Website: www.VCEplus.io

Twitter: https://twitter.com/VCE_Plus

Exam Code: 350-701
Exam Name: Implementing and Operating Cisco Security Core Technologies

Exam A

QUESTION 1
Which two characteristics of messenger protocols make data exfiltration difficult to detect and prevent?
(Choose two)

A. Outgoing traffic is allowed so users can communicate with outside organizations.

B. Malware infects the messenger application on the user endpoint to send company data.

C. Traffic is encrypted, which prevents visibility on firewalls and IPS systems.

D. An exposed API for the messaging platform is used to send large amounts of data.

E. Messenger applications cannot be segmented with standard network controls

Correct Answer: C, E
Section:

QUESTION 2
Which Cisco AMP file disposition valid?

A. pristine

B. malware

C. dirty

D. non malicious

Correct Answer: B
Section:

QUESTION 3
When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?

A. Spero analysis

B. dynamic analysis

C. sandbox analysis

D. malware analysis

Correct Answer: B
Section:
Explanation:
Spero analysis examines structural characteristics such as metadata and header information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configguidev60/Reference_a_wrapper_Chapter_topic_here.html-> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does notupload thewhole file. Dynamic analysis sends files to AMP ThreatGrid.
Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco Threat Grid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your

organization did not submit.

Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Security

Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources. -> Malware analysis does not upload files to anywhere, it only checks the files locally.

There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in a virtual machine.

QUESTION 4

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

Correct Answer: C
Section:

QUESTION 5
An engineer has enabled LDAP accept queries on a listener. Malicious actors must be prevented from quickly identifying all valid recipients. What must be done on the Cisco ESA to accomplish this goal?

A. Configure incoming content filters
B. Use Bounce Verification
C. Configure Directory Harvest Attack Prevention
D. Bypass LDAP access queries in the recipient access table

Correct Answer: C
Section:
Explanation:
A Directory Harvest Attack (DHA) is a technique used by spammers to find valid/existent email addresses at a domain either by using Brute force or by guessing valid e-mail addresses at a domain using different permutations of common username. Its easy for attackers to get hold of a valid email address if your organization uses standard format for official e-mail alias (for example: jsmith@example.com). We can configure DHA Prevention to prevent malicious actors from quickly identifying valid recipients.
Note: Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email programs use to look up contact information from a server, such as ClickMail Central Directory. For example, here's an LDAP search translated into plain
English: "Search for all people located in Chicago who's name contains "Fred" that have an email address. Please return their full name, email, title, and description.

QUESTION 6
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

Correct Answer: D
Section:

QUESTION 7
Which two configurations must be made on Cisco ISE and on Cisco TrustSec devices to force a session to be adjusted after a policy change is made? (Choose two)

A. posture assessment
B. aaa authorization exec default local
C. tacacs-server host 10.1.1.250 key password

D. aaa server radius dynamic-author

E. CoA

Correct Answer: D, E
Section:

QUESTION 8
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

Correct Answer: C
Section:

QUESTION 9
Which feature is used in a push model to allow for session identification, host reauthentication, and session termination?

A. AAA attributes

B. CoA request

C. AV pair

D. carrier-grade NAT

Correct Answer: B
Section:

QUESTION 10
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

Correct Answer: B
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa- general-cli/ monitor-nsel.pdf ... -- Delays the export of flow-create events. The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions: ... -- Delays the export of flow-create events. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa- general-cli/ monitor-nsel.pdf

QUESTION 11
An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?

A. TCP 6514

B. UDP 1700

C. TCP 49

D. UDP 1812

Correct Answer: B

Section:

Explanation:

CoA Messages are sent on two different udp ports depending on the platform. Cisco standardizes on UDP port 1700, while the actual RFC calls out using UDP port 3799.

QUESTION 12

Which public cloud provider supports the Cisco Next Generation Firewall Virtual?

A. Google Cloud Platform

B. Red Hat Enterprise Visualization

C. VMware ESXi

D. Amazon Web Services

Correct Answer: D

Section:

Explanation:

Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco's Firepower next generation firewall.

The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure.

In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet.

In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions.

Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtualappliance-asav/ white-paper-c11-740505.html

QUESTION 13

What is the purpose of the My Devices Portal in a Cisco ISE environment?

A. to register new laptops and mobile devices

B. to request a newly provisioned mobile device

C. to provision userless and agentless systems

D. to manage and deploy antivirus definitions and patches on systems owned by the end user

Correct Answer: A

Section:

Explanation:

Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network.

Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html

QUESTION 14

Refer to the exhibit.

```
ip dhcp snooping
ip dhcp snooping vlan 41,44
!
interface GigabitEthernet1/0/1
 description Uplink_To_Distro_Switch_g1/0/11
 switchport trunk native vlan 999
 switchport trunk allowed vlan 40,41,44
 switchport mode trunk
```

An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained. Which command should be configured on the switch interface in order to provide the user with network connectivity?

A. ip dhcp snooping verify mac-address

B. ip dhcp snooping limit 41

C. ip dhcp snooping vlan 41

D. ip dhcp snooping trust

Correct Answer: D

Section:

Explanation:

To understand DHCP snooping we need to learn about DHCP spoofing attack first.

DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients.

The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle".

The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.

DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.

Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.

The port connected to a DHCP server should be configured as trusted port with the "ip dhcp snooping trust" command. Other ports connecting to hosts are untrusted ports by default.

In this question, we need to configure the uplink to "trust" (under interface Gi1/0/1) as shown below.

QUESTION 15

Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?

A. cloud web services

B. network AMP

C. private cloud

D. public cloud

Correct Answer: C

Section:

QUESTION 16

Which capability is exclusive to a Cisco AMP public cloud instance as compared to a private cloud instance?

A. RBAC

B. ETHOS detection engine

C. SPERO detection engine

D. TETRA detection engine

Correct Answer: B
Section:

QUESTION 17
An engineer is configuring AMP for endpoints and wants to block certain files from executing. Which outbreak control method is used to accomplish this task?

A. device flow correlation

B. simple detections

C. application blocking list

D. advanced custom detections

Correct Answer: C
Section:

QUESTION 18
Which function is the primary function of Cisco AMP threat Grid?

A. automated email encryption

B. applying a real-time URI blacklist

C. automated malware analysis

D. monitoring network traffic

Correct Answer: C
Section:

QUESTION 19
Which two behavioral patterns characterize a ping of death attack? (Choose two)

A. The attack is fragmented into groups of 16 octets before transmission.

B. The attack is fragmented into groups of 8 octets before transmission.

C. Short synchronized bursts of traffic are used to disrupt TCP connections.

D. Malformed packets are used to crash systems.

E. Publicly accessible DNS servers are typically used to execute the attack.

Correct Answer: B, D
Section:
Explanation:
Ping of Death (PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.
A correctly-formed ping packet is typically 56 bytes in size, or 64 bytes when the ICMP header is considered, and 84 including Internet Protocol version 4 header. However, any IPv4 packet (including pings) may be as large as 65,535 bytes.
Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented Like other large but well-formed packets, a ping of death is fragmented into groups of 8 octets before transmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code.

QUESTION 20
Which two preventive measures are used to control cross-site scripting? (Choose two)

A. Enable client-side scripts on a per-domain basis.

B. Incorporate contextual output encoding/escaping.

C. Disable cookie inspection in the HTML inspection engine.

D. Run untrusted HTML input through an HTML sanitization engine.

E. Same Site cookie attribute should not be used.

Correct Answer: A, B
Section:

QUESTION 21
What is the difference between deceptive phishing and spear phishing?

A. Deceptive phishing is an attacked aimed at a specific user in the organization who holds a C-level role.

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

C. Spear phishing is when the attack is aimed at the C-level executives of an organization.

D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Correct Answer: B
Section:
Explanation:
In deceptive phishing, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.
Spear phishing is carefully designed to get a single recipient to respond. Criminals select an individual target within an organization, using social media and other public information – and craft a fake email tailored for that person.

QUESTION 22
Which attack is commonly associated with C and C++ programming languages?

A. cross-site scripting

B. water holing

C. DDoS

D. buffer overflow

Correct Answer: D
Section:
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.

QUESTION 23
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

Correct Answer: A

Section:

Explanation:

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

QUESTION 24

Which two capabilities does TAXII support? (Choose two)

A. Exchange

B. Pull messaging

C. Binding

D. Correlation

E. Mitigating

Correct Answer: A, B

Section:

Explanation:

QUESTION 25

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

Correct Answer: A, D

Section:

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.

QUESTION 26

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

A. url

B. terminal

C. profile

D. selfsigned

Correct Answer: C
Section:
Explanation:
A trustpoint enrollment mode, which also defines the trustpoint authentication mode, can be performed via 3 main methods:
1. Terminal Enrollment – manual method of performing trustpoint authentication and certificate enrolment using copy-paste in the CLI terminal.
2. SCEP Enrollment – Trustpoint authentication and enrollment using SCEP over HTTP.
3. Enrollment Profile – Here, authentication and enrollment methods are defined separately. Along with terminal and SCEP enrollment methods, enrollment profiles provide an option to specify HTTP/TFTP commands to perform file retrieval from the Server, which is defined using an authentication or enrollment url under the profile.
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructurepki/211333-IOSPKI-Deployment-Guide-Initial-Design.html

QUESTION 27
What are two rootkit types? (Choose two)

A. registry

B. virtual

C. bootloader

D. user mode

E. buffer mode

Correct Answer: C, D
Section:
Explanation:
The term 'rootkit' originally comes from the Unix world, where the word 'root' is used to describe a user with the highest possible level of access privileges, similar to an 'Administrator' in Windows. The word 'kit' refers to the software that grants root-level access to the machine. Put the two together and you get 'rootkit', a program that gives someone – with legitimate or malicious intentions – privileged access to a computer.
There are four main types of rootkits: Kernel rootkits, User mode rootkits, Bootloader rootkits, Memory rootkits

QUESTION 28
Which form of attack is launched using botnets?

A. EIDDOS

B. virus

C. DDOS

D. TCP flood

Correct Answer: C
Section:
Explanation:
A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them.
Cyber criminals use botnets to instigate botnet attacks, which include malicious activities such as credentials leaks, unauthorized access, data theft and DDoS attacks.

QUESTION 29
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

Correct Answer: A
Section:

QUESTION 30
Which type of attack is social engineering?

A. trojan

B. phishing

C. malware

D. MITM

Correct Answer: B
Section:
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 or financial institution that requests account information, often suggesting that there is a problem.

QUESTION 31
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

Correct Answer: C, D
Section:
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

QUESTION 32
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.

Correct Answer: B, D
Section:

QUESTION 33
Which algorithm provides encryption and authentication for data plane communication?

A. AES-GCM

B. SHA-96

C. AES-256

D. SHA-384

Correct Answer: A

Section:

Explanation:

The data plane of any network is responsible for handling data packets that are transported across the network.

(The data plane is also sometimes called the forwarding plane.)

Maybe this Qwants to ask about the encryption and authentication in the data plane of a SD-WAN network (but SD-WAN is not a topic of the SCOR 350-701 exam?).

In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetrickey algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates.

Reference:

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/securitybook/security-overview.html

QUESTION 34

Elliptic curve cryptography is a stronger more efficient cryptography method meant to replace which current encryption technology?

A. 3DES

B. RSA

C. DES

D. AES

Correct Answer: B

Section:

Explanation:

Compared to RSA, the prevalent public-key cryptography of the Internet today, Elliptic Curve Cryptography (ECC) offers smaller key sizes, faster computation,as well as memory, energy and bandwidth savings and is thus better suited forsmall devices.

QUESTION 35

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

Correct Answer: C

Section:

Explanation:

Configure a Crypto ISAKMP Key In order to configure apresharedauthentication key, enter thecrypto isakmp keycommand in global configuration mode: 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

QUESTION 36

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

A. DMVPN

B. FlexVPN

C. IPsec DVTI

D. GET VPN

Correct Answer: D

Section:

Explanation:

Cisco's Group Encrypted Transport VPN (GETVPN) introduces the concept of a trusted group to eliminate point-to-point tunnels and their associated overlay routing. All group members (GMs) share a common security association (SA), also known as a group SA. This enables GMs to decrypt traffic that was encrypted by any other GM.

GETVPN provides instantaneous large-scale any-to-any IP connectivity using a group IPsec security paradigm.

Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encryptedtransport-vpn/GETVPN_DIG_version_2_0_External.pdf

QUESTION 37

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

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

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

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

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

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

Correct Answer: C, E

Section:

Explanation:

Stateful failover for IP Security (IPsec) enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This failover process is transparent to users and does not require adjustment or reconfiguration of any remote peer.

Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators.

Prerequisites for Stateful Failover for IPsec

Complete, Duplicate IPsec and IKE Configuration on the Active and Standby Devices This document assumes that you have a complete IKE and IPsec configuration.

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

That is, the crypto configuration must be identical with respect to Internet Security Association and Key Management Protocol (ISAKMP) policy, ISAKMP keys (preshared), IPsec profiles, IPsec transform sets, all crypto map sets that are used for stateful failover, all access control lists (ACLs) that are used in match address statements on crypto map sets, all AAA configurations used for crypto, client configuration groups, IP local pools used for crypto, and ISAKMP profiles.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpnavailability-15-mt-book/sec-state-fail-ipsec.htmlAlthough the prerequisites only stated that "Both routers should be the same type of device" but inthe"Restrictions for Stateful Failover for IPsec" section of the link above, it requires "Both the active andstandby devices must run the identical version of the Cisco IOS software" so answer E is better thananswer B.

QUESTION 38

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

A. SSL VPN

B. GET VPN

C. FlexVPN

D. DMVPN

Correct Answer: C

Section:

Explanation:

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

QUESTION 39
A network engineer is configuring DMVPN and entered the crypto isakmp key cisc0380739941 address 0.0.0.0 command on hostA. The tunnel is not being established to hostB. What action is needed to authenticate the VPN?

A. Change isakmp to ikev2 in the command on hostA.

B. Enter the command with a different password on hostB.

C. Enter the same command on hostB.

D. Change the password on hostA to the default password.

Correct Answer: C
Section:

QUESTION 40
Refer to the exhibit.

```
*Jun 30 16:52:33.795: ISAKMP:(1002): retransmission skipped for phase 1 (time
since last transmission 504)
R1#
*Jun 30 16:52:40.183: ISAKMP:(1001):purging SA., sa=68CEE058, delme=68CEE058
R1#
*Jun 30 16:52:43.291: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:43.291: ISAKMP (1002): incrementing error counter on sa, attempt 5
of 5: retransmit phase 1
*Jun 30 16:52:43.295: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002): sending packet to 10.10.12.2 my_port 500
peer_port 500 (I) MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002):Sending an IKE IPv4 Packet.
R1#
*Jun 30 16:52:53.299: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:53.299: ISAKMP:(1002):peer does not do paranoid keepalives.

*Jun 30 16:52:53.299: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.303: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.307: ISAKMP: Unlocking peer struct 0x68287318 for
isadb_mark_sa_deleted(), count 0
*Jun 30 16:52:53.307: ISAKMP: Deleting peer node by peer_reap for 10.10.12.2:
68287318
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node 79875537 error FALSE reason "IKE
deleted"
R1#
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node -484575753 error FALSE reason
"IKE deleted"
*Jun 30 16:52:53.315: ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL
*Jun 30 16:52:53.319: ISAKMP:(1002):Old State = IKE_I_MM5 New State = IKE_DEST_SA
```

A network administrator configured a site-to-site VPN tunnel between two Cisco IOS routers, and hosts are unable to communicate between two sites of VPN. The network administrator runs the debug crypto isakmp sa command to track VPN status. What is the problem according to this command output?

A. hashing algorithm mismatch

B. encryption algorithm mismatch

C. authentication key mismatch

D. interesting traffic was not applied

Correct Answer: C
Section:

QUESTION 41
What is a difference between FlexVPN and DMVPN?

A. DMVPN uses IKEv1 or IKEv2, FlexVPN only uses IKEv1

B. DMVPN uses only IKEv1 FlexVPN uses only IKEv2

C. FlexVPN uses IKEv2, DMVPN uses IKEv1 or IKEv2

D. FlexVPN uses IKEv1 or IKEv2, DMVPN uses only IKEv2

Correct Answer: C
Section:

QUESTION 42
Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?

A. TLSv1.2

B. TLSv1.1

C. BJTLSv1

D. DTLSv1

Correct Answer: D
Section:
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.

QUESTION 43
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

Correct Answer: D
Section:
Explanation:

In its essence, FlexVPN is the same as DMVPN. Connections between devices are still point-to-point GRE tunnels, spoke-to-spoke connectivity is still achieved with NHRP redirect message, IOS routers even run the same NHRP code for both DMVPN and FlexVPN, which also means that both are Cisco's proprietary technologies.
Reference: https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/

QUESTION 44
The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

A. SDN controller and the cloud

B. management console and the SDN controller

C. management console and the cloud

D. SDN controller and the management solution

Correct Answer: D
Section:

QUESTION 45
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

Correct Answer: B, C
Section:
Explanation:
What Cisco DNA Center enables you to do
Automate: Save time by using a single dashboard to manage and automate your network. Quickly scale your business with intuitive workflows and reusable templates. Configure and provision thousands of network devices across your enterprise in minutes, not hours.
Secure policy: Deploy group-based secure access and network segmentation based on business needs. With Cisco DNA Center, you apply policy to users and applications instead of to your network devices. Automation reduces manual operations and the costs associated with human errors, resulting in more uptime and improved security. Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent.
Assurance: Monitor, identify, and react in real time to changing network and wireless conditions.
Cisco DNA Center uses your network's wired and wireless devices to create sensors everywhere, providing real-time feedback based on actual network conditions. The Cisco DNA Assurance engine correlates network sensor insights with streaming telemetry and compares this with the current context of these data sources. With a quick check of the health scores on the Cisco DNA Center dashboard, you can see where there is a performance issue and identify the most likely cause in minutes.
Extend ecosystem: With the new Cisco DNA Center platform, IT can now integrate Cisco® solutions and thirdparty technologies into a single network operation for streamlining IT workflows and increasing business value and innovation.
Cisco DNA Center allows you to run the network with open interfaces with IT and business applications, integrates across IT operations and technology domains, and can manage heterogeneous network devices.
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dnacenter/nb-06- cisco-dna-center-aag-cte-en.html

QUESTION 46
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

Correct Answer: A
Section:
Explanation:
The Southbound API is used to communicate between Controllers and network devices

QUESTION 47
Which API is used for Content Security?

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

Correct Answer: D
Section:

QUESTION 48
Which two request of REST API are valid on the Cisco ASA Platform? (Choose two)

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

Correct Answer: A, C
Section:
Explanation:
The ASA REST API gives you programmatic access to managing individual ASAs through a Representational State Transfer (REST) API. The API allows external clients to perform CRUD (Create, Read, Update, Delete) operations on ASA resources; it is based on the HTTPS protocol and REST methodology.
All API requests are sent over HTTPS to the ASA, and a response is returned.
Request Structure
Available request methods are:
GET – Retrieves data from the specified object.
PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist.
POST – Creates the object with the supplied information.
DELETE – Deletes the specified object
PATCH – Applies partial modifications to the specified object.
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html

QUESTION 49
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

Correct Answer: B
Section:

QUESTION 50
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

Correct Answer: D
Section:
Explanation:
The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computersacross your organization that Advanced Malware Protection (AMP) sees.
Reference: https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1

QUESTION 51
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

Correct Answer: B
Section:

QUESTION 52
Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two)

A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS

B. Cisco FTDv with one management interface and two traffic interfaces configured

C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises

D. Cisco FTDv with two management interfaces and one traffic interface configured

E. Cisco FTDv configured in routed mode and IPv6 configured

Correct Answer: A, C
Section:

QUESTION 53
Which option is the main function of Cisco Firepower impact flags?

A. They alert administrators when critical events occur.

B. They highlight known and suspected malicious IP addresses in reports.

C. They correlate data about intrusions and vulnerability.

D. They identify data that the ASA sends to the Firepower module.

Correct Answer: C
Section:

QUESTION 54
An administrator wants to ensure that all endpoints are compliant before users are allowed access on the corporate network. The endpoints must have the corporate antivirus application installed and be running the latest build of Windows 10.
What must the administrator implement to ensure that all devices are compliant before they are allowed on the network?

A. Cisco Identity Services Engine and AnyConnect Posture module

B. Cisco Stealthwatch and Cisco Identity Services Engine integration

C. Cisco ASA firewall with Dynamic Access Policies configured

D. Cisco Identity Services Engine with PxGrid services enabled

Correct Answer: A
Section:

QUESTION 55
An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the endpoint to apply a new or updated policy from ISE. Which CoA type achieves this goal?

A. Port Bounce

B. CoA Terminate

C. CoA Reauth

D. CoA Session Query

Correct Answer: C
Section:

QUESTION 56
Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two)

A. RADIUS

B.   TACACS+

C.   DHCP

D.   sFlow

E.   SMTP

Correct Answer: A, C
Section:

QUESTION 57
Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?

A.   RSA SecureID

B.   Internal Database

C.   Active Directory

D.   LDAP

Correct Answer: C
Section:

QUESTION 58
An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17- 010 patch was not installed, which left the endpoint vulnerable to WannaCry ransomware. Which two solutions mitigate the risk of this ransom ware infection? (Choose two)

A.   Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.

B.   Set up a profiling policy in Cisco Identity Service Engine to check and endpoint patch level before allowing access on the network.

C.   Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.

D.   Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.

E.   Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.

Correct Answer: A, C
Section:
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.

File Conditions List > pc_W10_64_KB4012606_Ms17-010_1507_W

File Condition

* Name   **pc_W10_64_KB4012606_Ms1**

Description   **Cisco Predefined Check: Micro**

* Operating System   Windows 10 (All)

Compliance Module   Any version

* File Type   FileVersion   (i)

* File Path   SYSTEM_32   \

* Operator   LaterThan

* File Version   **10.0.10240.17318**

Cancel

QUESTION 59
Which feature of Cisco ASA allows VPN users to be postured against Cisco ISE without requiring an inline posture node?

A. RADIUS Change of Authorization

B. device tracking

C. DHCP snooping

D. VLAN hopping

Correct Answer: A
Section:

QUESTION 60
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+

Correct Answer: B, D
Section:

QUESTION 61

For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two)

A. Windows service

B. computer identity

C. user identity

D. Windows firewall

E. default browser

Correct Answer: A, D
Section:

QUESTION 62

Which compliance status is shown when a configured posture policy requirement is not met?

A. compliant

B. unknown

C. authorized

D. noncompliant

Correct Answer: D
Section:
Explanation:
Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies.
A posture policy is a collection of posture requirements that are associated with one or more identity groups and operating systems.
Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies.
+ If a mandatory requirement fails, the user will be moved to Non-Compliant state + If an optional requirement fails, the user is allowed to skip the specified optional requirements and the user is moved to Compliant state This Qdid not clearly specify the type of posture policy requirement (mandatory or optional) is not met so the user can be in Non-compliant or compliant state. But "noncompliant" is the best answer here.
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_sample_chapter_010111.html

QUESTION 63

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.

Correct Answer: A
Section:

QUESTION 64

Which IPS engine detects ARP spoofing?

A. Atomic ARP Engine

B. Service Generic Engine

C. ARP Inspection Engine

D. AIC Engine

Correct Answer: A
Section:

QUESTION 65
What is a characteristic of Dynamic ARP Inspection?

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

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

C. DAI associates a trust state with each switch.

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

Correct Answer: A
Section:

QUESTION 66
What is a characteristic of traffic storm control behavior?

A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.

B. Traffic storm control cannot determine if the packet is unicast or broadcast.

C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.

D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

Correct Answer: A
Section:

QUESTION 67
A malicious user gained network access by spoofing printer connections that were authorized using MAB on four different switch ports at the same time. What two catalyst switch security features will prevent further violations? (Choose two)

A. DHCP Snooping

B. 802.1AE MacSec

C. Port security

D. IP Device track

E. Dynamic ARP inspection

F. Private VLANs

Correct Answer: A, E
Section:

QUESTION 68
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

Correct Answer: A
Section:

QUESTION 69
Which RADIUS attribute can you use to filter MAB requests in an 802.1 x deployment?

