Cisco

(350-701)

Implementing and Operating Cisco Security Core Technologies

Total: **669 Questions**

Link:

Question: 1

Which functions of an SDN architecture require southbound APIs to enable communication?

A. SDN controller and the network elements
B. management console and the SDN controller
C. management console and the cloud
D. SDN controller and the cloud

Answer: A

Explanation:

The correct answer is **A. SDN controller and the network elements**. Software-Defined Networking (SDN) architectures are characterized by separating the control plane from the data plane. The **SDN controller**, acting as the brain of the network, resides in the control plane. It needs to instruct the underlying **network elements**, such as switches and routers, which operate in the data plane. This communication happens via **southbound APIs**. These APIs are specifically designed to allow the controller to push policies, configurations, and forwarding rules to the network devices, effectively dictating how they should handle traffic. Without functional southbound APIs, the controller would be unable to manage and program the physical
infrastructure. The management console, used by administrators, typically interacts with the SDN controller through northbound APIs, not southbound APIs. Similarly, the cloud might use higher-level abstractions to interact with the controller but doesn't directly use southbound APIs to the network elements. Therefore, option A directly addresses the core communication needed to implement the principles of SDN architecture.

Authoritative Links:

Open Networking Foundation (ONF) - SDN Architecture:https://opennetworking.org/sdn-resources/sdn-definition/ This link provides a general overview of SDN architecture and its key components.
Software-Defined Networking: A Comprehensive Guide (Cisco):
https://www.cisco.com/c/en/us/solutions/data-center-virtualization/software-defined-networking/index.html This Cisco resource explains SDN concepts and its benefits.

Question: 2

Which two request methods of REST API are valid on the Cisco ASA Platform? (Choose two.)

A. put
B. options
C. get
D. push
E. connect

Answer: AC

Explanation:

The correct REST API request methods valid on the Cisco ASA platform are **GET** and **PUT**.

Here's why:

GET: The GET method is fundamental to RESTful APIs. It's used to retrieve or read data from a specified resource. In the context of Cisco ASA, you would use GET to retrieve the current configuration, statistics, or other operational data. Think of it as asking the ASA, "Give me the information about this specific thing."

PUT: The PUT method is employed to update or create a resource. When modifying ASA settings using the REST API, you would use PUT to send the modified configuration data back to the ASA, effectively applying new configurations or changing existing ones. It can overwrite the resource if it exists. This means, you are essentially telling the ASA, "Here's the complete updated data. Use this."

Let's look at why the other options aren't valid:

OPTIONS: While OPTIONS is a valid HTTP method, it's primarily used to discover the available communication options for a particular resource, like available methods (GET, PUT etc). While Cisco ASA's REST API might technically respond to an OPTIONS call, it is not a way to perform an action, hence it is not the answer to what methods are valid to operate on the ASA.

PUSH There isn't an standard HTTP method named PUSH in REST API. It is a technology that allows the server to initiate data transfers to clients without them having to explicitly request it, and is typically handled through WebSockets or Server-Sent Events.

CONNECT: The CONNECT method is typically used for establishing a network connection, often for tunneling through a proxy. It's not relevant to the standard REST API usage on the Cisco ASA platform for configuration or monitoring.

In summary, the Cisco ASA platform uses a standard subset of REST API methods. GET to read information and PUT to update existing resources or create new ones. These methods align with core REST principles. The other methods are not used for primary manipulation operations on the ASA.

Authoritative Links for Further Research:

Cisco ASA REST API Documentation:https://www.cisco.com/c/en/us/td/docs/security/asa/api/asa-rest-api.html This is the official Cisco documentation for their ASA REST API, which should always be the first point of reference.

REST API Method Definitions:https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods Mozilla Developer Network provides a good description of standard HTTP methods

Question: 3

The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

A. SDN controller and the cloud
B. management console and the SDN controller
C. management console and the cloud
D. SDN controller and the management solution

Answer: D

Explanation:

The correct answer is **D. SDN controller and the management solution**. Northbound APIs in Software-Defined Networking (SDN) act as interfaces for the SDN controller to communicate with higher-level management and orchestration systems. These systems, often referred to as the management solution, handle tasks such as policy definition, service provisioning, and overall network management. They send instructions and configurations to the SDN controller using the northbound API. The SDN controller, in turn, translates these requests into low-level commands for the network devices. Therefore, the northbound API is the key communication bridge between the intelligence and management layer (management solution) and the network control layer (SDN controller). Options A, B, and C do not accurately represent the primary purpose of the northbound API. Option A, while SDN can interact with cloud services, the northbound API's direct function isn't primarily cloud communication. Option B is incorrect since a management console generally

interfaces with the management solution, not directly with the SDN controller via a northbound API. Option C is incorrect because the management console doesn't directly communicate with the cloud using northbound APIs. The northbound API facilitates the interaction between high-level management applications and the network's control plane, allowing for dynamic and automated network configurations.

For further research, consider the following resources:

Open Networking Foundation (ONF):https://opennetworking.org/ (Focus on SDN architecture and components)
SDN Central:https://www.sdncentral.com/ (Extensive information on SDN and its related concepts) **Network World:**https://www.networkworld.com/ (Articles and analysis on networking trends, including SDN)

Question: 4

What is a feature of the open platform capabilities of Cisco DNA Center?

A. application adapters
B. domain integration
C. intent-based APIs
D. automation adapters

Answer: C

Explanation:

The correct answer is **C. intent-based APIs**. Cisco DNA Center's open platform capabilities are primarily characterized by its programmable interface that uses intent-based APIs. These APIs allow external applications and systems to communicate with DNA Center by expressing desired network outcomes (the "intent") rather than specifying low-level configuration details. This aligns with a key tenet of software-defined networking (SDN), where policy abstraction simplifies network management and automation.

Intent-based APIs enable orchestration and integration across various domains and third-party tools. For instance, a security orchestration platform can use these APIs to automatically provision security policies or change network configurations based on detected threats. This facilitates a more agile and responsive security posture, moving beyond traditional manual configuration processes. This promotes a more open and flexible approach to network management, allowing for easy integration and development of customized solutions.

Options A, B, and D, while related to the overall functionality of DNA Center, do not primarily characterize its open platform capabilities. Application adapters (A) connect to specific applications, while domain integration (B) enables interaction with other Cisco solutions. Automation adapters (D) help automate specific tasks but are internal mechanisms for DNA center. Intent-based APIs (C), however, directly facilitate external interaction and extension of DNA Center functionality, making it an open and programmable platform.

Authoritative links:

Cisco DNA Center Platform:https://www.cisco.com/c/en/us/solutions/enterprise-networks/dna-center-platform.html
Cisco DNA Center REST APIs Documentation:https://developer.cisco.com/site/dna-center/ (Explore the API documentation for insights into intent-based interactions)
Intent-Based Networking:https://www.cisco.com/c/en/us/solutions/enterprise-networks/intent-based-networking.html

Question: 5

```
import requests

client_id = 'a1b2c3d4e5'

api_key = 'a1b2c3d4-e5f6-g7h8'

url = 'https://api.amp.cisco.com/v1/computers'

response = requests.get(url, auth=(client_id, api_key))

response_json = response.json()

for computer in response_json['data']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
        mac = network_interface.get('mac')
        ip = network_interface.get('ip')
        ipv6 = network_interface.get('ipv6')
        print(mac, ip, ipv6)
```

Refer to the exhibit. What does the API do when connected to a Cisco security appliance?

A. create an SNMP pull mechanism for managing AMP
B. gather network telemetry information from AMP for endpoints
C. get the process and PID information from the computers in the network D.
gather the network interface information about the computers AMP sees

Answer: D

Explanation:

gather the network interface information about the computers AMP sees

Question: 6

Which form of attack is launched using botnets?

A. TCP flood
B. DDOS
C. DOS
D. virus

Answer: B

Explanation:

The correct answer is B, DDOS (Distributed Denial of Service). Botnets are networks of compromised computers, often infected with malware, that are controlled by a single attacker (the bot herder). These compromised machines, known as bots or zombies, are then used to launch coordinated attacks. A DDoS attack is characterized by multiple sources overwhelming a target system or network with malicious traffic, rendering it unavailable to legitimate users. Botnets are the primary means by which DDoS attacks are executed due to their ability to generate a high volume of traffic from a multitude of locations simultaneously. Options A, TCP flood, and C, DOS (Denial of Service), are related but represent different aspects. A TCP flood is a specific type of DOS attack that exploits the TCP handshake process. DOS, as opposed to DDoS, involves a single source overwhelming the target. While viruses (D) can be a component of how machines become bots in a botnet, they aren't the form of attack launched using the botnet. Therefore, the coordinated and distributed nature of botnet traffic directly aligns with the characteristics of a DDoS attack, making it the correct choice.

Authoritative Links:

Cloudflare: What is a Botnet? - https://www.cloudflare.com/learning/bots/what-is-a-botnet/
Akamai: What is a DDoS Attack? - https://www.akamai.com/resources/ddos-protection **Cisco: Understanding DDoS Attacks** - https://www.cisco.com/c/en/us/products/security/ddos-protection/index.html

Question: 7

In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

A. smurf
B. distributed denial of service
C. cross-site scripting
D. rootkit exploit

Answer: C

Explanation:

The correct answer is C, Cross-Site Scripting (XSS). Alternate encoding, like hexadecimal representation, is frequently used in XSS attacks to obfuscate malicious JavaScript code injected into a web application. This obfuscation helps bypass basic input validation or filtering mechanisms that might look for specific keywords or characters. For instance, a simple <script> tag could be encoded as <script> or \x3cscript\x3e, which would still be interpreted as valid HTML by the browser but could avoid a naive filter. Attackers use various encoding techniques (URL encoding, HTML encoding, base64 encoding, etc.) to achieve this. The goal is to insert malicious scripts into a vulnerable website, which are then executed in the context of the victim's browser, potentially leading to session hijacking, cookie theft, or data breaches. Smurf attacks (A) leverage ICMP echo request broadcasts, DDoS attacks (B) overwhelm a server with traffic, and rootkit exploits (D) focus on gaining privileged access at the system level; they typically do not rely heavily on encoded scripts for their execution. Therefore, alternate encoding is most closely associated with the evasion tactics characteristic of XSS attacks.

Further Research:

OWASP Cross-site Scripting (XSS): https://owasp.org/www-project-top-ten/
Understanding XSS Encoding:

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Question: 8

Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

A. user input validation in a web page or web application
B. Linux and Windows operating systems
C. database
D. web page images

Answer: A

Explanation:

The correct answer is A, user input validation in a web page or web application. SQL injection exploits a fundamental weakness in how applications handle user-provided data. Specifically, it targets the lack of proper sanitization and validation of input fields. When a web application directly incorporates unsanitized user input into SQL queries, an attacker can insert malicious SQL code. This injected code manipulates the database query, potentially bypassing security measures, extracting sensitive information, modifying or deleting data, or even gaining administrative control. Poor input validation is the primary flaw exploited, as the application fails to distinguish between legitimate data and malicious SQL commands. Operating systems (B), the database itself (C), or images on web pages (D) are not the direct vulnerability points for SQL injection attacks. While database configuration and operating system security are important, SQL injection focuses on flaws within the application layer's data handling practices. This is a critical vulnerability because it sits between the user and the database, often involving direct access to a sensitive resource. Proper input validation, using parameterized queries or prepared statements, is crucial for mitigating SQL injection risks by separating SQL commands from user-provided data, ensuring that input is treated as data, not executable code.

OWASP SQL Injection: This resource provides detailed information on SQL injection, including attack techniques and prevention methods.CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'): This entry in the Common Weakness Enumeration database details the specifics of the SQL injection vulnerability.

Question: 9

What is the difference between deceptive phishing and spear phishing?

A. Deceptive phishing is an attacked aimed at a specific user in the organization who holds a C-level role.
B. A spear phishing campaign is aimed at a specific person versus a group of people.
C. Spear phishing is when the attack is aimed at the C-level executives of an organization.
D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Answer: B

Explanation:

The correct answer is **B. A spear phishing campaign is aimed at a specific person versus a group of people.**

Here's the justification:

Phishing, in general, is a cyberattack that uses deceptive tactics to trick individuals into revealing sensitive information like login credentials or financial details. This is typically done through emails, messages, or websites disguised to look legitimate. Spear phishing and deceptive phishing are subtypes of phishing, with key differences.

Spear phishing attacks are highly targeted. Instead of sending out a generic phishing message to a large group, spear phishing focuses on a specific individual or a small group of individuals, often within the same organization. Attackers usually research their target, crafting messages that appear highly personalized, increasing the likelihood of success. The attacker uses information gathered about the target such as role, projects and colleague's names to create a believable narrative.

Deceptive phishing, while also aiming to trick victims, is not necessarily targeted. Deceptive phishing usually involves a more generic approach, sending out a wider array of attacks that may appear to come from reputable sources, but without the research and personalized targeting of spear phishing. Deceptive phishing casts a wider net in the hopes of landing a catch. This might include fake invoices, password reset requests, or security alerts that attempt to entice the user into taking an action the attacker desires.

Option A is incorrect because spear phishing is not exclusive to C-level roles. Although, those roles can be targeted, other roles and individuals might also be targets of this attack. Option C is incorrect because it defines the target of spear phishing too narrowly. The attack can be against any person or group not necessarily C-level executives. Option D describes a type of DNS attack, which is not related to phishing.

Therefore, option B correctly highlights the distinction: spear phishing targets specific individuals, while deceptive phishing is more general.

Authoritative Links for Further Research:

CISA (Cybersecurity and Infrastructure Security Agency):

Understanding Phishing
Recognizing and Avoiding Email Scams
NIST (National Institute of Standards and Technology):

NIST Special Publication 800-53 (This publication covers security controls, including aspects related to phishing and awareness)
SANS Institute:

Phishing

These resources offer comprehensive information on phishing, spear phishing, and related cybersecurity concepts.

Question: 10

Which two behavioral patterns characterize a ping of death attack? (Choose two.)

A. The attack is fragmented into groups of 16 octets before transmission.
B. The attack is fragmented into groups of 8 octets before transmission.
C. Short synchronized bursts of traffic are used to disrupt TCP connections.
D. Malformed packets are used to crash systems.
E. Publicly accessible DNS servers are typically used to execute the attack.

Answer: BD

Explanation:

A Ping of Death attack exploits vulnerabilities in how systems handle oversized ICMP (Internet Control Message Protocol) echo request packets (pings). Option B is correct because, traditionally, a ping of death attack involves fragmenting the oversized ICMP packet into smaller segments. Older systems had limitations on the maximum size they could process, and they would reassemble these fragments at the destination. If the fragments combined to exceed the maximum allowed size, this could cause a buffer overflow and crash the target system. These fragments were typically in sizes less than the maximum allowed by the Internet Protocol, not specifically 8 octets. Option D is correct because the core principle of a Ping of Death attack relies on malformed or oversized packets. When a system attempts to process this unusual packet, it often leads to system instability and a crash. This is because the oversized or malformed packet can exceed the buffer size or cause unexpected state transitions in the network stack. Options A and C don't describe the technique. Fragmentation used in option A is not specific to a Ping of Death attack. Option C describes a different attack vector (like SYN flood attacks). Finally, while some attacks may use publicly accessible DNS servers to amplify the impact, option E is not specific to ping of death attack, and it is more associated with DNS amplification attacks.

Authoritative Links:

Wikipedia:https://en.wikipedia.org/wiki/Ping_of_death
Cisco: (You can search Cisco's website with terms like "Ping of Death" and relevant concepts for more specific documentation.)

Question: 11

Which two mechanisms are used to control phishing attacks? (Choose two.)

A. Enable browser alerts for fraudulent websites.
B. Define security group memberships.
C. Revoke expired CRL of the websites.
D. Use antispyware software.
E. Implement email filtering techniques.

Answer: AE

Explanation:

The correct answer is A and E. Phishing attacks primarily leverage deceptive emails and websites to trick users into revealing sensitive information. Enabling browser alerts for fraudulent websites (A) is a crucial defense mechanism. These alerts, often powered by regularly updated lists of known malicious sites, warn users when they are about to access a potentially harmful webpage, directly hindering the success of a phishing link. Similarly, implementing email filtering techniques (E) is essential. These filters analyze incoming emails for suspicious characteristics like spoofed senders, malicious attachments, and links to known phishing domains, effectively blocking or quarantining potentially dangerous messages before they reach the user's inbox. Security group memberships (B) control access to network resources and are not directly involved in preventing phishing attacks. Revoking expired CRLs (C), while important for overall security, primarily relates to certificate management and not the interception of phishing attempts. Antispyware software (D) targets malicious software like keyloggers and Trojans which may be delivered via phishing links but is not a primary control against the attack itself. Therefore, the core defense against phishing is to alert users of malicious websites and prevent the delivery of phishing emails altogether.

Further research:

Anti-Phishing Working Group (APWG):https://apwg.org/ - Provides resources and reports on phishing trends

and countermeasures.

National Institute of Standards and Technology (NIST):https://www.nist.gov/ - Offers guidance on information security, including protection against phishing.

Google Safe Browsing:https://safebrowsing.google.com/ - Details how browser alerts work.

Email Security Gateways: Researching vendors like Proofpoint, Mimecast, or Cisco Email Security will explain filtering techniques.

Question: 12

Which attack is commonly associated with C and C++ programming languages?

A. cross-site scripting

B. water holing

C. DDoS

D. buffer overflow

Answer: D

Explanation:

The correct answer is D, buffer overflow. Buffer overflows are particularly prevalent in applications developed using C and C++ due to their low-level memory management capabilities. These languages directly manipulate memory addresses, which, while powerful, can lead to vulnerabilities if not handled meticulously.

