Free Cisco 350-701 SCOR Practice Questions

Shared by Cohen on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

[Security Concepts]

Which algorithm provides asymmetric encryption?

Options:

A- RC4
B- AES
C- RSA
D- 3DES

Answer:

C

Explanation:

Asymmetric encryption, also known as public-key cryptography, is a type of encryption that uses a pair of keys to encrypt and decrypt data. The pair of keys includes a public key, which can be shared with anyone, and a private key, which is kept secret by the owner. In asymmetric encryption, the sender uses the recipient's public key to encrypt the data. The recipient then uses their private key to decrypt the data. This approach allows for secure communication between two parties without the need for both parties to have the same secret key. RSA is one of the most commonly used asymmetric encryption algorithms. It is based on the mathematical problem of factoring large numbers, which is believed to be hard to solve. RSA stands for Rivest-Shamir-Adleman, the names of the three inventors of the algorithm. RSA can be used for both encryption and digital signatures. To generate an RSA key pair, the following steps are performed:

Choose two large prime numbers, p and q, and compute their product, n = pq. This is called the modulus.

Choose a small number, e, that is relatively prime to (p-1)(q-1). This is called the public exponent.

Compute a number, d, that satisfies the equation ed 1 (mod (p-1)(q-1)). This is called the private exponent.

The public key is (n, e) and the private key is (n, d).

To encrypt a message, m, with the public key (n, e), the following formula is used:

c = m^e mod n

To decrypt a ciphertext, c, with the private key (n, d), the following formula is used:

m = c^d mod n

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 3: VPN Technologies, Lesson 3.1: Site-to-Site VPNs, Topic 3.1.2: IPsec VPNs

What is Asymmetric Encryption? - GeeksforGeeks

What is asymmetric encryption? | Asymmetric vs. symmetric ... - Cloudflare

Question 2

Question Type: MultipleChoice

[Security Concepts]

Under which two circumstances is a CoA issued? (Choose two)

Options:

A- A new authentication rule was added to the policy on the Policy Service node.
B- An endpoint is deleted on the Identity Service Engine server.
C- A new Identity Source Sequence is created and referenced in the authentication policy.
D- An endpoint is profiled for the first time.
E- A new Identity Service Engine server is added to the deployment with the Administration persona

Answer:

B, D

Explanation:

The profiling service issues the change of authorization in the following cases:

-- Endpoint deleted---When an endpoint is deleted from the Endpoints page and the endpoint is disconnected

or removed from the network.

An exception action is configured---If you have an exception action configured per profile that leads to an

unusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to the

corresponding static profile by issuing a CoA.

-- An endpoint is profiled for the first time---When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.

+ An endpoint identity group has changed---When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.

The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:

++ The endpoint identity group changes for endpoints when they are dynamically profiled

++ The endpoint identity group changes when the static assignment flag is set to true for a dynamic endpoint -- An endpoint profiling policy has changed and the policy is used in an authorization policy---When an endpoint profiling policy changes, and the policy is included in a logical profile that is used in an authorization policy. The endpoint profiling policy may change due to the profiling policy match or when an endpoint is statically assigned to an endpoint profiling policy, which is associated to a logical profile. In both the cases, the profiling service issues a CoA, only when the endpoint profiling policy is used in an authorization policy.

Question 3

Question Type: MultipleChoice

[Security Concepts]

Which ASA deployment mode can provide separation of management on a shared appliance?

Options:

A- DMZ multiple zone mode
B- transparent firewall mode
C- multiple context mode
D- routed mode

Answer:

C

Question 4

Question Type: MultipleChoice

Which interface mode does a Cisco Secure IPS device use to block suspicious traffic?

Options:

A- Passive
B- Inline
C- Promiscuous
D- Active

Answer:

B

Question 5

Question Type: MultipleChoice

[Security Concepts]

Which direction do attackers encode data in DNS requests during exfiltration using DNS tunneling?

