Free Cisco 300-740 SCAZT Practice Questions

Shared by Hull on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which web application firewall deployment in the Cisco Secure DDoS protects against application layer and volumetric attacks?

Options:

A- Hybrid
B- On-demand
C- Always-on
D- Active/passive

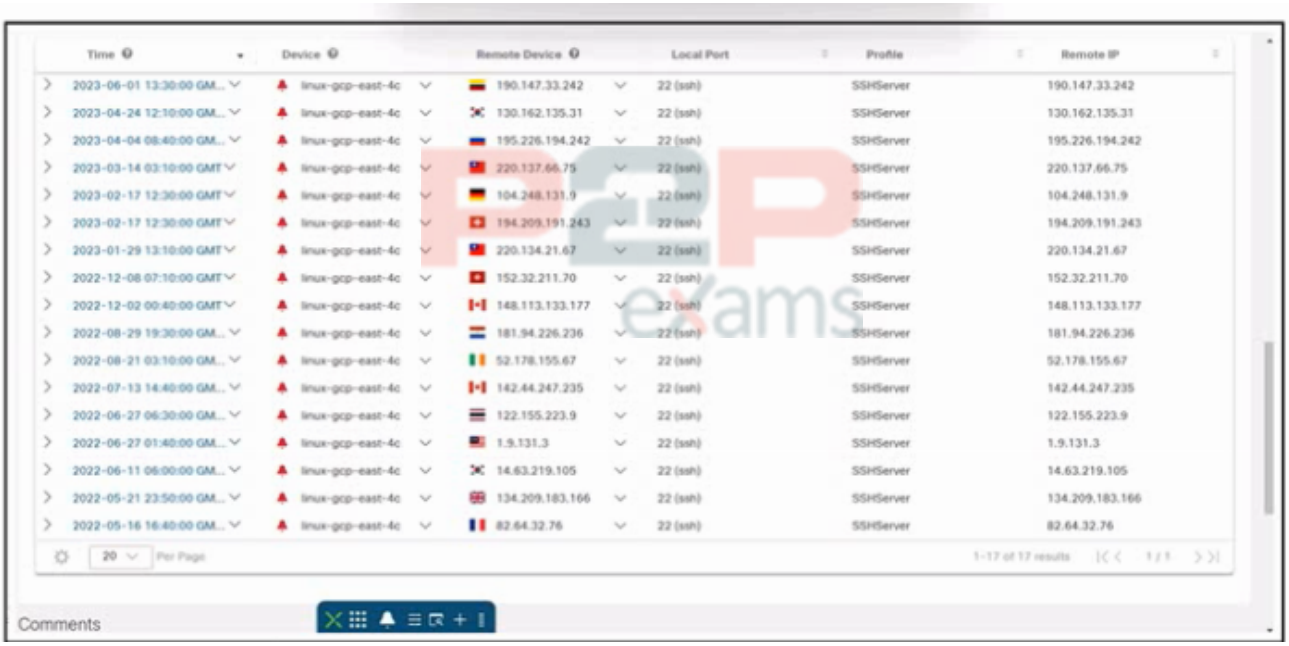
Answer:

