.0/24	□	🟩
192.10.5.0/30	192.10.2.0/24	□	🟩
IP Any	IP Any	🟩	□

We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.30.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:



FIREWALL ACCESS CONTROL LIST(ACL)

Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	√	
0.0.0.0	192.10.0.0/24		√
192.10.3.0/24	192.10.1.0/24		√
192.10.3.0/24	192.10.2.0/24		√
192.10.4.0/24	192.10.0.0/16		√
0.0.0.0	192.10.4.0/29		√
0.0.0.0	192.100.3.0/24	√	
192.10.5.0/30	192.10.0.0/16		√
192.10.5.0/30	192.10.1.0/24		√
192.10.5.0/30	192.10.2.0/24		√
IP Any	IP Any	√	

QUESTION 3

A Chief Information Security Officer (CISO) received a call from the Chief Executive Officer (CEO) about a data breach from the SOC lead around 9:00 a.m. At 10:00 a.m. The CEO informs the CISO that a breach of the firm is being reported on national news. Upon investigation, it is determined that a network administrator has reached out to a vendor prior to the breach for information on a security patch that failed to be installed. Which of the following should the CISO do to

prevent this from happening again?

A. Properly triage events based on brand imaging and ensure the CEO is on the call roster.

B. Create an effective communication plan and socialize it with all employees.

C. Send out a press release denying the breach until more information can be obtained.

D. Implement a more robust vulnerability identification process.

Correct Answer: B

QUESTION 4

A cloud engineer needs to identify appropriate solutions to:

1.

Provide secure access to internal and external cloud resources.

2.

Eliminate split-tunnel traffic flows.

3.

Enable identity and access management capabilities.

Which of the following solutions arc the most appropriate? (Select two).

A. Federation

B. Microsegmentation

C. CASB

D. PAM

E. SD-WAN

F. SASE

Correct Answer: CF

To provide secure access to internal and external cloud resources, eliminate split-tunnel traffic flows, and enable identity and access management capabilities, the most appropriate solutions are CASB (Cloud Access Security Broker) and

SASE (Secure Access Service Edge).

Why CASB and SASE?

CASB (Cloud Access Security Broker):

SASE (Secure Access Service Edge):

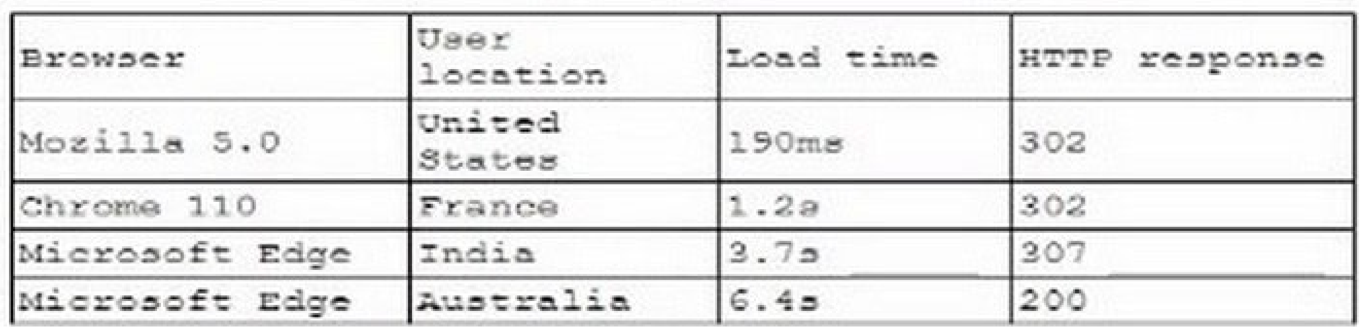
Other options, while useful, do not comprehensively address all the requirements:

A. Federation: Useful for identity management but does not eliminate split-tunnel traffic or provide comprehensive security.

B. Microsegmentation: Enhances security within the network but does not directly address secure access to cloud resources or split-tunnel traffic. D. PAM (Privileged Access Management): Focuses on managing privileged accounts and does not provide comprehensive access control for internal and external resources. E. SD-WAN: Enhances WAN performance but does not inherently provide the identity and access management capabilities or eliminate split-tunnel traffic. References: CompTIA SecurityX Study Guide "CASB: Cloud Access Security Broker," Gartner Research

QUESTION 5

A company receives several complaints from customers regarding its website. An engineer implements a parser for the web server logs that generates the following output:



Browser	User location	Load time	HTTP response
Mozilla 5.0	United States	190ms	302
Chrome 110	France	1.2s	302
Microsoft Edge	India	3.7s	307
Microsoft Edge	Australia	6.4s	200

which of the following should the company implement to best resolve the issue?

A. IDS

B. CDN

C. WAF

D. NAC

Correct Answer: B

The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencing significantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website\\'s performance. A. IDS (Intrusion Detection System): While an IDS is useful for detecting malicious activities, it does not address performance issues related to latency and geographical distribution of content.

B. CDN (Content Delivery Network): A CDN stores copies of the website\\'s content in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user

experience globally.

C. WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency. D. NAC (Network Access Control): NAC solutions control access to network resources but are not designed to address web performance issues. Implementing a CDN is the best solution to resolve the performance issues observed in the log output.

References:

CompTIA Security+ Study Guide

"CDN: Content Delivery Networks Explained" by Akamai Technologies NIST SP 800-44, "Guidelines on Securing Public Web Servers"