Specifically, when a program attempts to write data beyond the allocated memory buffer, a buffer overflow occurs. This can overwrite adjacent memory regions, corrupting data, potentially altering program execution flow, or even leading to remote code execution, making it a significant security concern. Unlike higher-level languages with automatic memory management, C and C++ require explicit handling of memory buffers, placing the responsibility of bounds checking squarely on the developer. This manual approach increases the potential for human error, thereby increasing the likelihood of buffer overflow vulnerabilities being introduced during development. Such vulnerabilities are often exploited by attackers to gain unauthorized access or disrupt systems. Cross-site scripting (XSS) involves web application vulnerabilities, while water holing targets specific groups of users, and DDoS attacks overwhelm networks with traffic, none of which are directly tied to a specific coding language vulnerability.

Further Research:

1. **OWASP (Open Web Application Security Project) - Buffer Overflow:**https://owasp.org/www-community/vulnerabilities/Buffer_Overflow
2. **CWE (Common Weakness Enumeration) - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'):**https://cwe.mitre.org/data/definitions/120.html
3. **SANS Institute - Understanding Buffer Overflows:**https://www.sans.org/reading-room/whitepapers/application/understanding-buffer-overflows-339

Question: 13

Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two.)

A. Check integer, float, or Boolean string parameters to ensure accurate values.

B. Use prepared statements and parameterized queries.

C. Secure the connection between the web and the app tier.

D. Write SQL code instead of using object-relational mapping libraries.

E. Block SQL code execution in the web application database login.

Answer: AB

Explanation:

Let's analyze why options A and B are the correct prevention techniques for mitigating SQL injection attacks.

Option A: Check integer, float, or Boolean string parameters to ensure accurate values.

This technique, known as input validation, is crucial. SQL injection exploits the way user-provided input is concatenated directly into SQL queries. By validating that the input received for parameters meant to be numbers (integers, floats) or Booleans indeed conforms to those data types, you prevent attackers from inserting malicious SQL code disguised as legitimate input. If the input is intended to be an integer, for example, the application should reject any input containing letters or SQL keywords. This helps filter out any attempts to inject code within data parameters.

Option B: Use prepared statements and parameterized queries.

Prepared statements and parameterized queries are a cornerstone of safe SQL coding. With these methods, the structure of the SQL query is defined first (the "prepared" part) and then the actual values that will be used in the query are passed as separate parameters to the database system. This separation of query structure and data prevents the database from interpreting user input as part of SQL code. The database understands the parameter is not part of the structure, and it won't execute it as commands. It effectively prevents the malicious injection of data disguised as SQL code.

Why other options are incorrect:

Option C: Secure the connection between the web and the app tier. While securing connections (e.g., using HTTPS) is essential for overall security, it doesn't specifically mitigate SQL injection. SQL injection happens at the database layer. Secure communication protects data in transit but does not modify the structure of queries themselves.

Option D: Write SQL code instead of using object-relational mapping libraries. Object-relational mapping (ORM) libraries can help prevent SQL injection if used correctly because they often include built-in parameterized query mechanisms. However, writing SQL directly, if not done with parameterized queries, can be vulnerable. It's not a primary prevention technique.

Option E: Block SQL code execution in the web application database login. Blocking SQL execution within a login is usually not feasible and would render the system unusable. The goal is not to prevent SQL from being executed in general, but to prevent injected SQL from being executed.

Authoritative Links:

1. **OWASP SQL Injection Prevention Cheat Sheet:** https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html 2. **CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'):** https://cwe.mitre.org/data/definitions/89.html
3. **SQL Injection Prevention - Wikipedia:**https://en.wikipedia.org/wiki/SQL_injection

Question: 14

Which two kinds of attacks are prevented by multifactor authentication? (Choose two.)

A. phishing

B. brute force

C. man-in-the-middle

D. DDOS

E. tear drop

Answer: AB

Explanation:

The correct answer is **A. phishing** and **B. brute force**. Multifactor authentication (MFA) significantly mitigates the risk of successful phishing and brute-force attacks by adding an extra layer of security beyond a simple username and password.

A phishing attack relies on tricking a user into revealing their credentials. While a user might be fooled into giving up their password, MFA requires a second factor, such as a code from a mobile app or a fingerprint, which is much harder for an attacker to obtain. Even if the attacker gets the password, they won't have access without this second factor.

Brute force attacks involve systematically trying many username/password combinations to gain unauthorized access. MFA makes these attempts substantially more difficult and time-consuming. If a valid password is guessed, the attacker still needs the second authentication factor, effectively stopping the breach.

While MFA provides a strong defense against compromised credentials, it does not directly prevent man-in-the-middle attacks, which focus on intercepting communication. Nor does it block DDoS attacks, which aim to overwhelm a service with traffic. Similarly, tear drop attacks, which exploit IP fragmentation vulnerabilities, are outside the scope of MFA protection. Therefore, options C, D, and E are not prevented by MFA.

In essence, MFA's strength lies in ensuring even if an attacker gets one piece of the puzzle (e.g., password through phishing or brute-force), they still lack the necessary secondary authentication, bolstering overall account security.

Authoritative Links for Further Research:

NIST Guidelines on Authentication: https://csrc.nist.gov/publications/detail/sp/800-63/3/final OWASP Multi-Factor Authentication Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html

Question: 15

What are two rootkit types? (Choose two.)

A. registry

B. buffer mode

C. user mode

D. bootloader

E. virtual

Answer: CD

Explanation:

The correct answers are C and D, user mode and bootloader rootkits, respectively. Rootkits are malicious software designed to conceal the presence of other malware on a system. They operate at different levels of the system, affecting how they function and are detected. User mode rootkits operate at the application level

(also known as the user space) and usually replace standard system executables or DLLs with modified, malicious versions. These rootkits are generally easier to create but also easier to detect than kernel or bootloader rootkits. Bootloader rootkits, on the other hand, operate at the lowest level, residing in the boot sector or master boot record (MBR). These rootkits are very dangerous as they load before the operating system, granting them complete control and making detection and removal incredibly difficult. A registry (A) is a database that stores configuration settings and is not a type of rootkit. Buffer mode (B) doesn't describe a rootkit type. The virtual (E) option is too general as rootkits can exist in virtualized environments but it's not specific enough to be a type. In essence, rootkits utilize different attack vectors to hide malicious operations, and user mode and bootloader represent two crucial levels where these attacks can manifest.

Further research can be conducted via the following links:

Microsoft's documentation on Rootkits:https://learn.microsoft.com/en-us/windows/security/threat-protection/intelligence/rootkits
Wikipedia's page on Rootkits:https://en.wikipedia.org/wiki/Rootkit
SANS Institute's resources on malware analysis:https://www.sans.org/information-security/

Question: 16

How is DNS tunneling used to exfiltrate data out of a corporate network?

A. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers

B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data

C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network

D. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks

Answer: B

Explanation:

The correct answer is **B**, which accurately describes how DNS tunneling is used for data exfiltration. DNS tunneling leverages the DNS protocol, which is typically allowed through firewalls, to create a covert communication channel. Malicious actors encode data into DNS queries, specifically within the domain name portion. These encoded queries are sent to a rogue DNS server controlled by the attacker. The rogue server receives these queries, extracts the encoded data, and reconstructs the exfiltrated information. The process works because DNS clients (like computers on a corporate network) are allowed to make DNS requests to external servers. By encoding the data within the DNS request, it appears like legitimate DNS traffic, making it hard to detect with traditional security tools. Options A, C, and D describe other attacks involving DNS but do not accurately portray how DNS tunneling is utilized for data exfiltration. DNS tunneling exploits the fact that DNS queries can include arbitrary text in domain name fields. This text, when cleverly crafted, becomes the channel for transmitting stolen information. It is a popular tactic because DNS is often overlooked by security mechanisms and has the necessary infrastructure to carry this kind of traffic.

Authoritative links for further research:

Cloudflare: What is DNS Tunneling?
CISA: Understanding DNS Security Threats
SANS Institute: DNS Tunneling

Question: 17

Which type of attack is social engineering?

A. trojan
B. MITM
C. phishing
D. malware

Answer: C

Explanation:

Phishing is a form of social engineering attack, not a type of malware or a man-in-the-middle (MITM) attack. Social engineering manipulates individuals into divulging confidential information or performing actions that compromise security. Phishing employs deceptive emails, messages, or websites that impersonate legitimate entities, like banks or service providers, to trick victims into revealing credentials, financial details, or other sensitive data. The attacker relies on human error, not technical vulnerabilities in a system, to achieve their objective. Trojans, on the other hand, are a type of malware that disguise themselves as legitimate software. MITM attacks intercept communication between two parties. While phishing can be used to deliver malware, it's fundamentally a social engineering tactic that leverages psychological manipulation rather than exploiting software flaws. Therefore, C. phishing, is the correct answer since phishing is a common social engineering method.

Authoritative resources:

NIST Computer Security Resource Center:https://csrc.nist.gov/glossary/term/social_engineering **CISA (Cybersecurity and Infrastructure Security Agency):**https://www.cisa.gov/news-events/news/protect-yourself-against-social-engineering-attacks
SANS Institute:https://www.sans.org/information-security/glossary/social-engineering

Question: 18

What are two DDoS attack categories? (Choose two.)

A. protocol
B. source-based
C. database
D. sequential
E. volume-based

Answer: AE

Explanation:

The correct answer is A and E, which represent **protocol-based** and **volume-based** DDoS attack categories respectively. Protocol-based attacks exploit weaknesses in network layer protocols, aiming to disrupt services by consuming server resources. For example, SYN flood attacks exploit the TCP handshake process, overwhelming the target with connection requests, causing the server to become unresponsive. These attacks specifically target the protocol behavior rather than solely the amount of traffic. Conversely, volume-based attacks aim to saturate the network bandwidth of a target or its associated infrastructure with sheer amounts of traffic. These attacks, like UDP floods or ICMP floods, rely on generating immense quantities of packets, often from compromised systems, to overwhelm the target's network capacity, making it inaccessible to

legitimate users. Options B, C, and D are not primary categories used for classifying DDoS attacks; source-based might be a relevant aspect, but is not a primary category, database refers to a type of service targeted, not a category of attack, and sequential is irrelevant. Thus, protocol-based (A) and volume-based (E) are the two established main categories.

Further research can be conducted on the following authoritative sources:

1. **Cloudflare Learning Center - DDoS Attacks:**https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
2. **Akamai - What is a DDoS Attack?:**https://www.akamai.com/what-is/ddos
3. **Imperva - DDoS Attack Types:**https://www.imperva.com/learn/ddos/ddos-attack-types/

Question: 19

In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?

A. man-in-the-middle
B. LDAP injection
C. insecure API
D. cross-site scripting

Answer: A

Explanation:

The correct answer is A, man-in-the-middle (MitM) attack. This type of attack involves an attacker positioning themselves between two communicating parties, intercepting, and potentially altering the messages exchanged. The attacker essentially acts as an intermediary, gaining unauthorized access to sensitive information. In cloud computing, MitM attacks can target various communication channels, including web traffic, API calls, and even virtual network connections. The attacker's machine actively participates in the conversation, making it seem like a legitimate part of the communication flow to both the victim and the target host. LDAP injection (B) is a technique where malicious code is inserted into LDAP queries. Insecure API (C) refers to vulnerabilities in the interfaces that enable different software applications to communicate.

Cross-site scripting (XSS) (D) involves injecting malicious scripts into websites viewed by other users. These other types of attacks don't involve an attacker directly sitting in between two communicating hosts as a third party, making MitM the defining characteristic that aligns with the description in the question. The core concept of MitM revolves around interception and manipulation of data in transit, which is distinct from other injection-based or scripting attacks. Therefore, only the man-in-the-middle attack precisely matches the scenario described.

Authoritative links for further research:

OWASP (Open Web Application Security Project) on Man-in-the-Middle Attacks:https://owasp.org/www-community/attacks/Man-in-the-middle
NIST (National Institute of Standards and Technology) Cybersecurity Framework:
https://www.nist.gov/cyberframework (This framework provides broader context for security risks including MitM attacks)
SANS Institute on Man-in-the-Middle Attacks:https://www.sans.org/blog/man-in-the-middle-mitm-attacks-explained/

Question: 20

How does Cisco Advanced Phishing Protection protect users?

A. It utilizes sensors that send messages securely.

B. It uses machine learning and real-time behavior analytics.

C. It validates the sender by using DKIM.

D. It determines which identities are perceived by the sender.

Answer: B

Explanation:

The correct answer is **B. It uses machine learning and real-time behavior analytics.** Cisco Advanced Phishing Protection leverages sophisticated techniques to identify and mitigate phishing attacks. Unlike simple sender validation methods like DKIM (Option C), which only verifies if the email was authorized by a sending domain, Advanced Phishing Protection delves deeper into the behavior of the email and its links. Option A is incorrect because while sensors might play a role in overall security, they are not the primary mechanism for phishing protection. Option D, focusing on identity perception by the sender, isn't a core mechanism of typical phishing defenses.

Machine learning algorithms are trained on vast datasets of phishing emails and legitimate communications.

This enables the system to recognize patterns, anomalies, and malicious intent often missed by traditional methods. Real-time behavior analysis examines the email's content, links, and embedded code as they are being processed, looking for suspicious activities. This includes unusual URL patterns, domain registrations, and deceptive language. These analyses occur rapidly, allowing the system to block or flag emails before they reach the user's inbox. By combining these methods, Advanced Phishing Protection effectively neutralizes evolving threats that evade conventional security measures. The focus on behavior rather than just static attributes is the cornerstone of its effectiveness. Cloud services often utilize these dynamic analysis techniques due to their ability to scale and update quickly.

For further research, consider these resources:

Cisco Advanced Email Security:https://www.cisco.com/c/en/us/products/security/email-security/index.html (This link will lead you to Cisco's general page on email security which often includes info on Advanced Phishing Protection features, or links to it.)
Machine Learning for Cybersecurity:https://www.sciencedirect.com/topics/computer-science/machine-learning-for-cybersecurity (This provides general information on the role of machine learning in cybersecurity).

Understanding Real-Time Behaviour Analytics:https://www.ibm.com/topics/behavior-analytics (This IBM link goes into more detail about the concept of behaviour analytics in cybersecurity)

Question: 21

How does DNS Tunneling exfiltrate data?

A.An attacker registers a domain that a client connects to based on DNS records and sends malware through that connection.

B.An attacker opens a reverse DNS shell to get into the client's system and install malware on it.

C.An attacker sends an email to the target with hidden DNS resolvers in it to redirect them to a malicious domain.

D.An attacker uses a non-standard DNS port to gain access to the organization's DNS servers in order to poison the resolutions.

Answer: A

Explanation:

The correct answer, A, accurately describes how DNS tunneling works to exfiltrate data. DNS tunneling leverages the Domain Name System (DNS) protocol, which is typically allowed through firewalls, to create a covert communication channel. Instead of using DNS queries for their intended purpose (resolving domain names to IP addresses), attackers embed data within the DNS query and response fields.

Specifically, an attacker registers a domain (e.g., attacker.com) and sets up a DNS server that they control. A compromised client within the target network, perhaps through malware, crafts DNS queries where the subdomain part contains the data to be exfiltrated. For instance, the client might send a query like "data1.data2.data3.attacker.com." The attacker's DNS server receives this query, extracts the encoded data (data1, data2, data3), and sends a valid, albeit manipulated, DNS response back to the client. The client, programmed to expect this, will extract the data from the response for further communication. This technique avoids direct network connections, making the communication look like ordinary DNS traffic. Option A correctly captures this process: the client "connects" to the domain by sending DNS queries, and the attacker uses this channel to exfiltrate data through encoded payloads.

Options B, C, and D are incorrect. Option B describes a reverse DNS shell which is more about gaining direct control of a system rather than exfiltration, it does not use reverse DNS this way. Option C depicts a typical phishing attempt utilizing malicious links and email redirect. Finally, option D describes DNS poisoning which seeks to corrupt the cache to redirect a user but does not exfiltrate data as described.

For further research, refer to these resources:

1. **Cloudflare:**Understanding DNS Tunneling - Cloudflare
2. **SANS Institute:**DNS Tunneling - SANS Institute
3. **Cisco:**DNS Tunneling Attacks: What Are They and How to Stop Them? - Cisco

Question: 22

An attacker needs to perform reconnaissance on a target system to help gain access to it. The system has weak passwords, no encryption on the VPN links, and software bugs on the system's applications. Which vulnerability allows the attacker to see the passwords being transmitted in clear text?

A.unencrypted links for traffic
B.weak passwords for authentication
C.improper file security
D.software bugs on applications

Answer: A

Explanation:

The correct answer is **A. unencrypted links for traffic**. Here's why:

Reconnaissance, in the context of a cyberattack, involves gathering information about a target system. In this scenario, the attacker's goal is to exploit vulnerabilities to gain access. The question specifically asks which vulnerability would allow the attacker to see passwords in clear text during transmission. Unencrypted links (like those without VPN encryption) transmit data, including passwords, without obfuscation. This makes them susceptible to interception using packet sniffers or network analyzers. If traffic is not encrypted, the attacker can simply capture the data stream and read the password directly.

Weak passwords, while making it easier to guess login credentials via brute force, wouldn't allow an attacker

to see passwords in transmission. Improper file security could expose stored passwords, not transmitted ones. Software bugs in applications could lead to various exploits, but do not directly expose transmitted passwords in clear text.

