Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

NEW QUESTION 1
- (Exam Topic 2)
A network administrator is configuring SNMPv3 on a new router. The users have already been created; however, an additional configuration is needed to facilitate access to the SNMP views. What must the administrator do to accomplish this?

A. map SNMPv3 users to SNMP views
B. set the password to be used for SNMPv3 authentication
C. define the encryption algorithm to be used by SNMPv3
D. specify the UDP port used by SNMP

Answer: B

NEW QUESTION 2
- (Exam Topic 2)
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. weak passwords for authentication
B. unencrypted links for traffic
C. software bugs on applications
D. improper file security

Answer: B

NEW QUESTION 3
- (Exam Topic 2)
What is a benefit of conducting device compliance checks?

A. It indicates what type of operating system is connecting to the network.
B. It validates if anti-virus software is installed.
C. It scans endpoints to determine if malicious activity is taking place.
D. It detects email phishing attacks.

Answer: B

NEW QUESTION 4
- (Exam Topic 2)
An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco Firepower. Which feature should be used to accomplish this?

A. NetFlow
B. Packet Tracer
C. Network Discovery
D. Access Control

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper

NEW QUESTION 5
- (Exam Topic 2)
What is a function of 3DES in reference to cryptography?

A. It hashes files.
B. It creates one-time use passwords.
C. It encrypts traffic.
D. It generates private keys.

Answer: C

NEW QUESTION 6
- (Exam Topic 2)
What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?

A. Cisco Cloudlock
B. Cisco Umbrella
C. Cisco AMP
D. Cisco App Dynamics

Answer: A

Explanation:

Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely.It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks,protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

NEW QUESTION 7
- (Exam Topic 2)
What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group?

A. posture assessment
B. CoA
C. external identity source
D. SNMP probe

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide

NEW QUESTION 8
- (Exam Topic 2)
An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?

A. SIEM
B. CASB
C. Adaptive MFA
D. Cisco Cloudlock

Answer: D

Explanation:
Reference: https://docs.umbrella.com/cloudlock-documentation/docs/endpointsNote:+ Security information and event management (SIEM) platforms collect log and event data from securitysystems, networks and computers, and turn it into actionable security insights.+ An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when acondition of an alerting policy has been met.

NEW QUESTION 9
- (Exam Topic 2)
What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

A. Multiple NetFlow collectors are supported
B. Advanced NetFlow v9 templates and legacy v5 formatting are supported
C. Secure NetFlow connections are optimized for Cisco Prime Infrastructure
D. Flow-create events are delayed

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.pdf

NEW QUESTION 10
- (Exam Topic 2)
An organization is trying to implement micro-segmentation on the network and wants to be able to gain visibility on the applications within the network. The solution must be able to maintain and force compliance. Which product should be used to meet these requirements?

A. Cisco Umbrella
B. Cisco AMP
C. Cisco Stealthwatch
D. Cisco Tetration

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22

NEW QUESTION 10
- (Exam Topic 2)
An engineer notices traffic interruption on the network. Upon further investigation, it is learned that broadcast packets have been flooding the network. What must be configured, based on a predefined threshold, to address this issue?

A. Bridge Protocol Data Unit guard
B. embedded event monitoring
C. storm control
D. access control lists

Answer: C

Explanation:
Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.By using the “storm-control broadcast level [falling-threshold]” we can limit the broadcast traffic on the switch.

NEW QUESTION 12
- (Exam Topic 2)
What is an attribute of the DevSecOps process?

A. mandated security controls and check lists
B. security scanning and theoretical vulnerabilities
C. development security
D. isolated security team

Answer: C

Explanation:
DevSecOps (development, security, and operations) is a concept used in recent years to describe how to movesecurity activities to the start of the development life cycle and have built-in security practices in the continuousintegration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closerto IT and business objectives.Three key things make a real DevSecOps environment:+ Security testing is done by the development team.+ Issues found during that testing is managed by the development team.+ Fixing those issues stays within the development team.

NEW QUESTION 16
- (Exam Topic 2)
In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint Protection Platform?

A. when there is a need for traditional anti-malware detection
B. when there is no need to have the solution centrally managed
C. when there is no firewall on the network
D. when there is a need to have more advanced detection capabilities

Answer: D

Explanation:
Endpoint protection platforms (EPP) prevent endpoint security threats like known and unknown malware.Endpoint detection and response (EDR) solutions can detect and respond to threats that your EPP and other security tools did not catch.EDR and EPP have similar goals but are designed to fulfill different purposes. EPP is designed to providedevice-level protection by identifying malicious files, detecting potentially malicious activity, and providing tools for incident investigation and response.The preventative nature of EPP complements proactive EDR. EPP acts as the first line of defense, filtering out attacks that can be detected by the organization’s deployed security solutions. EDR acts as a second layer of protection, enabling security analysts to perform threat hunting and identify more subtle threats to the endpoint.Effective endpoint defense requires a solution that integrates the capabilities of both EDR and EPP to provide protection against cyber threats without overwhelming an organization’s security team.

NEW QUESTION 18
- (Exam Topic 2)
A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?

A. Use MAB with profiling
B. Use MAB with posture assessment.
C. Use 802.1X with posture assessment.
D. Use 802.1X with profiling.

Answer: A

Explanation:
Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456

NEW QUESTION 20
- (Exam Topic 2)
What is a benefit of using Cisco FMC over Cisco ASDM?

A. Cisco FMC uses Java while Cisco ASDM uses HTML5.
B. Cisco FMC provides centralized management while Cisco ASDM does not.
C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.
D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheetc78-736775.ht

NEW QUESTION 25
- (Exam Topic 2)
Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?

A. file access from a different user
B. interesting file access
C. user login suspicious behavior
D. privilege escalation

Answer: C

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-7403

NEW QUESTION 27
- (Exam Topic 2)
A Cisco Firepower administrator needs to configure a rule to allow a new application that has never been seen on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose
two)

A. permit
B. trust
C. reset
D. allow
E. monitor

Answer: BE

Explanation:
Each rule also has an action, which determines whether you monitor, trust, block, or allow matching traffic.Note: With action “trust”, Firepower does not do any more inspection on the traffic. There will be no intrusion protection and also no file-policy on this traffic.

NEW QUESTION 28
- (Exam Topic 1)
What is a commonality between DMVPN and FlexVPN technologies?

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

Answer: D

Explanation:
Reference: https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/

NEW QUESTION 32
- (Exam Topic 1)
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:
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- cisco-dna-center-aag-cte-en.html

NEW QUESTION 33
- (Exam Topic 1)
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

NEW QUESTION 38
- (Exam Topic 1)
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: C

Explanation:
Configure a Crypto ISAKMP Key
In order to configure a preshared
configuration mode:
authentication key, enter thcerypto isakmp key
command in global
crypto isakmp key cisco123 address 172.16.1.1
https://community.cisco.com/t5/vpn/isakmp-with-0-0-0-0-dmvpn/td-p/4312380
It is a bad practice but it is valid. 172.16.0.0/16 the full range will be accepted as possible PEER
https://www.examtopics.com/discussions/cisco/view/46191-exam-350-701-topic-1-question-71-discussion/#:~:t Testing without a netmask shows that command interpretation has a preference for /16 and /24.
CSR-1(config)#crypto isakmp key cisco123 address 172.16.0.0
CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.0.0 [255.255.0.0] cisco123
CSR-1(config)#no crypto isakmp key cisco123 address 172.16.0.0 CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.0 CSR-1(config)#do show crypto isakmp key | i cisco
default 172.16.1.0 [255.255.255.0] cisco123
CSR-1(config)#no crypto isakmp key cisco123 address 172.16.1.0 CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.128
CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.1.128 cisco123 CSR-1(config)#

NEW QUESTION 41
- (Exam Topic 1)
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:
FlexVPN is an IKEv2-based VPN technology that provides several benefits beyond traditional site-to-site VPN implementations. FlexVPN is a standards-based solution that can interoperate with non-Cisco IKEv2implementations. Therefore FlexVPN can support a multivendor environment. All of the three VPN technologies support traffic between sites (site-to-site or spoke-to-spoke).

NEW QUESTION 44
- (Exam Topic 1)
Why would a user choose an on-premises ESA versus the CES solution?

A. Sensitive data must remain onsite.
B. Demand is unpredictable.
C. The server team wants to outsource this service.
D. ESA is deployed inline.

Answer: A

NEW QUESTION 46
- (Exam Topic 1)
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:
The AES encryption algorithm encrypts and decrypts data in blocks of 128 bits (block size). It can do this using 128-bit, 192-bit, or 256-bit keys

NEW QUESTION 49
- (Exam Topic 1)
Refer to the exhibit.

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

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:
The syntax of this command is shown below:snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]}] [read read-view] [write write-view] [notify notify-view] [access access-list]The command above restricts which IP source addresses are allowed to access SNMP functions on the router. You could restrict SNMP access by simply applying an interface ACL to block incoming SNMP packets that don't come from trusted servers. However, this would not be as effective as using the global SNMP commands shown in this recipe. Because you can apply this method once for the whole router, it is much simpler than applying ACLs to block SNMP on all interfaces separately. Also, using interface ACLs would block not only SNMP packets intended for this router, but also may stop SNMP packets that just happened to be passing through on their way to some other destination device.

NEW QUESTION 53
- (Exam Topic 1)
What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?

A. EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.
B. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.
C. EPP focuses on network security, and EDR focuses on device security.
D. EDR focuses on network security, and EPP focuses on device security.

Answer: A

NEW QUESTION 57
- (Exam Topic 1)
A company is experiencing exfiltration of credit card numbers that are not being stored on-premise. The company needs to be able to protect sensitive data throughout the full environment. Which tool should be used to accomplish this goal?

A. Security Manager
B. Cloudlock
C. Web Security Appliance
D. Cisco ISE

Answer: B

Explanation:
Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

NEW QUESTION 61
- (Exam Topic 1)
When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

A. Application Control
B. Security Category Blocking
C. Content Category Blocking
D. File Analysis

Answer: B

NEW QUESTION 64
- (Exam Topic 1)
Which technology is used to improve web traffic performance by proxy caching?

A. WSA
B. Firepower
C. FireSIGHT
D. ASA

Answer: A

NEW QUESTION 65
- (Exam Topic 1)
Which RADIUS attribute can you use to filter MAB requests in an 802.1 x deployment?

A. 1
B. 2
C. 6
D. 31

Answer: C

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networkingservices/config_

NEW QUESTION 67
- (Exam Topic 1)
Which deployment model is the most secure when considering risks to cloud adoption?