A. 1

B. 2

C. 6

D. 31

Correct Answer: C
Section:
Explanation:
Because MAB uses the MAC address as a username and password, you should make sure that the RADIUS server can differentiate MAB requests from other types of requests for network access. This precaution will prevent other clients from attempting to use a MAC address as a valid credential.
Cisco switches uniquely identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB Access- Request message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server.
Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-basednetworkingservices/config_guide_c17-663759.html

QUESTION 70
A network administrator configures Dynamic ARP Inspection on a switch. After Dynamic ARP Inspection is applied, all users on that switch are unable to communicate with any destination. The network administrator checks the interface status of all interfaces, and there is no err-disabled interface. What is causing this problem?

A. DHCP snooping has not been enabled on all VLANs.

B. The ip arp inspection limit command is applied on all interfaces and is blocking the traffic of all users.

C. Dynamic ARP Inspection has not been enabled on all VLANs

D. The no ip arp inspection trust command is applied on all user host interfaces

Correct Answer: D
Section:
Explanation:
Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in- the-middle attacks. After enabling DAI, all ports become untrusted ports.

QUESTION 71
Refer to the exhibit.

```
SwitchA(config)#interface gigabitethernet1/0/1
SwitchA(config-if)#dot1x host-mode multi-host
SwitchA(config-if)#dot1x timeout quiet-period 3
SwitchA(config-if)#dot1x timeout tx-period 15
SwitchA(config-if)#authentication port-control
auto
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 12
```

An engineer configured wired 802.1x on the network and is unable to get a laptop to authenticate.
Which port configuration is missing?

A. authentication open
B. dotlx reauthentication
C. cisp enable
D. dot1x pae authenticator

Correct Answer: D
Section:

QUESTION 72
Which SNMPv3 configuration must be used to support the strongest security possible?

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

Correct Answer: D
Section:

QUESTION 73
Refer to the exhibit.

```
Interface   MAC Address      Method   Domain  Status  Fg Session I
Gi4/15      0050.b6d4.8a60   dot1x    DATA    Auth    0A021982000
Gi8/43      0024.c4fe.1832   dot1x    VOICE   Auth    0A021982000
Gi10/25     0026.7391.bbd1   dot1x    DATA    Auth    0A021982000
Gi8/28      0026.0b5e.51d5   dot1x    VOICE   Auth    0A021982000
Gi4/13      0025.4593.e575   dot1x    VOICE   Auth    0A021982000
Gi10/23     0025.8418.217f   dot1x    VOICE   Auth    0A021982000
Gi7/4       0025.8418.1bc7   dot1x    VOICE   Auth    0A021982000
Gi7/7       0026.0b5e.50fb   dot1x    VOICE   Auth    0A021982000
Gi8/14      c85b.7604.fa1d   dot1x    DATA    Auth    0A021982000
Gi10/29     0026.0b5e.528a   dot1x    VOICE   Auth    0A021982000
Gi4/2       0026.0b5e.4f9f   dot1x    VOICE   Auth    0A021982000
Gi10/30     0025.4593.e5ac   dot1x    VOICE   Auth    0A021982000
Gi8/29      68bd.aba5.2e44   dot1x    VOICE   Auth    0A021982000
Gi7/4       54ee.75db.d766   dot1x    DATA    Auth    0A021982000
Gi2/34      e804.62eb.a658   dot1x    VOICE   Auth    0A021982000
Gi10/22     482a.e307.d9c8   dot1x    DATA    Auth    0A021982000
Gi9/22      0007.b00c.8c35   mab      DATA    Auth    0A021982000
```

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

A. show authentication registrations

B. show authentication method

C. show dot1x all

D. show authentication sessions

Correct Answer: D
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137Displaying the Summary of All Auth Manager Sessions on the SwitchEnter the following:

Switch# show authentication sessions

Interface MAC Address Method Domain Status Session ID
Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C
Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58
Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

QUESTION 74
What Cisco command shows you the status of an 802.1X connection on interface gi0/1?

A. show authorization status

B. show authen sess int gi0/1

C. show connection status gi0/1

D. show ver gi0/1

Correct Answer: B
Section:

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

Correct Answer: B
Section:
Explanation:
The syntax of this command is shown below: snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]}] [read read-view] [write writeview] [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.

QUESTION 76
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

Correct Answer: B, D
Section:
Explanation:
The profiling service issues the change of authorization in the following cases:
– Endpoint deleted—When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network.
An exception action is configured—If you have an exception action configured per profile that leads to an unusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to the corresponding static profile by issuing a CoA.
– An endpoint is profiled for the first time—When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.
+ An endpoint identity group has changed—When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.
The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:
++ The endpoint identity group changes for endpoints when they are dynamically profiled ++ The endpoint identity group changes when the static assignment flag is set to true for a dynamic endpoint – An endpoint profiling policy has changed and the policy is used in an authorization policy—When an endpoint profiling policy changes, and the policy is included in a logical profile that is used in an authorization policy. The endpoint profiling policy may change due to the profiling policy match or when an endpoint is statically assigned to an endpoint profiling policy, which is associated to a logical profile. In both the cases, the profiling service issues a CoA, only when the endpoint profiling policy is used in an authorization policy.
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_20_chapter_010100.html

QUESTION 77
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

Correct Answer: B
Section:
Explanation:
The user "admin5" was configured with privilege level 5. In order to allow configuration (enter global configuration mode), we must type this command:
(config)#privilege exec level 5 configure terminal
Without 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)

QUESTION 78
A network engineer has entered the snmp-server user andy myv3 auth sha cisco priv aes 256 cisc0380739941 command and needs to send SNMP information to a host at 10.255.254.1. Which command achieves this goal?

A. snmp-server host inside 10.255.254.1 version 3 andy
B. snmp-server host inside 10.255.254.1 version 3 myv3
C. snmp-server host inside 10.255.254.1 snmpv3 andy
D. snmp-server host inside 10.255.254.1 snmpv3 myv3

Correct Answer: A
Section:
Explanation:
The command "snmp-server user user-name group-name [remote ip-address [udp-port port]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]" adds a new user (in this case "andy") to an SNMPv3 group (in this case group name "myv3") and configures a password for the user.
In the "snmp-server host" command, we need to:
+ Specify the SNMP version with key word "version {1 | 2 | 3}"
+ Specify the username ("andy"), not group name ("myv3").
Note: In "snmp-server host inside …" command, "inside" is the interface name of the ASA interface through which the NMS (located at 10.255.254.1) can be reached.

QUESTION 79
Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?

A. interpacket variation
B. software package variation

C. flow insight variation

D. process details variation

Correct Answer: A
Section:
Explanation:
The telemetry information consists of three types of data:
+ Flow information: This information contains details about endpoints, protocols, ports, when the flow started, how long the flow was active, etc.
+ Interpacket variation: This information captures any interpacket variations within the flow.
Examples include variation in Time To Live (TTL), IP and TCP flags, payload length, etc + Context details: Context information is derived outside the packet header. It includes details about variation in buffer utilization, packet drops within a flow, association with tunnel endpoints, etc.
Reference: https://www.cisco.com/c/dam/global/en_uk/products/switches/cisco_nexus_9300_ex_platform_switches_white_paper_uki.pdf

QUESTION 80
How is ICMP used an exfiltration technique?

A. by flooding the destination host with unreachable packets

B. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address

C. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host

D. by overwhelming a targeted host with ICMP echo-request packets

Correct Answer: C
Section:

QUESTION 81
Which exfiltration method does an attacker use to hide and encode data inside DNS requests and queries?

A. DNS tunneling

B. DNSCrypt

C. DNS security

D. DNSSEC

Correct Answer: A
Section:
Explanation:
DNS Tunneling is a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses. DNS tunneling often includes data payloads that can be added to an attacked DNS server and used to control a remote server and applications.

QUESTION 82
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 damage and theft on the network.

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

Correct Answer: B
Section:

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:
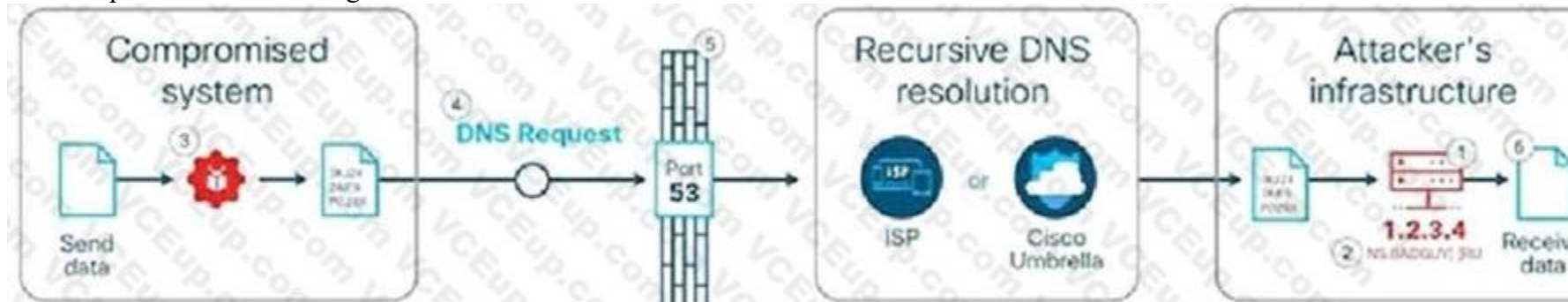
The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNS nameserver (NS) and malicious payload.
2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. attackerdomain.com) is registered or reused. The registrar informs the top-level domain (.com) nameservers to refer requests for attackerdomain.com to ns.attackerdomain.com, which has a DNS record mapped to 1.2.3.4 3. 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 a part of the domain name (e.g. 3KJ242AIE9.attackerdomain.com). Depending on the attacker's patience and stealth, requests can be spaced out over days or months to avoid suspicious network activity.
5. The requests are forwarded to a recursive DNS resolver. During resolution, the requests are sent to the attacker's authoritative DNS nameserver, 6. The tunneling kit parses the encoded strings and rebuilds the exfiltrated data.
Reference: https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0

QUESTION 83
What are two list types within AMP for Endpoints Outbreak Control? (Choose two)

A. blocked ports
B. simple custom detections
C. command and control
D. allowed applications
E. URL

Correct Answer: B, D
Section:
Explanation:
Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed
Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists.
A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine.
Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf

QUESTION 84
What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?

A. Enable IP Layer enforcement.

B. Activate the Advanced Malware Protection license
C. Activate SSL decryption.
D. Enable Intelligent Proxy.

Correct Answer: D
Section:

QUESTION 85
When wired 802.1X authentication is implemented, which two components are required? (Choose two)

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

Correct Answer: A, C
Section:

QUESTION 86
Refer to the exhibit.


```
Sysauthcontrol              Enabled
Dot1x Protocol Version         3

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

Which command was used to display this output?

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

Correct Answer: A
Section:

QUESTION 87
Refer to the exhibit.