Encryption, such as TLS/SSL or VPN encryption, is designed to scramble data, making it unreadable without the decryption key. The lack of encryption on VPN links leaves the data, including authentication credentials, vulnerable to being intercepted and read. This highlights the critical role of encryption in securing communication channels and protecting sensitive information during transmission.

Authoritative Links for Further Research:

1. **OWASP (Open Web Application Security Project) - Transport Layer Security:** https://owasp.org/www-project-top-ten/ (Specifically, look for the 'Insufficient Cryptography' section related to insecure transport of data.)
2. **National Institute of Standards and Technology (NIST) - Special Publication 800-53:** https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (This document provides security and privacy controls, including those regarding data in transit and encryption.)
3. **SANS Institute - Securing Network Traffic:**https://www.sans.org/reading-room/whitepapers/network/securing-network-traffic-33452 (This provides information about why encryption is so important to network security).

Question: 23

A user has a device in the network that is receiving too many connection requests from multiple machines. Which type of attack is the device undergoing?

A.SYN flood
B.slowloris
C.phishing
D.pharming

Answer: A

Explanation:

The correct answer is A, SYN flood. A SYN flood attack is a type of denial-of-service (DoS) attack that exploits the TCP three-way handshake. In a normal TCP connection, a client sends a SYN (synchronize) packet to a server. The server responds with a SYN-ACK (synchronize-acknowledge) packet. Finally, the client sends an ACK (acknowledge) packet, establishing the connection. During a SYN flood, an attacker sends a large volume of SYN packets to the target server, but never completes the three-way handshake by sending the final ACK.

This leaves the server with numerous half-open connections, consuming resources like memory and processing power. The server becomes overwhelmed and unable to process legitimate connection requests from other users, effectively denying service. The attack originates from multiple source machines, which is consistent with the scenario described. Options B, C, and D are not appropriate in this context. A slowloris attack (B) aims to exhaust server resources by slowly sending HTTP headers, but does not typically involve a large volume of connection requests. Phishing (C) is a social engineering attack to steal credentials, and pharming (D) manipulates DNS records to redirect users to malicious sites, neither of which directly involves connection request overload. The description of a device receiving too many connection requests specifically indicates a volume-based attack like the SYN flood.

Authoritative Links:

Cisco - SYN Flood Attack:https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23610-syn-

flood.html
Cloudflare - What is a SYN Flood Attack?:https://www.cloudflare.com/learning/ddos/syn-flood-attack/
Imperva - SYN Flood Attack:https://www.imperva.com/learn/ddos/syn-flood-attack/

Question: 24

Which two preventive measures are used to control cross-site scripting? (Choose two.)

A.Enable client-side scripts on a per-domain basis.
B.Incorporate contextual output encoding/escaping.
C.Disable cookie inspection in the HTML inspection engine.
D.Run untrusted HTML input through an HTML sanitization engine.
E.SameSite cookie attribute should not be used.

Answer: BD

Explanation:

Here's a detailed justification for why options B and D are the correct preventive measures against Cross-Site Scripting (XSS) attacks, while A, C, and E are not:

Justification:

Cross-Site Scripting (XSS) attacks occur when malicious scripts are injected into websites viewed by other users. Effective prevention involves handling user-supplied data carefully to prevent this injection.

Option B: Incorporate contextual output encoding/escaping. This is a crucial defense. When user input is displayed on a webpage, it should be encoded or "escaped" based on its context. For instance, if user input is placed inside an HTML tag, characters like < and > should be converted to their HTML entities (< and >, respectively). This prevents the browser from interpreting the input as code and rendering it, instead displaying it as plain text. This ensures that any attempted malicious script becomes inert data, thus preventing the execution of XSS payloads.

Option D: Run untrusted HTML input through an HTML sanitization engine. This involves filtering potentially dangerous elements and attributes from user-provided HTML. Sanitization ensures that user-submitted HTML doesn't contain scripts or other malicious constructs. A sanitization engine parses the input and removes or modifies any elements or attributes that could be used for XSS attacks, such as <script>, onclick, and onload. This process effectively limits the potential for execution of arbitrary JavaScript code.

Why other options are incorrect:

Option A: Enable client-side scripts on a per-domain basis. While controlling client-side scripting is important for overall security, this does not directly prevent XSS attacks. XSS occurs through vulnerabilities in web applications, not because client-side scripts are enabled. This option would not prevent the injection of a malicious script.

Option C: Disable cookie inspection in the HTML inspection engine. Cookie inspection is used for other security purposes, such as preventing cookie manipulation attacks; disabling it does not address XSS vulnerabilities. Furthermore, HTML inspection does not contribute to XSS attacks.

Option E: SameSite cookie attribute should not be used. The SameSite attribute is a security measure that helps to prevent CSRF (Cross-Site Request Forgery) attacks by controlling cookie behavior in cross-site contexts. However, it's not directly related to XSS prevention.

In Summary: The correct solutions, B and D, both focus on sanitizing and encoding user input before it's displayed on the page. These approaches make it extremely difficult for malicious scripts to get interpreted

as code by the user's web browser.

Authoritative Links:

OWASP Cross-site Scripting (XSS):https://owasp.org/www-project-top-ten/ This page provides a general overview of XSS, its impact and prevention.

OWASP XSS (Cross Site Scripting) Prevention Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html This resource delves into techniques for escaping and sanitizing user inputs.

Mozilla Web security: Cross-site scripting (XSS):https://developer.mozilla.org/en-US/docs/Web/Security/Types_of_attacks#cross-site_scripting_xss This details the nature of XSS attacks and how they are caused.

Question: 25

Which threat involves software being used to gain unauthorized access to a computer system?

A.ping of death
B.HTTP flood
C.NTP amplification
D.virus

Answer: D

Explanation:

The correct answer is **D. virus**. A virus is a type of malicious software (malware) specifically designed to replicate itself and spread from one computer to another. Viruses typically attach themselves to legitimate files or programs, and when those files or programs are executed, the virus activates and can perform various malicious actions, including granting unauthorized access to the system. This unauthorized access can enable attackers to steal data, control the system remotely, or perform other harmful activities. Options A, B, and C are all types of denial-of-service (DoS) attacks, where the aim is to disrupt service availability rather than directly gaining unauthorized access to a computer system. A "ping of death" (A) exploits the ping utility, an HTTP flood (B) overwhelms a web server with HTTP requests, and NTP amplification (C) exploits the Network Time Protocol to generate a large volume of traffic. These attacks can indirectly cause harm by crippling system functionality, but they do not constitute the act of software directly enabling unauthorized access in the way a virus does. For further information on viruses and malware, consider exploring resources from organizations like the National Institute of Standards and Technology (NIST): https://csrc.nist.gov/glossary/term/virus or Cisco itself: https://www.cisco.com/c/en/us/products/security/index.html.

Question: 26

Which two capabilities does TAXII support? (Choose two.)

A.exchange
B.pull messaging
C.binding
D.correlation
E.mitigating

Answer: AB

Explanation:

TAXII (Trusted Automated eXchange of Indicator Information) is a protocol designed for the standardized exchange of cyber threat intelligence. Its core functionalities revolve around enabling the sharing and retrieval of threat data. Option A, "exchange," is a fundamental aspect of TAXII. The protocol facilitates the sharing of threat information between different entities, enabling organizations to collaborate and enhance their security posture through collective knowledge. Option B, "pull messaging," aligns with TAXII's mechanism for data retrieval. Clients can 'pull' or request specific threat intelligence from servers or repositories according to their needs. This pull-based approach allows for controlled access to information, ensures that clients receive only relevant data, and reduces unnecessary data transfers.

Options C, "binding," "correlation," and E, "mitigating," are not primary capabilities of TAXII. Binding, in networking, typically refers to associating network addresses or ports, which TAXII does not focus on. Correlation involves identifying relationships between data points, while mitigating involves actions to reduce risk; these are often subsequent processes performed with the data received through TAXII rather than being inherent features of the protocol itself. Therefore, while threat information gained from TAXII might be used for correlation or mitigation, those actions aren't within TAXII's scope. TAXII's core purpose is to facilitate the standardized exchange of threat intelligence, not to provide functionality for correlation or mitigation.

For further research, consider the following authoritative resources:

OASIS Open:https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=taxii (The official TAXII specification and resources)
MITRE ATT&CK:https://attack.mitre.org/ (Often used in conjunction with TAXII for threat intelligence sharing)
The TAXII Project:https://taxiiproject.github.io/ (Community driven project documentation and implementations of TAXII)

Question: 27

Which two conditions are prerequisites for stateful failover for IPsec? (Choose two.)

A.Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically.

B.The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.

C.The IPsec configuration that is set up on the active device must be duplicated on the standby device.

D.Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically.

E.The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device.

Answer: CE

Explanation:

The correct answer, CE, highlights two crucial prerequisites for achieving stateful failover in IPsec environments using Cisco devices. Stateful failover ensures that active IPsec connections are maintained when a device failure occurs, minimizing disruption. Option C is correct because consistent IPsec configurations, including transform sets, access lists, and crypto maps, must be present on both the active and standby devices. These identical configurations allow the standby to seamlessly take over the IPsec tunnels without re-negotiation. Option E is also correct because running the same Cisco IOS version and device type is essential for compatibility and reliable state synchronization. This ensures that both devices

can understand and process IPsec configurations, state information, and control messages consistently. Inconsistent versions or device types can lead to failed failovers due to discrepancies in software behavior.

Option A is incorrect because both IKE and IPsec configurations require manual synchronization. Option D is incorrect because IKE configurations, like pre-shared keys, policies, and certificates, must be duplicated.

Option B is incorrect because version consistency is a key prerequisite for successful stateful failover. Therefore, C and E are the only correct options.

For further research, consult the official Cisco documentation on IPsec high availability and stateful failover features:

Cisco IPsec VPN with High Availability:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpn/configuration/15-sy/sec-ipsec-vpn-15-sy-book/ipsec-ha.html
Cisco ASA High Availability:https://www.cisco.com/c/en/us/td/docs/security/asa/asa912/configuration/asa-912-config-guide/ha-stateful-failover.html

Question: 28

Which algorithm provides encryption and authentication for data plane communication?

A.AES-GCM
B.SHA-96
C.AES-256
D.SHA-384

Answer: A

Explanation:

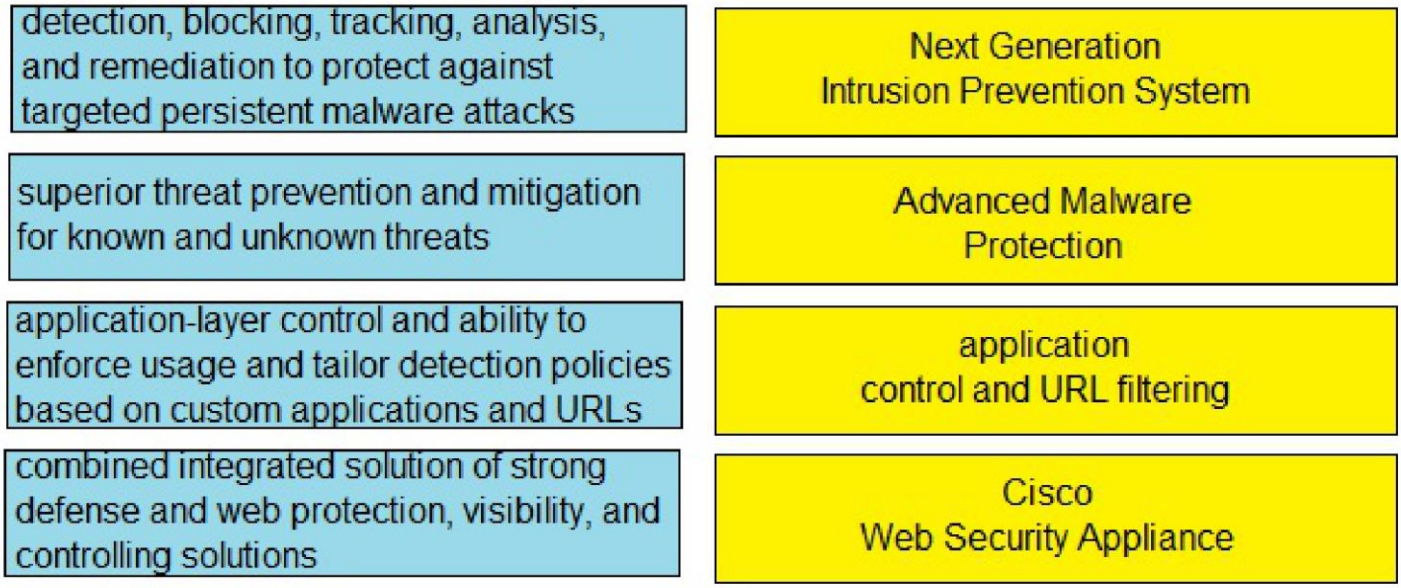
The correct answer is A, AES-GCM, because it's an authenticated encryption algorithm that provides both confidentiality (encryption) and integrity/authentication of data. AES (Advanced Encryption Standard) is a symmetric block cipher widely used for encryption. GCM (Galois/Counter Mode) is a mode of operation for block ciphers that adds authentication. This combination ensures that data is not only encrypted but also verifiable, meaning if the data is tampered with, it's detectable. Options B, SHA-96 and D, SHA-384, are cryptographic hash functions. They provide data integrity by producing a unique fingerprint of data but don't offer encryption. Option C, AES-256, is a strong encryption algorithm but, by itself, does not provide authentication; a separate mechanism is needed for that. In data plane communication, securing the payload requires a method that both encrypts and ensures integrity. AES-GCM accomplishes this efficiently, making it a preferred choice for securing network traffic, particularly in virtual private networks (VPNs), and protocols like IPSec, TLS, and SSH. It's commonly implemented in hardware and software for high throughput, low latency secure data transfer, vital for performance and security in cloud environments. Using only an encryption algorithm like AES-256, without authentication, can leave systems vulnerable to attacks like man-in-the-middle attacks. Hence, AES-GCM's authenticated encryption is necessary for secure data plane communication.

Further Reading:

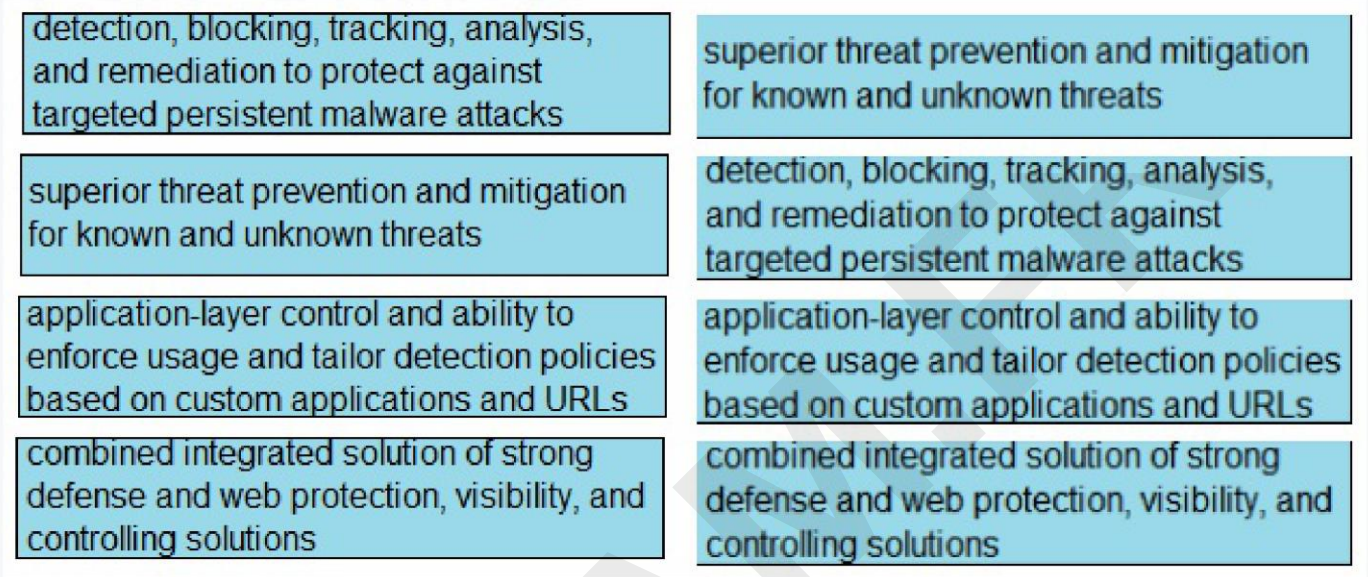
NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf **RFC 5288:** AES Galois Counter Mode (GCM) Cipher Suites for TLS: https://www.rfc-editor.org/rfc/rfc5288 **Cloud Security Alliance:** Understanding Data Encryption:
https://cloudsecurityalliance.org/blog/understanding-data-encryption/

Question: 29

DRAG DROP -
Drag and drop the capabilities from the left onto the correct technologies on the right.
Select and Place:



Answer:



Explanation:

Key word: prevention = Next generation intrusion prevention systemProtect = Advanced Malware ProtectionApplication Layer = Application control and URL filteringCombined integrated = Cisco web security Appliance

Question: 30

Which two key and block sizes are valid for AES? (Choose two.)

A.64-bit block size, 112-bit key length
B.64-bit block size, 168-bit key length
C.128-bit block size, 192-bit key length
D.128-bit block size, 256-bit key length

E.192-bit block size, 256-bit key length

Answer: CD

Explanation:

AES (Advanced Encryption Standard) is a symmetric block cipher, meaning it uses the same key for both encryption and decryption. A fundamental aspect of AES is its block size and key length. AES operates on a fixed block size of 128 bits (16 bytes). This means it encrypts data in 128-bit chunks. Options that refer to a 64-bit or 192-bit block size are, therefore, incorrect. AES supports three key lengths: 128, 192, and 256 bits. Key length impacts the security level of the encryption, with longer keys generally offering better protection against brute-force attacks. Thus, options C and D are valid AES configurations. Option A and B mention 64 bit blocks which are invalid for AES. Option E mentions a 192-bit block size, which is also invalid. The correct options are C: a 128-bit block size and 192-bit key length, and D: a 128-bit block size and 256-bit key length.

Here are some authoritative links for further research:

1. **NIST (National Institute of Standards and Technology) - FIPS 197:** This is the official document standardizing AES. It provides all the technical details of the algorithm.
   https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
2. **Wikipedia - Advanced Encryption Standard:** A comprehensive overview of AES, including its history, operation, and security aspects. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard 3. **Cloudflare - What is AES Encryption?** - Provides a practical explanation of AES and its common usage.
https://www.cloudflare.com/learning/ssl/what-is-aes-encryption/

Question: 31

Which two descriptions of AES encryption are true? (Choose two.)

A.AES is less secure than 3DES.
B.AES is more secure than 3DES.
C.AES can use a 168-bit key for encryption.
D.AES can use a 256-bit key for encryption.
E.AES encrypts and decrypts a key three times in sequence.

Answer: BD

Explanation:

Here's a detailed justification for why options B and D are the correct descriptions of AES encryption:

Justification:

AES (Advanced Encryption Standard) is a symmetric-key block cipher widely adopted for its robust security and efficiency. It replaced the older DES (Data Encryption Standard) and 3DES (Triple DES) due to vulnerabilities identified in them. Option B is correct because AES is indeed considered more secure than 3DES. 3DES is essentially DES applied three times, which, while an improvement over the original DES, is still weaker than AES because it has a smaller key size and is more susceptible to cryptanalysis.

Option D is also correct because AES can use key lengths of 128, 192, or 256 bits. The 256-bit key option, specifically, provides a significantly higher level of security than smaller key sizes, as it makes brute-force attacks computationally infeasible even with current technology. Option A is incorrect; AES is not less secure than 3DES, rather it's a more advanced and robust algorithm. Option C is incorrect as AES does not use a 168-bit key. The 168-bit key size is associated with 3DES, not AES. Lastly, Option E is incorrect as AES does not

involve encrypting and decrypting a key multiple times; it encrypts and decrypts data using a single key. AES operates on fixed-size blocks of data, processing them in rounds based on the chosen key size.

In summary, AES's security strength is primarily derived from its use of larger key sizes and sophisticated mathematical operations. These factors contribute to its overall effectiveness against various types of attacks, making it the preferred choice for encryption in most applications.

Authoritative Links:

1. **NIST (National Institute of Standards and Technology) - FIPS 197, Advanced Encryption Standard (AES):** This is the official standard document defining the AES algorithm. It provides detailed information about the algorithm's structure, key sizes, and operational modes: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
2. **Cloudflare Learning Center - AES Encryption:** A clear explanation of AES and its use cases in cloud security: https://www.cloudflare.com/learning/ssl/what-is-aes-encryption/
3. **Wikipedia - Advanced Encryption Standard:** A good overview of AES with explanations of its history and design principles: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Question: 32

What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?

A. STIX
B. XMPP
C. pxGrid
D. SMTP

Answer: A

Explanation:

The correct answer is **A. STIX (Structured Threat Information Expression)**. STIX is a standardized language and serialization format specifically designed for representing and exchanging cyber threat intelligence. It provides a structured way to describe various aspects of a threat, such as malicious actors, attack patterns, malware, and indicators of compromise (IOCs). This structured approach allows for automated sharing and processing of threat information, enabling better situational awareness and response capabilities. The TAXII (Trusted Automated Exchange of Indicator Information) protocol, on the other hand, is a transport mechanism that defines how threat intelligence, often formatted in STIX, can be securely transmitted between systems.

While the other options have their uses, they are not the correct answer. XMPP (Extensible Messaging and Presence Protocol) is a communication protocol primarily used for instant messaging and presence information, not for threat intelligence exchange. pxGrid is a Cisco platform used for context sharing and policy enforcement within a Cisco security ecosystem. SMTP (Simple Mail Transfer Protocol) is used for email transmission and not threat intelligence. Therefore, only STIX aligns with the described purpose of
exchanging threat intelligence through TAXII.

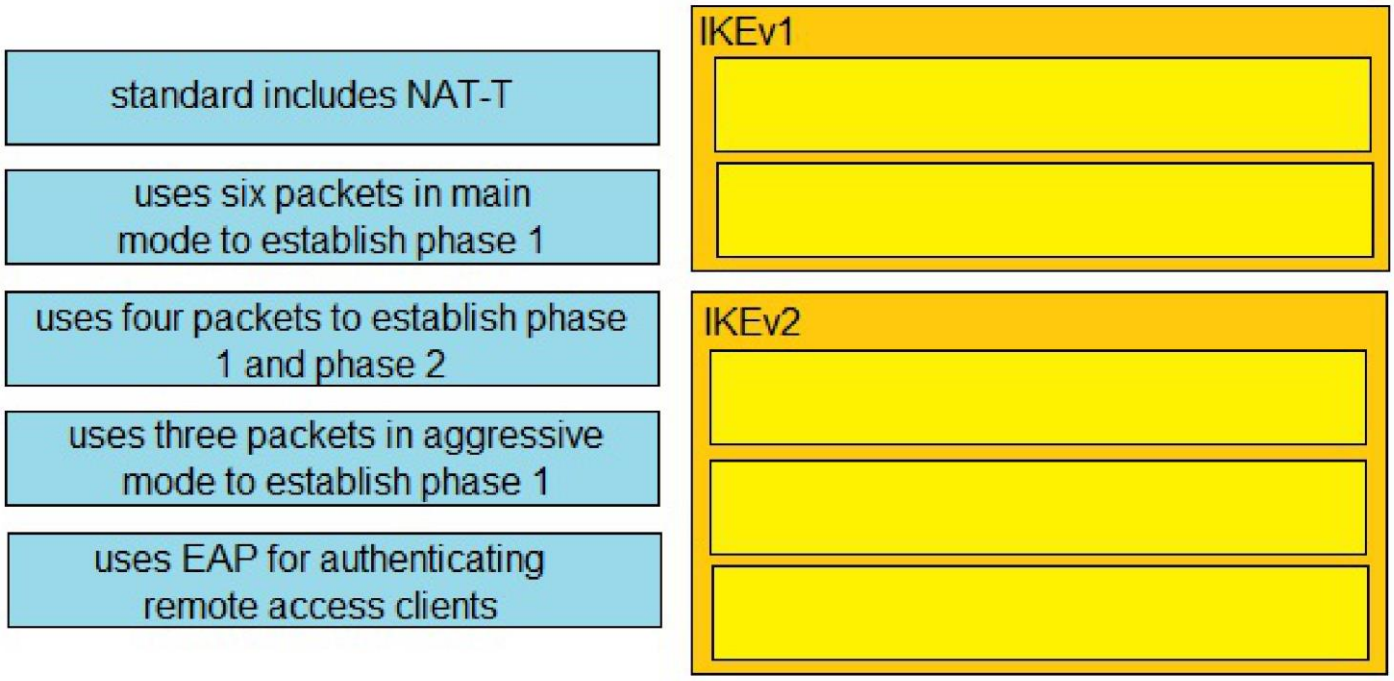
Here are authoritative links for further research:

OASIS STIX Standard:https://oasis-open.github.io/cti-documentation/ - Official documentation and specifications for STIX.
OASIS TAXII Standard:https://oasis-open.github.io/cti-documentation/taxii/ - Official documentation and specifications for TAXII.
CISA STIX/TAXII Informationhttps://www.cisa.gov/resources-tools/resources/stix-and-taxii - U.S.

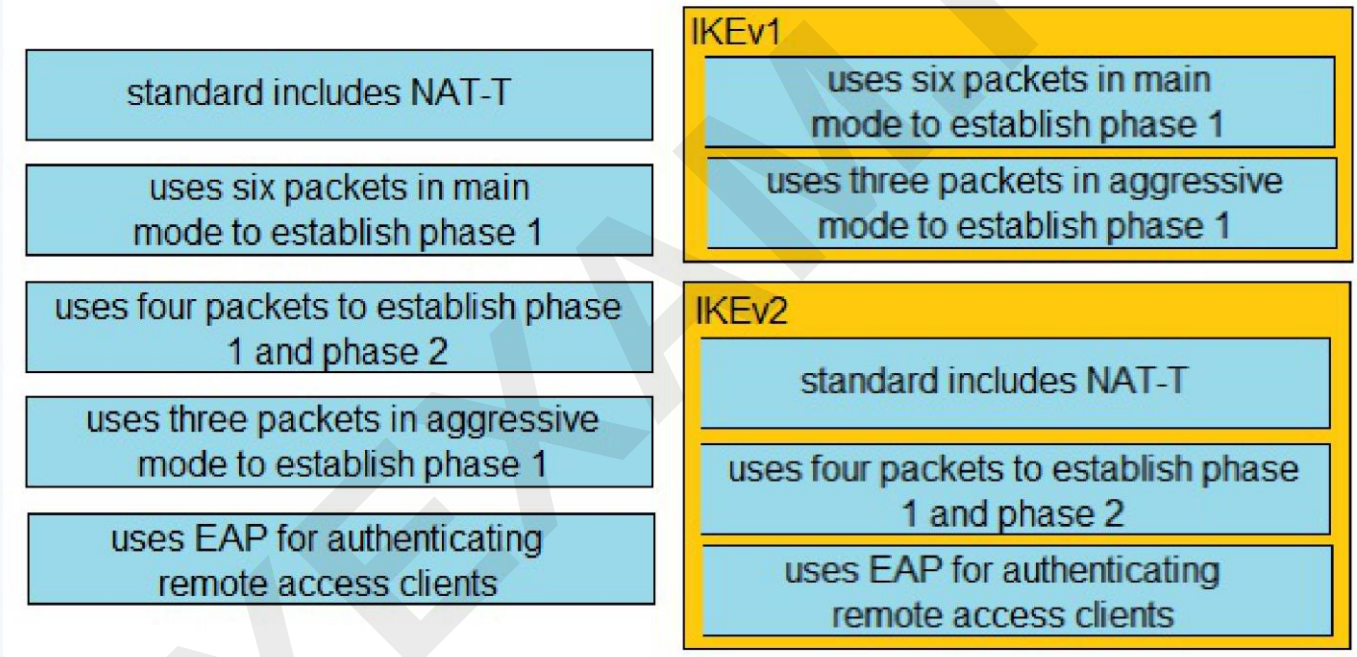
Cybersecurity and Infrastructure Security Agency (CISA) provides information about STIX and TAXII.

Question: 33

DRAG DROP -
Drag and drop the descriptions from the left onto the correct protocol versions on the right.
Select and Place:



Answer:



Question: 34

Which VPN technology can support a multivendor environment and secure traffic between sites?

A.SSL VPN
B.GET VPN
C.FlexVPN
D.DMVPN

Answer: C

Explanation:

The correct answer is C, FlexVPN. Here's why:

FlexVPN is designed as a highly versatile VPN solution, supporting a wide range of platforms and vendor interoperability. It's built around the IKEv2 protocol, a modern standard that allows for strong encryption and flexible authentication, facilitating secure connections between diverse network devices. This makes FlexVPN ideal for securing traffic between sites with different vendors, unlike options like GET VPN which is Cisco proprietary, or DMVPN which relies heavily on Cisco's technology. SSL VPNs are primarily used for remote access and client-to-site connections, not typically for site-to-site secure communications in a diverse environment. FlexVPN's hub-and-spoke, point-to-point, or full-mesh topologies provide flexible network configurations suitable for different network needs. FlexVPN also allows you to dynamically establish tunnels, reducing management overhead and improves network scalability. For an in-depth look at FlexVPN and its capabilities, Cisco's official documentation offers a comprehensive overview:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpn/configuration/15-sy/sec-flex-vpn-15-sy-book.htmlhttps://www.cisco.com/c/en/us/products/security/flexvpn/index.html

Question: 35

Which technology must be used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

A. DMVPN
B. FlexVPN
C. IPsec DVTI
D. GET VPN

Answer: D

Explanation:

The correct answer is **D. GET VPN (Group Encrypted Transport VPN)**. Here's why:

GET VPN is specifically designed for establishing secure, scalable, and any-to-any VPN connectivity over a private IP cloud (like an MPLS network). Its key advantage is that it leverages a single security association (SA) for all branches within a group. This eliminates the need for individual tunnel configurations between each branch, significantly reducing complexity and management overhead, especially in large networks. Unlike DMVPN or FlexVPN, which create individual tunnels and scale based on dynamic routing, GET VPN allows multiple sites to connect to a single centralized device or a group of devices using a singular SA, enabling efficient multicast communication where needed within the group.

DMVPN (Dynamic Multipoint VPN) is effective for hub-and-spoke topologies with dynamic IP addressing, establishing direct tunnels between spokes only when needed, not providing a group-based, any-to-any solution. FlexVPN is also versatile, supporting hub-and-spoke and point-to-point but not natively designed for the same scale or group-based nature as GET VPN. IPsec DVTI (Dynamic Virtual Tunnel Interface) provides

dynamically created interfaces for point-to-point IPSec tunnels and does not scale well in any-to-any scenarios with numerous branches. GET VPN utilizes group keys, which are distributed to each member of the VPN group and do not require a pairwise SA setup between members, thus simplifying the configuration and scalability.

Therefore, GET VPN perfectly fits the requirements of this scenario, offering secure, any-to-any connectivity over a private IP cloud while being scalable, efficient, and easier to manage compared to other VPN alternatives.

Authoritative Links for Further Research:

1. **Cisco - GET VPN Deployment Guide**: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Oct2015/CVD-GETVPN-Oct2015.html 2. **Cisco - Group Encrypted Transport VPN (GET VPN)**: https://www.cisco.com/c/en/us/products/security/group-encrypted-transport-vpn-get-vpn/index.html
3. **Cisco - Comparing VPN Technologies (GET VPN vs DMVPN vs FlexVPN)**: (Look for articles or documents comparing the technologies in a Cisco context)

Question: 36

What is a commonality between DMVPN and FlexVPN technologies?

A.FlexVPN and DMVPN use the new key management protocol, IKEv2
B.FlexVPN and DMVPN use IS-IS routing protocol to communicate with spokes
C.IOS routers run the same NHRP code for DMVPN and FlexVPN
D.FlexVPN and DMVPN use the same hashing algorithms

Answer: C

Explanation:

The correct answer is **C: IOS routers run the same NHRP code for DMVPN and FlexVPN**.

Here's the justification: Both DMVPN (Dynamic Multipoint VPN) and FlexVPN, while distinct in their capabilities and configurations, rely on the Next Hop Resolution Protocol (NHRP) for dynamic tunnel endpoint discovery and mapping in Cisco IOS routers. NHRP is fundamental to enabling the "hub-and-spoke" dynamic VPN topology. It allows spokes to dynamically learn the public IP addresses of other spokes or the hub, facilitating direct communication once a tunnel is established. This commonality in using the same NHRP code is a crucial similarity between the two.

Options A, B, and D are incorrect. FlexVPN uses IKEv2 (Internet Key Exchange version 2) extensively, while DMVPN traditionally used IKEv1. Option B is incorrect as DMVPN primarily uses EIGRP (Enhanced Interior Gateway Routing Protocol) or OSPF (Open Shortest Path First) for routing, and while FlexVPN might use IS-IS (Intermediate System to Intermediate System), it's not a default or required configuration. Lastly, option D is incorrect, as both technologies can use various hashing algorithms and the choice depends on the cryptographic policies applied, not a pre-defined common set. Thus, the shared dependency on the underlying NHRP implementation is the defining similarity between DMVPN and FlexVPN in this context.

Authoritative Links:

Cisco Documentation on NHRP:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-i.html#GUID-15E53899-96D5-4490-8737-11B5448C1109
Cisco Documentation on DMVPN:https://www.cisco.com/c/en/us/solutions/enterprise/design-

zone/security/dmvpn-design.html
Cisco Documentation on FlexVPN:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_vpn/configuration/15-s/sec-flexvpn-15-s-book/sec-flexvpn-intro.html

Question: 37

Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?

A.DTLSv1
B.TLSv1
C.TLSv1.1
D.TLSv1.2

Answer: A

Explanation:

The correct answer is A, DTLSv1 (Datagram Transport Layer Security version 1). While both DTLS and TLS are cryptographic protocols used for secure communication, DTLS is specifically designed for datagram-oriented protocols like UDP, which is crucial for VPN performance. DTLS offers advantages over TLS, particularly in high-latency or lossy network environments commonly encountered in internet-based VPN connections. TLS, designed for reliable, ordered byte streams of TCP, introduces overhead with its handshake processes and retransmission mechanisms, which can be detrimental to VPN throughput. DTLS, on the other hand, allows for parallel packet processing, reducing latency and improving overall speed. DTLS's lack of strict ordering also means that a lost packet won't halt the entire flow, contributing to greater resilience. Cisco AnyConnect leverages DTLS to provide a more responsive experience over VPN. Using DTLS over UDP enables a quicker data transfer because it eliminates the TCP three-way handshake and congestion avoidance algorithms, resulting in faster VPN throughput when compared to a TLS-based VPN tunnel. Cisco recommends DTLS for situations where latency and performance are paramount when using AnyConnect. In summary, DTLS's design tailored for datagrams combined with its resilience and lower latency yields superior throughput in Cisco AnyConnect VPN connections compared to TLS.