A. Public Cloud
B. Hybrid Cloud
C. Community Cloud
D. Private Cloud

Answer: D

NEW QUESTION 68
- (Exam Topic 1)
Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'

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)
```

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

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

Answer: D

Explanation:
Reference:
https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.

NEW QUESTION 73
- (Exam Topic 1)
An MDM provides which two advantages to an organization with regards to device management? (Choose two)

A. asset inventory management
B. allowed application management
C. Active Directory group policy management
D. network device management
E. critical device management

Answer: AB

NEW QUESTION 74
- (Exam Topic 1)
Which network monitoring solution uses streams and pushes operational data to provide a near real-time view of activity?

A. SNMP
B. SMTP
C. syslog
D. model-driven telemetry

Answer: D

Explanation:
Reference: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide

NEW QUESTION 75

- (Exam Topic 1)
Which two risks is a company vulnerable to if it does not have a well-established patching solution for endpoints? (Choose two)

A. exploits
B. ARP spoofing
C. denial-of-service attacks
D. malware
E. eavesdropping

Answer: AD

Explanation:
Malware means “malicious software”, is any software intentionally designed to cause damage to a computer, server, client, or computer network. The most popular types of malware includes viruses, ransomware and spyware. Virus Possibly the most common type of malware, viruses attach their malicious code to clean code and wait to be run.
Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again.Spyware is spying software that can secretly record everything you enter, upload, download, and store on your computers or mobile devices. Spyware always tries to keep itself hidden.An exploit is a code that takes advantage of a software vulnerability or security flaw.Exploits and malware are two risks for endpoints that are not up to date. ARP spoofing and eavesdropping are attacks against the network while denial-of-service attack is based on the flooding of IP packets.

NEW QUESTION 78
- (Exam Topic 1)
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. teardrop

Answer: BC

NEW QUESTION 79
- (Exam Topic 1)
Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

A. Correlation
B. Intrusion
C. Access Control
D. Network Discovery

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introd

NEW QUESTION 80
- (Exam Topic 1)
Which two fields are defined in the NetFlow flow? (Choose two)

A. type of service byte
B. class of service bits
C. Layer 4 protocol type
D. destination port
E. output logical interface

Answer: AD

Explanation:
Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share seven values which define a unique key for the flow:+ Ingress interface (SNMP ifIndex)+ Source IP address+ Destination IP address+ IP protocol+ Source port for UDP or TCP, 0 for other protocols+ Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols+ IP Type of ServiceNote: A flow is a unidirectional series of packets between a given source and destination.

NEW QUESTION 82
- (Exam Topic 1)
What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services? (Choose two)

A. multiple factor auth
B. local web auth
C. single sign-on
D. central web auth
E. TACACS+

Answer: BD

NEW QUESTION 83

- (Exam Topic 1)
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)

A. Patch for cross-site scripting.
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.
D. Install a spam and virus email filter.
E. Protect systems with an up-to-date antimalware program

Answer: DE

Explanation:
Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputablesource. It is usually done through email. The goal is to steal sensitive data like credit card and login information,or to install malware on the victim's machine.

NEW QUESTION 85
- (Exam Topic 1)
An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA. Which Cisco ASA command must be used?

A. flow-export destination inside 1.1.1.1 2055
B. ip flow monitor input
C. ip flow-export destination 1.1.1.1 2055
D. flow exporter

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_nsel.h

NEW QUESTION 86
- (Exam Topic 1)
What must be used to share data between multiple security products?

A. Cisco Rapid Threat Containment
B. Cisco Platform Exchange Grid
C. Cisco Advanced Malware Protection
D. Cisco Stealthwatch Cloud

Answer: B

NEW QUESTION 87
- (Exam Topic 1)
Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?

A. It allows the endpoint to authenticate with 802.1x or MAB.
B. It verifies that the endpoint has the latest Microsoft security patches installed.
C. It adds endpoints to identity groups dynamically.
D. It allows CoA to be applied if the endpoint status is compliant.

Answer: A

NEW QUESTION 89
- (Exam Topic 1)
Which two features of Cisco Email Security can protect your organization against email threats? (Choose two)

A. Time-based one-time passwords
B. Data loss prevention
C. Heuristic-based filtering
D. Geolocation-based filtering
E. NetFlow

Answer: BD

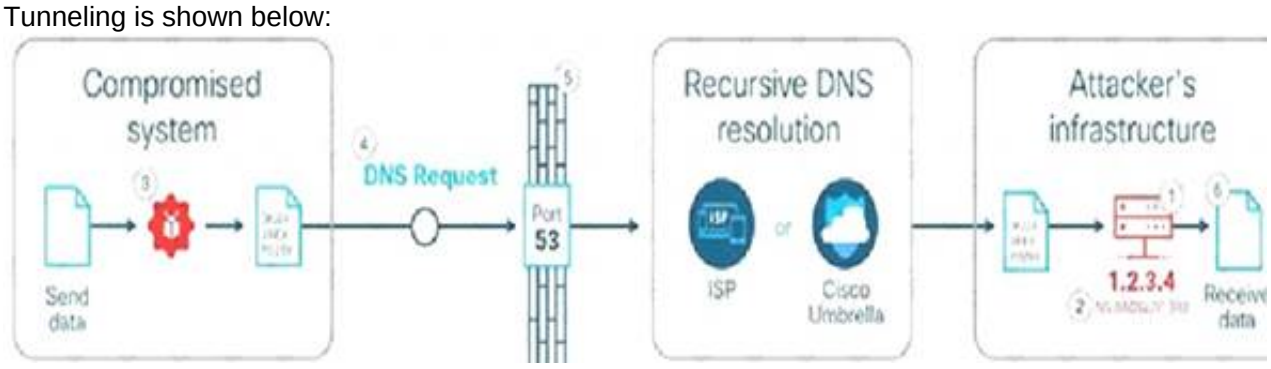
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA

NEW QUESTION 91
- (Exam Topic 1)
How is DNS tunneling used to exfiltrate data out of a corporate network?

A. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.
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 damageand theft on the network.
D. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.

Answer: B

Explanation:
Domain name system (DNS) is the protocol that translates human-friendly URLs, such as securitytut.com, into IP addresses, such as 183.33.24.13. Because DNS messages are only used as the beginning of each communication and they are not intended for data transfer, many organizations do not monitor their DNS traffic for malicious activity. As a result, DNS-based attacks can be effective if launched against their networks. DNS tunneling is one such attack.An example of DNS Tunneling is shown below:



The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNSnameserver (NS) and malicious payload.2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. attackerdomain.com) is registered or reused. The registrar informs the top-level domain (.com) nameservers to refer requests for attackerdomain.com to ns.attackerdomain.com, which has a DNS record mapped to 1.2.3.43. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, P028X977W,…).4. The payload initiates thousands of unique DNS record requests to the attacker's domain with each string as
Reference: https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0

NEW QUESTION 94
- (Exam Topic 1)
Which statement describes a traffic profile on a Cisco Next Generation Intrusion Prevention System?

A. It allows traffic if it does not meet the profile.
B. It defines a traffic baseline for traffic anomaly deduction.
C. It inspects hosts that meet the profile with more intrusion rules.
D. It blocks traffic if it does not meet the profile.

Answer: B

NEW QUESTION 97
- (Exam Topic 1)
Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

A. File Analysis
B. SafeSearch
C. SSL Decryption
D. Destination Lists

Answer: C

Explanation:
Reference:
https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-IntelligentProxy

NEW QUESTION 101
- (Exam Topic 1)
Which benefit does endpoint security provide the overall security posture of an organization?

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

Answer: D

NEW QUESTION 102
- (Exam Topic 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 Southbound API is used to communicate between Controllers and network devices

NEW QUESTION 104
- (Exam Topic 1)
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:
Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on.For example the code below is written in hex: <ahref=javascript:alert&#x28'XSS')>Click Hereis equivalent to:Click HereNote: In the format "&#xhhhh", hhhh is the code point in hexadecimal form.

NEW QUESTION 105
- (Exam Topic 1)
An engineer needs a solution for TACACS+ authentication and authorization for device administration. The engineer also wants to enhance wired and wireless network security by requiring users and endpoints to use 802.1X, MAB, or WebAuth. Which product meets all of these requirements?

A. Cisco Prime Infrastructure
B. Cisco Identity Services Engine
C. Cisco Stealthwatch
D. Cisco AMP for Endpoints

Answer: B

NEW QUESTION 106
- (Exam Topic 1)
Which technology reduces data loss by identifying sensitive information stored in public computing environments?

A. Cisco SDA
B. Cisco Firepower
C. Cisco HyperFlex
D. Cisco Cloudlock

Answer: D

NEW QUESTION 111
- (Exam Topic 1)
Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?

A. Advanced Malware Protection
B. Platform Exchange Grid
C. Multifactor Platform Integration
D. Firepower Threat Defense

Answer: B

Explanation:
With Cisco pxGrid (Platform Exchange Grid), your multiple security products can now share data and work together. This open, scalable, and IETF standards-driven platform helps you automate security to get answers and contain threats faster.

NEW QUESTION 112
- (Exam Topic 1)
Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

A. Nexus
B. Stealthwatch
C. Firepower
D. Tetration

Answer: D

NEW QUESTION 115
- (Exam Topic 1)
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:

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to

write the data to the buffer overwrites adjacent memory locations.
Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's alloted memory space. This happens quite frequently in the case of arrays.

NEW QUESTION 116
- (Exam Topic 1)
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:
The profiling service issues the change of authorization in the following cases:– Endpoint deleted—When an endpoint is deleted from the Endpoints page and the endpoint is disconnectedor removed from the network.An exception action is configured—If you have an exception action configured per profile that leads to anunusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to thecorresponding static profile by issuing a CoA.– An endpoint is profiled for the first time—When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.+ An endpoint identity group has changed—When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide

NEW QUESTION 118
- (Exam Topic 1)
Refer to the exhibit.

```
def add_device_to_dnac(dnac_ip, device_ip, snmp_version,
    snmp_ro_community, snmp_rw_community,
    snmp_retry, snmp_timeout,
    cli_transport, username, password, enable_password):
    device_object = {
        'ipAddress': [
            device_ip
        ],
       'type': 'NETWORK_DEVICE',
        'computeDevice': False,
        'snmpVersion': snmp_version,
        'snmpROCommunity': snmp_ro_community,
        'snmpRWCommunity': snmp_rw_community,
        'snmpRetry': snmp_retry,
        'snmpTimeout': snmp_timeout,
        'cliTransport': cli_transport,
        'userName': username,
        'password': password,
        'enablePassword': enable_password
    }
    response = requests.post(
        'https://{}/dna/intent/api/v1/network-
device'.format(dnac_ip),
        data=json.dumps(device_object),
        headers={
            'X-Auth-Token': '{}'.format(token),
      "      'Content-type': 'application/json'
        },
        verify=False
    )
    return response.json()
```

What is the result of this Python script of the Cisco DNA Center API?

A. adds authentication to a switch
B. adds a switch to Cisco DNA Center
C. receives information about a switch
D. deletes a switch from Cisco DNA Center

Answer: B

NEW QUESTION 123
- (Exam Topic 1)
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:

TAXII (Trusted Automated Exchange of Indicator Information) is a standard that provides a transport

NEW QUESTION 126
- (Exam Topic 1)
Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware? (Choose two)

A. Sophos engine
B. white list
C. RAT
D. outbreak filters
E. DLP

Answer: AD

NEW QUESTION 130
- (Exam Topic 1)
Which command enables 802.1X globally on a Cisco switch?

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

Answer: A

NEW QUESTION 133
- (Exam Topic 1)
Which threat involves software being used to gain unauthorized access to a computer system?

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

Answer: A

NEW QUESTION 136
- (Exam Topic 1)
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

NEW QUESTION 140
- (Exam Topic 1)
Refer to the exhibit.

