CAS-003$^{\text{Q\&As}}$

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

QUESTION 1

A security manager recently categorized an information system. During the categorization effort, the manager determined the loss of integrity of a specific information type would impact business significantly. Based on this, the security manager recommends the implementation of several solutions. Which of the following, when combined, would BEST mitigate this risk? (Select TWO.)

A. Access control

B. Whitelisting

C. Signing

D. Validation

E. Boot attestation

Correct Answer: AD

QUESTION 2

A company recently implemented a variety of security services to detect various types of traffic that pose a threat to the company. The following services were enabled within the network:

1.

Scan of specific subsets for vulnerabilities

2.

Categorizing and logging of website traffic

3.

Enabling specific ACLs based on application traffic

4.

Sending suspicious files to a third-party site for validation A report was sent to the security team that identified multiple incidents of users sharing large amounts of data from an on-premise server to a public site. A small percentage of that data also contained malware and spyware Which of the following services MOST likely identified the behavior and sent the report?

A. Content filter

B. User behavioral analytics

C. Application sandbox

D. Web application firewall

E. Endpoint protection

F. Cloud security broker

Correct Answer: B

QUESTION 3

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

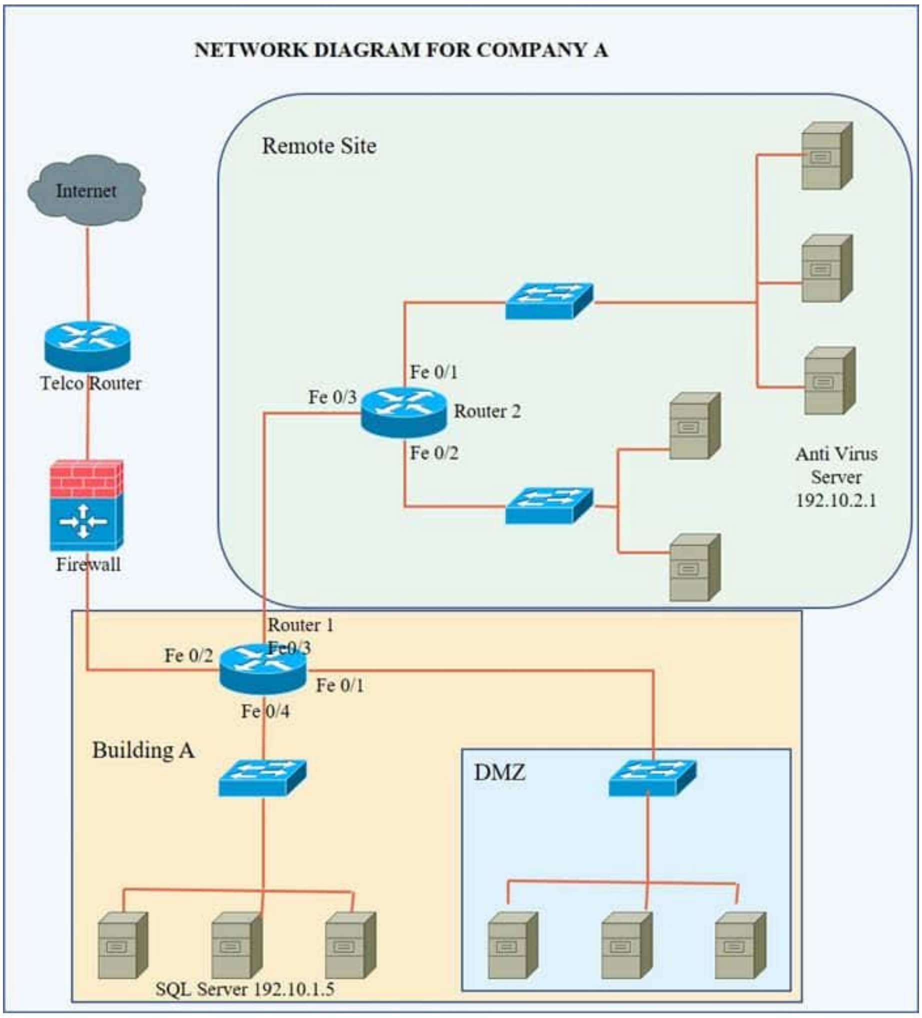
site. The Telco router interface uses the 192.10.5.0/30 IP range.