For further research:

Cisco's Documentation on AnyConnect DTLS:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa912/configuration/general/asa-912-general-config/vpn-anyconnect.html
RFC 6347 - Datagram Transport Layer Security Version 1.2:https://datatracker.ietf.org/doc/html/rfc6347
Comparison of TLS vs. DTLS:https://www.cloudflare.com/learning/ssl/what-is-dtls/

Question: 38

Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats?

A. Talos
B. PSIRT
C. SCIRT
D. DEVNET

Answer: A

Explanation:

The correct answer is A, Talos. Cisco Talos is Cisco's threat intelligence and research organization. Talos employs a vast team of security experts who actively monitor and analyze the global threat landscape. A core function of Talos is disseminating crucial security information to the wider cybersecurity community. This dissemination often occurs through various channels, a key one being a weekly newsletter. This newsletter, produced by Talos, offers updates on the latest threats, vulnerabilities, and attack campaigns, enabling cybersecurity professionals to remain well-informed. PSIRT (Product Security Incident Response Team) focuses on responding to security vulnerabilities within Cisco products. SCIRT (Security Cisco Incident Response Team) handles incident response within Cisco. DEVNET is a Cisco developer program. While these teams play vital roles, they don't produce a publicly available weekly threat newsletter like Talos. Talos's mission revolves around threat research and intelligence sharing, which directly aligns with publishing such a newsletter. Hence, Talos is the sole group within Cisco fitting this description.

Authoritative Links:

Cisco Talos:https://www.talosintelligence.com/ - This is the main website for Cisco Talos, where you can find information about their research, threat intelligence, and the weekly newsletter.
Cisco PSIRT:https://www.cisco.com/c/en/us/about/security-center/psirt.html - Information about Cisco's Product Security Incident Response Team.
Cisco DevNet:https://developer.cisco.com/ - Information about Cisco's developer program.

Question: 39

When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, which name is used?

A.Common Vulnerabilities, Exploits and Threats
B.Common Vulnerabilities and Exposures
C.Common Exploits and Vulnerabilities
D.Common Security Exploits

Answer: B

Explanation:

The correct answer is **B. Common Vulnerabilities and Exposures (CVE)**. CVE is a standardized, publicly accessible dictionary of known security vulnerabilities and exposures. It provides a unique identifier for each vulnerability, allowing security professionals, software vendors, and users to readily identify and address specific threats. Cisco, like other industry leaders, utilizes CVEs when communicating security findings. This ensures clarity and consistency in vulnerability reporting and management. Using a common identifier simplifies patching processes, security audits, and incident response across diverse systems and
organizations. A standardized catalog like CVE facilitates efficient sharing of security intelligence, allowing for better proactive defenses. Options A, C and D are not industry standards; they either mix terms or lack wide adoption. CVE is maintained by the MITRE Corporation and is a widely recognized component of vulnerability management frameworks globally. The CVE system enables consistent communication about vulnerabilities, and enables users to quickly identify solutions and patches from vendors.

Authoritative Links:

MITRE CVE Website:https://cve.mitre.org/
NIST National Vulnerability Database (NVD):https://nvd.nist.gov/ (The NVD uses the CVE identifiers as a key part of their database).

Question: 40

Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two.)

A.accounting
B.assurance
C.automation
D.authentication
E.encryption

Answer: BC

Explanation:

The correct answer identifies **B. assurance** and **C. automation** as key features of Cisco DNA Center that are integral to a Software Defined Network (SDN) solution. SDNs centralize network control and management, shifting away from traditional device-centric configurations. Cisco DNA Center, acting as the SDN controller, heavily leverages both assurance and automation to achieve this.

Automation in Cisco DNA Center streamlines network tasks such as device onboarding, configuration deployment, and policy enforcement. Instead of manually configuring individual network devices,
administrators define network behavior through a centralized policy interface. DNA Center then automatically pushes those configurations to the managed devices, significantly reducing manual effort and potential human error. This concept aligns with the core tenets of SDN, promoting efficiency and agility.

Assurance, on the other hand, focuses on proactively monitoring and ensuring the network's health and performance. Cisco DNA Center gathers telemetry data from the network infrastructure and analyzes it to identify performance bottlenecks, security threats, and other potential issues. This insight allows for proactive troubleshooting and optimization, ensuring a stable and reliable network experience. Assurance capabilities are vital in SDN environments where dynamic network changes need real-time validation. Both automation and assurance features contribute to the operational efficiency and agility that are core benefits of SDN.

Options A (accounting), D (authentication), and E (encryption), while important security aspects, are not features that are central to the core functionality of DNA Center within the context of SDN, rather they are important aspects that are leveraged by DNA Center for an overall solution. Accounting is important for record-keeping, authentication validates user identity, and encryption safeguards data transmission. While these are crucial for overall network security, they are not the defining features of how DNA Center facilitates SDN management.

Authoritative Links:

Cisco DNA Center Overview:https://www.cisco.com/c/en/us/solutions/enterprise-networks/dna-center/index.html
Software Defined Networking (SDN) Concepts:https://www.sdxcentral.com/networking/software-defined-networking-sdn/definitions/software-defined-networking-sdn/

Question: 41

What provides the ability to program and monitor networks from somewhere other than the DNAC GUI?

A.ASDM
B.NetFlow
C.API

D.desktop client

Answer: C

Explanation:

The correct answer is **C. API**. APIs (Application Programming Interfaces) serve as the fundamental mechanism for interacting with network devices and systems programmatically, bypassing the need for direct GUI access.

In the context of Cisco DNAC (Digital Network Architecture Center), APIs enable external applications, scripts, and automation tools to communicate and control the network infrastructure. This capability is crucial for integrating DNAC functionalities with other management platforms, orchestrating complex workflows, and building custom solutions tailored to specific network requirements. While options like ASAD, Netflow, and desktop clients provide network information or management, they do not offer the same programmable access and control that APIs offer. ASDM is a device-specific GUI, Netflow is for flow monitoring, and a desktop client is just another method to access the DNAC GUI. APIs are designed for machine-to-machine interaction, whereas the alternatives typically rely on human intervention through a graphical interface.

Through API-driven automation, network operations can become more efficient, agile, and consistent, leveraging modern DevOps principles. Cisco's DNAC platform exposes its functionality through a RESTful API. Cisco DNAC API documentation provides extensive details on using the API for diverse network management tasks.

Question: 42

What is a function of 3DES in reference to cryptography?

A.It encrypts traffic.

B.It creates one-time use passwords.

C.It hashes files.

D.It generates private keys.

Answer: A

Explanation:

3DES (Triple DES) is a symmetric-key block cipher, meaning it uses the same key for encryption and decryption. Its primary function is to encrypt data, transforming plaintext into ciphertext, making it unreadable without the correct key. Option A correctly identifies this core purpose. The process involves applying the original DES algorithm three times to each data block, with either two or three distinct keys, significantly increasing its security compared to single DES. This makes 3DES suitable for securing sensitive data during transmission or storage. It's a core cryptographic operation for achieving confidentiality in communications or data management. Although other options might relate to security in general, they are not the specific function of 3DES. Option B describes one-time passwords or tokens, not related to the 3DES encryption process. Option C refers to hashing, which is a one-way function producing a fixed-size output, used for integrity verification, and distinct from encryption. Option D is about key generation, while 3DES operates using pre-existing secret keys, not generating new ones.

For further information, you can refer to:

1. **National Institute of Standards and Technology (NIST) Special Publication 800-57**: https://csrc.nist.gov/publications/detail/sp/800-57/rev-5/final (Look for sections on symmetric encryption algorithms.)
2. **Wikipedia article on Triple DES**: https://en.wikipedia.org/wiki/Triple_DES
3. **Cisco's documentation on encryption**: Search Cisco's official website for their documentation on

encryption and specific technologies they support that utilize 3DES.

Question: 43

Which two activities can be done using Cisco DNA Center? (Choose two.)

A.DHCP
B.design
C.accounting
D.DNS
E.provision

Answer: BE

Explanation:

Cisco DNA Center is a network management and automation platform, primarily focused on simplifying and optimizing network operations. Its core functions revolve around intent-based networking, which includes designing, deploying, and managing networks based on business requirements.

Option B, 'design,' is a fundamental capability of Cisco DNA Center. It allows administrators to model and plan network infrastructure, defining network topologies, device roles, and policies before any physical deployment. This design phase is crucial for building a network that aligns with specific organizational needs.

Option E, 'provision,' accurately reflects another key function of Cisco DNA Center. Once a design is in place, the platform automates the configuration and deployment of network devices. This includes pushing configurations, setting up VLANs, and establishing access policies, all from a centralized interface. The automation capabilities significantly reduce manual effort and the potential for human error.

Options A, C, and D are not core functions of Cisco DNA Center. DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name System) are services typically provided by dedicated servers or other network infrastructure components, while accounting, relating to network usage billing, falls outside of DNA Center's scope.

Therefore, the correct activities within Cisco DNA Center are network 'design' and 'provision'. These capabilities align with its role as a network management platform focused on intent-based networking.

Authoritative Links for further research:

1. Cisco DNA Center Overview: https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html
2. Cisco DNA Center Documentation: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/series.html

Question: 44

Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?

A.terminal
B.selfsigned
C.url

D.profile

Answer: D

Explanation:

The correct answer is D, **profile**, because it's the PKI enrollment method that offers a distinct separation between authentication and enrollment steps. This separation is crucial for enhanced security and flexibility. In a profile-based enrollment, the device first authenticates with the Certificate Authority (CA), possibly using existing credentials. Following authentication, a pre-defined profile that specifies enrollment parameters is applied. This profile contains configuration information including the CA server's URL, certificate types, and necessary cryptographic algorithms. Crucially, it can also specify HTTP or TFTP commands to download files like Root CA certificates or other required configuration files from a server, thereby automating the deployment of critical components. The terminal method (A) involves manual certificate requests, and while it allows some control, it doesn't offer a separation of authentication and enrollment like profiles do. Selfsigned (B) doesn't involve a CA at all and thus, no enrollment. The url method (C) usually refers to directly specifying a CA server's URL for simpler enrollments and lacks the comprehensive control and separation of concerns offered by profiles. Therefore, profile enrollment (D) is the only method that fulfills both specified
requirements in the question, supporting separated authentication and enrollment alongside file retrieval commands.

Authoritative Links:

Cisco Documentation on PKI Enrollment Methods:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/pki/configuration/15-sy/sec-pki-15-sy-book/sec-pki-enroll.html
Understanding Cisco PKI Concepts:https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/10958-pki-faq.html

Question: 45

Which type of API is being used when a security application notifies a controller within a software-defined network architecture about a specific security threat?

A.southbound API
B.westbound API
C.eastbound API
D.northbound API

Answer: D

Explanation:

The correct answer is **D. northbound API**. In a software-defined network (SDN) architecture, communication pathways between different layers are defined directionally. Southbound APIs facilitate communication between the SDN controller and the underlying network infrastructure (like switches and routers), handling device configurations and data collection. Conversely, northbound APIs enable communication between the SDN controller and higher-level applications or services, such as security applications, orchestration platforms, or business intelligence tools.

When a security application notifies the SDN controller about a security threat, this represents data flow from a higher-level application (the security application) to a lower-level control plane (the SDN controller). This interaction clearly falls under the domain of a northbound API. The security application utilizes this API to convey threat information, enabling the controller to respond by adjusting network policies or initiating mitigation actions. Westbound and Eastbound APIs typically relate to lateral communication within or

between similar layers of an architecture, not applicable in this context.

Therefore, the northbound API provides the necessary interface for security applications to communicate threat intelligence to the SDN controller for dynamic network security management.

Authoritative Links:

SDN Architecture & APIs:https://www.sdxcentral.com/resources/sdn/software-defined-networking-architecture/
Northbound vs Southbound API Explanation:https://www.networkcomputing.com/networking/sdn-apis-northbound-vs-southbound
SDN Security:https://www.vmware.com/topics/glossary/content/software-defined-networking-security

Question: 46

An organization has two machines hosting web applications. Machine 1 is vulnerable to SQL injection while machine 2 is vulnerable to buffer overflows. What action would allow the attacker to gain access to machine 1 but not machine 2?

A. sniffing the packets between the two hosts
B. sending continuous pings
C. overflowing the buffer's memory
D. inserting malicious commands into the database

Answer: D

Explanation:

The correct answer is **D. inserting malicious commands into the database.** This option exploits the specific vulnerability of Machine 1, which is SQL injection. SQL injection involves crafting malicious SQL queries that are then executed by the database server, potentially granting unauthorized access to data or even control of the server itself. This method directly targets the database interaction of Machine 1, not the operating system layer where a buffer overflow would be exploited. Machine 2's vulnerability to buffer overflows is irrelevant here. Option A, sniffing packets, would allow an attacker to observe traffic but not necessarily gain direct access to either machine's internal systems or data. Option B, sending continuous pings, is a basic network diagnostic tool and does not exploit vulnerabilities. Option C, overflowing a buffer, would target Machine 2, not Machine 1. The key difference lies in the specific attack targeting a specific vulnerability of an application on Machine 1 versus a vulnerability on Machine 2. SQL injection works by injecting malicious SQL code into input fields that are not sanitized to prevent attacks; this could, for example, involve a user login field.

Therefore, inserting malicious commands into the database via the SQL injection vulnerability on Machine 1 will allow the attacker access only to that machine and not the other machine vulnerable to a buffer overflow attack.

For further research:

OWASP SQL Injection:https://owasp.org/www-project-top-ten/ (Look for the SQL Injection section within the OWASP Top Ten)
Buffer Overflow:https://owasp.org/www-community/vulnerabilities/Buffer_Overflow

Question: 47

What is the function of SDN southbound API protocols?

A.to allow for the static configuration of control plane applications
B.to enable the controller to use REST
C.to enable the controller to make changes
D.to allow for the dynamic configuration of control plane applications

Answer: C

Explanation:

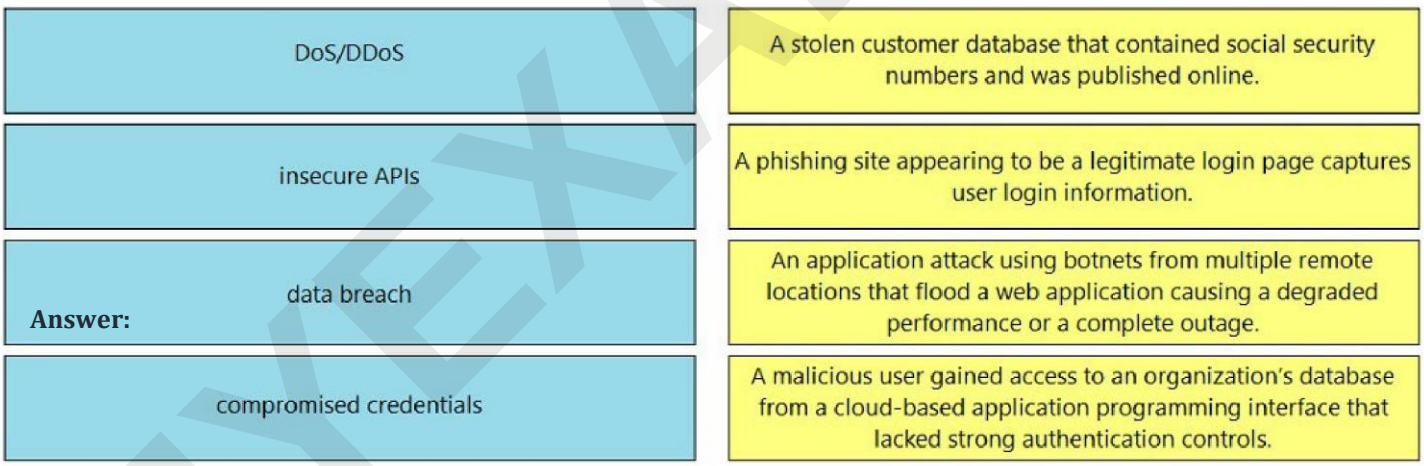
The correct answer is C, "to enable the controller to make changes." Southbound APIs in Software-Defined Networking (SDN) are the communication pathways between the SDN controller (the brain of the network) and the network devices (like switches and routers, the infrastructure). These APIs are not primarily for static configuration (A), which is less dynamic and would defeat the purpose of SDN's agility. While REST (B) can be used, it's a specific type of protocol and not the core function of all southbound APIs. Southbound APIs' fundamental purpose is to allow the controller to control the network by sending instructions to the data plane devices, encompassing actions like adding, modifying, or deleting flow rules. This is dynamic reconfiguration (D), and the primary activity is making changes to the network's behavior based on network requirements. Hence, "to enable the controller to make changes" most accurately describes the function of southbound API protocols in the context of SDN. These changes are essential for implementing network policies, enabling virtualization, and responding to dynamic traffic patterns. Without this capacity to push instructions down, the SDN controller would be just an observer.

