Cisco

300-740

Designing and Implementing Secure Cloud Access for Users and Endpoints Exam

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

According to Cisco Security Reference Architecture, which solution provides threat intelligence and malware analytics?

A. Cisco pxGrid
B. Cisco XDR
C. Cisco Talos
D. Cisco Umbrella

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Cisco Talos is Cisco's threat intelligence organization, delivering real-time threat intelligence and malware analytics to help organizations detect and prevent threats before they impact the network. According to the SCAZT guide, Talos provides comprehensive coverage of threat data including signatures, indicators of compromise, and context-driven analytics. This intelligence feeds into Cisco security platforms such as Cisco SecureX and Cisco Secure Endpoint to enhance detection, investigation, and response capabilities. Talos is explicitly referenced in the Threat Response section as the primary source of threat intelligence and malware analytics that supports cloud and endpoint security frameworks.
Reference: Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) Study Guide, Section 6: Threat Response, Pages 112-115.

Question: 2

Which types of algorithm does a web application firewall use for zero-day DDoS protection?

A. Reactive and heuristic-based
B. Stochastic and event-based
C. Correlative and feedback-based
D. Adaptive and behavioral-based

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to the SCAZT documentation, web application firewalls (WAFs) designed to protect against zero-day Distributed Denial of Service (DDoS) attacks leverage adaptive and behavioral-based

algorithms. These algorithms dynamically analyze traffic patterns, baseline normal behavior, and detect anomalies that could indicate novel or zero-day attacks. Unlike signature-based detection, adaptive and behavioral methods adjust in real-time to emerging threats, learning from ongoing traffic without relying on pre-defined rules. This proactive approach enables rapid detection and mitigation of unknown DdoS vectors, critical for cloud and network security where threats evolve constantly.
Reference: Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) Study Guide, Section 3: Network and Cloud Security, Pages 75-77.

Question: 3

An administrator must deploy an endpoint posture policy for all users. The organization wants to have all endpoints checked against antimalware definitions and operating system updates and ensure that the correct Secure Client modules are installed properly. How must the administrator meet the requirements?

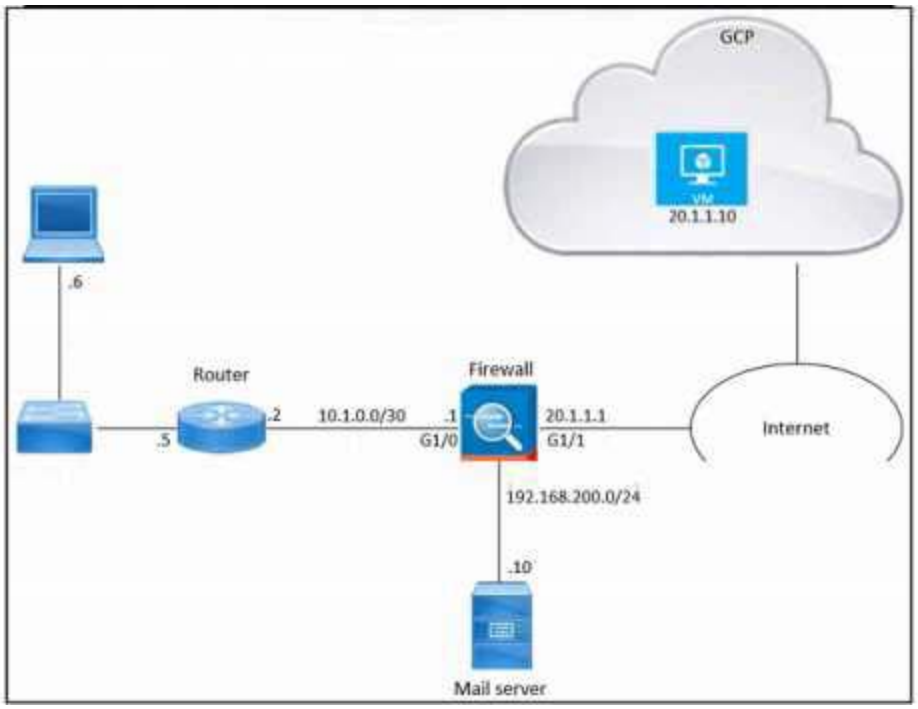
A. Configure the WLC to provide local posture services, and configure Cisco ISE to receive the compliance verification from the WLC to be used in an authorization policy.
B. Create an ASA Firewall posture policy, upload the Secure Client images to the NAD, and create a local client provisioning portal.
C. Create the required posture policy within Cisco ISE, configure redirection on the NAD, and ensure that the client provisioning policy is correct.
D. Identify the antimalware being used, create an endpoint script to ensure that it is updated, and send the update log to Cisco ISE for processing.

Answer: C

Question: 4

Refer to the exhibit.

Rule Number	Source	Destination	Service	Action	Log	Time
1	20.1.1.10	20.1.1.1	https	Allow	Log	Any
2	Any	Any	Any	Deny	Log	Any



Refer to the exhibit. An engineer must provide HTTPS access from the Google Cloud Platform virtual machine to the on-premises mail server. All other connections from the virtual machine to the mail server must be blocked. The indicated rules were applied to the firewall; however, the virtual machine cannot access the mail server. Which two actions should be performed on the firewall to meet the requirement? (Choose two.)

A. Set IP address 192.168.200.10 as the destination in rule 1.
B. Move up rule 2.
C. Set IP address 20.1.1.1 as the source in rule 1.
D. Configure a NAT rule.
E. Configure a security group.

Answer: A, D

Question: 5

Refer to the exhibit.

Refer to the exhibit. A security engineer deployed Cisco Secure XDR, and during testing, the log entry shows a security incident. Which action must the engineer take first?

A. Uninstall the malware.
B. Block IP address 10.77.17.45.

C. Isolate the endpoint.
D. Rebuild the endpoint.

Answer: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/