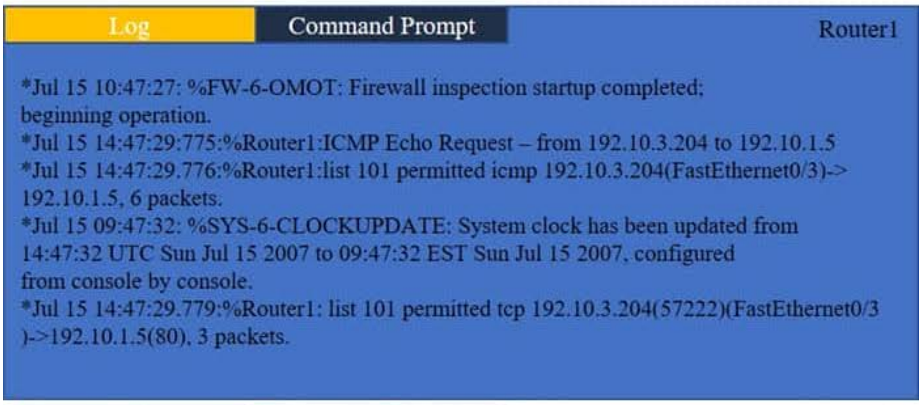
Instructions: Click on the simulation button to refer to the Network Diagram for Company A.

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

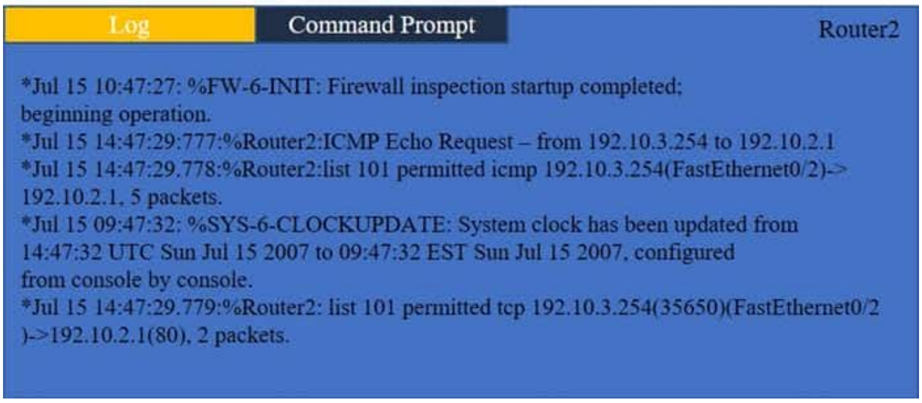
Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.