For further research on SDN southbound APIs, refer to resources from these links:

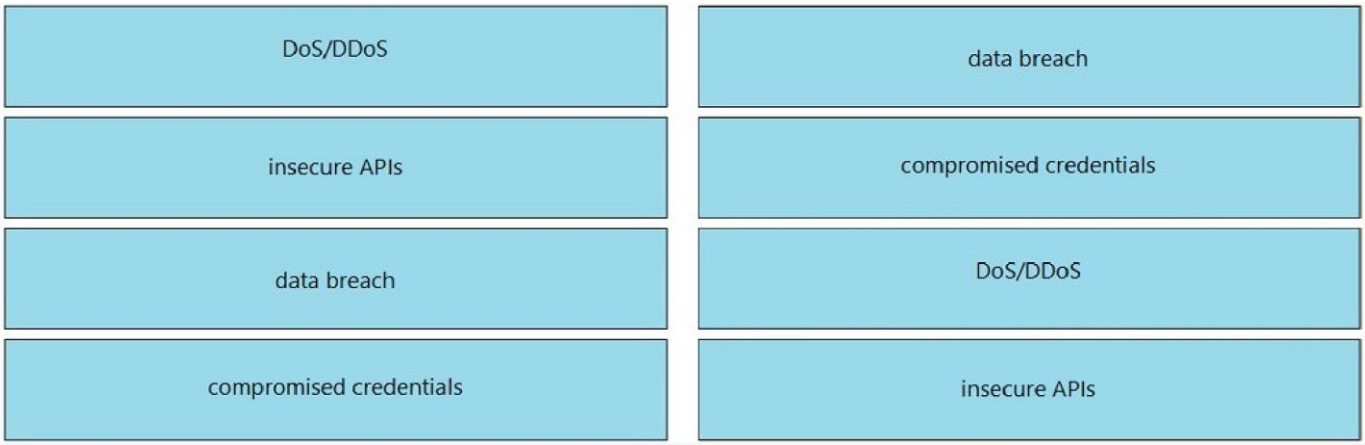
1. **Open Networking Foundation (ONF):**https://opennetworking.org/ (Focus on standards and general SDN architecture).
2. **Cisco DevNet:**https://developer.cisco.com/ (Resources on Cisco's approach to SDN and associated APIs)
3. **SDN Central:**https://www.sdncentral.com/ (A comprehensive site on SDN concepts and news). 4. **Cloud Native Computing Foundation (CNCF):**https://www.cncf.io/ (While broader than SDN, look for resources on network automation and orchestration).

Question: 48

DRAG DROP -
Drag and drop the threats from the left onto examples of that threat on the right.
Select and Place:



Answer:



Question: 49

What is the difference between Cross-site Scripting and SQL Injection attacks?

A.Cross-site Scripting is when executives in a corporation are attacked, whereas SQL Injection is when a database is manipulated.

B.Cross-site Scripting is an attack where code is executed from the server side, whereas SQL Injection is an attack where code is executed from the client side.

C.Cross-site Scripting is a brute force attack targeting remote sites, whereas SQL Injection is a social engineering attack.

D.Cross-site Scripting is an attack where code is injected into a database, whereas SQL Injection is an attack where code is injected into a browser.

Answer: B

Explanation:

The correct answer is **B**. Here's why:

Cross-Site Scripting (XSS) exploits vulnerabilities in web applications to inject malicious scripts into web pages viewed by other users. These scripts typically execute client-side, meaning they run within the user's web browser. An attacker doesn't directly target the server but instead targets user sessions by injecting client-side script that the victim's browser will interpret and execute. The malicious script can be used to steal cookies, redirect users to malicious sites, or deface the webpage.

SQL Injection is a different type of attack targeting the database backend of web applications. Attackers inject malicious SQL code into input fields of a web form. When the application executes this modified SQL query, it can expose sensitive data, modify database records, or even gain control of the server. It is a server-side vulnerability that an attacker abuses to alter the database. The attacker directly targets the application's interaction with the database.

Option A is incorrect because it conflates terms and provides a false premise. Cross-site scripting has nothing to do with executive attacks. Option C is incorrect because cross-site scripting is not a brute force attack, and SQL injection is not social engineering. Option D is incorrect because the injected code for cross-site scripting executes client-side (in the browser), and the injected code in SQL injection executes server-side (in the database).

Therefore, option B is correct as it accurately portrays the fundamental difference: XSS exploits client-side vulnerabilities, and SQL Injection exploits server-side vulnerabilities, typically in the database access logic.

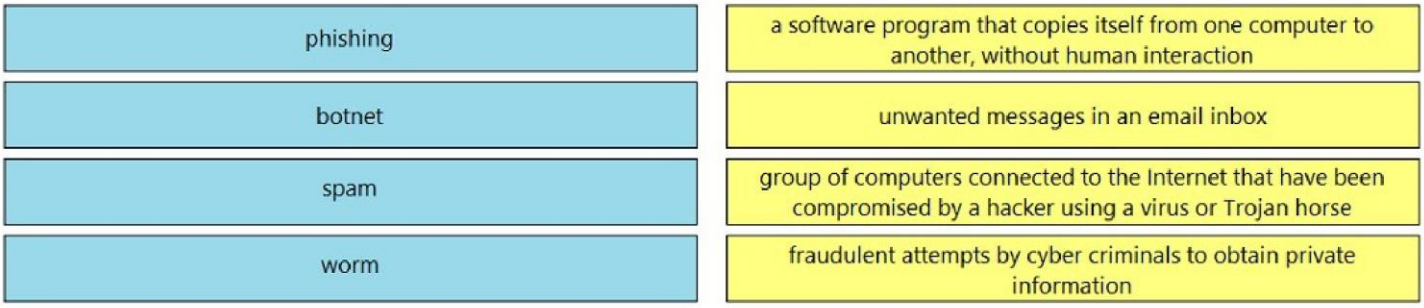
Authoritative Links for Further Research:

OWASP (Open Web Application Security Project) on XSS:https://owasp.org/www-project-top-ten/ (Search

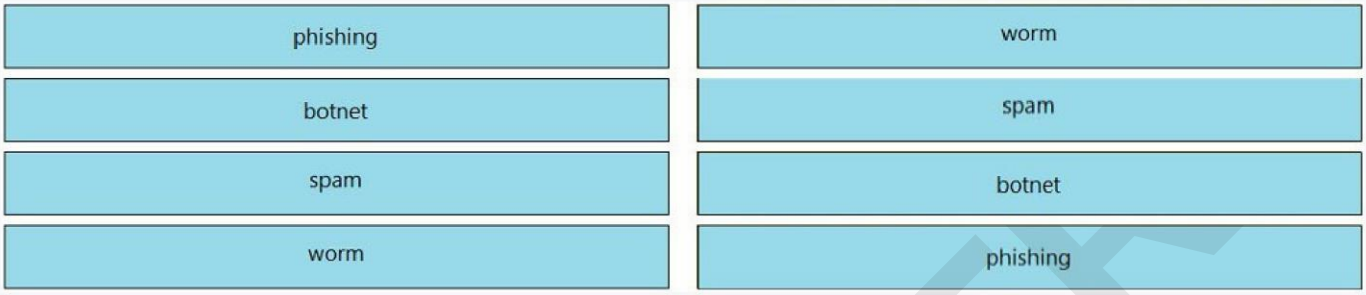
for XSS or Cross-site Scripting)
OWASP on SQL Injection:https://owasp.org/www-project-top-ten/ (Search for SQL Injection)
Cisco Security website:https://www.cisco.com/c/en/us/solutions/security.html (Search for specific security threats)

Question: 50

DRAG DROP -
Drag and drop the common security threats from the left onto the definitions on the right.
Select and Place:



Answer:



Question: 51

Which type of dashboard does Cisco DNA Center provide for complete control of the network?

A. distributed management
B. service management
C. application management
D. centralized management

Answer: D

Explanation:

Cisco DNA Center is designed to provide a centralized management platform for network infrastructure. This implies a single pane of glass through which administrators can control, monitor, and automate the network. Options A, B, and C do not align with this core functionality of Cisco DNA Center. A "distributed management" model suggests control dispersed across multiple locations, contrary to Cisco DNA Center's centralized approach. "Service management" and "application management," while important, are specific aspects managed within the broader centralized framework offered by Cisco DNA Center; they don't describe the overall control paradigm. The primary purpose of Cisco DNA Center is to provide a holistic view and single control point for the entire network, encompassing policy, provisioning, assurance, and analytics. This is realized through its single, overarching management console, aligning directly with the concept of
"centralized management." Therefore, option D is the most accurate and appropriate description of the type

of dashboard that Cisco DNA Center offers. Centralized management streamlines operations, reduces complexity, and enables greater consistency across the network.

Authoritative Links for Further Research:

1. **Cisco DNA Center Documentation:**https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html
2. **Cisco DNA Center Solution Overview:** https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/dna-center/solution-overview-c22-743767.pdf

Question: 52

```
import requests
url = https://api.amp.cisco.com/v1/computers
headers = {
    'accept': 'application/json',
    'Content-type': 'application/json',
    'authorization': "Basic <API Credentials",
    'cache-control': "no-cache",
    }
response = requests.request("GET", url, headers=headers)
print(response.text)
```

Refer to the exhibit. What will happen when this Python script is run?

A. The list of computers, policies, and connector statuses will be received from Cisco AMP.
B. The list of computers and their current vulnerabilities will be received from Cisco AMP.
C. The compromised computers and malware trajectories will be received from Cisco AMP.
D. The compromised computers and what compromised them will be received from Cisco AMP.

Answer: A

Explanation:

A https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.amp.cisco.com&api_resource=Computer&api_version=v1

Question: 53

```
import requests
clinet_id = '<Client ID>'
api_key = '<API Key>'
url = 'https://api.amp.cisco.com/v1/computers'
response = requests.get(url, auth=(client_id, api_key))
response_json = response.json()
for computer in response_json['data']:
    hostname = computer['hostname']
    print(hostname)
```

Refer to the exhibit. What will happen when the Python script is executed?

A. The hostname will be printed for the client in the client ID field.
B. The hostname will be translated to an IP address and printed.
C. The script will pull all computer hostnames and print them.
D. The script will translate the IP address to FQDN and print it.

Answer: C

Explanation:

The script will pull all computer hostnames and print them.

Question: 54

With which components does a southbound API within a software-defined network architecture communicate?

A. applications
B. controllers within the network
C. appliances
D. devices such as routers and switches

Answer: D

Explanation:

The correct answer is **D. devices such as routers and switches.** Southbound APIs in a Software-Defined Networking (SDN) architecture facilitate communication between the SDN controller and the underlying network infrastructure. These devices, like routers and switches, are the physical or virtual network elements that carry data traffic. The southbound API provides a standardized interface for the controller to instruct these devices on how to forward packets, manage their configurations, and report their operational status.

Essentially, the controller uses the southbound API to push policies and configurations to the devices, effectively controlling them centrally. Conversely, the devices use the southbound API to communicate telemetry and status information back to the controller. While applications (A) utilize northbound APIs to interact with the controller, and controllers (B) might communicate amongst themselves using other protocols, they don't directly interact with a southbound API. Appliances (C) is too broad a term; while some appliances may contain devices that the southbound API talks to, the term is not specific enough. Therefore, the devices themselves (D) are the specific entities that communicate through the southbound API with the

controller in an SDN environment.

For further information, consider researching these resources:

SDN and OpenFlow: Learn more about the fundamental architecture and protocols used in software-defined networking. https://www.sdxcentral.com/sdn/definitions/what-is-software-defined-networking-sdn/ **Southbound Interface in SDN:** Explore specific details about the functionality and purpose of southbound APIs. https://www.juniper.net/us/en/research-topics/software-defined-networking-explained.html **OpenFlow Protocol:** Understand a specific example of a widely used southbound protocol.
https://www.opennetworking.org/openflow/

Question: 55

Which method is used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources?

A. BYOD onboarding
B. MAC authentication bypass
C. client provisioning
D. Simple Certificate Enrollment Protocol

Answer: A

Explanation:

The correct answer is **A. BYOD onboarding**. Here's a detailed justification:

BYOD (Bring Your Own Device) onboarding is the process by which personal mobile devices are configured to access an organization's network securely. A crucial part of this process is the deployment of certificates.
These certificates serve as digital identities, verifying the device's legitimacy and enabling encrypted communication.

During BYOD onboarding, devices typically undergo a series of steps. These often involve downloading a profile or agent that automatically installs the required certificate. This process also configures the supplicant, which is the software component on the device responsible for network authentication. Specifically, the supplicant is configured with the appropriate network credentials and encryption protocols based on the installed certificate.

Methods like MAC authentication bypass (MAB), while useful in certain network access control scenarios, do not involve certificate-based authentication or automatic supplicant configuration. Instead, MAB relies on a device's MAC address for authorization, often bypassing more robust security measures. Client provisioning, while a broad term encompassing software deployment, often isn't focused on the specific certificate and supplicant requirements of BYOD. Simple Certificate Enrollment Protocol (SCEP) is a protocol for certificate enrollment, but it is just one part of the broader BYOD onboarding process, specifically focusing on certificate deployment and not the entire device configuration process for network access.

In essence, BYOD onboarding provides a comprehensive approach to ensure that mobile devices gain access to network resources securely through a combination of certificate deployment and proper supplicant configuration.

For further research on BYOD onboarding and related concepts, refer to these resources:

Cisco's Documentation on BYOD and Network Access:
https://www.cisco.com/c/en/us/solutions/enterprise/bring-your-own-device/index.html
NIST Guidelines on Mobile Security:https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final

Wikipedia on BYOD:https://en.wikipedia.org/wiki/Bring_your_own_device

Question: 56

What are two characteristics of Cisco DNA Center APIs? (Choose two.)

A.They are Cisco proprietary.
B.They do not support Python scripts.
C.They view the overall health of the network.
D.They quickly provision new devices.
E.Postman is required to utilize Cisco DNA Center API calls.

Answer: CD

Explanation:

The correct answer, C and D, accurately describe key characteristics of Cisco DNA Center APIs. Option C is correct because these APIs provide visibility into the network's overall health, allowing administrators to monitor performance, identify potential issues, and ensure optimal operation. This aligns with the broader concept of network observability, which is crucial for proactive management and troubleshooting. Cisco DNA Center's APIs facilitate the collection and analysis of network data, providing valuable insights into the network's operational state. Option D is correct because the APIs are designed to enable rapid device provisioning. Through these APIs, configurations can be pushed to new devices, greatly reducing the manual effort typically required for onboarding. This aligns with the principles of infrastructure-as-code, allowing for automated and repeatable network deployments. These APIs abstract away the complexities of individual device configurations and provide a simplified interface for rapid provisioning. Option A is incorrect as Cisco DNA Center APIs are based on RESTful principles, widely adopted and not exclusive to Cisco. Option B is incorrect because the APIs are designed to support scripting languages like Python, enabling automation and integration with other systems. Option E is also incorrect as while tools like Postman can simplify working with the APIs, they are not a strict requirement; developers can use various HTTP clients or scripting methods.

Authoritative links for further research:

1. Cisco DNA Center API Documentation: https://developer.cisco.com/site/dna-center/ 2. REST API Overview: https://www.restapitutorial.com/
3. Infrastructure-as-Code: https://martinfowler.com/bliki/InfrastructureAsCode.html

Question: 57

A company discovered an attack propagating through their network via a file. A custom file detection policy was created in order to track this in the future and ensure no other endpoints execute to infected file. In addition, it was discovered during testing that the scans are not detecting the file as an indicator of compromise. What must be done in order to ensure that the policy created is functioning as it should?

A. Create an IP block list for the website from which the file was downloaded.
B. Block the application that the file was using to open.
C. Upload the hash for the file into the policy.
D. Send the file to Cisco Threat Grid for dynamic analysis.

Answer: C

Explanation:

The correct answer is **C. Upload the hash for the file into the policy.**

Here's why:

The scenario describes a custom file detection policy failing to identify a malicious file. This indicates that the policy lacks the specific identifier to recognize the file. File detection policies, especially those designed for custom threat hunting, rely on unique fingerprints of the file to trigger alerts or prevention actions. A common method is using cryptographic hashes (like SHA-256 or MD5). These hashes represent the file's content in a fixed-length string, acting as a unique identifier. Option C addresses this directly by suggesting uploading the file's hash into the policy. This allows the security system to compare the hash of any scanned file against the hash provided in the policy. A match triggers the intended policy action.

Options A and B are not the primary solutions to identify the specific file. Blocking the website where the file originated might prevent future downloads but does not address the existing issue with the custom detection policy not detecting the file. Similarly, blocking the application that opens the file does not specifically target the malicious file itself. Option D is helpful for understanding the file's behavior, but in this case is not directly related to making the custom file detection policy function. It is important to have the hash in the policy, then we could send the file to Cisco Threat Grid, if we desired more information. Therefore, uploading the file's hash is the most immediate and effective step in ensuring the custom policy functions as intended.

Authoritative Links:

Cisco Secure Firewall File Policies:
https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/m_file_policies.html
What are File Hashes and Why are they Important:https://www.crowdstrike.com/cybersecurity-101/hash-values-file-hashing/

Question: 58

```
import http.client
import base64
import ssl
import sys

host = sys.argv[1]#"10.10.10.240"
user = sys.argv[2]#"ersad"
password = sys.argv[3]#"Password1"

conn = http.client.HTTPSConnection("{}:9060".format(host),
context=ssl.SSLContext(ssl.PROTOCOL_TLSv1_2))

creds = str.encode(':'.join((user, password)))
encodedAuth = bytes.decode(base64.b64encode(creds))

headers = {
    'accept': "application/json",
    'authorization': " ".join(("Basic",encodedAuth)),
    'cache-control': "no-cache",
    }

conn.request("GET", "/ers/config/internaluser/", headers=headers)

res = conn.getresponse()
data = res.read()

print("Status: {}".format(res.status))
print("Header:\n{}".format(res.header))
print("Body:\n{}".format(data.decode("utf-8")))
```

Refer to the exhibit. What does the Python script accomplish?

A. It authenticates to a Cisco ISE server using the username or ersad.

B. It lists the LDAP users from the external identity store configured on Cisco ISE. C. It authenticates to a Cisco ISE with an SSH connection.

D. It allows authentication with TLSv1 SSL protocol.

Answer: B

Explanation:

A discarded C and D also

Question: 59

What is a difference between GETVPN and IPsec?

A. GETVPN is used to build a VPN network with multiple sites without having to statically configure all devices. B. GETVPN is based on IKEv2 and does not support IKEv1.

C. GETVPN provides key management and security association management.

D. GETVPN reduces latency and provides encryption over MPLS without the use of a central hub.

Answer: D

Explanation:

Okay, here's a detailed justification for why option D is the correct answer, along with supporting information:

Justification:

The key difference between GETVPN and traditional IPsec lies in their architecture and deployment models, particularly regarding scalability and hub-and-spoke topologies. IPsec, while robust, often utilizes a hub-and-spoke or peer-to-peer model, requiring pre-configured tunnel endpoints and intricate key management, especially when dealing with many sites. This can lead to significant configuration overhead and challenges in dynamic network environments. GETVPN, on the other hand, introduces a group-based approach where multiple devices can participate in the same encrypted VPN without the complexities of individual site-to-site IPsec tunnels.

Option D, stating that GETVPN reduces latency and provides encryption over MPLS without a central hub, accurately reflects this advantage. GETVPN allows direct communication between participating sites over an MPLS network, encrypting the traffic without needing to pass through a central hub. This results in lower latency and improved performance, making it ideal for large, meshed networks.

GETVPN uses group encryption, where all members of a group share the same encryption keys, simplifying the configuration and key management processes. This contrasts sharply with IPsec, where each tunnel has individual keys needing management. Furthermore, GETVPN's key management uses a group controller/key server, making it centralized and scalable.

While GETVPN employs IPsec for the actual data encryption, it uses a different mechanism for key management and security association management, which isn't provided directly by traditional IPsec. This means options A and C are inaccurate in their claims, since GETVPN does rely on key management, just in a streamlined fashion. Additionally, option B is incorrect since GETVPN can support both IKEv1 and IKEv2, although IKEv2 is generally preferred.

Authoritative Links for Further Research:

1. **Cisco GETVPN Technology Overview:** https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/group-encrypted-transport-vpn-getvpn/solution-overview-c22-524828.html - This Cisco page provides a good overview of GETVPN technology, its components and benefits.

2. **Understanding Cisco GET VPN Deployment:**https://www.ciscopress.com/articles/article.asp?p=2180773&seqNum=5 - This article from Cisco Press goes in-depth on GETVPN Deployment, providing clear distinctions between it and IPsec.

3. **Group Encrypted Transport VPN (GETVPN):** https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/GETVPN_Design_Guide.pdf- A more in-depth guide covering design and implementation details of GETVPN, including security features and scalability.

In conclusion, GETVPN's ability to function without a central hub for encryption in a MPLS environment, thereby reducing latency, is a significant differentiator from IPsec, making option D the correct answer.

Question: 60

Which algorithm provides asymmetric encryption?

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

Answer: D

Explanation:

The correct answer is D, RSA. RSA (Rivest-Shamir-Adleman) is a widely used public-key cryptosystem, meaning it employs asymmetric encryption. Asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. The public key can be shared openly, while the private key must be kept secret. In RSA, mathematical properties make it computationally infeasible to derive the private key from the public key, ensuring secure communication.

The other options are symmetric encryption algorithms. Symmetric encryption utilizes the same key for both encryption and decryption. 3DES (Triple DES), RC4, and AES (Advanced Encryption Standard) all operate this way. While symmetric algorithms are faster and more efficient for bulk data encryption, they require a secure channel for key exchange, making them less suitable for initial secure communication establishment or digital signatures. RSA, therefore, excels in situations demanding secure key exchange and digital authentication, which are essential aspects of security in cloud environments.

For more information on asymmetric and symmetric encryption, you can refer to these authoritative resources:

NIST - Computer Security Resource Center:https://csrc.nist.gov/glossary/term/symmetric_cryptography and https://csrc.nist.gov/glossary/term/asymmetric_cryptography
Cloud Security Alliance:https://cloudsecurityalliance.org/ (Search their resources for information on encryption techniques)
Wikipedia:https://en.wikipedia.org/wiki/RSA_(cryptosystem)

Question: 61

What is a difference between an XSS attack and an SQL injection attack?

A.SQL injection is a hacking method used to attack SQL databases, whereas XSS attack can exist in many different types of applications.

B.XSS attacks are used to steal information from databases, whereas SQL injection attacks are used to redirect users to websites where attackers can steal data from them.

C.XSS is a hacking method used to attack SQL databases, whereas SQL injection attacks can exist in many different types of applications.

D.SQL injection attacks are used to steal information from databases, whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

Answer: D

Explanation:

The correct answer is **D**. Here's why:

SQL Injection: This attack directly targets a website's database. Malicious SQL code is injected into input fields (like login forms or search bars) with the intent to manipulate or extract database content, potentially revealing sensitive user data, passwords, or other confidential information. This directly exploits vulnerabilities within the application's data access layer.
Cross-Site Scripting (XSS): XSS exploits vulnerabilities in a web application's output. An attacker injects

malicious client-side scripts (usually JavaScript) into a trusted website. When a user interacts with the compromised page, their browser executes the malicious code. This code can then redirect the user to a malicious site, steal session cookies, modify page content, or perform other malicious actions within the user's browser, leading to data theft or user account compromise.

Therefore, **D** accurately reflects these differences: SQL injection focuses on database breaches to steal data, while XSS redirects users to malicious locations, potentially leading to data theft from the user's browser.

Option **A** incorrectly states that XSS is limited in application; it can exist in any app accepting user input. Option **B** swaps the purpose of the attacks. Option **C** also incorrectly assigns purposes between XSS and SQL injection.

Here are some authoritative links for further research:

OWASP (Open Web Application Security Project):

SQL Injection
Cross-Site Scripting (XSS)
SANS Institute:SQL Injection and XSS
CISA (Cybersecurity and Infrastructure Security Agency):SQL Injection and XSS

Question: 62

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

A.A DoS attack is where a computer is used to flood a server with TCP packets, whereas DDoS attack is where a computer is used to flood a server with UDP packets.

B.A DoS attack is where a computer is used to flood a server with UDP packets, whereas DDoS attack is where a computer is used to flood a server with TCP packets.

C.A DoS attack is where a computer is used to flood a server with TCP and UDP packets, whereas DDoS attack is where a computer is used to flood multiple servers that are distributed over a LAN.

D.A DoS attack is where a computer is used to flood a server with TCP and UDP packets, whereas DDoS attack is where multiple systems target a single system with a DoS attack.

Answer: D

Explanation:

The correct answer is **D**. A Denial-of-Service (DoS) attack involves a single source attempting to overwhelm a target system, typically a server, with traffic, making it unavailable to legitimate users. The attacker achieves this by sending a large volume of TCP, UDP, or other types of packets. A Distributed Denial-of-Service (DDoS) attack, on the other hand, employs multiple compromised computers or devices, often forming a botnet, to launch a coordinated attack against a single target system. Each participating device sends its own stream of malicious traffic, amplifying the impact of the attack. Therefore, the key distinction between a DoS and DDoS is the scale and source of the attack. DoS uses one source, and DDoS uses multiple sources, all attacking one system. Options A, B, and C incorrectly define the protocols used or the number of servers targeted. Option D correctly identifies that both DoS and DDoS attacks flood servers using TCP or UDP but that DDoS utilizes many attackers versus one.

Authoritative Links:

Cloudflare: What is a DDoS Attack?
Microsoft Azure: DoS attacks and DDoS attacks
US-CERT: Understanding Denial-of-Service Attacks

Question: 63

What are two advantages of using Cisco AnyConnect over DMVPN? (Choose two.)

A.It provides spoke-to-spoke communications without traversing the hub.
B.It enables VPN access for individual users from their machines.
C.It allows multiple sites to connect to the data center.
D.It allows different routing protocols to work over the tunnel.
E.It allows customization of access policies based on user identity.

Answer: BE

Explanation:

Here's a detailed justification for why options B and E are the correct advantages of using Cisco AnyConnect over DMVPN, within the context of secure network access:

Option B: "It enables VPN access for individual users from their machines." This is a core function of AnyConnect. It's primarily a client-based VPN solution designed to provide secure remote access for individual users connecting from various devices (laptops, desktops, smartphones) outside the corporate network. DMVPN, on the other hand, focuses on creating site-to-site VPN tunnels, not individual user access. Think of AnyConnect as the "user-to-network" connector.

Option E: "It allows customization of access policies based on user identity." This highlights AnyConnect's sophisticated security features. It integrates with authentication and authorization systems allowing administrators to define granular access policies based on who the user is, not just where they are connecting from. This can include things like restricting access to specific resources based on group memberships or user roles. DMVPN, while secure, does not offer this user-centric identity-based access control, it's more about connecting the sites securely to the hub.

Options A, C and D are incorrect because they are features of DMVPN.

Option A: "It provides spoke-to-spoke communications without traversing the hub." This describes a direct spoke-to-spoke tunnel within a DMVPN network, which AnyConnect does not provide. AnyConnect is used to connect to a gateway/hub rather than peer-to-peer.

Option C: "It allows multiple sites to connect to the data center." While AnyConnect can have multiple users, its purpose is not connecting multiple sites, it is connecting users. This is the primary use case of DMVPN which creates tunnels between sites and a hub.

Option D: "It allows different routing protocols to work over the tunnel." DMVPN is indeed flexible in that it can work with different routing protocols. AnyConnect does not deal with this kind of routing protocol selection.

In summary, AnyConnect is designed for user-centric remote access with identity-based policies, while DMVPN is tailored for site-to-site VPN connectivity with a hub-and-spoke architecture. This distinction makes options B and E the correct advantages of AnyConnect over DMVPN.

Authoritative Links for Further Research:

Cisco AnyConnect Secure Mobility Client:https://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/index.html
Cisco Dynamic Multipoint VPN (DMVPN):https://www.cisco.com/c/en/us/solutions/enterprise/design-zone/index.html?dtid=osscdc000283

Question: 64

What is the difference between a vulnerability and an exploit?

A.A vulnerability is a weakness that can be exploited by an attacker.
B.A vulnerability is a hypothetical event for an attacker to exploit.
C.An exploit is a hypothetical event that causes a vulnerability in the network.
D.An exploit is a weakness that can cause a vulnerability in the network.

Answer: A

Explanation:

The correct answer is A: "A vulnerability is a weakness that can be exploited by an attacker." This distinction is fundamental in cybersecurity. A vulnerability is an inherent flaw or weakness in a system, application, or network. Think of it as an open window in a house – it's a potential point of entry. These weaknesses can arise from coding errors, misconfigurations, or design flaws. An exploit, on the other hand, is the method or code that an attacker uses to take advantage of that vulnerability. Continuing the house analogy, an exploit would be a tool or technique used to enter the house through the open window. It's the actual act of leveraging the weakness for malicious purposes. In essence, vulnerabilities are passive weaknesses, while exploits are active actions. Without a vulnerability, an exploit wouldn't have a target. Options B, C, and D are incorrect because they confuse the roles of vulnerability and exploit. A vulnerability isn't a hypothetical event; it's a real weakness. Exploits don't cause vulnerabilities, they leverage existing ones. Understanding this distinction is crucial for security professionals to effectively identify, mitigate, and remediate security risks.

Further reading on vulnerabilities and exploits:

OWASP (Open Web Application Security Project): A good resource for learning about common web application vulnerabilities. https://owasp.org/
NIST (National Institute of Standards and Technology) National Vulnerability Database: An extensive database of vulnerabilities. https://nvd.nist.gov/
SANS Institute: Provides cybersecurity training and research, with in-depth explanations on vulnerabilities and exploits. https://www.sans.org/

Question: 65

What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?

A.threat intelligence
B.Indicators of Compromise
C.trusted automated exchange
D.The Exploit Database

Answer: A

Explanation:

The correct answer is **A. threat intelligence**. Threat intelligence is the term for curated, actionable information about existing or emerging threats and threat actors. It provides context around malicious activities, including who the attackers are, their motivations, the methods they use, and the targets they pursue. This knowledge allows organizations to proactively identify, assess, and mitigate potential security risks. Effective threat intelligence facilitates better informed security decisions, enables faster incident response, and reduces the overall impact of cyberattacks. It can encompass various data feeds, analysis reports, and community sharing platforms. Indicators of Compromise (IoCs), option B, are pieces of evidence suggesting that a system or network has been breached or is under attack, but they are a component of

threat intelligence, not the overall concept. Trusted Automated Exchange, option C, refers to standardized formats for sharing threat information and is not the encompassing term. The Exploit Database, option D, is a repository of exploits and vulnerabilities but is not the broad definition of proactive security information.

Therefore, only threat intelligence provides the comprehensive knowledge needed to proactively defend against threats.

Supporting Links:

National Institute of Standards and Technology (NIST) - Guide to Threat Intelligence:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
SANS Institute - Understanding Threat Intelligence:https://www.sans.org/blog/understanding-threat-intelligence/
ENISA - Threat Intelligence for Cybersecurity:https://www.enisa.europa.eu/topics/threat-risk-management/threat-intelligence

Question: 66

```
crypto ikev2 name-mangler MANGLER
 dn organization-unit
```

Refer to the exhibit. An engineer is implementing a certificate based VPN. What is the result of the existing configuration?

A.Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully.

B.The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.

C.The OU of the IKEv2 peer certificate is set to MANGLER.

D.The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER.

Answer: B

Explanation:

The correct answer is B.The "match identity certificate" command in the IKEv2 authorization policy is used to specify that the OU (Organizational Unit) attribute of the IKEv2 peer certificate should be used as the identity when matching the policy. The OU attribute is set to "MANGLER" in this case.So, when an IKEv2 peer with a certificate that has an OU attribute of "MANGLER" attempts to establish an IKEv2 SA, the router will use the OU attribute as the identity when matching the authorization policy. If the policy is a match, the SA will be established successfully.

Question: 67

Which kind of API that is used with Cisco DNA Center provisions SSIDs, QoS policies, and update software versions on switches?

A.event

B.intent

C.integration

D.multivendor

Answer: B

Explanation:

The correct answer is **B. Intent API**. Cisco DNA Center leverages an intent-based networking (IBN) approach, where network operations are defined by business goals or "intents" rather than low-level, device-specific configurations. An Intent API allows administrators to specify the desired network behavior (e.g., desired SSID configuration, QoS policies, and software versions) at a high level. Cisco DNA Center then translates these intents into the necessary device configurations, effectively automating the deployment and management of the network. This contrasts with event-driven (A) APIs which react to changes, integration (C) APIs that facilitate communication between systems, and multi-vendor (D) APIs that focus on managing devices from various vendors. The Intent API facilitates network automation, simplifies operations, and allows for rapid deployment and updates. In the scenario mentioned, the intent-driven approach allows administrators to express the desired network settings, and the Intent API is the mechanism to communicate this intent to Cisco DNA Center. The system, in turn, translates the intent into the necessary low-level device configurations, thus realizing the requested settings. The intent-based approach simplifies the process for the administrator, as they do not have to worry about the details on a per-device basis.

Further research:

Cisco DNA Center APIs:https://developer.cisco.com/docs/dna-center/ (This provides access to Cisco's official documentation on DNA Center APIs.)
Intent-Based Networking:https://www.cisco.com/c/en/us/solutions/enterprise-networks/intent-based-networking.html (Cisco's page on Intent-Based Networking explains the concepts.)
Cisco DNA Center Intent APIs Introduction:
https://www.cisco.com/c/en/us/td/docs/cloud_services/Cisco_DNA_Center/dnac_api/cisco-dna-center-intent-apis-guide/b-cisco-dna-center-intent-apis-guide/m-intent-apis-introduction.html (This details the use of intent APIs in Cisco DNA Center)

Question: 68

A network engineer needs to select a VPN type that provides the most stringent security, multiple security associations for the connections, and efficient VPN establishment with the least bandwidth consumption. Why should the engineer select either FlexVPN or DMVPN for this environment?

A.DMVPN because it uses multiple SAs and FlexVPN does not.
B.DMVPN because it supports IKEv2 and FlexVPN does not.
C.FlexVPN because it supports IKEv2 and DMVPN does not.
D.FlexVPN because it uses multiple SAs and DMVPN does not.

Answer: D

Explanation:

The correct answer is **D. FlexVPN because it uses multiple SAs and DMVPN does not.**

Here's a detailed justification:

The question specifies a requirement for "stringent security, multiple security associations (SAs) for connections, and efficient VPN establishment with low bandwidth consumption." These criteria point towards FlexVPN as the better choice over DMVPN.

FlexVPN excels in this scenario due to its flexible and granular control over security protocols. Specifically, it can utilize multiple SAs per connection, which enhances security. Multiple SAs provide distinct secure tunnels for different types of traffic or even for different users, thus reducing the risk of a single point of compromise.

FlexVPN leverages IKEv2 for key exchange, which is known for its improved security and efficiency compared to older IKE versions. While DMVPN can also use IKEv2, it inherently focuses on dynamic mesh topologies and does not prioritize multiple SAs for single connections to the same degree as FlexVPN.