```
aaa new-model
radius-server host 10.0.0.12 key
secret12
```

Which statement about the authentication protocol used in the configuration is true?

A. The authentication request contains only a password

B. The authentication request contains only a username

C. The authentication and authorization requests are grouped in a single packet

D. There are separate authentication and authorization request packets

Correct Answer: C
Section:
Explanation:
This command uses RADIUS which combines authentication and authorization in one function (packet).

QUESTION 88
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

Correct Answer: B
Section:

QUESTION 89
Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?

A. aaa server radius dynamic-author

B. aaa new-model

C. auth-type all

D. ip device-tracking

Correct Answer: B
Section:

QUESTION 90
A network administrator is configuring a rule in an access control policy to block certain URLs and selects the "Chat and Instant Messaging" category. Which reputation score should be selected to accomplish this goal?

A. 1

B. 3

C. 5

D. 10

Correct Answer: D
Section:
Explanation:
We choose "Chat and Instant Messaging" category in "URL Category":

Edit Action

Quarantine

Encrypt on Delivery

Strip Attachment by Content

Strip Attachment by File Info

URL Category

URL Reputation

Add Disclaimer Text

Bypass Outbreak Filter Scanning

Bypass DKIM Signing

Send Copy (Bcc:)

Notify

Change Recipient to

Send to Alternate Destination Host

Deliver from IP Interface

Strip Header

Add/Edit Header

Add Message Tag

Add Log Entry

S/MIME Sign/Encrypt on Delivery

Encrypt and Deliver Now (Final Action)

S/MIME Sign/Encrypt (Final Action)

Bounce (Final Action)

Skip Remaining Content Filters (Final Action)

Drop (Final Action)

URL Category   Help

Does any URL in the message body or subject belong to one of the selected categories?

Available Categories: Selected Categories:

Advertisements   Add >   Adult
Alcohol   Child Abuse Content
Arts   Illegal Activities
Astrology   < Remove   Illegal Downloads
Auctions   Illegal Drugs
Business and Industry
Chat and Instant Messagir
Cheating and Plagiarism
Computer Security
Computers and Internet

Use a URL whitelist: None   ⟷ ⑦

Action on URL:

⦿ Defang URL ⑦

○ Redirect to Cisco Security Proxy ⑦

○ Replace URL with text message

Perform Action for:

⦿ All messages

○ Unsigned messages

To block certain URLs we need to choose URL Reputation from 6 to 10.

Edit Condition

Message Body or Attachment	**URL Reputation**
Message Body	What is the reputation of URL's in the message? This rule
URL Category	evaluates URL's using their Web Based Reputation Score (W
URL Reputation	
Message Size	URL Reputation is:
Attachment Content	● Malicious (-10.0 to -6.0)
Attachment File Info	
Attachment Protection	○ Suspect (-5.9 to 5.9)
Subject Header	○ Clean (6.0 to 10.0)
Other Header	
Envelope Sender	○ Custom Range (min to max)
Envelope Recipient	
Receiving Listener	○ No Score
Remote IP/Hostname	
Reputation Score	Use a URL whitelist: [None ⬍] ⑦

QUESTION 91
Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats?

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

Correct Answer: B
Section:
Explanation:
Talos Threat Source is a regular intelligence update from Cisco Talos, highlighting the biggest threats each week and other security news.
Reference: https://talosintelligence.com/newsletters

QUESTION 92
What are the two types of managed Intercloud Fabric deployment models? (Choose two)

A. Service Provider managed

B. Public managed

C. Hybrid managed

D. User managed

E. Enterprise managed

Correct Answer: A, E

Section:

Explanation:

Many enterprises prefer to deploy development workloads in the public cloud, primarily for convenience and faster deployment. This approach can cause concern for IT administrators, who must control the flow of IT traffic and spending and help ensure the security of data and intellectual property. Without the proper controls, data and intellectual property can escape this oversight. The Cisco Intercloud Fabric solution helps control this shadow IT, discovering resources deployed in the public cloud outside IT control and placing these resources under Cisco Intercloud Fabric control.

Cisco Intercloud Fabric addresses the cloud deployment requirements appropriate for two hybrid cloud deployment models: Enterprise Managed (an enterprise manages its own cloud environments) and Service Provider Managed (the service provider administers and controls all cloud resources).

Reference:

https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric.pdfThe Cisco Intercloud Fabric architecture provides two product configurations to address the followingtwoconsumption models:

+ Cisco Intercloud Fabric for Business

+ Cisco Intercloud Fabric for Providers

Reference:

https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric/Intercloud_Fabric_2.html

QUESTION 93

What are two DDoS attack categories? (Choose two)

A. sequential

B. protocol

C. database

D. volume-based

E. screen-based

Correct Answer: B, D
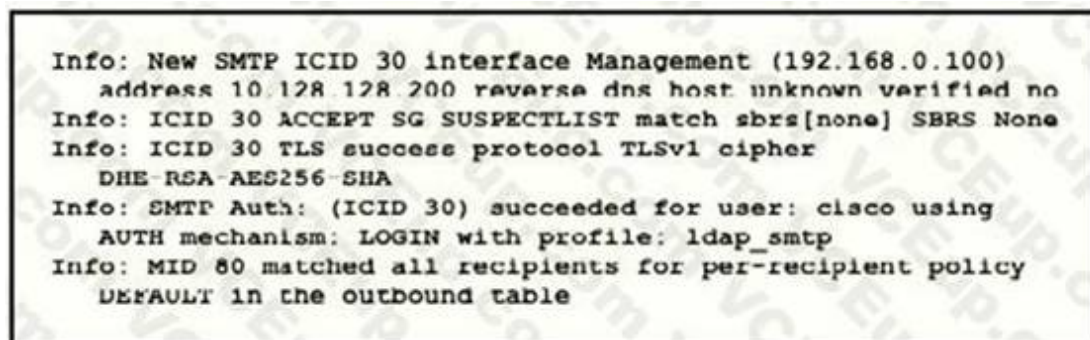
Section:

Explanation:

There are three basic categories of attack:

+ volume-based attacks, which use high traffic to inundate the network bandwidth + protocol attacks, which focus on exploiting server resources + application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks Reference: https://www.esecurityplanet.com/networks/types-of-ddosattacks/

QUESTION 94

Refer to the exhibit.


```
Info: New SMTP ICID 30 interface Management (192.168.0.100)
    address 10.128.128.200 reverse dns host unknown verified no
Info: ICID 30 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS None
Info: ICID 30 TLS success protocol TLSv1 cipher
    DHE-RSA-AES256-SHA
Info: SMTP Auth: (ICID 30) succeeded for user: cisco using
    AUTH mechanism: LOGIN with profile: ldap_smtp
Info: MID 80 matched all recipients for per-recipient policy
    DEFAULT in the outbound table
```

Which type of authentication is in use?

A. LDAP authentication for Microsoft Outlook

B. POP3 authentication

C. SMTP relay server authentication

D. external user and relay mail authentication

Correct Answer: A
Section:
Explanation:
The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118844-technoteesa-00.htmlThe exhibit in this Qshows a successful TLS connection from the remote host (reception) in the maillog.

QUESTION 95
An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically.
What must be configured to accomplish this?

A. Configure the Cisco WSA to modify policies based on the traffic seen

B. Configure the Cisco ESA to receive real-time updates from Talos

C. Configure the Cisco WSA to receive real-time updates from Talos

D. Configure the Cisco ESA to modify policies based on the traffic seen

Correct Answer: D
Section:
Explanation:
The Mail Policies menu is where almost all of the controls related to email filtering happens. All the security and content filtering policies are set here, so it's likely that, as an ESA administrator, the pages on this menu are where you are likely to spend most of your time.

QUESTION 96
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

Correct Answer: B
Section:

QUESTION 97
What are two differences between a Cisco WSA that is running in transparent mode and one running in explicit mode? (Choose two)

A. When the Cisco WSA is running in transparent mode, it uses the WSA's own IP address as the HTTP request destination.
B. The Cisco WSA responds with its own IP address only if it is running in explicit mode.
C. The Cisco WSA is configured in a web browser only if it is running in transparent mode.
D. The Cisco WSA uses a Layer 3 device to redirect traffic only if it is running in transparent mode.
E. The Cisco WSA responds with its own IP address only if it is running in transparent mode.

Correct Answer: B, D
Section:
Explanation:
The Cisco Web Security Appliance (WSA) includes a web proxy, a threat analytics engine, antimalware engine, policy management, and reporting in a single physical or virtual appliance. The main use of the Cisco WSA is to

protect users from accessing malicious websites and being infected by malware.
You can deploy the Cisco WSA in two different modes:
– Explicit forward mode
– Transparent mode
In explicit forward mode, the client is configured to explicitly use the proxy, subsequently sending all web traffic to the proxy. Because the client knows there is a proxy and sends all traffic to the proxy in explicit forward mode, the client does not perform a DNS lookup of the domain before requesting the URL. The Cisco WSA is responsible for DNS resolution, as well.
When you configure the Cisco WSA in explicit mode, you do not need to configure any other network infrastructure devices to redirect client requests to the Cisco WSA. However, you must configure each client to send traffic to the Cisco WSA.
-> Therefore in explicit mode, WSA only checks the traffic between client & web server. WSA does not use its own IP address to request -> Answer B is not correct.
When the Cisco WSA is in transparent mode, clients do not know there is a proxy deployed. Network infrastructure devices are configured to forward traffic to the Cisco WSA. In transparent mode deployments, network infrastructure devices redirect web traffic to the proxy. Web traffic redirection can be done using policybased routing (PBR)—available on many routers —or using Cisco's Web Cache Communication Protocol (WCCP) on Cisco ASA, Cisco routers, or switches.
The Web Cache Communication Protocol (WCCP), developed by Cisco Systems, specifies interactions between one or more switches) and one or more web-caches. The purpose of the interaction is to establish and maintain the transparent redirectio of traffic flowing through a group of routers.
Reference: https://www.cisco.com/c/en/us/tech/content-networking/web-cache-communicationsprotocol-wccp/index.html->Therefore answer D is correct as redirection can be done on Layer 3 device only.
In transparent mode, the client is unaware its traffic is being sent to a proxy (Cisco WSA) and, as a result, the client uses DNS to resolve the domain name in the URL and send the web request destined for the web server (not the proxy).
When you configure the Cisco WSA in transparent mode, you need to identify a network choke point with a redirection device (a Cisco ASA) to redirect traffic to the proxy.
WSA in Transparent mode
Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide -> Therefore in Transparent mode, WSA uses its own IP address to initiate a new connection the Web Server (in step 4 above) -> Answer E is correct.
Answer C is surely not correct as WSA cannot be configured in a web browser in either mode.
Answer A seems to be correct but it is not. This answer is correct if it states "When the Cisco WSA is running in transparent mode, it uses the WSA's own IP address as the HTTP request source" (not destination).

QUESTION 98
After a recent breach, an organization determined that phishing was used to gain initial access to the network before regaining persistence. The information gained from the phishing attack was a result of users visiting known malicious websites. What must be done in order to prevent this from happening in the future?

A. Modify an access policy
B. Modify identification profiles
C. Modify outbound malware scanning policies
D. Modify web proxy settings

Correct Answer: D
Section:
Explanation:
URL conditions in access control rules allow you to limit the websites that users on your network can access. This feature is called URL filtering. There are two ways you can use access control to specify URLs you want to block (or, conversely, allow):
– With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic.
– With a URL Filtering license, you can also control access to websites based on the URL's general classification, or category, and risk level, or reputation. The system displays this category and reputation data in connection logs, intrusion events, and application details.
Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new
URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configguidev60/Access_Control_Rules__URL_Filtering.html

QUESTION 99

What is the function of SDN southbound API protocols?

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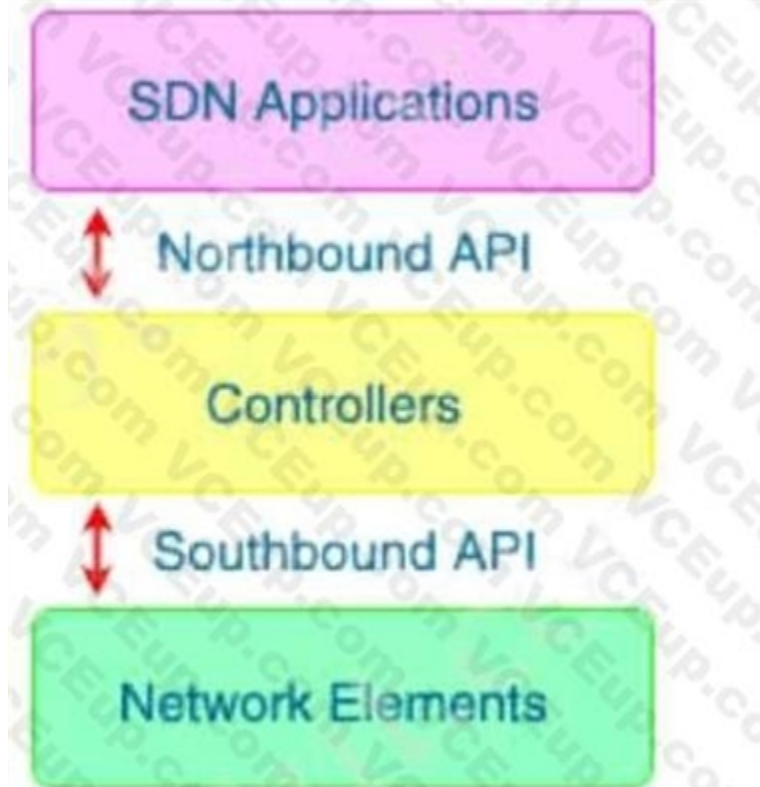D. to allow for the static configuration of control plane applications

Correct Answer: B
Section:
Explanation:
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs.
Reference: https://www.ciscopress.com/articles/article.asp?p=3004581&seqNum=2

Note: Southbound APIs helps us communicate with data plane (not control plane) applications

QUESTION 100
Refer to the exhibit.

