CAS-004$^{\text{Q\&As}}$

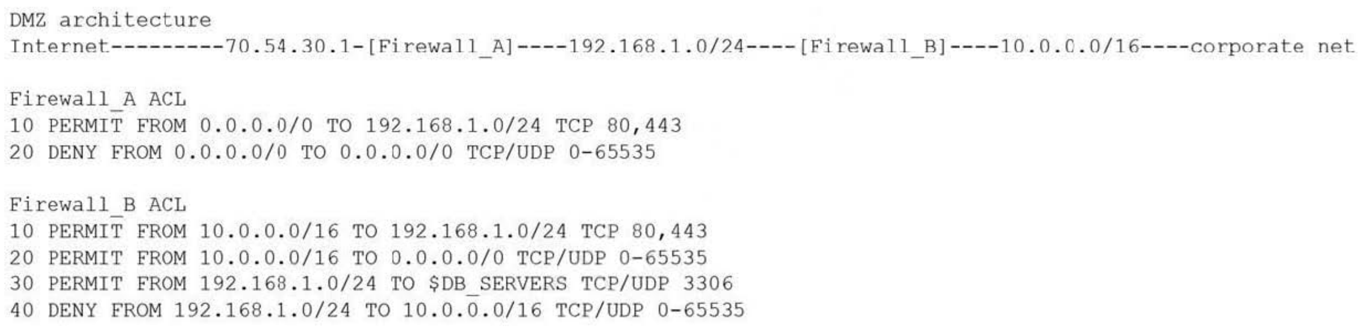
CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A security architect is reviewing the following proposed corporate firewall architecture and configuration:



```
DMZ architecture
Internet---------70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:

1.

Web servers must receive all updates via HTTP/S from the corporate network.

2.

Web servers should not initiate communication with the Internet.

3.

Web servers should only connect to preapproved corporate database servers.

4.

Employees\\' computing devices should only connect to web services over ports 80 and 443.

Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443

B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443

C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535

D. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535

E. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535

F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

Correct Answer: AF

QUESTION 2

A financial services company wants to migrate its email services from on-premises servers to a cloud-based email solution. The Chief information Security Officer (CISO) must brief board of directors on the potential security concerns related to this migration. The board is concerned about the following.

1.

Transactions being required by unauthorized individual

2.

Complete discretion regarding client names, account numbers, and investment information.

3.

Malicious attacker using email to distribute malware and ransom ware.

4.

Exfiltration of sensitivity company information.

The cloud-based email solution will provide an6-malware, reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board\\'s concerns for this email migration?

A. Data loss prevention

B. Endpoint detection response

C. SSL VPN

D. Application whitelisting

Correct Answer: A

QUESTION 3

A company\\'s product site recently had failed API calls, resulting in customers being unable to check out and purchase products. This type of failure could lead to the loss of customers and damage to the company\\'s reputation in the market. Which of the following should the company implement to address the risk of system unavailability?

A. User and entity behavior analytics

B. Redundant reporting systems

C. A self-healing system

D. Application controls

Correct Answer: D

QUESTION 4

An organization is in frequent litigation and has a large number of legal holds. Which of the following types of functionality should the organization\\'s new email system provide?

A. DLP

B. Encryption

C. E-discovery

D. Privacy-level agreements

Correct Answer: C

QUESTION 5

A security architect is analyzing an old application that is not covered for maintenance anymore because the software company is no longer in business. Which of the following techniques should have been implemented to prevent these types of risks?

A. Code reviews

B. Supply chain visibility

C. Software audits

D. Source code escrows

Correct Answer: D