DMVPN (Dynamic Multipoint VPN) is designed for creating scalable and dynamic mesh VPN topologies, typically with spokes connecting to a hub. While it offers good security, its strength lies in simplifying complex, large-scale VPN deployments. DMVPN typically uses a single SA per tunnel between endpoints, which contrasts directly with the multiple SA capability of FlexVPN. This makes DMVPN less suitable for scenarios requiring multiple security associations for a single connection.

Therefore, FlexVPN, due to its ability to leverage multiple SAs per connection, fits the criteria of "stringent security" more effectively than DMVPN. Furthermore, IKEv2 helps achieve secure and efficient VPN establishment. Because DMVPN does not inherently support multiple SAs per connection, and focuses instead on a single SA, it is the less correct choice for this scenario.

Here are some authoritative links for further research:

Cisco FlexVPN Configuration Guide:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_vpn/configuration/16-12/sec-vpn-16-12-book/sec-flexvpn.html
Cisco DMVPN Overview:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/DMVPN_Guide/DMVPN_Overview.htm
IKEv2 Protocol Explained:https://datatracker.ietf.org/doc/html/rfc7296

Question: 69

Interface	MAC Address	Method	Domain	Status	Fg Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth	0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth	0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth	0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth	0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth	0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth	0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth	0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth	0A02198200000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth	0A02198200001
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth	0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth	0A02198200000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth	0A02198200000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth	0A02198200000
Gi7/4	54ee.75db.d766	dot1x	DATA	Auth	0A02198200001
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth	0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth	0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth	0A02198200000

Refer to the exhibit. Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

A.show authentication registrations
B.show authentication method
C.show dot1x all
D.show authentication sessions

Answer: D

Explanation:

D is correct.The following example shows how to display all authentication sessions on the switch:Device# show authentication sessions Interface MAC Address Method Domain Status Session IDGi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05CGi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10

Question: 70

```
snmp-server group SNMP v3 auth access 15
```

Refer to the exhibit. What does the number 15 represent in this configuration?

A.privilege level for an authorized user to this router
B.access list that identifies the SNMP devices that can access the router
C.interval in seconds between SNMPv3 authentication attempts
D.number of possible failed attempts until the SNMPv3 user is locked out

Answer: B

Explanation:

B is correct. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-16/snmp-xe-16-book/nm-snmp-cfg-snmp-support.html#GUID-10FB2FAD-39A6-41D8-AB14-0C4B6E20911F

Question: 71

What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?

A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX

Answer: B

Explanation:

The command crypto isakmp key ciscXXXXXXXX address 172.16.0.0 configures a pre-shared key for IKE (Internet Key Exchange) authentication. Specifically, it defines the string ciscXXXXXXXX as the secret key to be used for authentication with a peer whose IP address is 172.16.0.0. The address keyword indicates that this key applies to a specific single peer, identified by that IP address. It does not refer to a range. The isakmp keyword refers to IKEv1. Option B correctly states that the command authenticates the IP address 172.16.0.0 peer using ciscXXXXXXXX. Option A incorrectly suggests the key applies to a 172.16.0.0/16 range, and mistakenly references IKEv2. Option C correctly references IKEv1, but incorrectly assumes a 172.16.0.0/16 range. Option D is incorrect as this command deals with pre-shared keys and not certificates.

Therefore, option B is the only accurate description. It highlights the specific peer IP, the pre-shared key, and the applicable IKE version, which is IKEv1 through ISAKMP. IKEv1 uses pre-shared keys, and this command configures one of them on the router. It is important to note the specific address is 172.16.0.0/32, not any wider subnet.

Authoritative Links:

Cisco Documentation on ISAKMP Configuration: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/vpn/configuration/15-sy/sec-vpn-15-sy-book/sec-cfg-isakmp.html
IKE Fundamentals: https://www.rfc-editor.org/rfc/rfc7296

Question: 72

Which command enables 802.1X globally on a Cisco switch?

A.dot1x system-auth-control
B.dot1x pae authenticator
C.authentication port-control auto
D.aaa new-model

Answer: A

Explanation:

The correct command to enable 802.1X globally on a Cisco switch is dot1x system-auth-control. Let's break down why this is the case and why the other options are incorrect.

802.1X is an IEEE standard for port-based Network Access Control (PNAC). It's used to authenticate devices connecting to a network. A Cisco switch, when acting as an authenticator, relies on specific commands to enable this functionality. The dot1x system-auth-control command enables the overall 802.1X framework globally across all interfaces on the switch. Once this command is enabled, the switch will listen for authentication requests according to the configured method. Without this command, the switch will not participate in 802.1X authentication.

Option B, dot1x pae authenticator, configures a particular port as an 802.1X authenticator, which is a port-specific configuration, not global. Option C, authentication port-control auto, is related to controlling the port's authorization state (auto, force-authorized, force-unauthorized) and how it reacts to authentication events, but does not enable the 802.1X process itself. Option D, aaa new-model, activates the Authentication, Authorization, and Accounting (AAA) framework, which is necessary for 802.1X but is not the command to enable the functionality itself. Think of aaa new-model as activating the building, while dot1x system-auth-control activates the doors.

The dot1x system-auth-control command enables the fundamental 802.1X functionality. Other port-specific configurations and authentication methods can then be applied as needed.

For further research, the official Cisco documentation is the best source. Specifically, the command reference guides for your Cisco IOS or IOS-XE version will have comprehensive information. Here is a general starting point for Cisco security commands:

Cisco Security Command References:https://www.cisco.com/c/en/us/support/security/security-command-references.html
Cisco 802.1X Configuration Guide: (Specific document will vary depending on your platform, search on Cisco support portal). You can find information about dot1x system-auth-control there.

Question: 73

What is a characteristic of Dynamic ARP Inspection?

A.DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCP snooping binding database.

B.In a typical network, make all ports as trusted except for the ports connecting to switches, which are untrusted.

C.DAI associates a trust state with each switch.

D.DAI intercepts all ARP requests and responses on trusted ports only.

Answer: A

Explanation:

The correct answer is A because Dynamic ARP Inspection (DAI) leverages the DHCP snooping binding database to validate ARP packets. This database contains legitimate IP-to-MAC address mappings learned from DHCP traffic. DAI checks incoming ARP requests and responses against this database. If an ARP packet's IP-to-MAC binding doesn't match a valid entry in the database, DAI drops the packet, preventing ARP spoofing and man-in-the-middle attacks.

Option B is incorrect because it misrepresents the concept of trusted and untrusted ports in DAI. Usually, ports connected to end-user devices are considered untrusted, while ports connecting to DHCP servers or upstream switches are trusted. Option C is incorrect as DAI associates trust states with ports, not switches. Option D is also incorrect because DAI inspects ARP packets on untrusted ports, not trusted ones, to protect the network from potential attacks originating from those ports. DAI only allows ARP traffic on trusted ports.

DAI's purpose is to secure the network against illegitimate ARP traffic, making the comparison with the database crucial.

In essence, DAI acts as a security mechanism within the network to verify the integrity of ARP communication based on dynamic learning of IP and MAC address relationships from DHCP. It specifically guards against malicious ARP activity by comparing observed ARP bindings against the previously validated ones provided by the DHCP snooping database. This allows a network to filter out spoofed ARP responses and prevent denial of service attacks or information interception attempts based on poisoning the ARP caches.

Authoritative links for further research:

1. **Cisco Dynamic ARP Inspection:** https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/15sg/configuration/guide/config/dynarp.html
2. **Dynamic ARP Inspection (DAI) - Wiki:**https://en.wikipedia.org/wiki/Dynamic_ARP_inspection 3. **Understanding ARP and ARP Attacks:**https://www.fortinet.com/resources/cyberglossary/arp-attack

Question: 74

Which statement about IOS zone-based firewalls is true?

A. An unassigned interface can communicate with assigned interfaces

B. Only one interface can be assigned to a zone.

C. An interface can be assigned to multiple zones.

D. An interface can be assigned only to one zone.

Answer: D

Explanation:

The correct answer, D, "An interface can be assigned only to one zone," accurately reflects a fundamental characteristic of Cisco IOS zone-based firewalls (ZBF). ZBF operates on the principle of dividing a network

into logical security zones. Each physical interface of a router is placed within one of these zones, and traffic flow is controlled based on policies defined between zones. Allowing an interface to belong to multiple zones would introduce ambiguity and potential conflicts in policy enforcement, defeating the purpose of clearly defined security boundaries. A zone acts as a container with its own set of rules, and an interface is a distinct point of entry or exit. Option A is incorrect because unassigned interfaces are implicitly part of the "outside" or uncontrolled region and cannot interact with interfaces within a zone without explicit rules. Option B is inaccurate as a zone can and typically does have multiple interfaces assigned. Finally, Option C is also incorrect, as allowing an interface to participate in multiple zones would create complex and often conflicting rulesets, breaking the simplicity and security of the model. This one-to-one relationship ensures clear traffic flows and policy application, allowing for easier management and a more robust security posture.

Authoritative Links for further research:

Cisco Documentation on Zone-Based Firewalls:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/firewall/configuration/15-sy/sec-firewall-15-sy-book/sec-zone-fw.html
Cisco Press - Implementing Cisco Network Security (CCNA Security): (You can search for this book on Amazon or other online booksellers, it includes detailed information on zone-based firewalls in the CCNA Security curriculum.)

Question: 75

When wired 802.1X authentication is implemented, which two components are required? (Choose two.)

A. authentication server: Cisco Identity Service Engine
B. supplicant: Cisco AnyConnect ISE Posture module
C. authenticator: Cisco Catalyst switch
D. authenticator: Cisco Identity Services Engine
E. authentication server: Cisco Prime Infrastructure

Answer: AC

Explanation:

The correct answer is A and C because 802.1X authentication, a standard for network access control, requires three key components: a supplicant (the device requesting network access), an authenticator (the network device that controls access), and an authentication server (the system that verifies the supplicant's credentials). In this context, option A correctly identifies the "authentication server" as Cisco Identity Services Engine (ISE), a centralized policy management and access control platform. Cisco ISE verifies user identities and device posture before granting network access. Option C accurately states that a Cisco Catalyst switch acts as the "authenticator" in a wired 802.1X setup. The switch intercepts connection requests from devices, forwards them to the authentication server, and based on the response, either grants or denies access. Cisco AnyConnect (B) is a VPN client, not primarily a 802.1X supplicant. Though the ISE Posture module can play a role, it's not the core supplicant. Cisco Identity Services Engine (D) is not an authenticator. Cisco Prime Infrastructure (E) is a network management system, not an authentication server in the context of 802.1x.

Therefore, a functional 802.1X setup mandates an authentication server like Cisco ISE and an authenticator like a Cisco Catalyst switch.

Further research:

Cisco Identity Services Engine (ISE) Documentation:
https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html
Cisco Catalyst Switches:https://www.cisco.com/c/en/us/products/switches/index.html
802.1X Authentication:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/15-

mt/sec-usr-8021x-15-mt-book/sec-ieee-8021x.html

Question: 76

Which SNMPv3 configuration must be used to support the strongest security possible?

A.asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

B.asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

C.asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

D.asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

Answer: D

Explanation:

Here's a detailed justification for why option D is the correct answer, focusing on SNMPv3 security best practices:

Option D represents the most secure SNMPv3 configuration due to its utilization of both authentication and encryption with the strongest available algorithms. The snmp-server group myv3 v3 priv command establishes a group named "myv3" configured for SNMPv3 with privacy (encryption). Subsequently, snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX defines a user "andy" within "myv3", enforcing SHA for authentication and AES-256 for encryption, the strongest combination of algorithms in this context. The snmp-server host inside 10.255.254.1 version 3 andy command specifies that SNMPv3 traps will be sent to the host at 10.255.254.1, utilizing the defined "andy" user.

In contrast, options A and C use 3DES, a weaker encryption algorithm compared to AES-256, making them less secure. Option B uses “noauth,” which disables authentication, leaving the communication vulnerable to tampering and eavesdropping. For comprehensive security, both authentication and encryption are crucial. SHA for authentication ensures the data source is legitimate and prevents unauthorized modification, while AES-256 encryption guarantees data confidentiality, preventing eavesdropping of SNMP data. The use of "priv" in the group definition and AES-256 in the user definition clearly indicate the intent for strong security, as "priv" is synonymous with employing encryption. Therefore, option D is the only option that adheres to best practices for maximum security in an SNMPv3 environment.

Further research can be conducted on the following Cisco documentation links:

Configuring SNMP:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-sy/snmp-15-sy-book/nm-snmp-config.html
SNMPv3 Security:https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/15102-snmpv3sec-15102.html

Question: 77

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

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: BD

Explanation:

A Change of Authorization (CoA) is a dynamic authorization mechanism used to update a network session's policies and permissions without disrupting the active connection. It's primarily employed in network access control systems like Cisco ISE. Option B, an endpoint deletion on the Identity Service Engine (ISE), directly impacts active sessions. If an endpoint is deleted, any existing connections associated with that endpoint need to have their authorization reviewed and potentially terminated or modified, triggering a CoA. This aligns with the principle of dynamic policy enforcement. Option D, an endpoint profiled for the first time, means the network has now categorized and understood the device type. This newly gained information could alter the access policies applicable to that device. For instance, a printer may now have a policy different from an unknown device, necessitating a CoA. It demonstrates real-time adaptation of security policies based on endpoint attributes. Options A and C concern changes to the configuration of the system, but don't directly involve an active session. Option E, adding a new ISE server with an administrative role, pertains to backend system management and does not directly trigger changes in user sessions. Therefore, only B and D present situations where CoA would be logically and operationally necessary. Further research can be done on Cisco ISE's CoA functionality and its role in network access control via Cisco's documentation: https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/b_ise_admin_guide_2_7/b_ise_admin_guide_27_chapter_01100.html and specific documentation on COA on the same site.

Question: 78

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

A. DMZ multiple zone mode

B. transparent firewall mode

C. multiple context mode

D. routed mode

Answer: C

Explanation:

The correct answer is **C. multiple context mode.** Cisco ASA multiple context mode allows a single physical ASA device to function as multiple independent virtual firewalls, each with its own security policies, interfaces, and administrators. This separation provides a robust way to isolate management responsibilities, ensuring that changes made within one context do not affect others. In contrast, DMZ multiple zone mode (A) still operates under a single management plane, offering network segmentation, not administrative separation. Transparent firewall mode (B) focuses on layer 2 operations and doesn't inherently provide independent management domains. Routed mode (D) is the basic firewall operation mode where routing decisions are made, again without administrative separation. Cloud environments often benefit from multi-tenancy, mirroring the logical separation offered by multiple context mode. This model is advantageous in shared resource scenarios where organizations want distinct security and administrative control over their portion of a shared appliance. Multiple context mode creates logically separate, fully functional instances, each with its own access control and configurations, thus effectively addressing the question's requirement.

Think of it as virtualizing the firewall itself, akin to how virtual machines operate on a hypervisor. Further details on Cisco ASA multiple context mode can be found in the official Cisco documentation:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/guide/asa_910_config/intro_contexts.ht

Question: 79

```
Sysauthcontrol              Enabled
Dot1x Protocol Version          3

Dot1x Info for GigabitEthernet1/0/12
-----------------------------------
PAE                     = AUTHENTICATOR
PortControl             = FORCE_AUTHORIZED
ControlDirection        = Both
HostMode                = SINGLE_HOST
QuietPeriod             = 60
ServerTimeout           = 0
SuppTimeout             = 30
ReAuthMax               = 2
MaxReq                  = 2
TxPeriod                = 30
```

Refer to the exhibit. Which command was used to display this output?

A.show dot1x all
B.show dot1x
C.show dot1x all summary
D.show dot1x interface gi1/0/12

Answer: A

Explanation:

Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021 x-xe-3se-3850-book/config-ieee-802x- pba.html

Question: 80

What is a characteristic of Cisco ASA NetFlow v9 Secure Event Logging?

A.It tracks flow-create, flow-teardown, and flow-denied events.

B.It provides stateless IP flow tracking that exports all records of a specific flow. C.It tracks the flow continuously and provides updates every 10 seconds.

D.Its events match all traffic classes in parallel.

Answer: A

Explanation:

Cisco ASA NetFlow v9 Secure Event Logging is designed to provide detailed security-related information about network traffic. Option A, "It tracks flow-create, flow-teardown, and flow-denied events," accurately reflects this functionality. NetFlow v9, in the context of ASA security logging, is specifically configured to capture these key events related to connection establishment, termination, and security policy violations (denied flows). This is vital for security analysis, incident response, and understanding traffic patterns.

Options B, C, and D are incorrect. While NetFlow is generally a flow-based technology, ASA NetFlow v9 logging does not export records of every single flow (as stated in B), nor does it provide continuous updates every 10 seconds (C). It's event-driven, triggered by specific flow actions rather than constant tracking.

Furthermore, it doesn't match all traffic classes in parallel (D), rather it focuses on flows that match configured logging criteria.

The significance of tracking flow-create, flow-teardown, and flow-denied events lies in the ability to reconstruct security incidents. For instance, detecting a high number of "flow-denied" events to a particular destination could indicate a denial-of-service attack attempt, while tracking flow creation and teardown helps analyze user behavior and resource consumption. This detailed, event-driven approach makes NetFlow v9 security logging a valuable security tool. It's also worth noting that the Cisco ASA NetFlow v9 implementation can be customized to log other specific attributes as well. In summary, the core function of Cisco ASA NetFlow v9 Secure Event Logging is to capture and report on essential flow-related security events, making Option A the correct characteristic.

Authoritative links:

1. Cisco ASA NetFlow v9 Configuration Guide:
   https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/firewall/asa-98-firewall-config/monitor-netflow.html
2. Cisco NetFlow Version 9 Export Format:
   https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800c3c28.h