```
> show crypto ipsec sa
interface: Outside
    Crypto map tag: CSM_Outside_map, seq num: 1, local addr:
209.165.200.225

    access-list CSM_IPSEC_ACL_1 extended permit ip 10.0.11.0
255.255.255.0 10.0.10.0 255.255.255.0
    local ident (addr/mask/prot/port): (10.0.11.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.0.10.0/255.255.255.0/0/0)
    current_peer: 209.165.202.129

    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 17
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp
failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 209.165.200.225/500, remote crypto endpt.:
209.165.202.129/500
    path mtu 1500, ipsec overhead 55(36), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: B6F5EA53
    current inbound spi : 84348DEE
```

Traffic is not passing through IPsec site-to-site VPN on the Firepower Threat Defense appliance. What is causing this issue?

A. No split-tunnel policy is defined on the Firepower Threat Defense appliance.

B. The access control policy is not allowing VPN traffic in.

C. Site-to-site VPN peers are using different encryption algorithms.

D. Site-to-site VPN preshared keys are mismatched.

Correct Answer: A
Section:
Explanation:
If sysopt permit-vpn is not enabled then an access control policy must be created to allow the VPN traffic through the FTD device. If sysopt permit-vpn is enabled skip creating an access control policy.
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ikeprotocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html

QUESTION 101
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

Correct Answer: B
Section:

QUESTION 102
Using Cisco Firepower's Security Intelligence policies, upon which two criteria is Firepower block based?
(Choose two)

A. URLs

B. protocol IDs

C. IP addresses

D. MAC addresses

E. port numbers

Correct Answer: A, C
Section:
Explanation:
Security Intelligence Sources
…C ustom Block lists or feeds (or objects or groups) Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects or groups.)
For example, if you become aware of malicious sites or addresses that are not yet blocked by a feed, add these sites to a custom Security Intelligence list and add this custom list to the Block list in the Security Intelligence tab of your access control policy.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmcconfigguide-v623/security_intelligence_blacklisting.html

QUESTION 103
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

Correct Answer: C
Section:
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.

File Conditions List > pc_W10_64_KB4012606_Ms17-010_1507_W

File Condition

* Name **pc_W10_64_KB4012606_Ms1**

Description **Cisco Predefined Check: Micro**

* Operating System   Windows 10 (All)

Compliance Module   Any version

* File Type   FileVersion

* File Path   SYSTEM_32

* Operator   LaterThan

* File Version **10.0.10240.17318**

Cancel

QUESTION 104
What are two benefits of Flexible NetFlow records? (Choose two)

A. They allow the user to configure flow information to perform customized traffic identification
B. They provide attack prevention by dropping the traffic
C. They provide accounting and billing enhancements
D. They converge multiple accounting technologies into one accounting mechanism
E. They provide monitoring of a wider range of IP packet information from Layer 2 to 4

Correct Answer: A, D
Section:
Explanation:
NetFlow is typically used for several key customer applications, including the following:
…B illing and accounting. NetFlow data provides fine-grained metering (for instance, flow data includes details such as IP addresses, packet and byte counts, time stamps, type of service (ToS), and application ports) for highly flexible and detailed resource utilization accounting. Service providers may use the information for billing based on time of day, bandwidth usage, application usage, quality of service, and so on. Enterprise customers may use the information for departmental charge back or cost allocation for resource utilization.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnffnetflow.htmlIf the predefined Flexible NetFlow records are not suitable for your traffic requirements, you cancreate a userdefined (custom) record using the Flexible NetFlow collect and match commands.
Before you can create a customized record, you must decide the criteria that you are going to use for the key and nonkey fields.
Reference: https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413 d9.html#wp1057997Note: Traditional NetFlow allows us to monitor from Layer 2 to 4 but Flexible NetFlow goes beyondtheselayers.

QUESTION 105
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.

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.

Correct Answer: A
Section:

QUESTION 106
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

Correct Answer: D
Section:

QUESTION 107
An organization is receiving SPAM emails from a known malicious domain. What must be configured in order to prevent the session during the initial TCP communication?

A. Configure the Cisco ESA to drop the malicious emails
B. Configure policies to quarantine malicious emails
C. Configure policies to stop and reject communication
D. Configure the Cisco ESA to reset the TCP connection

Correct Answer: D
Section:

QUESTION 108
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

Correct Answer: B, E
Section:
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.

QUESTION 109

What is the purpose of the certificate signing request when adding a new certificate for a server?

A. It is the password for the certificate that is needed to install it with.

B. It provides the server information so a certificate can be created and signed

C. It provides the certificate client information so the server can authenticate against it when installing

D. It is the certificate that will be loaded onto the server

Correct Answer: B
Section:
Explanation:
A certificate signing request (CSR) is one of the first steps towards getting your own SSL Certificate.
Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) that the Certificate Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key

QUESTION 110
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

Correct Answer: A
Section:
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.

QUESTION 111
What is managed by Cisco Security Manager?

A. access point

B. WSA

C. ASA

D. ESA

Correct Answer: C
Section:
Explanation:
Cisco Security Manager provides a comprehensive management solution for:
– Cisco ASA 5500 Series Adaptive Security Appliances
– Cisco intrusion prevention systems 4200 and 4500 Series Sensors
– Cisco AnyConnect Secure Mobility Client
Reference: https://www.cisco.com/c/en/us/products/security/security-manager/index.html

QUESTION 112
How does Cisco Advanced Phishing Protection protect users?

A. It validates the sender by using DKIM.
B. It determines which identities are perceived by the sender
C. It utilizes sensors that send messages securely.
D. It uses machine learning and real-time behavior analytics.

Correct Answer: B
Section:
Explanation:
Cisco Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to protect against identity deception-based threats.
Reference: https://docs.ces.cisco.com/docs/advanced-phishing-protection

QUESTION 113
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

Correct Answer: B
Section:
Explanation:
Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct
Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system "You cannot use an FMC to manage ASA firewall functions."
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepowercompatibility.htmlThe Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases theeffectiveness of your Cisco network security solutions by providing centralized, integrated, andstreamlined management.
Reference: https://www.cisco.com/c/en/us/products/collateral/security/firesight-managementcenter/datasheetc78-736775.html

QUESTION 114
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.

Correct Answer: C
Section:

QUESTION 115
An organization is implementing URL blocking using Cisco Umbrell a. The users are able to go to some sites but other sites are not accessible due to an error. Why is the error occurring?

A. Client computers do not have the Cisco Umbrella Root CA certificate installed.
B. IP-Layer Enforcement is not configured.
C. Client computers do not have an SSL certificate deployed from an internal CA server.

D. Intelligent proxy and SSL decryption is disabled in the policy

Correct Answer: A
Section:
Explanation:
Other features are dependent on SSL Decryption functionality, which requires the Cisco Umbrella root certificate. Having the SSL Decryption feature improves:
Custom URL Blocking—Required to block the HTTPS version of a URL.
…U mbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed.
Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you may wish to prevent it from appearing.
To avoid these error pages, install the Cisco Umbrella root certificate into your browser or the browsers of your users—if you're a network admin.
Reference: https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-importinformation

QUESTION 116
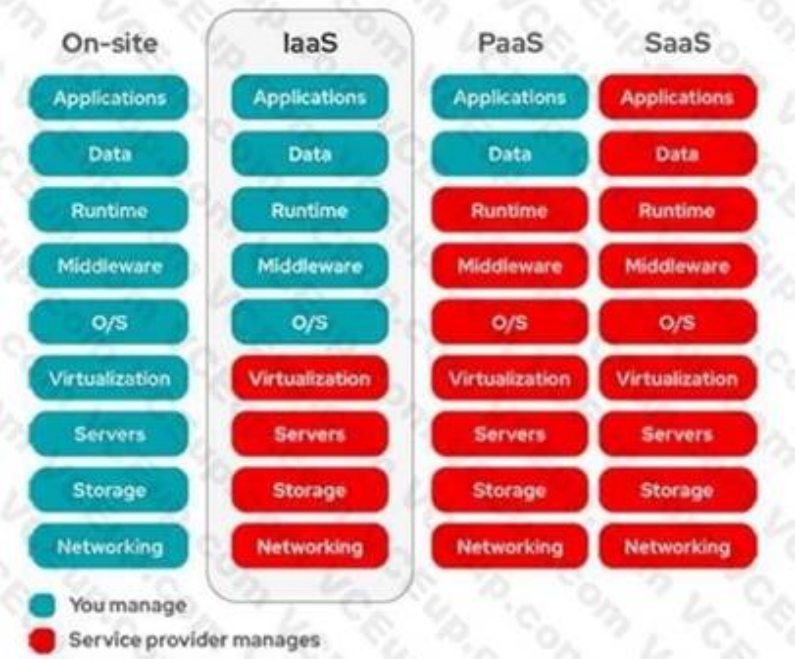Which two aspects of the cloud PaaS model are managed by the customer but not the provider?
(Choose two)

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

Correct Answer: D, E
Section:
Explanation:
Customers must manage applications and data in PaaS.

QUESTION 117
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

Correct Answer: C
Section:
Explanation:
DevSecOps (development, security, and operations) is a concept used in recent years to describe how to move security activities to the start of the development life cycle and have built-in security practices in the continuous integration/
continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer to 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.

QUESTION 118
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

Correct Answer: C
Section:
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.

QUESTION 119
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

Correct Answer: C, E
Section:
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.

QUESTION 120
In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?

A. LDAP injection

B. man-in-the-middle

C. cross-site scripting

D. insecure API

Correct Answer: B
Section:

QUESTION 121
Which Dos attack uses fragmented packets to crash a target machine?

A. smurf

B. MITM

C. teardrop

D. LAND

Correct Answer: C
Section:
Explanation:
A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

QUESTION 122
Why is it important to have logical security controls on endpoints even though the users are trained to spot security threats and the network devices already help prevent them?

A. to prevent theft of the endpoints

B. because defense-in-depth stops at the network

C. to expose the endpoint to more threats

D. because human error or insider threats will still exist

Correct Answer: D
Section:

QUESTION 123
Which type of API is being used when a security application notifies a controller within a softwaredefined network architecture about a specific security threat?

A. westbound AP

B. southbound API

C. northbound API

D. eastbound API

Correct Answer: C
Section:

QUESTION 124
When planning a VPN deployment, for which reason does an engineer opt for an active/active FlexVPN configuration as opposed to DMVPN?

A. Multiple routers or VRFs are required.
B. Traffic is distributed statically by default.
C. Floating static routes are required.
D. HSRP is used for faliover.

Correct Answer: B
Section:

QUESTION 125
Which algorithm provides asymmetric encryption?

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

Correct Answer: C
Section:

QUESTION 126
What are two functions of secret key cryptography? (Choose two)

A. key selection without integer factorization
B. utilization of different keys for encryption and decryption
C. utilization of large prime number iterations
D. provides the capability to only know the key on one side
E. utilization of less memory

Correct Answer: B, D
Section:

QUESTION 127
For Cisco IOS PKI, which two types of Servers are used as a distribution point for CRLs? (Choose two)

A. SDP
B. LDAP
C. subordinate CA
D. SCP
E. HTTP

Correct Answer: B, E
Section:
Explanation:
Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). This module identifies and describes

concepts that are needed to understand, plan for, and implement a PKI.
A PKI is composed of the following entities: …
– A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs)
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mtbook/sec-pki-overview.html

QUESTION 128
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

Correct Answer: A
Section:
Explanation:
Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to its intended 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 IP broadcast address.

QUESTION 129
What is a difference between DMVPN and sVTI?

A. DMVPN supports tunnel encryption, whereas sVTI does not.

B. DMVPN supports dynamic tunnel establishment, whereas sVTI does not.

C. DMVPN supports static tunnel establishment, whereas sVTI does not.

D. DMVPN provides interoperability with other vendors, whereas sVTI does not.

Correct Answer: B
Section:

QUESTION 130
What features does Cisco FTDv provide over ASAv?

A. Cisco FTDv runs on VMWare while ASAv does not

B. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not

C. Cisco FTDv runs on AWS while ASAv does not

D. Cisco FTDv supports URL filtering while ASAv does not

Correct Answer: D
Section:

QUESTION 131
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

Correct Answer: D
Section:
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 provide device-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.

QUESTION 132
Which type of API is being used when a controller within a software-defined network architecture dynamically makes configuration changes on switches within the network?
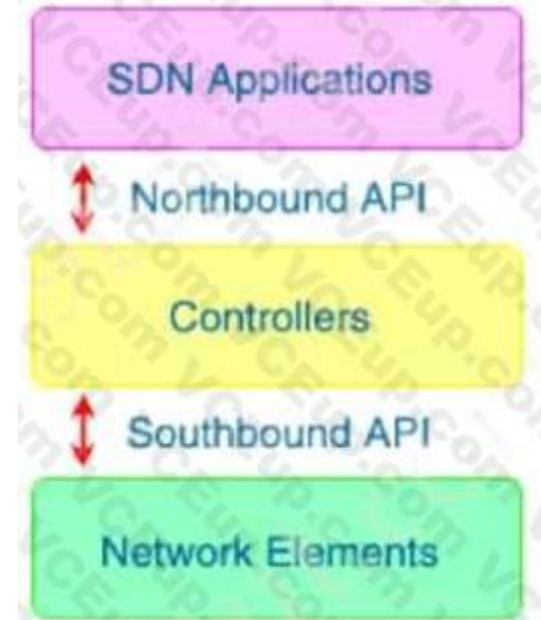
A. westbound AP
B. southbound API
C. northbound API
D. eastbound API

Correct Answer: B
Section:
Explanation:
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs.

QUESTION 133
An organization has two systems in their DMZ that have an unencrypted link between them for communication.
The organization does not have a defined password policy and uses several default accounts on the systems.
The application used on those systems also have not gone through stringent code reviews. Which vulnerability would help an attacker brute force their way into the systems?

A. weak passwords
B. lack of input validation

C. missing encryption

D. lack of file permission

Correct Answer: C
Section:
Explanation:
The version 9 export format uses templates to provide access to observations of IP packet flows in a flexible and extensible manner. A template defines a collection of fields, with corresponding descriptions of structure and semantics.
Reference: https://tools.ietf.org/html/rfc3954

QUESTION 134
What is provided by the Secure Hash Algorithm in a VPN?

A. integrity

B. key exchange

C. encryption

D. authentication

Correct Answer: A
Section:
Explanation:
The HMAC-SHA-1-96 (also known as HMAC-SHA-1) encryption technique is used by IPSec to ensure that a message has not been altered. (-> Therefore answer "integrity" is the best choice). HMACSHA- 1 uses the SHA-1 specified in
FIPS-190-1, combined with HMAC (as per RFC 2104), and is described in RFC 2404.
Reference: https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=4

QUESTION 135
In which two ways does Easy Connect help control network access when used with Cisco TrustSec?
(Choose two)

A. It allows multiple security products to share information and work together to enhance security posture in the network.

B. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.

C. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.

D. It integrates with third-party products to provide better visibility throughout the network.

E. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups
(PassiveID).

Correct Answer: C, E
Section:
Explanation:
Easy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity.
Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprisenetworks/trustsec/trustsec-witheasy-connect-configuration-guide.pdf

QUESTION 136
What is the benefit of installing Cisco AMP for Endpoints on a network?

A. It provides operating system patches on the endpoints for security.

B. It provides flow-based visibility for the endpoints network connections.

C. It enables behavioral analysis to be used for the endpoints.

D. It protects endpoint systems through application control and real-time scanning

Correct Answer: D
Section:

QUESTION 137
An administrator is configuring a DHCP server to better secure their environment. They need to be able to ratelimit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?
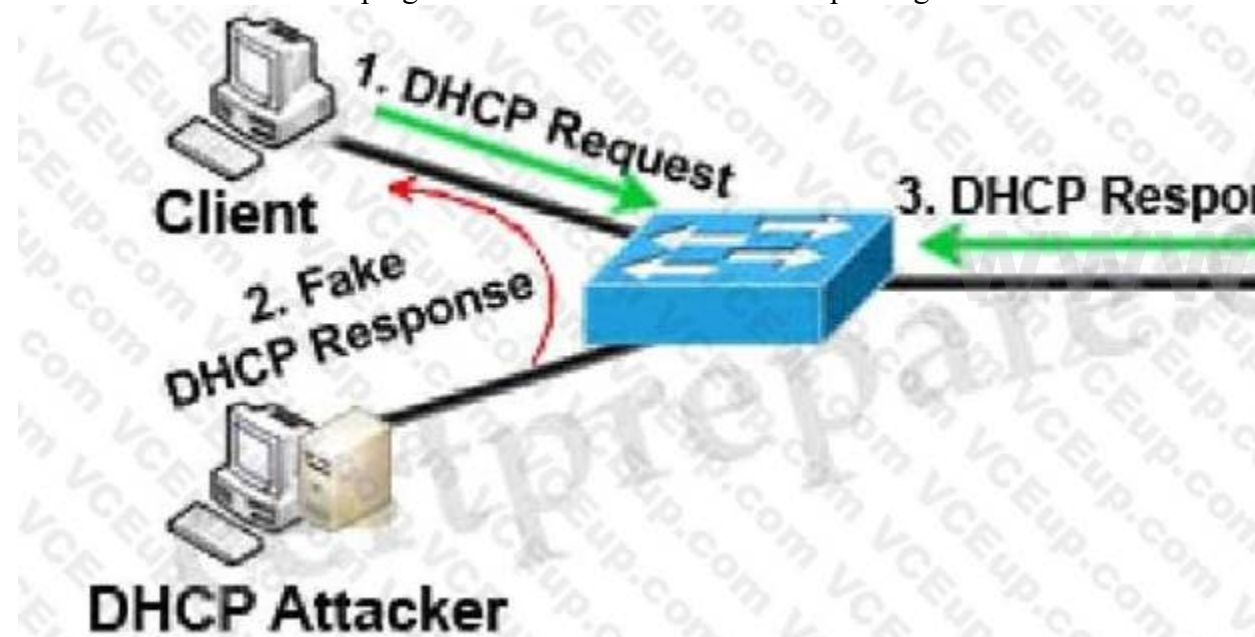
A. Set a trusted interface for the DHCP server

B. Set the DHCP snooping bit to 1

C. Add entries in the DHCP snooping database

D. Enable ARP inspection for the required VLAN
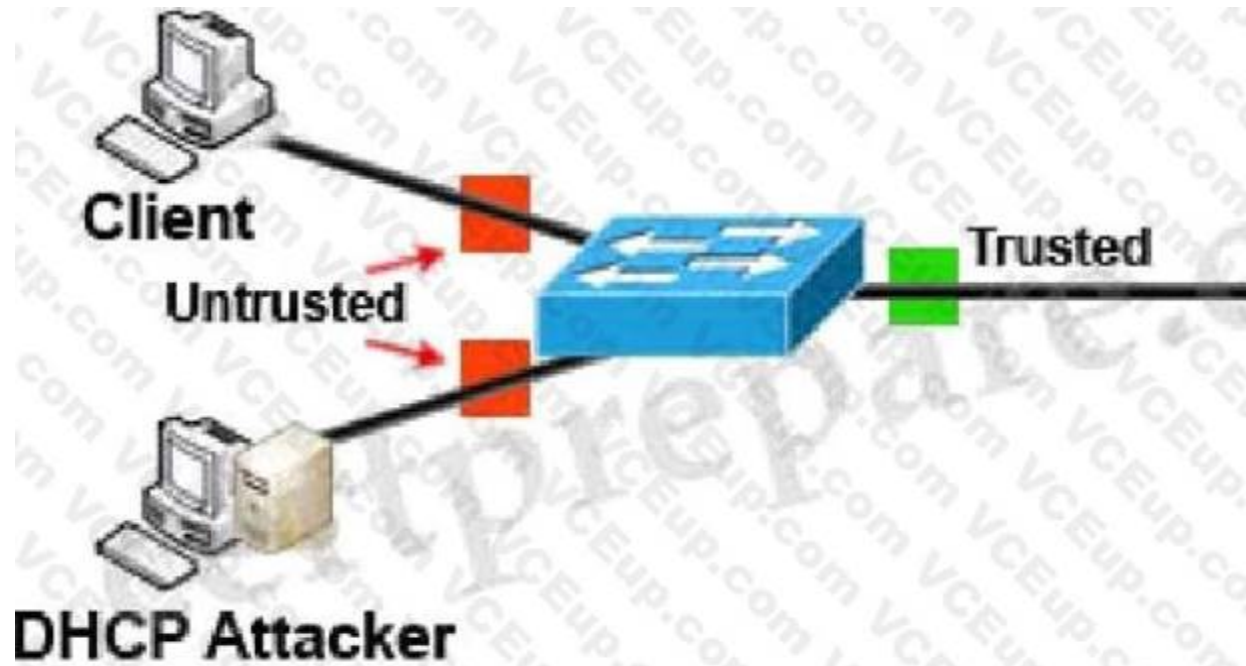
Correct Answer: A
Section:
Explanation:
To understand DHCP snooping we need to learn about DHCP spoofing attack first.

DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle".
The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.
DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.

DHCP Attacker

Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.

QUESTION 138
Refer to the exhibit.