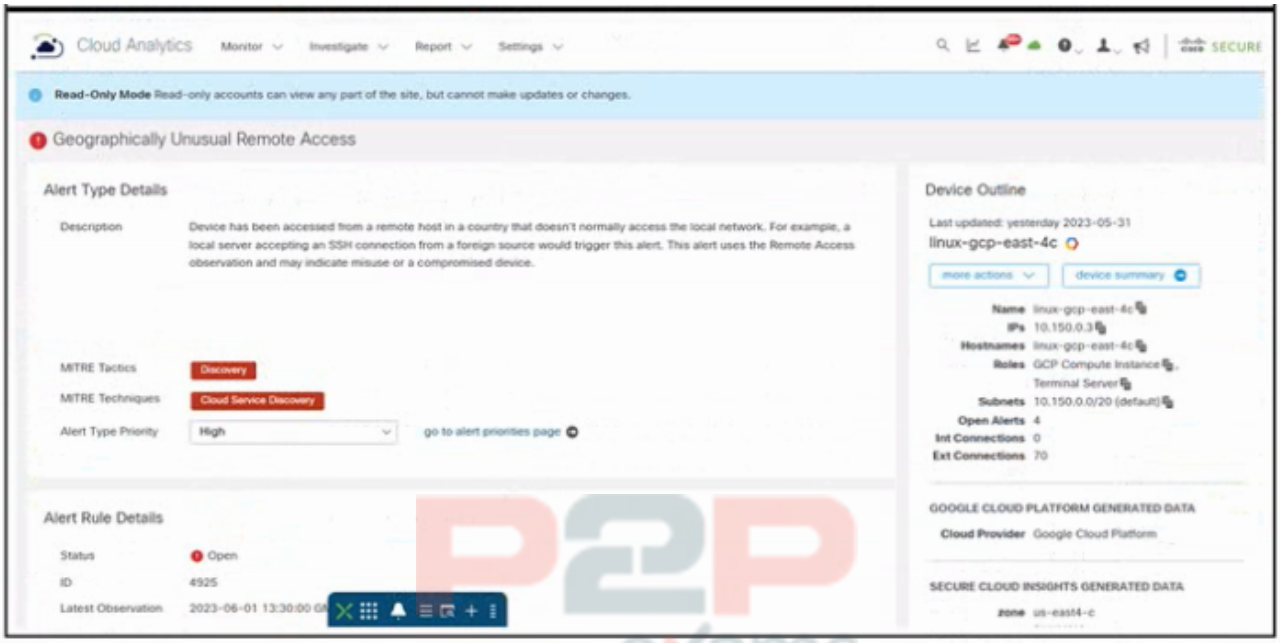
C

Question 2

Question Type: MultipleChoice

Refer to the exhibit.





Refer to the exhibit. An engineer is investigating an issue by using Cisco Secure Cloud Analytics. The engineer confirms that the connections are unauthorized and informs the incident management team. Which two actions must be taken next? (Select two.)

Options:

A- Reinstall the host from a recent backup.
B- Quarantine the host
C- Reinstall the host from scratch.
D- Create a firewall rule that has a source of linux-gcp-east-4c, a destination of Any, and a protocol of SSH.
E- Create a firewall rule that has a source of Any, a destination of linux-gcp-east-4c, and a protocol of SSH.

Answer:

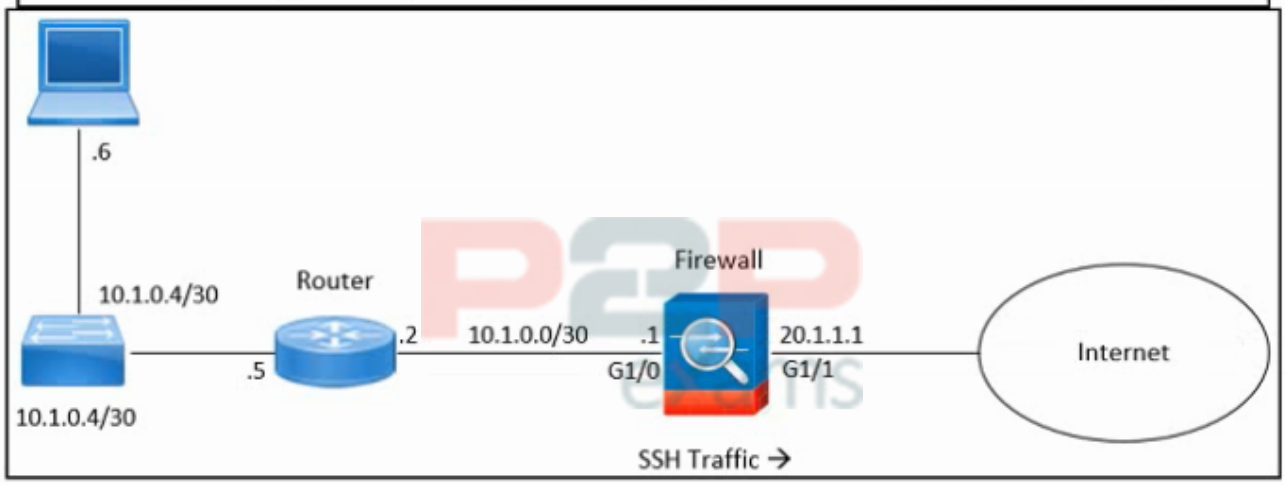
B, E

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

Rule Number	Source	Destination	Service	Action	Log	Time
1	10.1.0.0/30	Any	SSH	Deny	Log	18h00 - 8h00am
2	10.1.0.0/30	Any	SSH	Allow	Log	8h00am - 18h00
3	10.1.0.0/30	Any	Any	Allow	Log	18h00 - 8h00am
4	10.1.0.4/30	Any	Any	Allow	Log	Any
5	10.1.0.4/30	Any	SSH	Deny	Log	18h00 - 8h00am
6	Any	Any	Any	Deny	Log	Any



Refer to the exhibit. An engineer must troubleshoot an issue with excessive SSH traffic leaving the internal network between the hours of 18:00 and 08:00. The engineer applies a policy to the Cisco ASA firewall to block outbound SSH during the indicated hours; however, the issue persists. What should be done to meet the requirement?

Options:

A- Change the time of rule 2.
B- Delete rule 4
C- Delete rule 3
D- Change the time of rule 5

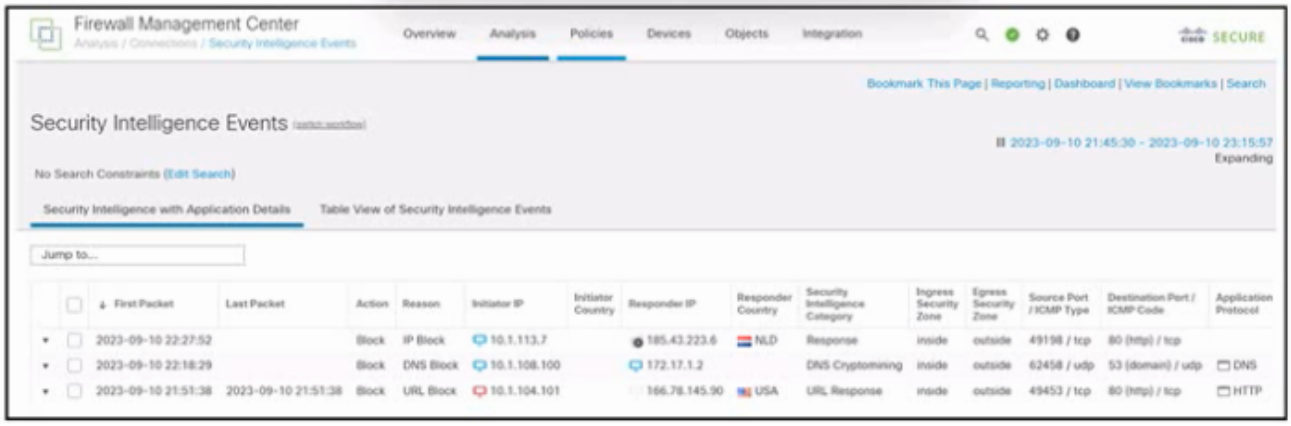
Answer:

B

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



Refer to the exhibit. An engineer is analyzing a Cisco Secure Firewall Management Center report. Which activity does the output verify?

Options:

A- An HTTP response from IP address 10.1.104.101 was blocked.
B- An HTTP request to IP address 10.1.113.7 was blocked.
C- A DNS request to IP address 172.17.1.2 was blocked.
D- A DNS response from IP address 10.1.108.100 was blocked.

Answer:

D

Question 5

Question Type: MultipleChoice

An administrator received an incident report indicating suspicious activity of a user using a corporate device. The manager requested that the credentials of user user1@cisco.com be reset and synced via the Active Directory. Removing the account should be avoided and used for further investigation on data leak. Which configuration must the administrator apply on the Duo Admin Panel?

Options:

A- Delete the user in the Users tab option and sync it with the domain controller.
B- Quarantine the user from all the policies on the Policies tab, including associated devices.
C- Request the password change on the Device tab on managed devices.
D- Disable the account on the Users tab and reset the password from the Active Directory.