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



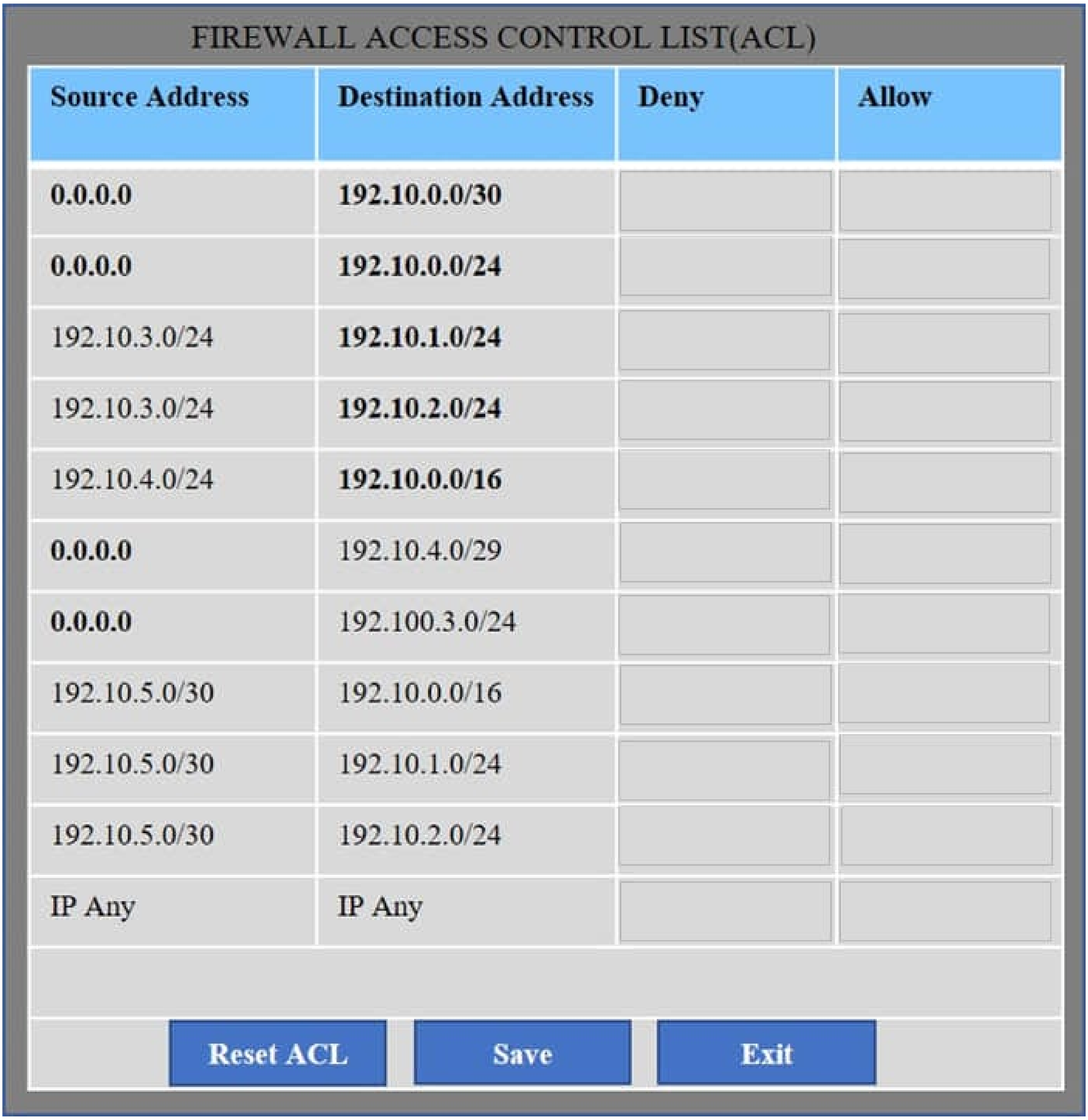


```
*Jul 15 10:47:27: %FW-6-OMOT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29:775:%Router1:ICMP Echo Request – from 192.10.3.204 to 192.10.1.5
*Jul 15 14:47:29.776:%Router1:list 101 permitted icmp 192.10.3.204(FastEthernet0/3)->
192.10.1.5, 6 packets.
*Jul 15 09:47:32: %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.
```

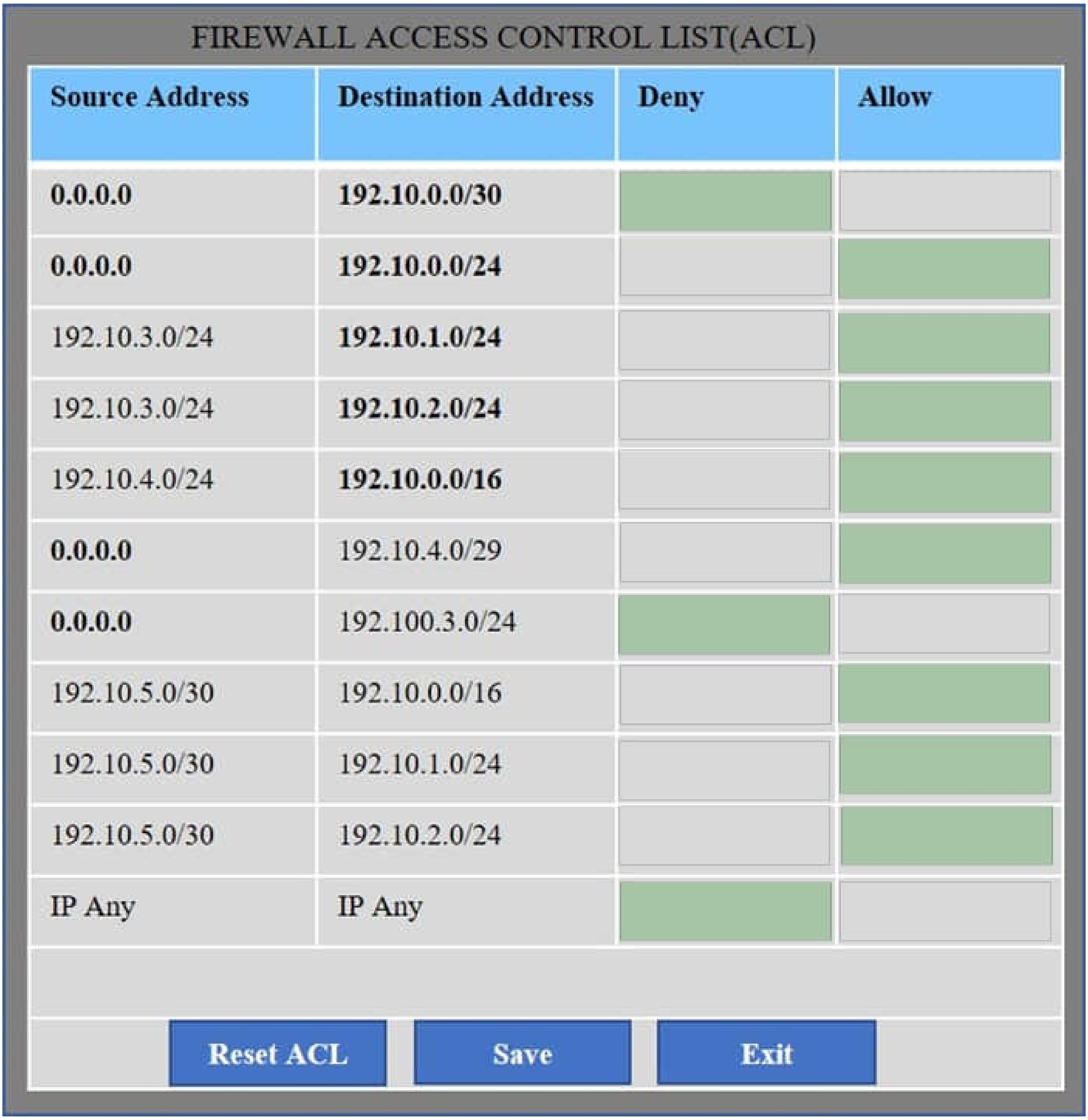
Hot Area:



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		

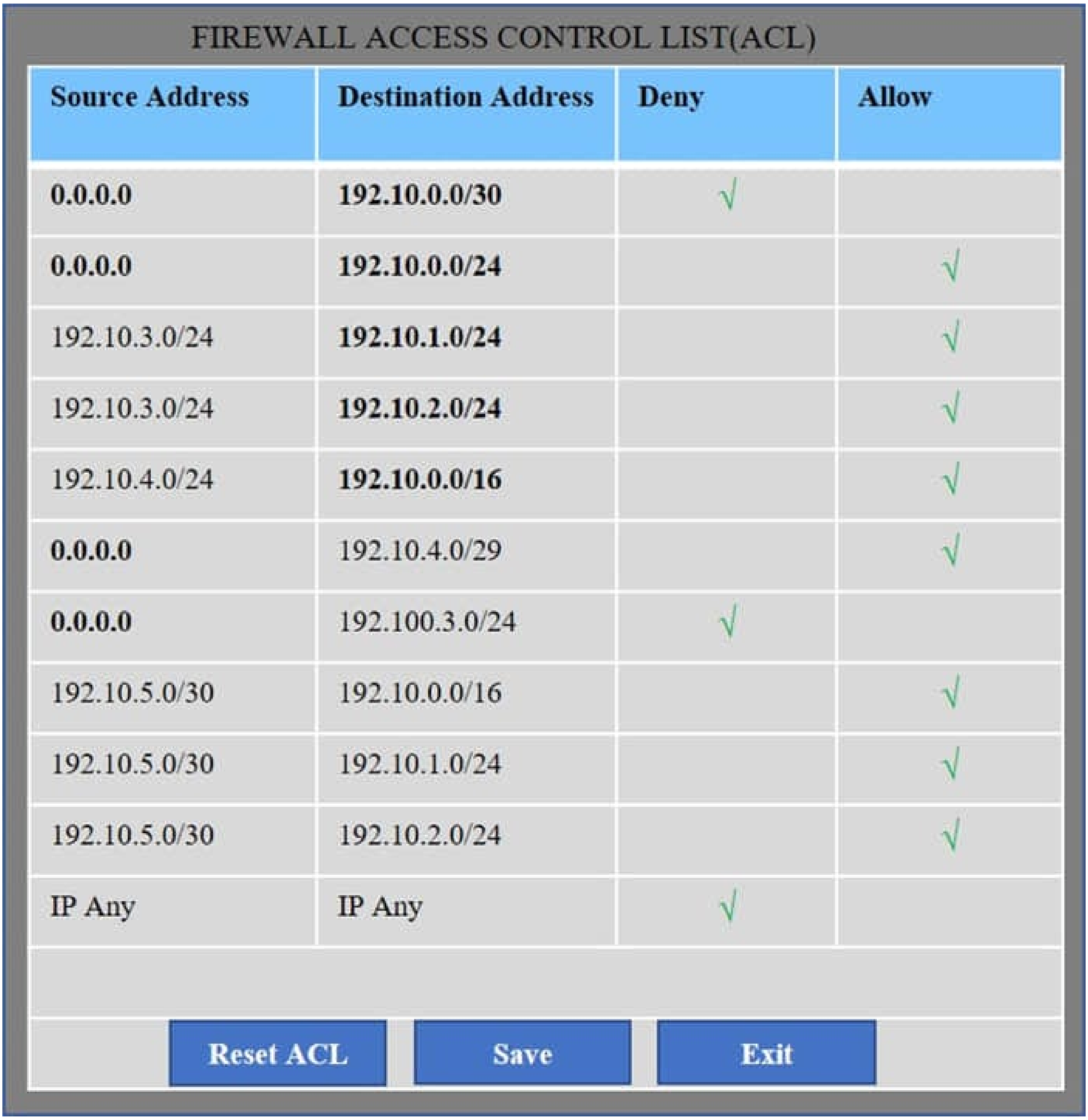
Correct Answer:



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 4

An external red team is brought into an organization to perform a penetration test of a new network-based application. The organization deploying the network application wants the red team to act like remote, external attackers, and instructs the team to use a black-box approach. Which of the following is the BEST methodology for the red team to follow?

A. Run a protocol analyzer to determine what traffic is flowing in and out of the server, and look for ways to alter the data stream that will result in information leakage or a system failure.

B. Send out spear-phishing emails against users who are known to have access to the network-based application, so the red team can go on-site with valid credentials and use the software.

C. Examine the application using a port scanner, then run a vulnerability scanner against open ports looking for known, exploitable weaknesses the application and related services may have.

D. Ask for more details regarding the engagement using social engineering tactics in an attempt to get the organization to disclose more information about the network application to make attacks easier.

Correct Answer: C

QUESTION 5

Two competing companies experienced similar attacks on their networks from various threat actors. To improve response times, the companies wish to share some threat intelligence about the sources and methods of attack.

Which of the following business documents would be BEST to document this engagement?

A. Business partnership agreement

B. Memorandum of understanding

C. Service-level agreement

D. Interconnection security agreement

Correct Answer: D

Latest CAS-003 Dumps CAS-003 PDF Dumps CAS-003 VCE Dumps