```
import requests
client_id = '<Client id>'
api_key = '<API Key>'
url = 'https://api.amp.cisco.com/v1/computers'
response = requests.get(url, auth=(client_id, api_key))
response_json = response.json()
for computer in response_json['data']:
    hostname = computer['hostname']
    print(hostname)
```
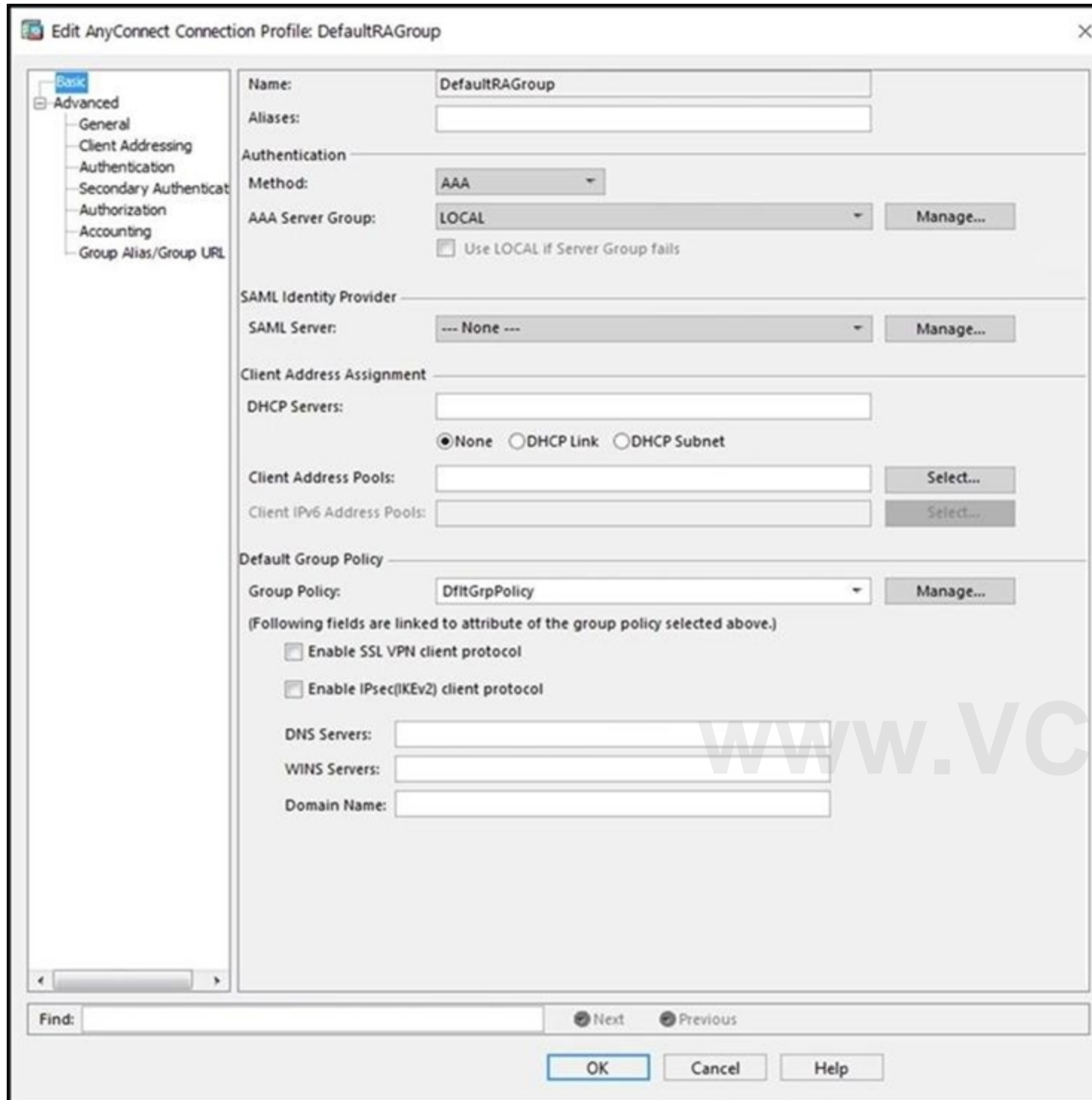
What will happen when the Python script is executed?

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

Correct Answer: C
Section:

QUESTION 139
Refer to the exhibit.

When configuring a remote access VPN solution terminating on the Cisco ASA, an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication using machine certificates. Which configuration item must be modified to allow this?

A. Group Policy
B. Method
C. SAML Server
D. DHCP Servers

Correct Answer: B
Section:
Explanation:

In order to use AAA along with an external token authentication mechanism, set the "Method" as "Both" in the Authentication.

QUESTION 140
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

Correct Answer: D
Section:
Explanation:
Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform.
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-websecurity/at-a-glance-c45- 738565.pdf

QUESTION 141
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

Correct Answer: D
Section:
Explanation:
+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy.
+ Cloudlock is API-based.
+ Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).
Reference: https://docs.umbrella.com/cloudlock-documentation/docs/endpointsNote:
+ Security information and event management (SIEM) platforms collect log and event data from security systems, 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 a condition of an alerting policy has been met.

QUESTION 142
Why is it important to implement MFA inside of an organization?

A. To prevent man-the-middle attacks from being successful.

B. To prevent DoS attacks from being successful.

C. To prevent brute force attacks from being successful.

D. To prevent phishing attacks from being successful.

Correct Answer: C
Section:

QUESTION 143
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

Correct Answer: B
Section:

QUESTION 144
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

Correct Answer: A
Section:
Explanation:
Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms.
Cisco Defense Orchestrator features:
….
Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms.
Reference: https://www.cisco.com/c/en/us/products/collateral/security/defenseorchestrator/datasheet-c78-736847.html

QUESTION 145
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.

Correct Answer: C
Section:

QUESTION 146
Which risk is created when using an Internet browser to access cloud-based service?

A. misconfiguration of infrastructure, which allows unauthorized access
B. intermittent connection to the cloud connectors
C. vulnerabilities within protocol
D. insecure implementation of API

Correct Answer: D
Section:

QUESTION 147

An organization has a Cisco ESA set up with policies and would like to customize the action assigned for violations. The organization wants a copy of the message to be delivered with a message added to flag it as a DLP violation. Which actions must be performed in order to provide this capability?

A. deliver and send copies to other recipients

B. quarantine and send a DLP violation notification

C. quarantine and alter the subject header with a DLP violation

D. deliver and add disclaimer text

Correct Answer: D
Section:
Explanation:
You specify primary and secondary actions that the appliance will take when it detects a possible DLP violation in an outgoing message. Different actions can be assigned for different violation types and severities.
Primary actions include:
– Deliver
– Drop
– Quarantine
Secondary actions include:
– Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message.
– Encrypting messages. The appliance only encrypts the message body. It does not encrypt the message headers.
– Altering the subject header of messages containing a DLP violation.
– Adding disclaimer text to messages.
– Sending messages to an alternate destination mailhost.
– Sending copies (bcc) of messages to other recipients. (For example, you could copy messages with critical DLP violations to a compliance officer's mailbox for examination.)
– Sending a DLP violation notification message to the sender or other contacts, such as a manager or DLP compliance officer.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html

QUESTION 148
Refer to the exhibit.

An administrator is adding a new Cisco FTD device to their network and wants to manage it with Cisco FMC.
The Cisco FTD is not behind a NAT device. Which command is needed to enable this on the Cisco FTD?

A. configure manager add DONTRESOLVE kregistration key>

B. configure manager add <FMC IP address> <registration key> 16

C. configure manager add DONTRESOLVE <registration key> FTD123

D. configure manager add <FMC IP address> <registration key>

Correct Answer: D
Section:
Explanation:
To let FMC manages FTD, first we need to add manager from the FTD and assign a register key of your choice. The command configure manager add 1.1.1.2 the_registration_key_you_want, where 1.1.1.2 is the IP address of the FMC, you need to use the same registration key in FMC when adding this FTD as a managed device.
Reference: https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/

QUESTION 149
A switch with Dynamic ARP Inspection enabled has received a spoofed ARP response on a trusted interface.
How does the switch behave in this situation?

A. It forwards the packet after validation by using the MAC Binding Table.

B. It drops the packet after validation by using the IP & MAC Binding Table.

C. It forwards the packet without validation.

D. It drops the packet without validation.

Correct Answer: B

Section:

QUESTION 150
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

Correct Answer: A
Section:

QUESTION 151
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

Correct Answer: A
Section:

QUESTION 152
Which posture assessment requirement provides options to the client for remediation and requires the remediation within a certain timeframe?

A. Audit
B. Mandatory
C. Optional
D. Visibility

Correct Answer: B
Section:
Explanation:
A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role and an operating system. All the clients connecting to your network must meet mandatory requirements during posture evaluation to become compliant on the network.
Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. If requirements are optional and clients fail these requirements, then the clients have an option to continue during posture evaluation of endpoints.
Mandatory Requirements
During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings.
For example, you have specified a mandatory requirement with a user-defined condition to check the existence of C:\temp\text.file in the absolute path. If the file does not exist, the mandatory requirement fails and the user will be moved to Non-Compliant state.
Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/ b_ise_admin_guide_14_chapter_010111.html

QUESTION 153
Which attribute has the ability to change during the RADIUS CoA?

A. NTP
B. Authorization
C. Accessibility
D. Membership

Correct Answer: B
Section:
Explanation:
The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html

QUESTION 154
With Cisco AMP for Endpoints, which option shows a list of all files that have been executed in your environment?

A. Prevalence
B. File analysis
C. Detections
D. Vulnerable software
E. Threat root cause

Correct Answer: A
Section:
Explanation:
Prevalence allows you to view files that have been executed in your deployment.
Note: Threat Root Cause shows how malware is getting onto your computers.
Reference: https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf

QUESTION 155
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

Correct Answer: C
Section:

QUESTION 156
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

Correct Answer: C
Section:
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.

QUESTION 157
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

Correct Answer: B
Section:
Explanation:

QUESTION 158
An organization configures Cisco Umbrella to be used for its DNS services. The organization must be able to block traffic based on the subnet that the endpoint is on but it sees only the requests from its public IP address instead of each internal IP address. What must be done to resolve this issue?

A. Set up a Cisco Umbrella virtual appliance to internally field the requests and see the traffic of each IP address
B. Use the tenant control features to identify each subnet being used and track the connections within the Cisco Umbrella dashboard
C. Install the Microsoft Active Directory Connector to give IP address information stitched to the requests in the Cisco Umbrella dashboard
D. Configure an internal domain within Cisco Umbrella to help identify each address and create policy from the domains

Correct Answer: A
Section:

QUESTION 159
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

Correct Answer: A
Section:

QUESTION 160
Which two capabilities of Integration APIs are utilized with Cisco DNA center? (Choose two)

A. Upgrade software on switches and routers
B. Third party reporting
C. Connect to ITSM platforms
D. Create new SSIDs on a wireless LAN controller
E. Automatically deploy new virtual routers

Correct Answer: B, C
Section:
Explanation:

QUESTION 161
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

Correct Answer: B
Section:

QUESTION 162
What is the purpose of CA in a PKI?

A. To issue and revoke digital certificates
B. To validate the authenticity of a digital certificate
C. To create the private key for a digital certificate
D. To certify the ownership of a public key by the named subject

Correct Answer: A
Section:
Explanation:
A trusted CA is the only entity that can issue trusted digital certificates. This is extremely important because while PKI manages more of the encryption side of these certificates, authentication is vital to understanding which entities own what keys. Without a trusted CA, anyone can issue their own keys, authentication goes out the window and chaos ensues.
Reference: https://cheapsslsecurity.com/blog/understanding-the-role-of-certificate-authorities-inpki/

QUESTION 163
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

Correct Answer: B
Section:

Explanation:
Unlike the traditional software life cycle, the CI/CD implementation process gives a weekly or daily update instead of monthly or quarterly. The fun part is customers won't even realize the update is in their applications, as they happen on the fly.
Reference: https://devops.com/how-to-implement-an-effective-ci-cd-pipeline/

QUESTION 164
Which parameter is required when configuring a Netflow exporter on a Cisco Router?

A. DSCP value

B. Source interface

C. Exporter name

D. Exporter description

Correct Answer: C
Section:
Explanation:
An example of configuring a NetFlow exporter is shown below: flow exporter Exporter destination 192.168.100.22 transport udp 2055

QUESTION 165
Which category includes DoS Attacks?

A. Virus attacks

B. Trojan attacks

C. Flood attacks

D. Phishing attacks

Correct Answer: C
Section:

QUESTION 166
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

Correct Answer: C, E
Section:

QUESTION 167
When choosing an algorithm to us, what should be considered about Diffie Hellman and RSA for key establishment?

A. RSA is an asymmetric key establishment algorithm intended to output symmetric keys

B. RSA is a symmetric key establishment algorithm intended to output asymmetric keys

C. DH is a symmetric key establishment algorithm intended to output asymmetric keys

D. DH is on asymmetric key establishment algorithm intended to output symmetric keys

Correct Answer: D
Section:
Explanation:
Diffie Hellman (DH) uses a private-public key pair to establish a shared secret, typically a symmetric key. DH is not a symmetric algorithm – it is an asymmetric algorithm used to establish a shared secret for a symmetric key algorithm.

QUESTION 168
Which type of DNS abuse exchanges data between two computers even when there is no direct connection?

A. Malware installation

B. Command-and-control communication

C. Network footprinting

D. Data exfiltration

Correct Answer: D
Section:
Explanation:
Malware installation: This may be done by hijacking DNS queries and responding with malicious IP addresses.
Command & Control communication: As part of lateral movement, after an initial compromise, DNS communications is abused to communicate with a C2 server. This typically involves making periodic DNS queries from a computer in the target network for a domain controlled by the adversary. The responses contain encoded messages that may be used to perform unauthorized actions in the target network.
Network footprinting: Adversaries use DNS queries to build a map of the network. Attackers live off the terrain so developing a map is important to them.
Data theft (exfiltration): Abuse of DNS to transfer data; this may be performed by tunneling other protocols like FTP, SSH through DNS queries and responses. Attackers make multiple DNS queries from a compromised computer to a domain owned by the adversary. DNS tunneling can also be used for executing commands and transferring malware into the target network.
Reference: https://www.netsurion.com/articles/5-types-of-dns-attacks-and-how-to-detect-them

QUESTION 169
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

Correct Answer: C
Section:

QUESTION 170
What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?

A. Telemetry uses a pull mehod, which makes it more reliable than SNMP

B. Telemetry uses push and pull, which makes it more scalable than SNMP

C. Telemetry uses push and pull which makes it more secure than SNMP

D. Telemetry uses a push method which makes it faster than SNMP

Correct Answer: D
Section:

Explanation:

SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts.

The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data.

Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc.

Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Referfence: https:// developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-startguide/ streaming telemetry

QUESTION 171

An organization wants to use Cisco FTD or Cisco ASA devices. Specific URLs must be blocked from being accessed via the firewall which requires that the administrator input the bad URL categories that the organization wants blocked into the access policy. Which solution should be used to meet this requirement?

A. Cisco ASA because it enables URL filtering and blocks malicious URLs by default, whereas Cisco FTD does not

B. Cisco ASA because it includes URL filtering in the access control policy capabilities, whereas Cisco FTD does not

C. Cisco FTD because it includes URL filtering in the access control policy capabilities, whereas Cisco ASA does not

D. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not

Correct Answer: C
Section:

QUESTION 172

An administrator configures a Cisco WSA to receive redirected traffic over ports 80 and 443. The organization requires that a network device with specific WSA integration capabilities be configured to send the traffic to the WSA to proxy the requests and increase visibility, while making this invisible to the users. What must be done on the Cisco WSA to support these requirements?

A. Configure transparent traffic redirection using WCCP in the Cisco WSA and on the network device

B. Configure active traffic redirection using WPAD in the Cisco WSA and on the network device

C. Use the Layer 4 setting in the Cisco WSA to receive explicit forward requests from the network device

D. Use PAC keys to allow only the required network devices to send the traffic to the Cisco WSA

Correct Answer: A
Section:

QUESTION 173

An administrator configures new authorization policies within Cisco ISE and has difficulty profiling the devices. Attributes for the new Cisco IP phones that are profiled based on the RADIUS authentication are seen however the attributes for

CDP or DHCP are not. What should the administrator do to address this issue?

A. Configure the ip dhcp snooping trust command on the DHCP interfaces to get the information to Cisco ISE

B. Configure the authentication port-control auto feature within Cisco ISE to identify the devices that are trying to connect

C. Configure a service template within the switch to standardize the port configurations so that the correct information is sent to Cisco ISE

D. Configure the device sensor feature within the switch to send the appropriate protocol information

Correct Answer: D
Section:
Explanation:

Device sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by Device Sensor can come from the following protocols:
+ Cisco Discovery Protocol (CDP)
+ Link Layer Discovery Protocol (LLDP)
+ Dynamic Host Configuration Protocol (DHCP)
Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-ConfigureDevice-Sensor-for-ISE-Profilin.html

Which command is used to log all events to a destination colector 209.165.201.107?

A. CiscoASA(config-pmap-c)#flow-export event-type flow-update destination 209.165.201.10
B. CiscoASA(config-cmap)# flow-export event-type all destination 209.165.201.
C. CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.10
D. CiscoASA(config-cmap)#flow-export event-type flow-update destination 209.165.201.10

Correct Answer: C
Section:

QUESTION 175
What is the most commonly used protocol for network telemetry?

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

Correct Answer: D
Section:

QUESTION 176
What are two functions of IKEv1 but not IKEv2? (Choose two)

A. NAT-T is supported in IKEv1 but rot in IKEv2.
B. With IKEv1, when using aggressive mode, the initiator and responder identities are passed cleartext
C. With IKEv1, mode negotiates faster than main mode
D. IKEv1 uses EAP authentication
E. IKEv1 conversations are initiated by the IKE_SA_INIT message

Correct Answer: C, E
Section:

QUESTION 177
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

Correct Answer: A
Section:

QUESTION 178
A company identified a phishing vulnerability during a pentest What are two ways the company can protect employees from the attack? (Choose two.)

A. using Cisco Umbrella

B. using Cisco ESA

C. using Cisco FTD

D. using an inline IPS/IDS in the network

E. using Cisco ISE

Correct Answer: A, B
Section:

QUESTION 179
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

Correct Answer: B
Section:

QUESTION 180
Refer to the exhibit.