Answer:

D

Question 6

Question Type: MultipleChoice

Refer to the exhibit.

Refer to the exhibit. An engineer configured a default segmentation policy in Cisco Secure Workload to block SMTP traffic. During testing, it is observed that the SMTP traffic is still allowed. Which action must the engineer take to complete the configuration?

Options:

A- Add 'port': [25, 25] to _rootScope
B- Add _SMTPScope to provider_filter_ref
C- Add 'port': [25, 25] to _params
D- Change consumer_filter_ref to: _SMTPScope

Answer:

C

Question 7

Question Type: MultipleChoice

Which common strategy should be used to mitigate directory traversal attacks in a cloud environment?

Options:

A- Use anti-cross-site request forgery tokens.

B- Apply the principle of least privilege.
C- Implement functionality validation.
D- Limit file system permissions.

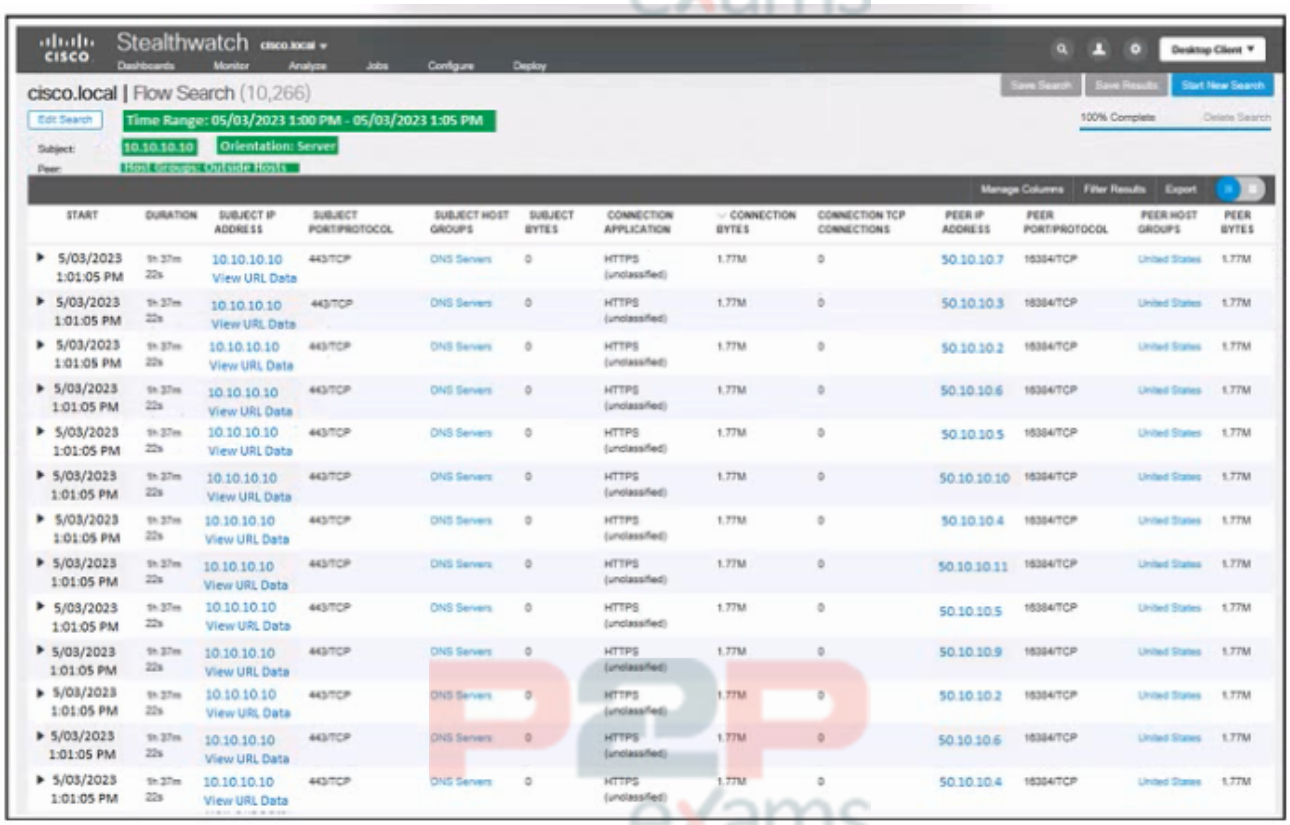
Answer:

D

Question 8

Question Type: MultipleChoice

Refer to the exhibit.



Refer to the exhibit. An engineer must troubleshoot an incident by using Cisco Secure Cloud Analytics. What is the cause of the issue?

Options:

A- SYN flood attack toward the DNS server that has IP address 10.10.10.10
B- DoS attack toward the 50.10.10.0/24 network from an internal IP address
C- Ping of Death attack toward the host that has IP address 10.10.10.10
D- TCP fingerprinting toward the 50.10.10.0/24 network

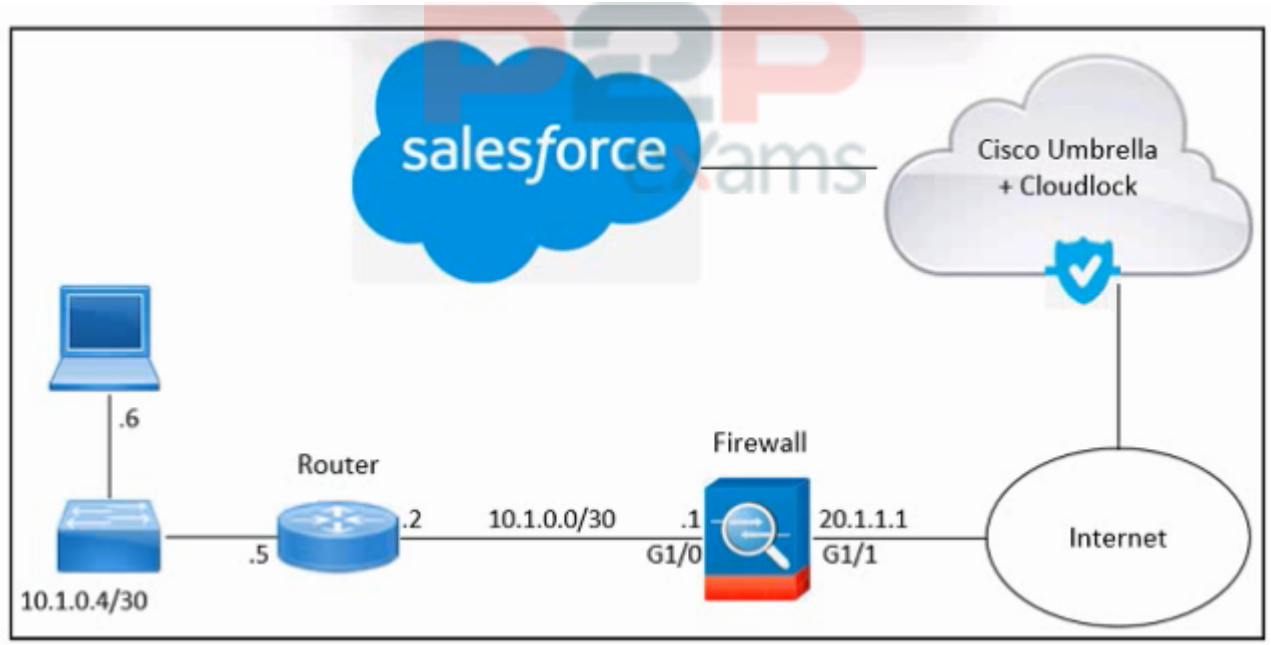
Answer:

A

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



Refer to the exhibit. An engineer must enable access to Salesforce using Cisco Umbrella and Cisco Cloudlock. These actions were performed:

From Salesforce, add the Cloudlock IP address to the allow list

From Cloudlock, authorize Salesforce

However, Salesforce access via Cloudlock is still unauthorized. What should be done to meet the requirements?

Options:

A- From the Salesforce admin page, grant API access to Cloudlock.
B- From the Salesforce admin page, grant network access to Cloudlock
C- From the Cloudlock dashboard, grant API access to Salesforce.
D- From the Cloudlock dashboard, grant network access to Salesforce.

Answer:

A

P2P exams