```
HQ_Router(config)#username admin5 privilege 5
HQ_Router(config)#privilege interface level 5
shutdown
HQ_Router(config)#privilege interface level 5 ip
HQ_Router(config)#privilege interface level 5
description
```

A network administrator configures command authorization for the admin5 user. What is the admin5 user able to do on HQ_Router after this configuration?

A. set the IP address of an interface
B. complete no configurations
C. complete all configurations
D. add subinterfaces

Answer: B

Explanation:

The user “admin5” was configured with privilege level 5. In order to allow configuration (enter globalconfiguration mode), we must type this command:(config)#privilege exec level 5 configure terminalWithout this command, this user cannot do any configuration.Note: Cisco IOS supports privilege levels from 0 to 15, but the privilege levels which are used by default are privilege level 1 (user EXEC) and level privilege 15 (privilege EXEC)

NEW QUESTION 145
- (Exam Topic 1)
Which Cisco security solution protects remote users against phishing attacks when they are not connected to the VPN?

A. Cisco Stealthwatch
B. Cisco Umbrella
C. Cisco Firepower
D. NGIPS

Answer: B

Explanation:
Cisco Umbrella protects users from accessing malicious domains by proactively analyzing and blocking unsafe destinations – before a connection is ever made. Thus it can protect from phishing attacks by blocking suspicious domains when users click on the given links that an attacker sent. Cisco Umbrella roaming protects your employees even when they are off the VPN.

NEW QUESTION 150
- (Exam Topic 1)
Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application traffic?

A. Cisco Security Intelligence
B. Cisco Application Visibility and Control
C. Cisco Model Driven Telemetry
D. Cisco DNA Center

Answer: B

Explanation:

Reference:
https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/guide/avc-user-guide/avc_tech_overview.html

NEW QUESTION 155
- (Exam Topic 1)
How is Cisco Umbrella configured to log only security events?

A. per policy
B. in the Reporting settings
C. in the Security Settings section
D. per network in the Deployments section

Answer: A

Explanation:
Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management

NEW QUESTION 158
- (Exam Topic 1)
Which API is used for Content Security?

A. NX-OS API
B. IOS XR API
C. OpenVuln API
D. AsyncOS API

Answer: D

NEW QUESTION 160
- (Exam Topic 1)
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:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/ security-overview.html

NEW QUESTION 161
- (Exam Topic 1)
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:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.html

NEW QUESTION 166
- (Exam Topic 1)
What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two)

A. data exfiltration
B. command and control communication
C. intelligent proxy
D. snort
E. URL categorization

Answer: AB

Explanation:
Reference:
https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-aglance-c45-73655

NEW QUESTION 169
- (Exam Topic 1)
How does Cisco Stealthwatch Cloud provide security for cloud environments?

A. It delivers visibility and threat detection.
B. It prevents exfiltration of sensitive data.
C. It assigns Internet-based DNS protection for clients and servers.
D. It facilitates secure connectivity between public and private networks.

Answer: A

Explanation:
Cisco Stealthwatch Cloud: Available as an SaaS product offer to provide visibility and threat detection within public cloud infrastructures such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

NEW QUESTION 173
- (Exam Topic 1)
Which type of attack is social engineering?

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

Answer: B

Explanation:
Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to
solicit personal,often financial, information. Attackers may send email seemingly from a reputable credit card company orfinancial institution that requests account information, often suggesting that there is a problem.

NEW QUESTION 178
- (Exam Topic 1)
How many interfaces per bridge group does an ASA bridge group deployment support?

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

Answer: B

Explanation:
Each of the ASAs interfaces need to be grouped into one or more bridge groups. Each of these groups acts as an independent transparent firewall. It is not possible for one bridge group to communicate with another bridge group without assistance from an external router.As of 8.4(1) upto 8 bridge groups are supported with 2-4 interface in each group. Prior to this only one bridge group was supported and only 2 interfaces.Up to 4 interfaces are permitted per bridge–group (inside, outside, DMZ1, DMZ2)

NEW QUESTION 180
- (Exam Topic 1)
Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?

A. TLSv1.2
B. TLSv1.1
C. BJTLSv1
D. DTLSv1

Answer: D

Explanation:
DTLS is used for delay sensitive applications (voice and video) as its UDP based while TLS is TCP based.Therefore DTLS offers strongest throughput performance. The throughput of DTLS at the time of AnyConnect connection can be expected to have processing performance close to VPN throughput.

NEW QUESTION 181
- (Exam Topic 1)
Which feature requires a network discovery policy on the Cisco Firepower Next Generation Intrusion Prevention System?

A. Security Intelligence
B. Impact Flags
C. Health Monitoring
D. URL Filtering

Answer: B

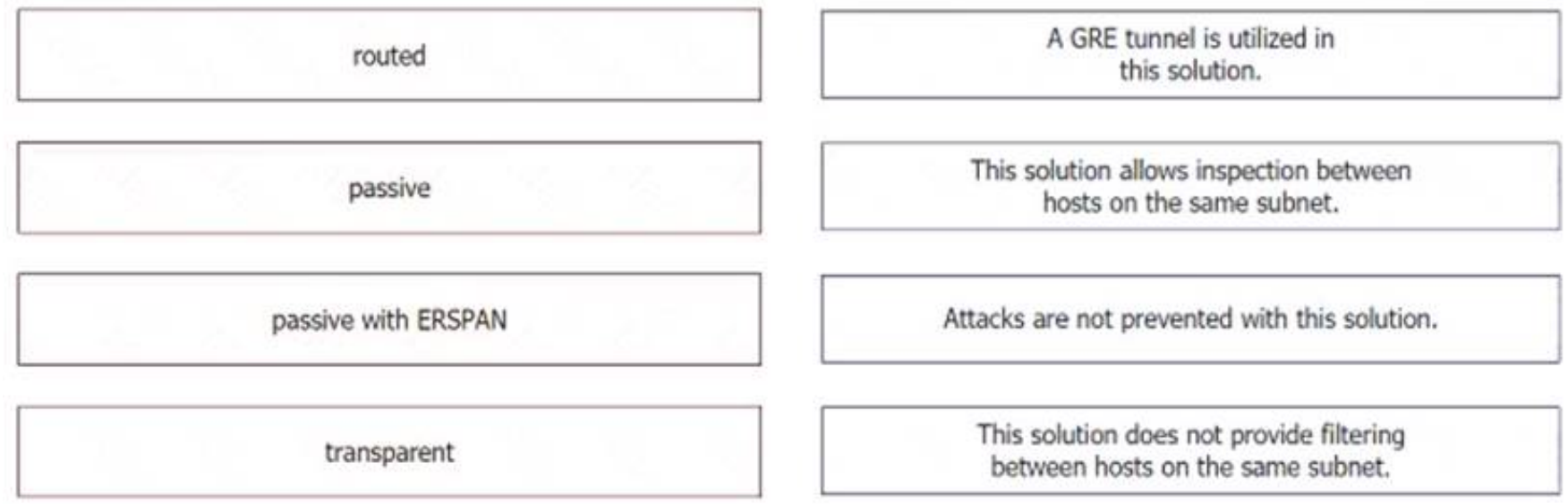
NEW QUESTION 185
- (Exam Topic 1)
Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two)

A. DDoS
B. antispam
C. antivirus
D. encryption
E. DLP

Answer: DE

Explanation:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security

NEW QUESTION 190
- (Exam Topic 3)
Drag and drop the deployment models from the left onto the explanations on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 193
- (Exam Topic 3)
During a recent security audit a Cisco IOS router with a working IPSEC configuration using IKEv1 was flagged for using a wildcard mask with the crypto isakmp key command The VPN peer is a SOHO router with a dynamically assigned IP address Dynamic DNS has been configured on the SOHO router to map the dynamic IP address to the host name of vpn sohoroutercompany.com In addition to the command crypto isakmp key Cisc425007536 hostname vpn.sohoroutercompany.com what other two commands are now required on the Cisco IOS router for the VPN to continue to function after the wildcard command is removed? (Choose two)

A. ip host vpn.sohoroutercompany.eom <VPN Peer IP Address>
B. crypto isakmp identity hostname
C. Add the dynamic keyword to the existing crypto map command
D. fqdn vpn.sohoroutercompany.com <VPN Peer IP Address>
E. ip name-server <DNS Server IP Address>

Answer: BC

NEW QUESTION 197
- (Exam Topic 3)
Which Cisco security solution integrates with cloud applications like Dropbox and Office 365 while protecting data from being exfiltrated?

A. Cisco Tajos
B. Cisco Steaithwatch Cloud
C. Cisco Cloudlock
D. Cisco Umbrella Investigate

Answer: C

NEW QUESTION 202
- (Exam Topic 3)
Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)

A. It must include the current date.
B. It must reside in the trusted store of the WSA.
C. It must reside in the trusted store of the endpoint.
D. It must have been signed by an internal CA.
E. it must contain a SAN.

Answer: AB

NEW QUESTION 203
- (Exam Topic 3)
How does Cisco Workload Optimization Manager help mitigate application performance issues?

A. It deploys an AWS Lambda system
B. It automates resource resizing
C. It optimizes a flow path
D. It sets up a workload forensic score

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-o

NEW QUESTION 207
- (Exam Topic 3)
Which solution stops unauthorized access to the system if a user's password is compromised?

A. VPN

B. MFA
C. AMP
D. SSL

Answer: B

NEW QUESTION 212
- (Exam Topic 3)
An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users. Which action accomplishes this goal?

A. Restrict access to only websites with trusted third-party signed certificates.
B. Modify the user's browser settings to suppress errors from Cisco Umbrella.
C. Upload the organization root CA to Cisco Umbrella.
D. Install the Cisco Umbrella root CA onto the user's device.

Answer: D

NEW QUESTION 216
- (Exam Topic 3)
What are two functionalities of SDN Northbound APIs? (Choose two.)

A. Northbound APIs provide a programmable interface for applications to dynamically configure the network.
B. Northbound APIs form the interface between the SDN controller and business applications.
C. OpenFlow is a standardized northbound API protocol.
D. Northbound APIs use the NETCONF protocol to communicate with applications.
E. Northbound APIs form the interface between the SDN controller and the network switches or routers.

Answer: AB

NEW QUESTION 217
- (Exam Topic 3)
An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1 1 11 using the flow record Stea!thwatch406397954 command Which additional command is required to complete the flow record?

A. transport udp 2055
B. match ipv4 ttl
C. cache timeout active 60
D. destination 1.1.1.1

Answer: B

NEW QUESTION 222
- (Exam Topic 3)
Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'
```

What does the API key do while working with https://api.amp.cisco.com/v1/computers?

A. displays client ID
B. HTTP authorization
C. Imports requests
D. HTTP authentication

Answer: D

NEW QUESTION 227
- (Exam Topic 3)
A customer has various external HTTP resources available including Intranet. Extranet, and Internet, with a proxy configuration running in explicit mode Which method allows the client desktop browsers to be configured to select when to connect direct or when to use the proxy?

A. Transparent mode
B. Forward file
C. PAC file
D. Bridge mode

Answer: C

NEW QUESTION 228
- (Exam Topic 3)
When a transparent authentication fails on the Web Security Appliance, which type of access does the end user get?

A. guest
B. limited Internet
C. blocked
D. full Internet

Answer: C

NEW QUESTION 229
- (Exam Topic 3)
An engineer is deploying Cisco Advanced Malware Protection (AMP) for Endpoints and wants to create a policy that prevents users from executing file named abc424952615.exe without quarantining that file What type of Outbreak Control list must the SHA.-256 hash value for the file be added to in order to accomplish this?

A. Advanced Custom Detection
B. Blocked Application
C. Isolation
D. Simple Custom Detection

Answer: B

NEW QUESTION 231
- (Exam Topic 3)
An engineer has been tasked with configuring a Cisco FTD to analyze protocol fields and detect anomalies in the traffic from industrial systems. What must be done to meet these requirements?

A. Implement pre-filter policies for the CIP preprocessor
B. Enable traffic analysis in the Cisco FTD
C. Configure intrusion rules for the DNP3 preprocessor
D. Modify the access control policy to trust the industrial traffic

Answer: C

Explanation:
"configure INTRUSION RULES for DNP3" -> Documentation states, that enabling INTRUSION RULES is mandatory for CIP to work + required preprocessors (in Network Access Policy - NAP) will be enabled automatically:
"If you want the CIP preprocessor rules listed in the following table to generate events, you MUST enable them. See Setting Intrusion Rule States for information on enabling rules."
"If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings, although the preprocessor remains disabled in the web interface for the corresponding network analysis policy."
[1]
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada

NEW QUESTION 232
- (Exam Topic 3)
Which cloud service offering allows customers to access a web application that is being hosted, managed, and maintained by a cloud service provider?

A. IaC
B. SaaS
C. IaaS
D. PaaS

Answer: B

NEW QUESTION 233
- (Exam Topic 3)
Which technology provides a combination of endpoint protection endpoint detection, and response?

A. Cisco AMP
B. Cisco Talos
C. Cisco Threat Grid
D. Cisco Umbrella

Answer: A

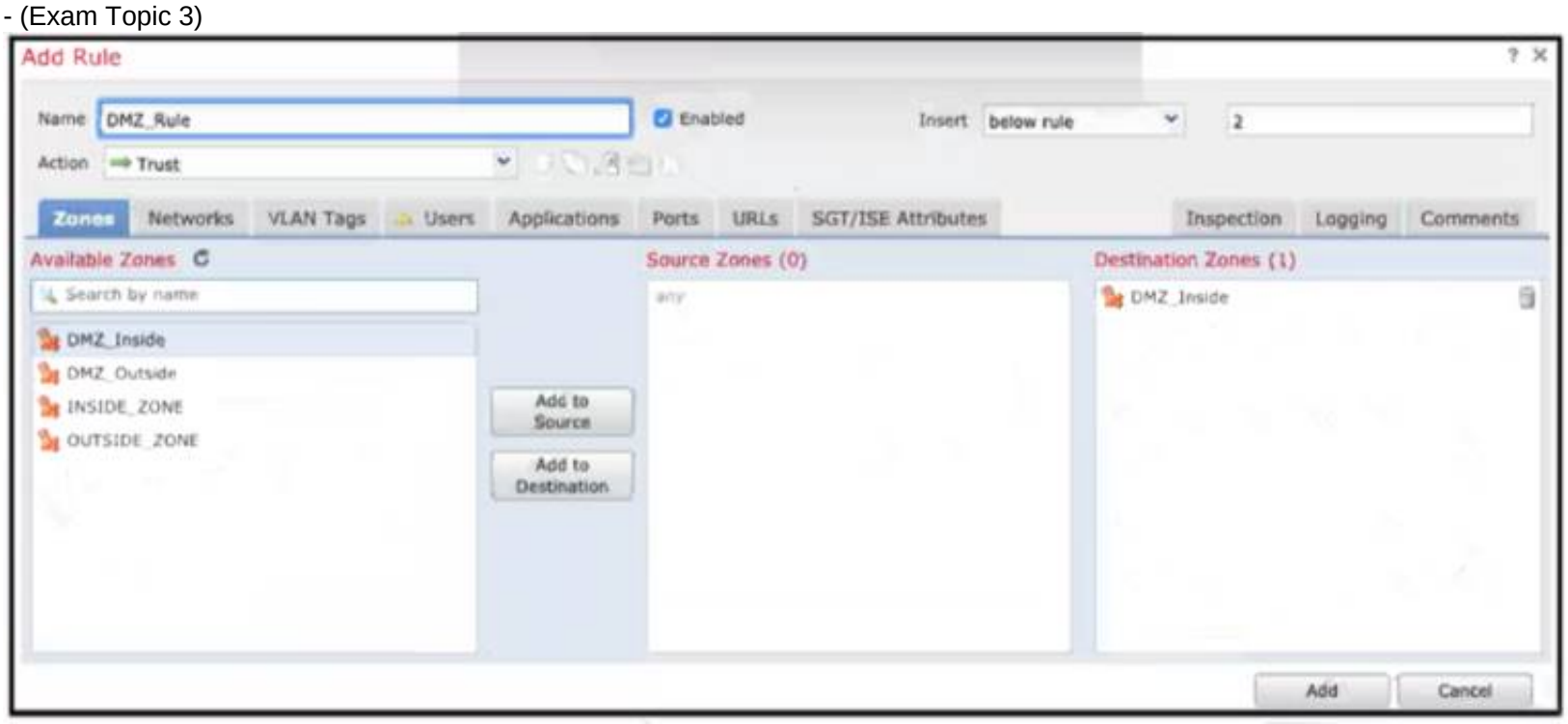
NEW QUESTION 235
- (Exam Topic 3)
A company discovered an attack propagating through their network via a file. A custom file policy was created in order to track this in the future and ensure no other endpoints execute the infected file. In addition, it was discovered during testing that the scans are not detecting the file as an indicator of compromise. What must be done in order to ensure that the 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

NEW QUESTION 239
- (Exam Topic 3)



Refer to the exhibit When configuring this access control rule in Cisco FMC, what happens with the traffic destined to the DMZjnside zone once the configuration is deployed?

A. All traffic from any zone to the DMZ_inside zone will be permitted with no further inspection
B. No traffic will be allowed through to the DMZ_inside zone regardless of if it's trusted or not
C. All traffic from any zone will be allowed to the DMZ_inside zone only after inspection
D. No traffic will be allowed through to the DMZ_inside zone unless it's already trusted

Answer: A

NEW QUESTION 243
- (Exam Topic 3)
Which solution is more secure than the traditional use of a username and password and encompasses at least two of the methods of authentication?

A. single-sign on
B. RADIUS/LDAP authentication
C. Kerberos security solution
D. multifactor authentication

Answer: D

NEW QUESTION 248
- (Exam Topic 3)
An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices. The default management port conflicts with other communications on the network and must be changed. What must be done to ensure that all devices can communicate together?

A. Manually change the management port on Cisco FMC and all managed Cisco FTD devices
B. Set the tunnel to go through the Cisco FTD
C. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices
D. Set the tunnel port to 8305

Answer: A

Explanation:
The FMC and managed devices communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305.Cisco strongly recommends that you keep the default settings for the remote management port, but if themanagement port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate with each other.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmtnw.html

NEW QUESTION 252
- (Exam Topic 3)
What does Cisco ISE use to collect endpoint attributes that are used in profiling?

A. probes
B. posture assessment
C. Cisco AnyConnect Secure Mobility Client
D. Cisco pxGrid

Answer: A

Explanation:
Reference:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/2-6/admin_guide

NEW QUESTION 254
- (Exam Topic 3)
Which security solution uses NetFlow to provide visibility across the network, data center, branch offices, and cloud?

A. Cisco CTA
B. Cisco Stealthwatch
C. Cisco Encrypted Traffic Analytics
D. Cisco Umbrella

Answer: B

NEW QUESTION 256
- (Exam Topic 3)
Which two components do southbound APIs use to communicate with downstream devices? (Choose two.)

A. services running over the network
B. OpenFlow
C. external application APIs
D. applications running over the network
E. OpFlex

Answer: BE

NEW QUESTION 261
- (Exam Topic 3)
A network engineer is tasked with configuring a Cisco ISE server to implement external authentication against Active Directory. What must be considered about the authentication requirements? (Choose two.)

A. RADIUS communication must be permitted between the ISE server and the domain controller.
B. The ISE account must be a domain administrator in Active Directory to perform JOIN operations.
C. Active Directory only supports user authentication by using MSCHAPv2.
D. LDAP communication must be permitted between the ISE server and the domain controller.
E. Active Directory supports user and machine authentication by using MSCHAPv2.

Answer: BC

NEW QUESTION 265
- (Exam Topic 3)
Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks? (Choose two.)

A. blocks malicious websites and adds them to a block list
B. does a real-time user web browsing behavior analysis
C. provides a defense for on-premises email deployments
D. uses a static algorithm to determine malicious
E. determines if the email messages are malicious

Answer: CE

NEW QUESTION 267
- (Exam Topic 3)
Which Cisco cloud security software centrally manages policies on multiple platforms such as Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS?

A. Cisco Defense Orchestrator
B. Cisco Configuration Professional
C. Cisco Secureworks
D. Cisco DNAC

Answer: A

NEW QUESTION 269
- (Exam Topic 3)
An engineer needs to configure a Cisco Secure Email Gateway (SEG) to prompt users to enter multiple forms of identification before gaining access to the SEG. The SEG must also join a cluster using the preshared key of cisc421555367. What steps must be taken to support this?

A. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG GUI.
B. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG CLI.
C. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG CLI
D. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG GUI.

Answer: C

Explanation:

Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA

NEW QUESTION 274
- (Exam Topic 3)
Which two parameters are used to prevent a data breach in the cloud? (Choose two.)

A. DLP solutions
B. strong user authentication
C. encryption
D. complex cloud-based web proxies
E. antispoofing programs

Answer: AB

NEW QUESTION 276
- (Exam Topic 3)
An engineer is adding a Cisco DUO solution to the current TACACS+ deployment using Cisco ISE. The engineer wants to authenticate users using their account when they log into network devices. Which action accomplishes this task?

A. Configure Cisco DUO with the external Active Directory connector and tie it to the policy set within Cisco ISE.
B. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE
C. Create an identity policy within Cisco ISE to send all authentication requests to Cisco DUO.
D. Modify the current policy with the condition MFASourceSequence DUO=true in the authorization conditions within Cisco ISE

Answer: B

NEW QUESTION 277
- (Exam Topic 3)
Which solution supports high availability in routed or transparent mode as well as in northbound and southbound deployments?

A. Cisco FTD with Cisco ASDM
B. Cisco FTD with Cisco FMC
C. Cisco Firepower NGFW physical appliance with Cisc
D. FMC
E. Cisco Firepower NGFW Virtual appliance with Cisco FMC

Answer: B

NEW QUESTION 279
- (Exam Topic 3)
Which metric is used by the monitoring agent to collect and output packet loss and jitter information?

A. WSAv performance
B. AVC performance
C. OTCP performance
D. RTP performance

Answer: D

NEW QUESTION 280
- (Exam Topic 3)
Which Cisco security solution stops exfiltration using HTTPS?

A. Cisco FTD
B. Cisco AnyConnect
C. Cisco CTA
D. Cisco ASA

Answer: C

Explanation:
https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-7365

NEW QUESTION 283
- (Exam Topic 3)
Which two actions does the Cisco Identity Services Engine posture module provide that ensures endpoint security? (Choose two.)

A. Assignments to endpoint groups are made dynamically, based on endpoint attributes.
B. Endpoint supplicant configuration is deployed.
C. A centralized management solution is deployed.
D. Patch management remediation is performed.
E. The latest antivirus updates are applied before access is allowed.

Answer: AD

NEW QUESTION 287
- (Exam Topic 3)
DoS attacks are categorized as what?

A. phishing attacks
B. flood attacks
C. virus attacks
D. trojan attacks

Answer: B

NEW QUESTION 292
- (Exam Topic 3)
Which type of data exfiltration technique encodes data in outbound DNS requests to specific servers and can be stopped by Cisco Umbrella?

A. DNS tunneling
B. DNS flood attack
C. cache poisoning
D. DNS hijacking

Answer: A

NEW QUESTION 293
- (Exam Topic 3)
What are two facts about WSA HTTP proxy configuration with a PAC file? (Choose two.)

A. It is defined as a Transparent proxy deployment.
B. In a dual-NIC configuration, the PAC file directs traffic through the two NICs to the proxy.
C. The PAC file, which references the proxy, is deployed to the client web browser.
D. It is defined as an Explicit proxy deployment.
E. It is defined as a Bridge proxy deployment.

Answer: CD

NEW QUESTION 297
- (Exam Topic 3)
Which DevSecOps implementation process gives a weekly or daily update instead of monthly or quarterly in the applications?

A. Orchestration
B. CI/CD pipeline
C. Container
D. Security

Answer: B

Explanation:
Reference: https://devops.com/how-to-implement-an-effective-ci-cd-pipeline/

NEW QUESTION 302
- (Exam Topic 3)
Which Cisco security solution provides patch management in the cloud?

A. Cisco Umbrella
B. Cisco ISE
C. Cisco CloudLock
D. Cisco Tetration

Answer: C

NEW QUESTION 303
- (Exam Topic 3)
What is a difference between GETVPN and IPsec?

A. GETVPN reduces latency and provides encryption over MPLS without the use of a central hub
B. GETVPN provides key management and security association management
C. GETVPN is based on IKEv2 and does not support IKEv1
D. GETVPN is used to build a VPN network with multiple sites without having to statically configure all devices

Answer: C

NEW QUESTION 308
- (Exam Topic 3)
An engineer is configuring IPsec VPN and needs an authentication protocol that is reliable and supports ACK and sequence. Which protocol accomplishes this goal?

A. AES-192

B. IKEv1
C. AES-256
D. ESP

Answer: D

NEW QUESTION 312
- (Exam Topic 3)
An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems. Why should the organization select either Platform as a Service or Infrastructure as a Service for this environment?

A. Platform as a Service because the customer manages the operating system
B. Infrastructure as a Service because the customer manages the operating system
C. Platform as a Service because the service provider manages the operating system
D. Infrastructure as a Service because the service provider manages the operating system

Answer: C

NEW QUESTION 317
- (Exam Topic 3)
A customer has various external HTTP resources available including Intranet Extranet and Internet, with a proxy configuration running in explicit mode. Which method allows the client desktop browsers to be
Configured to select when to connect direct or when to use the proxy?

A. Transport mode
B. Forward file
C. PAC file
D. Bridge mode

Answer: C

Explanation:
A Proxy Auto-Configuration (PAC) file is a JavaScript function definition that determines whether web browserrequests (HTTP, HTTPS, and FTP) go direct to the destination or are forwarded to a web proxy server.PAC files are used to support explicit proxy deployments in which client browsers are explicitly configured tosend traffic to the web proxy. The big advantage of PAC files is that they are usually relatively easy to createand maintain.

NEW QUESTION 322
- (Exam Topic 3)
An engineer needs to detect and quarantine a file named abc424400664 zip based on the MD5 signature of the file using the Outbreak Control list feature within Cisco Advanced Malware Protection (AMP) for Endpoints The configured detection method must work on files of unknown disposition Which Outbreak Control list must be configured to provide this?

A. Blocked Application
B. Simple Custom Detection
C. Advanced Custom Detection
D. Android Custom Detection

Answer: C

NEW QUESTION 324
- (Exam Topic 3)
An engineer is configuring Cisco WSA and needs to deploy it in transparent mode. Which configuration component must be used to accomplish this goal?

A. MDA on the router
B. PBR on Cisco WSA
C. WCCP on switch
D. DNS resolution on Cisco WSA

Answer: C

NEW QUESTION 329
- (Exam Topic 3)
What is the target in a phishing attack?

A. perimeter firewall
B. IPS
C. web server
D. endpoint

Answer: D

NEW QUESTION 332
- (Exam Topic 3)
Which action must be taken in the AMP for Endpoints console to detect specific MD5 signatures on endpoints and then quarantine the files?

A. Configure an advanced custom detection list.
B. Configure an IP Block & Allow custom detection list

C. Configure an application custom detection list
D. Configure a simple custom detection list

Answer: A

NEW QUESTION 337
- (Exam Topic 3)
How is data sent out to the attacker during a DNS tunneling attack?

A. as part of the UDP/53 packet payload
B. as part of the domain name
C. as part of the TCP/53 packet header
D. as part of the DNS response packet

Answer: A

NEW QUESTION 342
- (Exam Topic 3)
Which standard is used to automate exchanging cyber threat information?

A. TAXII
B. MITRE
C. IoC
D. STIX

Answer: A

NEW QUESTION 347
- (Exam Topic 3)
Drag and drop the exploits from the left onto the type of security vulnerability on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 349
- (Exam Topic 3)

A company recently discovered an attack propagating throughout their Windows network via a file named abc428565580xyz exe The malicious file was uploaded to a Simple Custom Detection list in the AMP for Endpoints Portal and the currently applied policy for the Windows clients was updated to reference the detection list Verification testing scans on known infected systems shows that AMP for Endpoints is not detecting the presence of this file as an indicator of compromise What must be performed to ensure detection of the malicious file?

A. Upload the malicious file to the Blocked Application Control List
B. Use an Advanced Custom Detection List instead of a Simple Custom Detection List
C. Check the box in the policy configuration to send the file to Cisco Threat Grid for dynamic analysis
D. Upload the SHA-256 hash for the file to the Simple Custom Detection List

Answer: D

NEW QUESTION 353
- (Exam Topic 3)
What is a feature of container orchestration?

A. ability to deploy Amazon ECS clusters by using the Cisco Container Platform data plane
B. ability to deploy Amazon EKS clusters by using the Cisco Container Platform data plane
C. ability to deploy Kubernetes clusters in air-gapped sites
D. automated daily updates

Answer: C

NEW QUESTION 356
- (Exam Topic 3)
Which IETF attribute is supported for the RADIUS CoA feature?

A. 24 State
B. 30 Calling-Station-ID
C. 42 Acct-Session-ID
D. 81 Message-Authenticator

Answer: A

NEW QUESTION 358
- (Exam Topic 3)
Which type of attack is MFA an effective deterrent for?

A. ping of death
B. phishing
C. teardrop
D. syn flood

Answer: B

NEW QUESTION 362
- (Exam Topic 3)
What is the purpose of the Cisco Endpoint IoC feature?

A. It provides stealth threat prevention.
B. lt is a signature-based engine.
C. lt is an incident response tool
D. It provides precompromise detection.

Answer: C

Explanation:
https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Secure_Mana

NEW QUESTION 364
- (Exam Topic 3)
Which security solution is used for posture assessment of the endpoints in a BYOD solution?

A. Cisco FTD
B. Cisco ASA
C. Cisco Umbrella
D. Cisco ISE

Answer: D

NEW QUESTION 366
- (Exam Topic 3)
Which two commands are required when configuring a flow-export action on a Cisco ASA? (Choose two.)

A. flow-export event-type
B. policy-map
C. access-list

D. flow-export template timeout-rate 15
E. access-group

Answer: AB

NEW QUESTION 367
- (Exam Topic 3)
What is a difference between a DoS attack and a DDoS attack?

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

Answer: A

NEW QUESTION 369
- (Exam Topic 3)
An engineer needs to add protection for data in transit and have headers in the email message Which configuration is needed to accomplish this goal?

A. Provision the email appliance
B. Deploy an encryption appliance.
C. Map sender !P addresses to a host interface.
D. Enable flagged message handling

Answer: D

NEW QUESTION 372
- (Exam Topic 3)
Which VMware platform does Cisco ACI integrate with to provide enhanced visibility, provide policy integration and deployment, and implement security policies with access lists?

A. VMware APIC
B. VMwarevRealize
C. VMware fusion
D. VMware horizons

Answer: B

NEW QUESTION 375
- (Exam Topic 3)
Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)

A. Cisco Umbrella
B. Cisco ISE
C. Cisco DNA Center
D. Cisco TrustSec
E. Cisco Duo Security

Answer: AE

NEW QUESTION 376
- (Exam Topic 3)
Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

A. OpenC2
B. OpenlOC
C. CybOX
D. STIX

Answer: D

NEW QUESTION 378
- (Exam Topic 3)
Which API method and required attribute are used to add a device into Cisco DNA Center with the native API?

A. GET and serialNumber
B. userSudiSerlalNos and deviceInfo
C. POST and name
D. lastSyncTime and pid

Answer: A

NEW QUESTION 383
- (Exam Topic 3)
What is a benefit of flexible NetFlow records?

A. They are used for security
B. They are used for accounting
C. They monitor a packet from Layer 2 to Layer 5
D. They have customized traffic identification

Answer: D

Explanation:
https://confluence.netvizura.com/display/NVUG/Traditional+vs.+Flexible+NetFlow

NEW QUESTION 386
- (Exam Topic 3)
An administrator needs to configure the Cisco ASA via ASDM such that the network management system can actively monitor the host using SNMPv3. Which two tasks must be performed for this configuration? (Choose two.)

A. Specify the SNMP manager and UDP port.
B. Specify an SNMP user group
C. Specify a community string.
D. Add an SNMP USM entry
E. Add an SNMP host access entry

Answer: BE

NEW QUESTION 390
- (Exam Topic 3)
With regard to RFC 5176 compliance, how many IETF attributes are supported by the RADIUS CoA feature?

A. 3
B. 5
C. 10
D. 12

Answer: D

NEW QUESTION 392
- (Exam Topic 3)
What is the most commonly used protocol for network telemetry?

A. SMTP
B. SNMP
C. TFTP
D. NctFlow

Answer: D

NEW QUESTION 395
- (Exam Topic 3)
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 attacks can exist in many different types of applications
B. XSS is a hacking method used to attack SQL databases, whereas SQL injection attacks can exist in many different types of applications
C. SQL injection attacks are used to steal information from databases whereas XSS attacks are used toredirect users to websites where attackers can steal data from them
D. 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

Answer: C

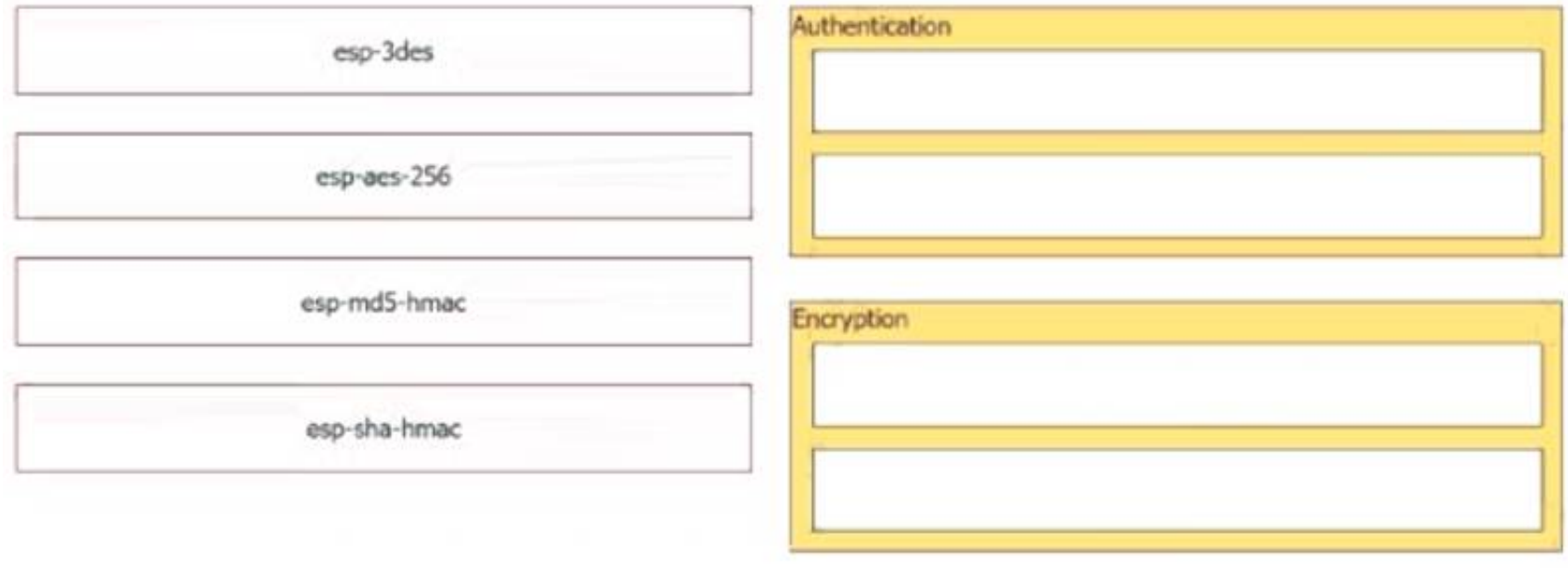
Explanation:
In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites where attackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POST parameters.

NEW QUESTION 396
- (Exam Topic 3)
An engineer musí set up 200 new laptops on a network and wants to prevent the users from moving their laptops around to simplify administration Which switch port MAC address security setting must be used?

A. sticky
B. static
C. aging
D. maximum

Answer: A

NEW QUESTION 399
- (Exam Topic 3)
Drag and drop the cryptographic algorithms for IPsec from the left onto the cryptographic processes on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 403
- (Exam Topic 3)
A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to
ensure that bandwidth is available for VPN users needing access to corporate resources on the10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the
network?

A. Use split tunneling to tunnel traffic for the 10.0.0.0/24 network only.
B. Configure VPN load balancing to distribute traffic for the 10.0.0.0/24 network,
C. Configure VPN load balancing to send non-corporate traffic straight to the internet.
D. Use split tunneling to tunnel all traffic except for the 10.0.0.0/24 network.

Answer: A

NEW QUESTION 404
- (Exam Topic 3)
What is a function of the Layer 4 Traffic Monitor on a Cisco WSA?

A. blocks traffic from URL categories that are known to contain malicious content
B. decrypts SSL traffic to monitor for malicious content
C. monitors suspicious traffic across all the TCP/UDP ports
D. prevents data exfiltration by searching all the network traffic for specified sensitive information

Answer: C

NEW QUESTION 405
- (Exam Topic 3)
What is a characteristic of an EDR solution and not of an EPP solution?

A. stops all ransomware attacks
B. retrospective analysis
C. decrypts SSL traffic for better visibility
D. performs signature-based detection

Answer: B

NEW QUESTION 410
- (Exam Topic 3)
Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using higher-level protocols without readdressing the network?

A. routed mode
B. transparent mode
C. single context mode
D. multiple context mode

Answer: B

NEW QUESTION 414
- (Exam Topic 3)
An engineer is trying to decide whether to use Cisco Umbrella, Cisco CloudLock, Cisco Stealthwatch, or Cisco AppDynamics Cloud Monitoring for visibility into data transfers as well as protection against data exfiltration Which solution best meets these requirements?

A. Cisco CloudLock
B. Cisco AppDynamics Cloud Monitoring
C. Cisco Umbrella
D. Cisco Stealthwatch

Answer: D

NEW QUESTION 415
- (Exam Topic 3)
Which direction do attackers encode data in DNS requests during exfiltration using DNS tunneling?

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

Answer: D

NEW QUESTION 416
- (Exam Topic 3)
A large organization wants to deploy a security appliance in the public cloud to form a site-to-site VPN and link the public cloud environment to the private cloud in the headquarters data center. Which Cisco security appliance meets these requirements?

A. Cisco Cloud Orchestrator
B. Cisco ASAV
C. Cisco WSAV
D. Cisco Stealthwatch Cloud

Answer: B

NEW QUESTION 417
- (Exam Topic 3)
A network engineer must monitor user and device behavior within the on-premises network. This data must be sent to the Cisco Stealthwatch Cloud analytics platform for analysis. What must be done to meet this
requirement using the Ubuntu-based VM appliance deployed in a VMware-based hypervisor?

A. Configure a Cisco FMC to send syslogs to Cisco Stealthwatch Cloud
B. Deploy the Cisco Stealthwatch Cloud PNM sensor that sends data to Cisco Stealthwatch Cloud
C. Deploy a Cisco FTD sensor to send network events to Cisco Stealthwatch Cloud
D. Configure a Cisco FMC to send NetFlow to Cisco Stealthwatch Cloud

Answer: B

Explanation:
Reference:
https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf

NEW QUESTION 418
- (Exam Topic 3)
An engineer is implementing Cisco CES in an existing Microsoft Office 365 environment and must route inbound email to Cisco CE.. record must be modified to accomplish this task?

A. CNAME
B. MX
C. SPF
D. DKIM

Answer: B

NEW QUESTION 421
- (Exam Topic 3)
Which threat intelligence standard contains malware hashes?

A. structured threat information expression
B. advanced persistent threat
C. trusted automated exchange or indicator information
D. open command and control

Answer: A

NEW QUESTION 424
- (Exam Topic 3)
What are two recommended approaches to stop DNS tunneling for data exfiltration and command and control call backs? (Choose two.)

A. Use intrusion prevention system.
B. Block all TXT DNS records.
C. Enforce security over port 53.
D. Use next generation firewalls.
E. Use Cisco Umbrella.

Answer: CE

NEW QUESTION 428
- (Exam Topic 3)
Which type of data does the Cisco Stealthwatch system collect and analyze from routers, switches, and firewalls?

A. NTP
B. syslog
C. SNMP
D. NetFlow

Answer: D

NEW QUESTION 429
- (Exam Topic 3)
Why should organizations migrate to a multifactor authentication strategy?

A. Multifactor authentication methods of authentication are never compromised
B. Biometrics authentication leads to the need for multifactor authentication due to its ability to be hacked easily
C. Multifactor authentication does not require any piece of evidence for an authentication mechanism
D. Single methods of authentication can be compromised more easily than multifactor authentication

Answer: D

NEW QUESTION 431
- (Exam Topic 3)
An engineer integrates Cisco FMC and Cisco ISE using pxGrid Which role is assigned for Cisco FMC?

A. client
B. server
C. controller
D. publisher

Answer: D

NEW QUESTION 433
- (Exam Topic 3)
Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?

A. SDLC
B. Docker
C. Lambda
D. Contiv

Answer: B

NEW QUESTION 437
- (Exam Topic 3)
How does Cisco Workload Optimization portion of the network do EPP solutions solely performance issues?

A. It deploys an AWS Lambda system
B. It automates resource resizing
C. It optimizes a flow path
D. It sets up a workload forensic score

Answer: B

NEW QUESTION 439
- (Exam Topic 3)
What is an advantage of the Cisco Umbrella roaming client?

A. the ability to see all traffic without requiring TLS decryption
B. visibility into IP-based threats by tunneling suspicious IP connections
C. the ability to dynamically categorize traffic to previously uncategorized sites
D. visibility into traffic that is destined to sites within the office environment

Answer: C

NEW QUESTION 441
- (Exam Topic 3)
Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?

A. Cisco Umbrella
B. Cisco AMP for Endpoints
C. Cisco ISE
D. Cisco Stealthwatch

Answer: C

NEW QUESTION 443
- (Exam Topic 3)
What is the recommendation in a zero-trust model before granting access to corporate applications and resources?

A. to use multifactor authentication
B. to use strong passwords
C. to use a wired network, not wireless
D. to disconnect from the network when inactive

Answer: A

NEW QUESTION 447
- (Exam Topic 3)
An organization is implementing AAA for their users. They need to ensure that authorization is verified for every command that is being entered by the network administrator. Which protocol must be configured in order to provide this capability?

A. EAPOL
B. SSH
C. RADIUS
D. TACACS+

Answer: D

NEW QUESTION 452
- (Exam Topic 3)
What are two workload security models? (Choose two.)

A. SaaS
B. PaaS
C. off-premises
D. on-premises
E. IaaS

Answer: CD

NEW QUESTION 455
- (Exam Topic 3)
Which industry standard is used to integrate Cisco ISE and pxGrid to each other and with other interoperable security platforms?

A. IEEE
B. IETF
C. NIST
D. ANSI

Answer: B

NEW QUESTION 460
- (Exam Topic 3)
An organization wants to secure data in a cloud environment. Its security model requires that all users be authenticated and authorized. Security configuration and posture must be continuously validated before access is granted or maintained to applications and data. There is also a need to allow certain application traffic and deny all other traffic by default. Which technology must be used to implement these requirements?

A. Virtual routing and forwarding
B. Microsegmentation
C. Access control policy
D. Virtual LAN

Answer: C

Explanation:
Zero Trust is a security framework requiring all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.The Zero Trust model uses

microsegmentation — a security technique that involves dividing perimeters into small zones to maintain separate access to every part of the network — to contain attacks.

NEW QUESTION 463
- (Exam Topic 3)
What is the intent of a basic SYN flood attack?

A. to solicit DNS responses
B. to exceed the threshold limit of the connection queue
C. to flush the register stack to re-initiate the buffers
D. to cause the buffer to overflow

Answer: B

NEW QUESTION 465
- (Exam Topic 3)
What is the function of the crypto is a kmp key cisc406397954 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel?

A. It defines what data is going to be encrypted via the VPN
B. lt configures the pre-shared authentication key
C. It prevents all IP addresses from connecting to the VPN server.
D. It configures the local address for the VPN server.

Answer: B

NEW QUESTION 468
- (Exam Topic 3)
A network engineer is trying to figure out whether FlexVPN or DMVPN would fit better in their environment. They have a requirement for more stringent security multiple security associations for the connections, more efficient VPN establishment as well consuming less bandwidth. Which solution would be best for this and why?

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

Answer: C

Explanation:
FlexVPN supports IKEv2 -> Answer A is not correct.DMVPN supports both IKEv1 & IKEv2 -> Answer B is not correct.FlexVPN support multiple SAs -> Answer D is not correct.

NEW QUESTION 471
- (Exam Topic 3)
How does Cisco AMP for Endpoints provide next-generation protection?

A. It encrypts data on user endpoints to protect against ransomware.
B. It leverages an endpoint protection platform and endpoint detection and response.
C. It utilizes Cisco pxGrid, which allows Cisco AMP to pull threat feeds from threat intelligence centers.
D. It integrates with Cisco FTD devices.

Answer: B

NEW QUESTION 472
- (Exam Topic 3)
What are two advantages of using Cisco Any connect over DMVPN? (Choose two)

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

Answer: CE

NEW QUESTION 475
- (Exam Topic 3)
Which service allows a user export application usage and performance statistics with Cisco Application Visibility and control?

A. SNORT
B. NetFlow
C. SNMP
D. 802.1X

Answer: B

Explanation:

Application Visibility and control (AVC) supports NetFlow to export application usage and performancestatistics. This data can be used for analytics, billing, and security policies.

NEW QUESTION 477
- (Exam Topic 3)
Which kind of API that is used with Cisco DNA Center provisions SSIDs, QoS policies, and update software versions on switches?

A. Integration
B. Intent
C. Event
D. Multivendor

Answer: B

NEW QUESTION 481
- (Exam Topic 3)
Refer to the exhibit.

```
interface GigabitEthernet1/0/18
 description ISE dot1x Port
 switchport access vlan 41
 switchport mode access
 switchport voice vlan 44
 device-tracking attach-policy IPDT_MAX_10
 authentication periodic
 authentication timer reauthenticate server
 access-session host-mode multi-domain
 access-session port-control auto
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 spanning-tree portfast
 service-policy type control subscriber POLICY_Gi1/0/18
```

What will occur when this device tries to connect to the port?

A. 802.1X will not work, but MAB will start and allow the device on the network.
B. 802.1X will not work and the device will not be allowed network access
C. 802 1X will work and the device will be allowed on the network
D. 802 1X and MAB will both be used and ISE can use policy to determine the access level

Answer: B

NEW QUESTION 485
- (Exam Topic 3)
Which Cisco AMP feature allows an engineer to look back to trace past activities, such as file and process activity on an endpoint?

A. endpoint isolation
B. advanced search
C. advanced investigation
D. retrospective security

Answer: D

NEW QUESTION 486
- (Exam Topic 3)
What is a benefit of using a multifactor authentication strategy?

A. It provides visibility into devices to establish device trust.
B. It provides secure remote access for applications.
C. It provides an easy, single sign-on experience against multiple applications
D. lt protects data by enabling the use of a second validation of identity.

Answer: D

NEW QUESTION 490
- (Exam Topic 3)
An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices The default management port conflicts with other communications on the network and must be changed What must be done to ensure that all devices can communicate together?

A. Set the sftunnel to go through the Cisco FTD
B. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices
C. Set the sftunnel port to 8305.
D. Manually change the management port on Cisco FMC and all managed Cisco FTD devices

Answer: D

NEW QUESTION 491
- (Exam Topic 3)
What is a feature of NetFlow Secure Event Logging?

A. It exports only records that indicate significant events in a flow.
B. It filters NSEL events based on the traffic and event type through RSVP.
C. It delivers data records to NSEL collectors through NetFlow over TCP only.
D. It supports v5 and v8 templates.

Answer: A

NEW QUESTION 495
- (Exam Topic 3)
A network engineer has configured a NTP server on a Cisco ASA. The Cisco ASA has IP reachability to the NTP server and is not filtering any traffic. The show ntp association detail command indicates that the configured NTP server is unsynchronized and has a stratum of 16. What is the cause of this issue?

A. Resynchronization of NTP is not forced
B. NTP is not configured to use a working server.
C. An access list entry for UDP port 123 on the inside interface is missing.
D. An access list entry for UDP port 123 on the outside interface is missing.

Answer: B

NEW QUESTION 497
- (Exam Topic 3)
Which Cisco ISE feature helps to detect missing patches and helps with remediation?

A. posture assessment
B. profiling policy
C. authentication policy
D. enabling probes

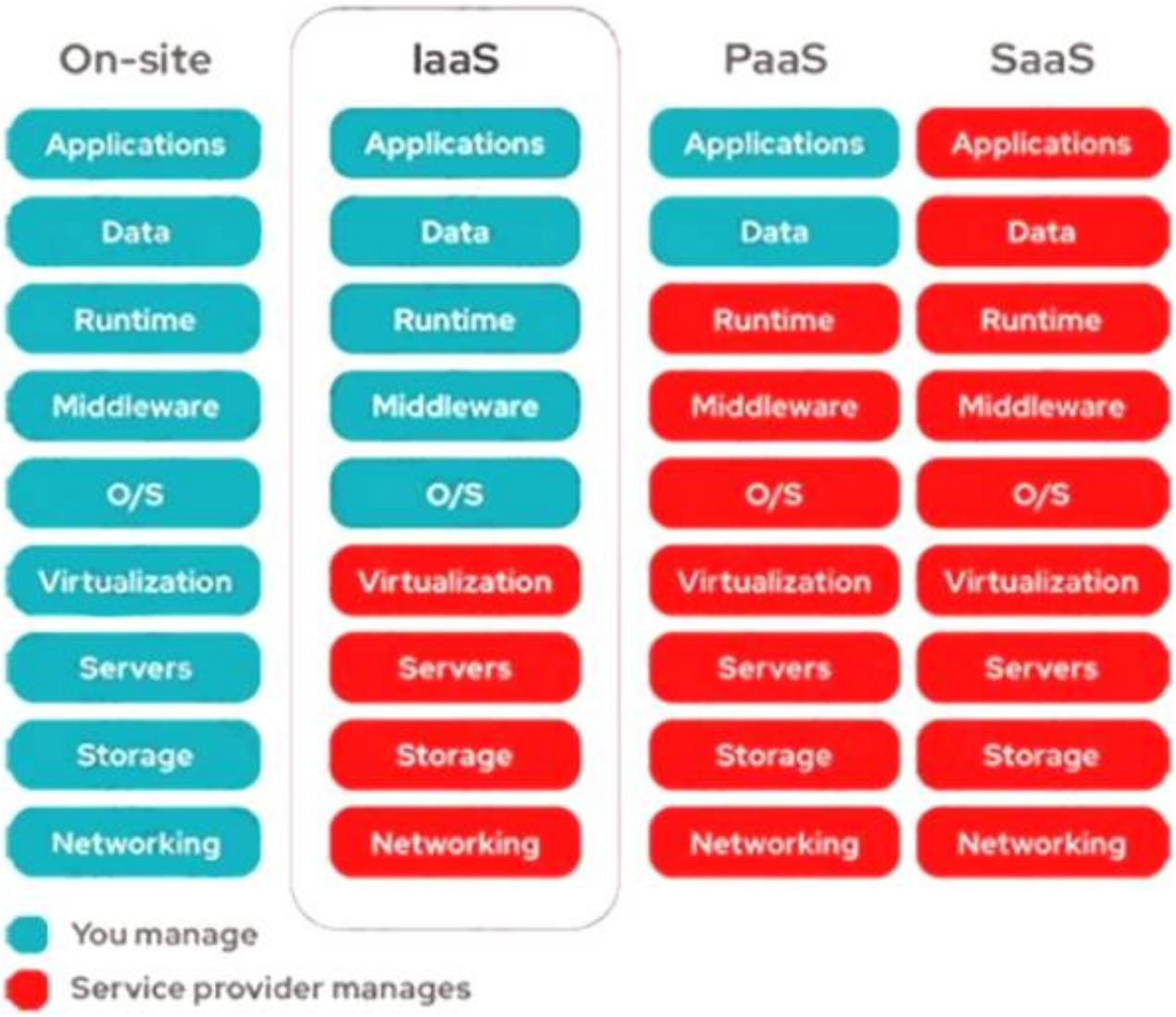
Answer: B

NEW QUESTION 500
- (Exam Topic 2)
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two)

A. virtualization
B. middleware
C. operating systems
D. applications
E. data

Answer: DE

Explanation:
Customers must manage applications and data in PaaS.



NEW QUESTION 503
- (Exam Topic 3)
Which DoS attack uses fragmented packets in an attempt to crash a target machine?

A. teardrop
B. smurf
C. LAND
D. SYN flood

Answer: A

Explanation:
Reference: https://www.radware.com/security/ddos-knowledge-center/ddospedia/teardrop-attack/

NEW QUESTION 506
- (Exam Topic 2)
What is a prerequisite when integrating a Cisco ISE server and an AD domain?

A. Place the Cisco ISE server and the AD server in the same subnet
B. Configure a common administrator account
C. Configure a common DNS server
D. Synchronize the clocks of the Cisco ISE server and the AD server

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_

NEW QUESTION 507
- (Exam Topic 2)
An engineer needs behavioral analysis to detect malicious activity on the hosts, and is configuring the organization's public cloud to send telemetry using the cloud provider's mechanisms to a security device.
Which mechanism should the engineer configure to accomplish this goal?

A. mirror port
B. Flow
C. NetFlow
D. VPC flow logs

Answer: C

NEW QUESTION 512
- (Exam Topic 2)
Which type of dashboard does Cisco DNA Center provide for complete control of the network?

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

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- dna-center-faq-cte-en.html

NEW QUESTION 513
- (Exam Topic 2)
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 uses a non-standard DNS port to gain access to the organization's DNS servers in order to poison the resolutions.
D. An attacker sends an email to the target with hidden DNS resolvers in it to redirect them to a malicious domain.

Answer: A

NEW QUESTION 514
- (Exam Topic 2)
What is a functional difference between a Cisco ASA and a Cisco IOS router with Zone-based policy firewall?

A. The Cisco ASA denies all traffic by default whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces
B. The Cisco IOS router with Zone-Based Policy Firewall can be configured for high availability, whereas the Cisco ASA cannot
C. The Cisco IOS router with Zone-Based Policy Firewall denies all traffic by default, whereas the Cisco ASA starts out by allowing all traffic until rules are added
D. The Cisco ASA can be configured for high availability whereas the Cisco IOS router with Zone-Based Policy Firewall cannot

Answer: A

NEW QUESTION 519
- (Exam Topic 2)
Which attack type attempts to shut down a machine or network so that users are not able to access it?

A. smurf
B. bluesnarfing
C. MAC spoofing
D. IP spoofing

Answer: A

Explanation:
Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to itsintended users.The Smurf attack is a DDoS attack in which large numbers of Internet Control Message Protocol (ICMP)packets with the intended victim's spoofed source IP are broadcast to a computer network using an IPbroadcast address.

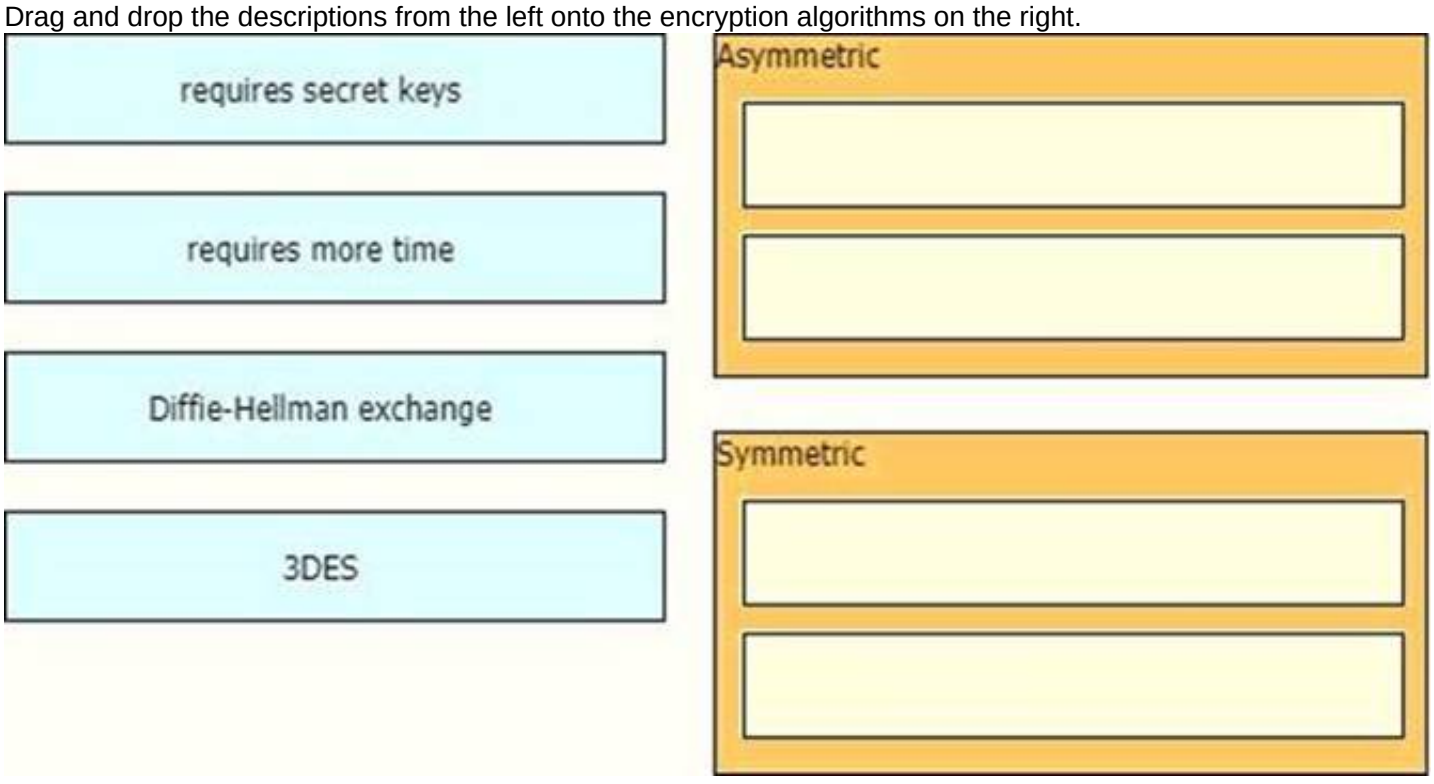
NEW QUESTION 521
- (Exam Topic 2)
What is a capability of Cisco ASA Netflow?

A. It filters NSEL events based on traffic
B. It generates NSEL events even if the MPF is not configured
C. It logs all event types only to the same collector
D. It sends NetFlow data records from active and standby ASAs in an active standby failover pair

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGui Policy Order The order in which policies are listed in a policy table determines the priority with which they are applied to Web requests. Web requests are checked against policies beginning at the top of the table and ending at the first policy matched. Any policies below that point in the table are not processed. If no user-defined policy is matched against a Web request, then the global policy for that policy type is applied. Global policies are always positioned last in Policy tables and cannot be re-ordered.

NEW QUESTION 525
- (Exam Topic 2)
Drag and drop the descriptions from the left onto the encryption algorithms on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetric encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.Asymmetric encryption takes relatively more time than the symmetric encryption.Diffie Hellman algorithm is an asymmetric algorithm used to establish a shared secret for a symmetric keyalgorithm. Nowadays most of the people uses hybrid crypto system i.e, combination of symmetric andasymmetric encryption. Asymmetric Encryption is used as a technique in key exchange mechanism to share secret key and after the key is shared between sender and receiver, the communication will take place using symmetric encryption. The shared secret key will be used to encrypt the communication.Triple DES (3DES), a symmetric-key algorithm for the encryption of electronic data, is the successor of DES (Data Encryption Standard) and provides more secure encryption then DES.Note: Although "requires secret keys" option in this question is a bit unclear but it can only be assigned toSymmetric algorithm.

NEW QUESTION 528
- (Exam Topic 2)

An engineer is implementing NTP authentication within their network and has configured both the client and server devices with the command ntp authentication-key 1 md5 Cisc392368270. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however it is unable to do so. Which command is required to enable the client to accept the server's authentication key?

A. ntp peer 1.1.1.1 key 1
B. ntp server 1.1.1.1 key 1
C. ntp server 1.1.1.2 key 1
D. ntp peer 1.1.1.2 key 1

Answer: B

Explanation:
To configure an NTP enabled router to require authentication when other devices connect to it, use thefollowing commands:NTP_Server(config)#ntp authentication-key 2 md5 securitytutNTP_Server(config)#ntp authenticateNTP_Server(config)#ntp trusted-key 2Then you must configure the same authentication-key on the client router:NTP_Client(config)#ntp authentication-key 2 md5 securitytutNTP_Client(config)#ntp authenticateNTP_Client(config)#ntp trusted-key 2NTP_Client(config)#ntp server 10.10.10.1 key 2Note: To configure a Cisco device as a NTP client, use the command ntp server <IP address>. For example:Router(config)#ntp server 10.10.10.1. This command will instruct the router to query 10.10.10.1 for the time.

NEW QUESTION 532
- (Exam Topic 2)
Which Cisco platform ensures that machines that connect to organizational networks have the recommended antivirus definitions and patches to help prevent an organizational malware outbreak?

A. Cisco WiSM
B. Cisco ESA
C. Cisco ISE
D. Cisco Prime Infrastructure

Answer: C

Explanation:
A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. We can configure ISE to check for the Windows patch at Work Centers > Posture > Posture Elements > Conditions > File.In this example, we are going to use the predefined file check to ensure that our Windows 10 clients have the critical security patch installed to prevent the Wanna Cry malware; and we can also configure ISE to update the client with this patch.

NEW QUESTION 536
- (Exam Topic 2)
What is a benefit of performing device compliance?

A. Verification of the latest OS patches
B. Device classification and authorization
C. Providing multi-factor authentication
D. Providing attribute-driven policies

Answer: A

NEW QUESTION 537
- (Exam Topic 2)
Which type of protection encrypts RSA keys when they are exported and imported?

A. file

B. passphrase
C. NGE
D. nonexportable

Answer: B

NEW QUESTION 539
- (Exam Topic 2)
Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?

A. Encrypted Traffic Analytics
B. Threat Intelligence Director
C. Cognitive Threat Analytics
D. Cisco Talos Intelligence

Answer: B

NEW QUESTION 544
- (Exam Topic 2)
An organization has noticed an increase in malicious content downloads and wants to use Cisco Umbrella to prevent this activity for suspicious domains while allowing normal web traffic. Which action will accomplish this task?

A. Set content settings to High
B. Configure the intelligent proxy.
C. Use destination block lists.
D. Configure application block lists.

Answer: B

Explanation:
Reference: https://docs.umbrella.com/deployment-umbrella/docs/what-is-the-intelligent-proxy

NEW QUESTION 549
- (Exam Topic 2)
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. phishing
B. slowloris
C. pharming
D. SYN flood

Answer: D

NEW QUESTION 554
- (Exam Topic 2)
A Cisco ESA administrator has been tasked with configuring the Cisco ESA to ensure there are no viruses before quarantined emails are delivered. In addition, delivery of mail from known bad mail servers must be prevented. Which two actions must be taken in order to meet these requirements? (Choose two)

A. Use outbreak filters from SenderBase
B. Enable a message tracking service
C. Configure a recipient access table
D. Deploy the Cisco ESA in the DMZ
E. Scan quarantined emails using AntiVirus signatures

Answer: AE

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_A Therefore Outbreak filters can be used to block emails from bad mail servers.Web servers and email gateways are generally located in the DMZ soNote: The recipient access table (RAT), not to be confused with remote-access Trojan (also RAT), is a Cisco ESA term that defines which recipients are accepted by a public listener.

NEW QUESTION 556
- (Exam Topic 2)
An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?

A. Cisco Umbrella
B. Cisco Cloud Email Security
C. Cisco NGFW
D. Cisco Cloudlock

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45- 738565.pdf

NEW QUESTION 557
- (Exam Topic 2)
Which component of Cisco umbrella architecture increases reliability of the service?

A. Anycast IP
B. AMP Threat grid
C. Cisco Talos
D. BGP route reflector

Answer: C

NEW QUESTION 559
- (Exam Topic 2)
An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?

A. Cisco Defense Orchestrator
B. Cisco Secureworks
C. Cisco DNA Center
D. Cisco Configuration Professional

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html

NEW QUESTION 562
- (Exam Topic 2)
Which two cryptographic algorithms are used with IPsec? (Choose two)

A. AES-BAC
B. AES-ABC
C. HMAC-SHA1/SHA2
D. Triple AMC-CBC
E. AES-CBC

Answer: CE

Explanation:
Cryptographic algorithms defined for use with IPsec include:+ HMAC-SHA1/SHA2 for integrity protection and authenticity.+ TripleDES-CBC for confidentiality+ AES-CBC and AES-CTR for confidentiality.+ AES-GCM and ChaCha20-Poly1305 providing confidentiality and authentication together efficiently.

NEW QUESTION 566
- (Exam Topic 2)
What is a key difference between Cisco Firepower and Cisco ASA?

A. Cisco ASA provides access control while Cisco Firepower does not.
B. Cisco Firepower provides identity-based access control while Cisco ASA does not.
C. Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not.
D. Cisco ASA provides SSL inspection while Cisco Firepower does not.

Answer: C

NEW QUESTION 571
- (Exam Topic 2)
Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps.
Which two actions must be taken to ensure that interfaces are put back into service? (Choose two)

A. Have Cisco Prime Infrastructure issue an SNMP set command to re-enable the ports after the pre configured interval.
B. Use EEM to have the ports return to service automatically in less than 300 seconds.
C. Enter the shutdown and no shutdown commands on the interfaces.
D. Enable the snmp-server enable traps command and wait 300 seconds
E. Ensure that interfaces are configured with the error-disable detection and recovery feature

Answer: CE

Explanation:
You can also bring up the port by using these commands:+ The “shutdown” interface configuration command followed by the “no shutdown” interface configurationcommand restarts the disabled port.+ The “errdisable recovery cause …” global configuration command enables the timer to automatically recover error-disabled state, and the “errdisable recovery interval interval” global configuration command specifies the time to recover error-disabled state.

NEW QUESTION 574
- (Exam Topic 2)
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.

privilege escalation	Tetration platform learns the normal behavior of users.
user login suspicious behavior	Tetration platform is armed to look at sensitive files.
interesting file access	Tetration platform watches user access failures and methods
file access from a different user	Tetration platform watches for movement in the process lineage tree.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-7403

NEW QUESTION 577
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

350-701 Practice Exam Features:

* 350-701 Questions and Answers Updated Frequently

* 350-701 Practice Questions Verified by Expert Senior Certified Staff

* 350-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 350-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year