```
aaa new-model
radius-server host 10.0.0.12 key secret12
```

What is the result of using this authentication protocol in the configuration?

A. The authentication request contains only a username.

B. The authentication request contains only a password.

C. There are separate authentication and authorization request packets.

D. The authentication and authorization requests are grouped in a single packet.

Correct Answer: D
Section:

QUESTION 181
Which feature must be configured before implementing NetFlow on a router?

A. SNMPv3

B. syslog

C. VRF

D. IP routing

Correct Answer: D
Section:

QUESTION 182
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

Correct Answer: B
Section:

QUESTION 183
What is a function of Cisco AMP for Endpoints?

A. It detects DNS attacks

B. It protects against web-based attacks

C. It blocks email-based attacks

D. It automates threat responses of an infected host

Correct Answer: D
Section:

QUESTION 184
An engineer is implementing DHCP security mechanisms and needs the ability to add additional attributes to profiles that are created within Cisco ISE Which action accomplishes this task?

A. Define MAC-to-lP address mappings in the switch to ensure that rogue devices cannot get an IP address

B. Use DHCP option 82 to ensure that the request is from a legitimate endpoint and send the information to Cisco ISE

C. Modify the DHCP relay and point the IP address to Cisco ISE.

D. Configure DHCP snooping on the switch VLANs and trust the necessary interfaces

Correct Answer: D
Section:

QUESTION 185
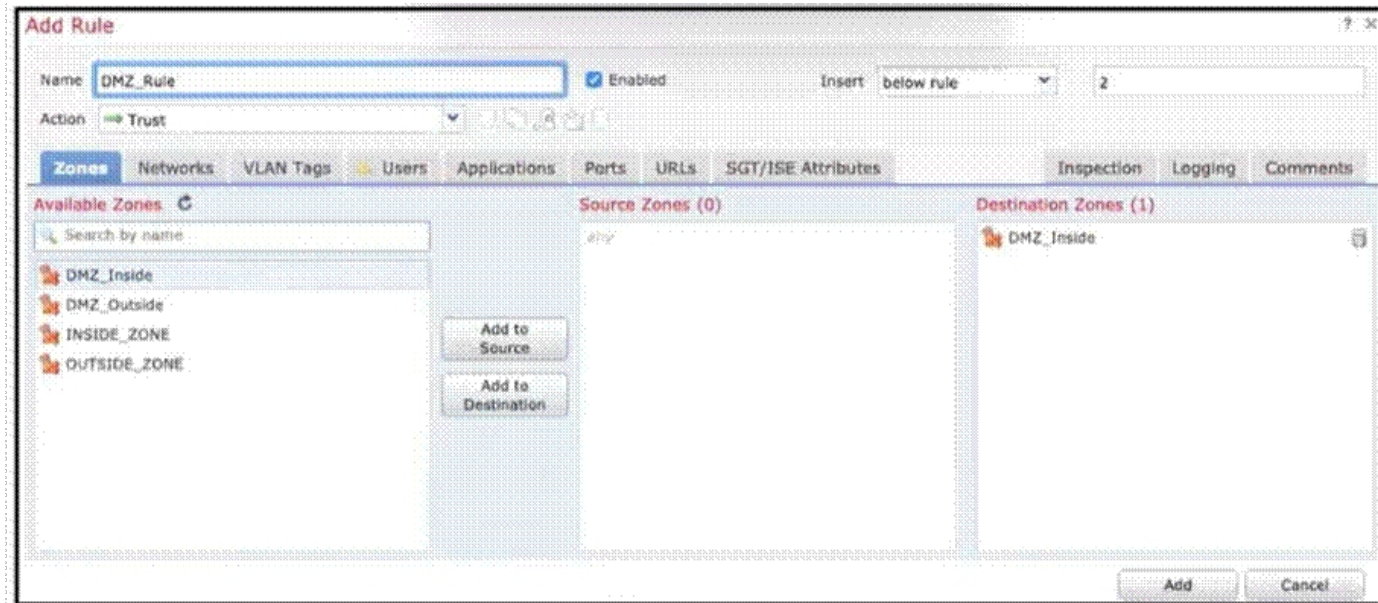Which feature requires that network telemetry be enabled?

A. per-interface stats

B. SNMP trap notification

C. Layer 2 device discovery

D. central syslog system

Correct Answer: D
Section:

QUESTION 186
Refer to the exhibit

When configuring this access control rule in Cisco FMC, what happens with the traffic destined to the DMZ_inside 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

Correct Answer: A
Section:

QUESTION 187
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

Correct Answer: D
Section:

QUESTION 188
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

Correct Answer: C

Section:

QUESTION 189
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

Correct Answer: B
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xe-16-10/sec-usr-aaa-xe-16-10-book/sec-rad-coa.pdf

QUESTION 190
An engineer is configuring cloud logging using a company-managed Amazon S3 bucket for Cisco Umbrella logs. What benefit does this configuration provide for accessing log data?

A. It is included m the license cost for the multi-org console of Cisco Umbrella
B. It can grant third-party SIEM integrations write access to the S3 bucket
C. No other applications except Cisco Umbrella can write to the S3 bucket
D. Data can be stored offline for 30 days.

Correct Answer: D
Section:

QUESTION 191
For a given policy in Cisco Umbrella, how should a customer block website based on a custom list?

A. by specifying blocked domains in me policy settings
B. by specifying the websites in a custom blocked category
C. by adding the websites to a blocked type destination list
D. by adding the website IP addresses to the Cisco Umbrella blocklist

Correct Answer: C
Section:

QUESTION 192
An engineer must 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

Correct Answer: A
Section:

QUESTION 193
Which Cisco Firewall solution requires zone definition?

A. CBAC

B. Cisco AMP

C. ZBFW

D. Cisco ASA

Correct Answer: C
Section:

QUESTION 194
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

Correct Answer: D
Section:

QUESTION 195
What is the concept of CI/CD pipelining?

A. The project is split into several phases where one phase cannot start before the previous phase finishes successfully.

B. The project code is centrally maintained and each code change should trigger an automated build and test sequence

C. The project is split into time-limited cycles and focuses on pair programming for continuous code review

D. Each project phase is independent from other phases to maintain adaptiveness and continual improvement

Correct Answer: A
Section:

QUESTION 196
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

Correct Answer: D
Section:

QUESTION 197
DRAG DROP
A network engineer is configuring NetFlow top talkers on a Cisco router Drag and drop the steps in the process from the left into the sequence on the right

VCEplus

Select and Place:

Configure the ip flow-top-talkers command.	step 1
Configure the ip flow command on an interface.	step 2
Configure IP routing and enable Cisco Express Forwarding.	step 3
Set the top-talkers sorting criterion.	step 4
Specify the maximum number of top talkers.	step 5

Correct Answer:

	Configure IP routing and enable Cisco Express Forwarding.
	Configure the ip flow-top-talkers command.
	Specify the maximum number of top talkers.
	Set the top-talkers sorting criterion.
	Configure the ip flow command on an interface.

Section:
Explanation:

QUESTION 198
Which DoS attack uses fragmented packets in an attempt to crash a target machine?

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

Correct Answer: A
Section:

QUESTION 199
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.

Correct Answer: C
Section:

QUESTION 200
What are two workload security models? (Choose two.)

A. SaaS

B. PaaS

C. off-premises

D. on-premises

E. IaaS

Correct Answer: C, D
Section:

QUESTION 201
Client workstations are experiencing extremely poor response time. An engineer suspects that an attacker is eavesdropping and making independent connections while relaying messages between victims to make them think they are talking to each other over a private connection. Which feature must be enabled and configured to provide relief from this type of attack?

A. Link Aggregation

B. Reverse ARP

C. private VLANs

D. Dynamic ARP Inspection

Correct Answer: D
Section:

QUESTION 202
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

Correct Answer: A
Section:

QUESTION 203
Which threat intelligence standard contains malware hashes?

A. advanced persistent threat

B. open command and control

C. structured threat information expression

D. trusted automated exchange of indicator information

Correct Answer: C
Section:

QUESTION 204
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

Correct Answer: A, B
Section:

QUESTION 205
Which Cisco security solution secures public, private, hybrid, and community clouds?

A. Cisco ISE

B. Cisco ASAv

C. Cisco Cloudlock

D. Cisco pxGrid

Correct Answer: C
Section:

QUESTION 206
A university policy must allow open access to resources on the Internet for research, but internal workstations are exposed to malware. Which Cisco AMP feature allows the engineering team to determine whether a file is installed on a selected few workstations?

A. file prevalence

B. file discovery

C. file conviction

D. file manager

Correct Answer: A
Section:

QUESTION 207
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

Correct Answer: A
Section:

QUESTION 208
What is the target in a phishing attack?

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

Correct Answer: D
Section:

QUESTION 209
Which two protocols must be configured to authenticate end users to the Cisco WSA? (Choose two.)

A. TACACS+
B. CHAP
C. NTLMSSP
D. RADIUS
E. Kerberos

Correct Answer: C, E
Section:

QUESTION 210
What is the purpose of the Cisco Endpoint IoC feature?

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

Correct Answer: A
Section:
Explanation:
The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

QUESTION 211
An organization is using DNS services for their network and want to help improve the security of the DNS infrastructure. Which action accomplishes this task?

A. Use DNSSEC between the endpoints and Cisco Umbrella DNS servers.
B. Modify the Cisco Umbrella configuration to pass queries only to non-DNSSEC capable zones.

C. Integrate Cisco Umbrella with Cisco CloudLock to ensure that DNSSEC is functional.
D. Configure Cisco Umbrella and use DNSSEC for domain authentication to authoritative servers.

Correct Answer: D
Section: