Question 1

An organization wants to reduce their attach surface for cloud applications. They want to understand application communications, detect abnormal application Behavior, and detect vulnerabilities within the applications. Which action accomplishes this task?

Options:

A- Configure Cisco Secure Workload to detect anomalies and vulnerabilities.

B- Use Cisco ISE to provide application visibility and restrict access to them.

C- Implement Cisco Umbrella lo control the access each application is granted.

D- Modify the Cisco Duo configuration to restrict access between applications.

Answer:

A

Explanation:

Cisco Secure Workload (formerly Tetration) is a solution that provides visibility, segmentation, and security for cloud applications. It can monitor application communications, detect abnormal application behavior, and identify vulnerabilities within the applications. Cisco

Question 2

Question Type: **MultipleChoice**

Which problem Is solved by deploying a multicontext firewall?

Options:

A- overlapping IP addressing plan

B- more secure policy

C- resilient high availability design

D- faster inspection

Answer:

A

Explanation:

A multicontext firewall is a feature that allows a single physical firewall to be divided into multiple virtual firewalls, also known as security contexts. Each context operates as an independent device, with its own security policy, interfaces, and administrators. This feature is useful for service providers, large enterprises, or any network that requires more than one firewall. One of the problems that a multicontext firewall can solve is an overlapping IP addressing plan. This means that different contexts can use the same IP addresses without causing conflicts, as long as they are separated by different interfaces or VLANs. This allows for more efficient use of IP address space and easier management of multiple networks.A multicontext firewall can also support dynamic routing protocols and VPNs within each context, providing more flexibility and functionality12Reference:=1: What Are Multi-Context Firewalls?- Franklin Fitch2: Multiple Context Mode - Cisco

Question 3

Question Type: **MultipleChoice**

A network engineer must create an access control list on a Cisco Adaptive Security Appliance firewall. The access control list must permit HTTP traffic to the internet from the organization's inside network 192.168.1.0/24. Which IOS command must oe used to create the access control list?

A.

```
access-list HTTP-ONLY extended permit tcp 192.168.1.0
255.255.255.0.
```

B.

```
access-list extended permit tcp 192.168.1.0
255.255.255.0 any eq 80.
```

C.

```
access-list HTTP-ONLY extended permit tcp 192.168.1.0
255.255.255.0 any eq 80.
```

D.

```
access-list permit http 192.168.1.0 255.255.255.0 any.
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

B

Question 4

Question Type: MultipleChoice

An engineer must modify an existing remote access VPN using a Cisco AnyConnect Secure Mobility client solution and a Cisco Secure Firewall. Currently, all the traffic generate by the user Is sent to the VPN tunnel and the engineer must now exclude some servers and access them directly instead. Which element must be modified to achieve this goat?

Options:

A- NAT exemption

B- encryption domain

C- routing table

D- group policy

Answer:

D

Explanation:

To achieve the goal of excluding some servers from the VPN tunnel and accessing them directly, the engineer must modify the group policy that is applied to the remote access VPN users. The group policy contains the settings for split tunneling, which is a feature that allows the VPN client to route some traffic through the VPN tunnel and some traffic directly to the internet. Split tunneling can be configured based on the destination IP address, the application, or the domain name of the traffic. By modifying the group policy, the engineer can specify which servers or networks should be excluded from the VPN tunnel and accessed directly by the VPN client. This can improve the performance and efficiency of the VPN connection, as well as reduce the load on the VPN gateway and the corporate network. However, split tunneling also introduces some security risks, such as exposing the VPN client to internet threats, bypassing the corporate firewall and security policies, and leaking sensitive dat

a. Therefore, the engineer must carefully evaluate the trade-offs and best practices of using split tunneling for remote access VPNs.Reference:=

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Secure Connectivity, Lesson 3.1: Implementing and Troubleshooting Remote Access VPN, Topic 3.1.4: Configure and Verify Remote Access VPN, Subtopic 3.1.4.2: Configure and Verify Split Tunneling

VPN Split Tunneling: What It Is & Pros and Cons

Question 5

Question Type: MultipleChoice

Which Cisco security solution gives the most complete view of the relationships and evolution of Internet domains IPs, and flies, and helps to pinpoint attackers' infrastructures and predict future threat?

Options:

A- Cisco Secure Network Analytics

B- Cisco Secure Cloud Analytics

C- Cisco Umbrella Investigate

D- Cisco pxGrid

Answer:

C

Question 6

An organization is implementing AAA for their users. They need to ensure that authorization is verified for every command that is being entered by the network administrator. Which protocol must be configured in order to provide this capability?

Options:
A- EAPOL

B- SSH

C- RADIUS

D- TACACS+

Answer:
D