Vendor: Cisco

Exam Code: 300-740

Exam Name: Designing and Implementing Secure Cloud Access for Users and Endpoints

Version: DEMO

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

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

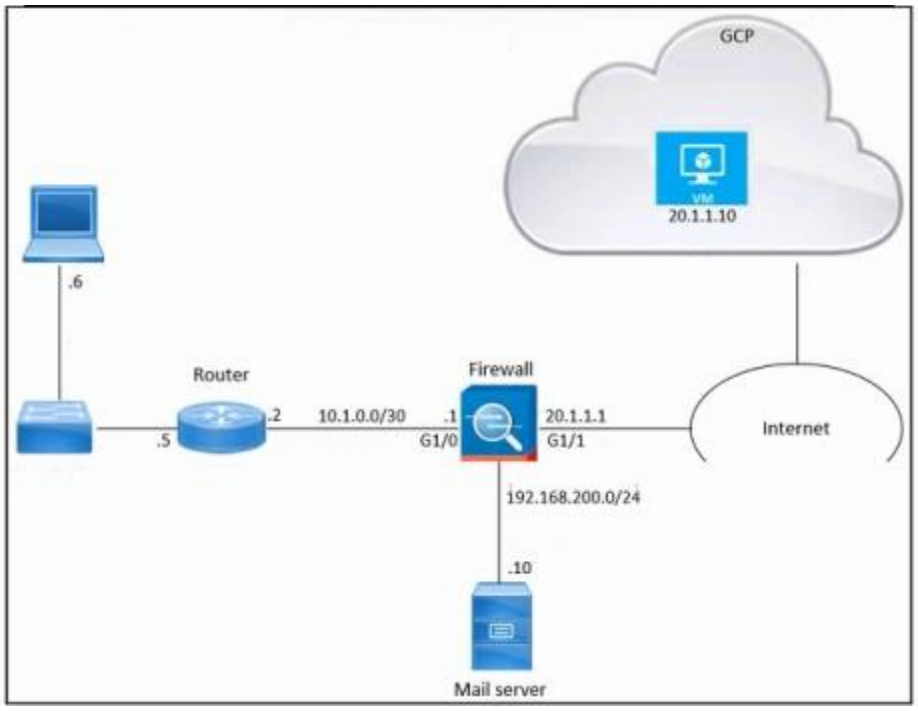
QUESTION 3
An administrator must deploy an endpoint posture policy for all users. The organization wants to have all endpoints checked against antimalware definitions and operating system updates and ensure that the correct Secure Client modules are installed properly. How must the administrator meet 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. 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.)

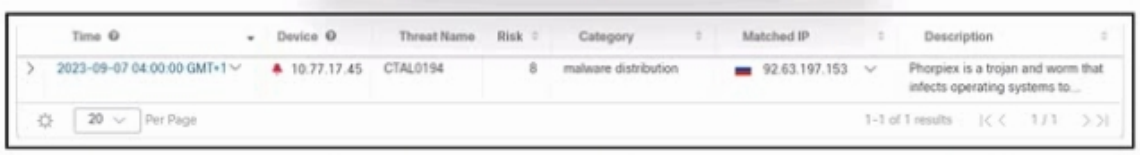
Rule Number	Source	Destination	Service	Action	Log	Time
1	20.1.1.10	20.1.1.1	https	Allow	Log	Any
2	Any	Any	Any	Deny	Log	Any



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: AD

QUESTION 5
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?

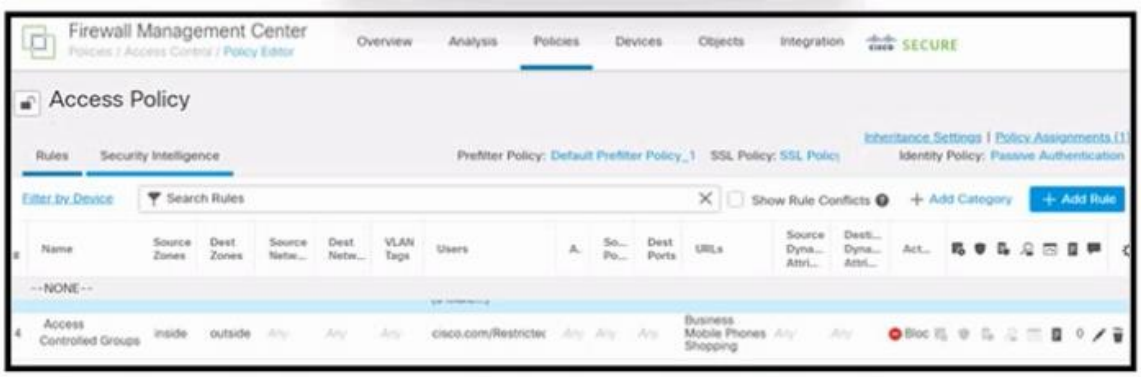


A. Uninstall the malware.
B. Block IP address 10.77.17.45.
C. Isolate the endpoint.
D. Rebuild the endpoint.

Answer: C

QUESTION 6
Refer to the exhibit. An engineer must create a policy in Cisco Secure Firewall Management Center to prevent restricted users from being able to browse any business or mobile phone

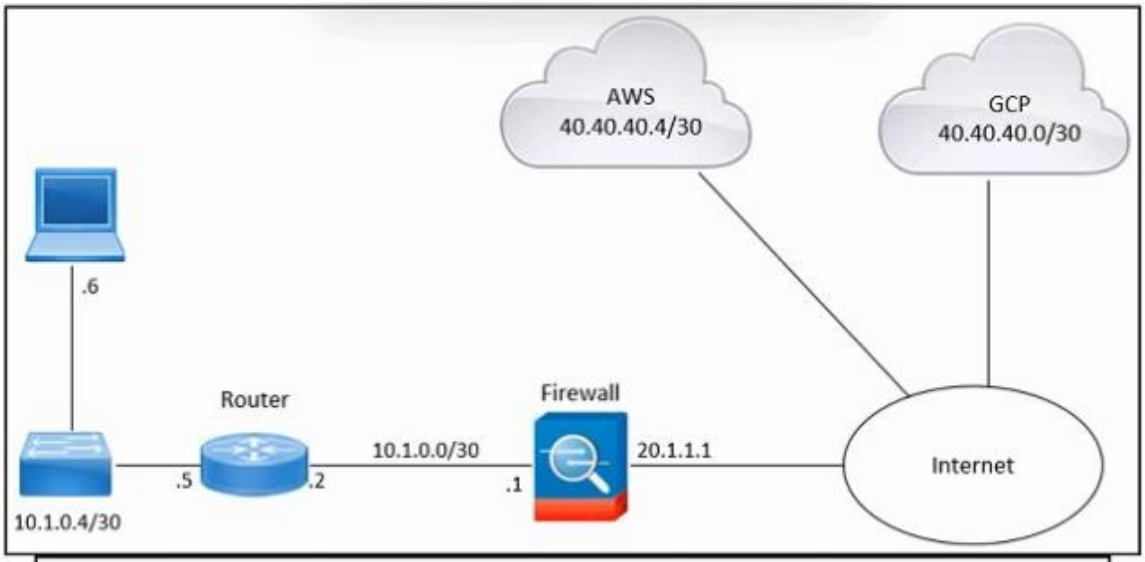
shopping websites. The indicated policy was applied; however, the restricted users still can browse on the mobile phone shopping websites during business hours. What should be done to meet the requirement?



A. Set Dest Zones to Business Mobile Phones Shopping.
B. Set Dest Networks to Business Mobile Phones Shopping.
C. Set Time Range for rule 4 of Access Controlled Groups to All.
D. Move rule 4 Access Controlled Groups to the top.

Answer: D

QUESTION 7
Refer to the exhibit. An engineer must provide RDP access to the AWS virtual machines and HTTPS access to the Google Cloud Platform virtual machines. All other connectivity must be blocked. The indicated rules were applied to the firewall; however, none of the virtual machines in AWS and Google Cloud Platform are accessible. What should be done to meet the requirement?



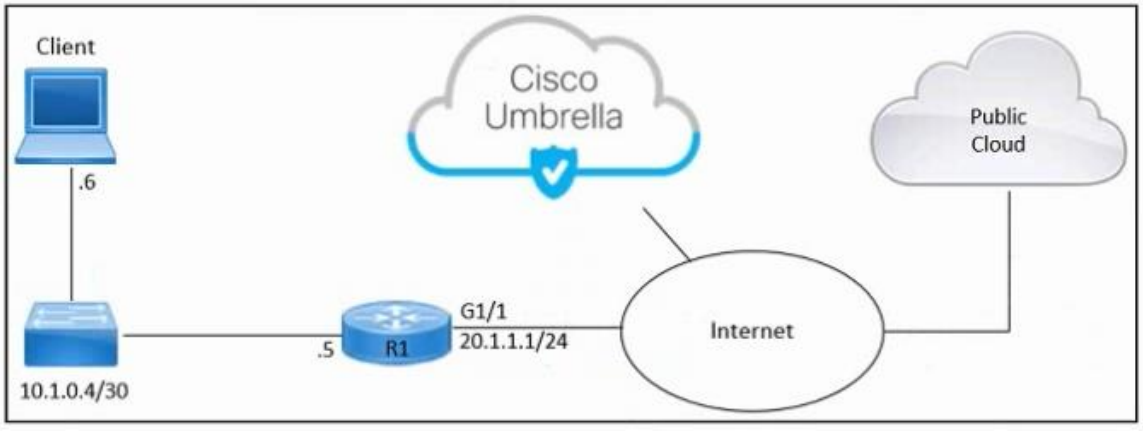
Rule Number	Source	Destination	Service	Action	Log	Time
1	Any	Any	Any	Deny	Log	Any
2	Any	40.40.40. 4 /30	RDP	Allow	Log	Any
3	Any	40.40.40.0/30	HTTPS	Allow	Log	Any

A. Move rule 2 to the first position.
B. Configure a NAT overload rule
C. Configure a virtual private cloud firewall rule
D. Move rule 1 to the last position

Answer: A

QUESTION 8
Refer to the exhibit. An engineer must connect an on-premises network to the public cloud using Cisco Umbrella as a Cloud Access Security Broker. The indicated configuration was applied to router R1; however, connectivity to Umbrella fails with this error: %OPENDNS-3-DNS_RES_FAILURE. Which action must be taken on R1 to enable the connection?

```
!
<output omitted>
!
ip domain lookup source-interface GigabitEthernet1/1
!
interface GigabitEthernet1/1
ip vrf forwarding INET
ip flow monitor CISCO-FLOWMONITOR input
ip flow monitor CISCO-FLOWMONITOR Output
ip address 20.1.1.1 255.255.255.0
ip nat outside
ip nbar protocol-discovery
zone-member security INTERNET
!
<output omitted>
!
```



A. Configure the Open DNS servers with the ip name-server command.
B. Configure a DHCP scope using the ip dhcp pool command.
C. Add the opendns in command to the interface configuration.
D. Add the opendns out command to the interface configuration.

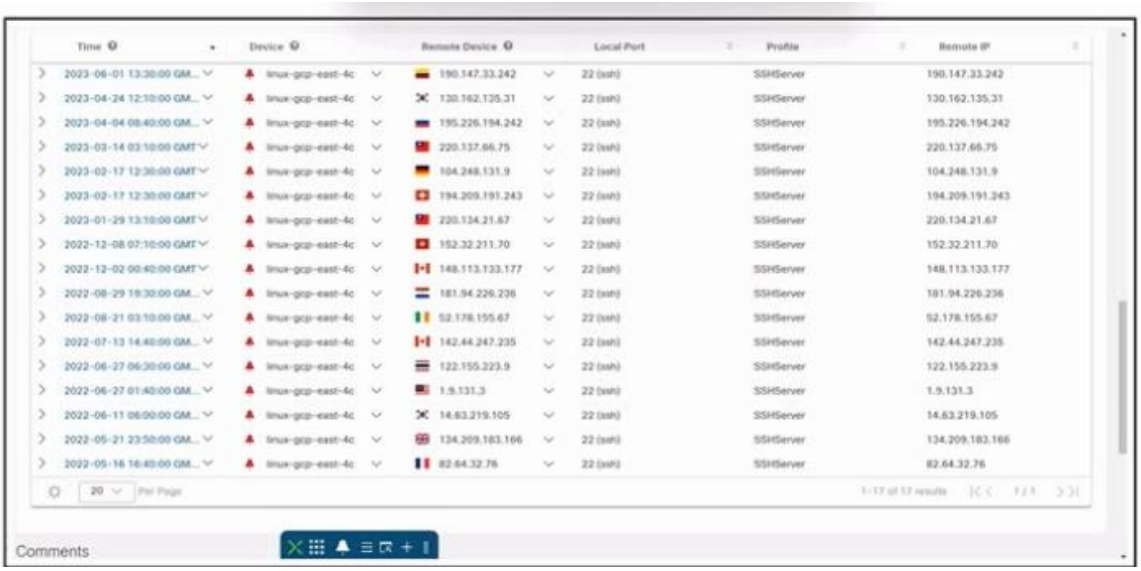
Answer: B

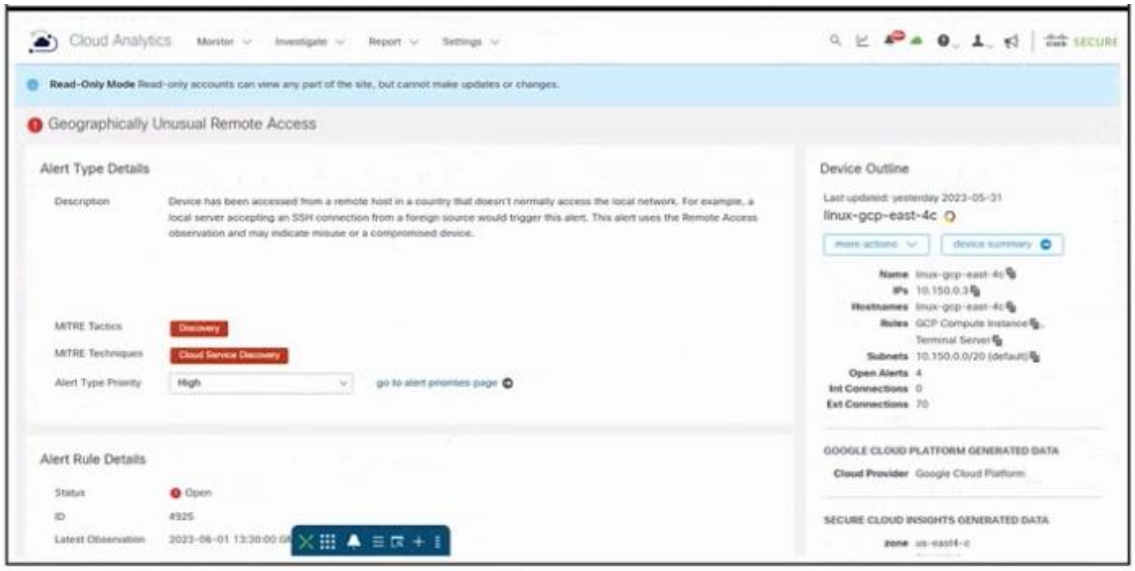
QUESTION 9
Which mitigation technique does a web application firewall use to protect a web server against DDoS attacks?

A. Source-specific ACL
B. Standard ACL
C. Packet filtering
D. Rate-based rules

Answer: D

QUESTION 10
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? (Choose two.)





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: BE

QUESTION 11
In the zero-trust network access model, which criteria is used for continuous verification to modify trust levels?

A. System patching status
B. Detected threat levels
C. User and device behavior
D. Network traffic patterns

Answer: C

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**