Options:

A- inbound
B- north-south
C- east-west
D- outbound

Answer:

D

Explanation:

DNS tunneling is a technique that encodes data of other programs and protocols in DNS queries, including data payloads that can be used to control a remote server and

applications1.DNS exfiltration is a form of DNS tunneling that allows attackers to extract data from a compromised system by sending encoded DNS requests to a domain under their control2. The direction of the data transfer in DNS exfiltration isoutbound, meaning from the victim's network to the attacker's network.This is different from inbound, which means from the attacker's network to the victim's network, or north-south and east-west, which are terms used to describe the traffic flow between different network segments or zones3.Outbound DNS requests are often allowed by default in many firewalls and network devices, making them an attractive channel for data exfiltration4.However, DNS exfiltration can be detected and prevented by using security solutions that monitor and analyze DNS traffic for anomalies and malicious patterns5.

:1: Improvements to DNS Tunneling & Exfiltration Detection - Cisco Umbrella2: DNS Exfiltration & Tunneling: How it Works & DNSteal Demo Setup3: What Is DNS Tunneling?- Palo Alto Networks4: DNS Data Exfiltration and DNS Tunneling | Vercara5: DNS Exfiltration: The Light at the End of the DNS Tunnel - site

Question 6

Question Type: MultipleChoice

[Security Concepts]

What is a difference between a DoS attack and a DDoS attack?

Options:

A- A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where multiple systems target a single system with a DoS attack
B- A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where a computer is used to flood multiple servers that are distributed over a LAN
C- A DoS attack is where a computer is used to flood a server with UDP packets whereas a DDoS attack is where a computer is used to flood a server with TCP packets
D- A DoS attack is where a computer is used to flood a server with TCP packets whereas a DDoS attack is where a computer is used to flood a server with UDP packets

Answer:

A

Explanation:

A DoS (Denial of Service) attack is a type of cyberattack that aims to disrupt the normal

functioning of a server, service, or network by overwhelming it with a large amount of traffic or requests. A DoS attack typically uses a single computer or device to launch the attack, sending TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) packets to the target server. TCP and UDP are two common protocols used to send data over the internet. TCP packets require a connection to be established between the sender and the receiver, and ensure that the data is delivered reliably and in order. UDP packets do not require a connection, and do not guarantee the delivery or order of the data. Both TCP and UDP packets can be used to flood a server with requests, consuming its resources and bandwidth, and preventing legitimate users from accessing the service.

A DDoS (Distributed Denial of Service) attack is a type of DoS attack that uses multiple computers or devices to launch the attack, creating a large network of attackers that can generate more traffic or requests than a single source. A DDoS attack often involves a botnet, which is a network of compromised computers or devices that are controlled by a malicious actor, usually through malware or hacking. The botnet can send TCP or UDP packets to the target server from different locations and IP addresses, making it harder to trace and block the attack. A DDoS attack can also target multiple servers or services that are distributed over a LAN (Local Area Network), such as a web hosting service or a cloud computing platform, affecting the availability and performance of the entire network.

The main difference between a DoS attack and a DDoS attack is the number and diversity of the sources that are involved in the attack. A DoS attack comes from a single source, while a DDoS attack comes from multiple sources. This makes a DDoS attack more powerful, faster, and harder to stop than a DoS attack.

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Malware Threats, Lesson 2: Identifying Network Attacks, Topic: DoS and DDoS Attacks

DoS Attack vs. DDoS Attack: Key Differences? | Fortinet

What's the Difference Between a DOS and DDoS Attack? - How-To Geek

Question 7

Question Type: MultipleChoice

[Security Concepts]

What is the primary role of the Cisco Email Security Appliance?

Options:

A- Mail Submission Agent
B- Mail Transfer Agent
C- Mail Delivery Agent

D- Mail User Agent

Answer:

B

Explanation:

Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work

by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing

email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within

the email-delivery chain. Another name for an MTA is a mail relay.

Question 8

Question Type: MultipleChoice

[Security Concepts]

Using Cisco Cognitive Threat Analytics, which platform automatically blocks risky sites, and test unknown sites for hidden advanced threats before allowing users to click them?

Options:

A- Cisco Identity Services Engine (ISE)
B- Cisco Enterprise Security Appliance (ESA)
C- Cisco Web Security Appliance (WSA)
D- Cisco Advanced Stealthwatch Appliance (ASA)

Answer:

C

Explanation:

Cisco Web Security Appliance (WSA) is the platform that automatically blocks risky sites, and tests unknown sites for hidden advanced threats before allowing users to click them, using Cisco Cognitive Threat Analytics. Cisco Cognitive Threat Analytics is a cloud-based solution that reduces the time to discovery of threats operating inside the network by analyzing web traffic and detecting anomalous behavior. Cisco WSA integrates with Cisco Cognitive Threat Analytics to provide enhanced web security and breach detection. Cisco WSA can also leverage other Cisco security solutions, such as Cisco Umbrella, Cisco Advanced Malware Protection (AMP), and Cisco Talos Intelligence Group, to provide comprehensive web security.Reference:

Cisco Web Security Appliance (WSA)

Cisco Cognitive Threat Analytics At-a-Glance

Introducing Cisco Cognitive Threat Analytics

Implementing and Operating Cisco Security Core Technologies (SCOR) - Module 3: Cloud and Content Security

Question 9

Question Type: MultipleChoice

[Security Concepts]

How many interfaces per bridge group does an ASA bridge group deployment support?

Options:

A- up to 2
B- up to 4
C- up to 8
D- up to 16

Answer:

B

Explanation:

Each of the ASAs interfaces need to be grouped into one or more bridge groups. Each of these groups acts as an independent transparent firewall. It is not possible for one bridge group to communicate with another bridge group without assistance from an external router.

As of 8.4(1) upto 8 bridge groups are supported with 2-4 interface in each group. Prior to this

only one bridge group was supported and only 2 interfaces.

Up to 4 interfaces are permitted per bridge--group (inside, outside, DMZ1, DMZ2)

Question 10

Question Type: MultipleChoice

[Endpoint Protection and Detection]

Which benefit does endpoint security provide the overall security posture of an organization?

Options:

A- It streamlines the incident response process to automatically perform digital forensics on the endpoint.
B- It allows the organization to mitigate web-based attacks as long as the user is active in the domain.
C- It allows the organization to detect and respond to threats at the edge of the network.
D- It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.

Answer:

D

Explanation:

Endpoint security is the process of protecting devices like workstations, servers, and other devices from malicious threats and cyberattacks. Endpoint security enables businesses to secure endpoints that employees use for work purposes or servers that are either on a network or in the cloud. Endpoint security is important because every device that connects to the corporate network is a potential vulnerability, providing a possible entry point for cyber criminals. Therefore, every device an employee uses to connect to any business system or resource carries the risk of becoming the chosen route for hacking into an organization.These devices can be exploited by malware that could leak or steal sensitive data from the business12.

One of the benefits of endpoint security is that it allows the organization to detect and mitigate threats that the perimeter security devices do not detect. Perimeter security devices, such as firewalls and intrusion prevention systems, are designed to protect the network from external attacks. However, they may not be able to prevent or detect attacks that originate from within the network, such as insider threats, compromised devices, or lateral movement. Endpoint security solutions can provide visibility and control over the devices that connect to the

network, and can monitor, analyze, and respond to suspicious or malicious activities on the endpoints.Endpoint security solutions can also leverage threat intelligence and advanced analytics to identify and block known and unknown threats, such as ransomware, zero-day exploits, and targeted attacks13.Reference:=1: What is Endpoint Security? How Does It Work?| Fortinet2: Microsoft Defender for Endpoint | Microsoft Security3: Endpoint Security - Check Point Software

P2P exams