Cisco

350-701 Exam

CCIE

Questions & Answers

(Full Version)

Thank you for Purchasing 350-701 Exam

CERT EMPIRE

Question: 1

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

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

Answer: C

Explanation:

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

Question: 2

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

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

Answer: A

Explanation:

SQL injection usually occurs when you ask a user for input, like their username/userid, but the user gives
("injects") you an SQL statement that you will unknowingly run on your database. For example:
Look at the following example, which creates a SELECT statement by adding a variable (txtUserId) to a select
string. The variable is fetched from user input (getRequestString):
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
If user enter something like this: "100 OR 1=1" then the SzQL statement will look like this:
SELECT * FROM Users WHERE UserId = 100 OR 1=1;
The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE. A
hacker might get access to all the user names and passwords in this database.

Question: 3

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

A. Check integer, float, or Boolean string parameters to ensure accurate values.
B. Use prepared statements and parameterized queries.
C. Secure the connection between the web and the app tier.
D. Write SQL code instead of using object-relational mapping libraries.
E. Block SQL code execution in the web application database login.

Answer: A, B

Explanation:

Question: 4

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

A. Patch for cross-site scripting.

B. Perform backups to the private cloud.

C. Protect against input validation and character escapes in the endpoint.

D. Install a spam and virus email filter.

E. Protect systems with an up-to-date antimalware program

Answer: D, E

Explanation:

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

Question: 5

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

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

Answer: A, E

Explanation:

Question: 6

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

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

Answer: B, D

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: 7

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.

Answer: A, B

Explanation:

Question: 8

What is the difference between deceptive phishing and spear phishing?

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

Answer: B

Explanation:

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: 9

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

A. cross-site scripting
B. water holing
C. DDoS

D. buffer overflow

Answer: D

Explanation:

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

Question: 10

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

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

Answer: A

Explanation:

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

Question: 11

Which two capabilities does TAXII support? (Choose two)

A. Exchange
B. Pull messaging
C. Binding
D. Correlation
E. Mitigating

Answer: B, C

Explanation:

The Trusted Automated eXchangeof Indicator Information (TAXII) specifies mechanisms for exchanging
structured cyber threat information between parties over the network.
TAXII exists to provide specific capabilities to those interested in sharing structured cyber threat

information.
TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilities
that this version of TAXII supports: push messaging, pull messaging, and discovery.
Although there is no "binding" capability in the list but it is the best answer here.

Question: 12

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

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

Answer: A, D

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: 13

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

Answer: C

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-infrastructure-pki/211333-IOSPKI-Deployment-Guide-Initial-Design.html

Question: 14

What are two rootkit types? (Choose two)

A. registry
B. virtual
C. bootloader
D. user mode
E. buffer mode

Answer: C, D

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: 15

Which form of attack is launched using botnets?

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

Answer: C

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: 16

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

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

Answer: A

Explanation:

Question: 17

Which type of attack is social engineering?

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

Answer: B

Explanation:

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

Question: 18

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

A. 64-bit block size, 112-bit key length

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

Answer: C, D

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: 19

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

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

Answer: B, D

Explanation:

Question: 20

Which algorithm provides encryption and authentication for data plane communication?

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

Answer: A

Explanation:

The 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 Q wants 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 symmetric key 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/security-book/ security-overview.html

Question: 21

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

Answer: B

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: 22

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

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

Answer: A

Explanation:

The syntax of above command is:
crypto isakmp key enc-type-digit keystring {address peer-address [mask] | ipv6 ipv6-address/ ipv6-prefix |
hostname hostname} [no-xauth]
The peer-address argument specifies the IP or IPv6 address of the remote peer.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp6039879000

Question: 23

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

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

Answer: D

Explanation:

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-encrypted-transport-vpn/
GETVPN_DIG_version_2_0_External.pdf

Question: 24

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

A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the
IPsec configuration is copied automatically
B. The active and standby devices can run different versions of the Cisco IOS software but must be the same
type of device.
C. The IPsec configuration that is set up on the active device must be duplicated on the standby device
D. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device;
the IKE configuration is copied automatically.
E. The active and standby devices must run the same version of the Cisco IOS software and must be the
same type of device

Answer: C, E

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.html
Although the prerequisites only stated that "Both routers should be the same type of device" but in the
"Restrictions for Stateful Failover for IPsec" section of the link above, it requires "Both the active and standby devices must run the identical version of the Cisco IOS software" so answer E is better than answer B.

Question: 25

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

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

Answer: C

Explanation:

FlexVPN is an IKEv2-based VPN technology that provides several benefits beyond traditional site-to-site VPN implementations. FlexVPN is a standards-based solution that can interoperate with non-Cisco 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: 26

A network engineer is configuring DMVPN and entered the crypto isakmp key cisc0380739941 address 0.0.0.0 command on host
A. 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.

Answer: C

Explanation:

Question: 27

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

Answer: C

Explanation:

Question: 28

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

Answer: C

Explanation:

Question: 29

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

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

Answer: D

Explanation:

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

Question: 30

What is a commonality between DMVPN and FlexVPN technologies?

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

Answer: D

Explanation:

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: 31

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

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

Answer: D

Explanation:

Question: 32

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

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

Answer: B, C

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 third party 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/dna-center/nb-06- cisco-dna-center-aag-cte-en.html

Question: 33

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

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

Answer: A

Explanation:

The Southbound API is used to communicate between Controllers and network devices

Question: 34

Which API is used for Content Security?

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

Answer: D

Explanation:

Question: 35

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

Answer: A, C

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: 36

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

Answer: B

Explanation:

Question: 37

Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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

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

response_json = response.json()

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


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

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

Answer: D

Explanation:

The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across 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: 38

Which feature requires a network discovery policy on the Cisco Firepower Next Generation Intrusion Prevention
System?

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

Answer: B

Explanation:

Question: 39

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

Answer: A, C

Explanation:

Question: 40

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.

Answer: C

Explanation:

Question: 41

On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed
devices?

A. health policy
B. system policy
C. correlation policy
D. access control policy
E. health awareness policy

Answer: A

Explanation:

Question: 42

Which license is required for Cisco Security Intelligence to work on the Cisco Next Generation Intrusion
Prevention System?

A. control
B. malware
C. URL filtering
D. protect

Answer: D

Explanation:

Question: 43

Which two are valid suppression types on a Cisco Next Generation Intrusion Prevention System? (Choose two)

A. Port
B. Rule
C. Source
D. Application
E. Protocol

Answer: B, C

Explanation:

Question: 44

Which feature is configured for managed devices in the device platform settings of the Firepower Management
Center?

A. quality of service
B. time synchronization
C. network address translations
D. intrusion policy

Answer: B

Explanation:

Question: 45

Which information is required when adding a device to Firepower Management Center?

A. username and password
B. encryption method
C. device serial number
D. registration key

Answer: D

Explanation:

Question: 46

Which two deployment modes does the Cisco ASA FirePower module support? (Choose two)

A. transparent mode
B. routed mode
C. inline mode
D. active mode
E. passive monitor-only mode

Answer: C, D

Explanation:

You can configure your ASA FirePOWER module using one of the following deployment models:
You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment.
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/firewall/asa-firewall-asdm/
modules-sfr.html

Question: 47

The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the
ASA be added on the Cisco UC Manager platform?

A. Certificate Trust List
B. Endpoint Trust List
C. Enterprise Proxy Service
D. Secured Collaboration Proxy

Answer: A

Explanation:

Question: 48

Which statement about the configuration of Cisco ASA NetFlow v9 Secure Event Logging is true?

A. To view bandwidth usage for NetFlow records, the QoS feature must be enabled.
B. A sysopt command can be used to enable NSEL on a specific interface.
C. NSEL can be used without a collector configured.
D. A flow-export event type must be defined under a policy

Answer: D

Explanation:

Question: 49

Which feature is supported when deploying Cisco ASAv within AWS public cloud?

A. multiple context mode
B. user deployment of Layer 3 networks
C. IPv6
D. clustering

Answer: B

Explanation:

The ASAv on AWS supports the following features:
+ Support for Amazon EC2 C5 instances, the next generation of the Amazon EC2 Compute Optimized instance
family.
+ Deployment in the Virtual Private Cloud (VPC)
+ Enhanced networking (SR-IOV) where available
+ Deployment from Amazon Marketplace
+ Maximum of four vCPUs per instance
+ User deployment of L3 networks
+ Routed mode (default)
Note: The Cisco Adaptive Security Virtual Appliance (ASAv) runs the same software as physical Cisco ASAs to deliver proven security functionality in a virtual form factor. The ASAv can be deployed in the public AWS cloud.
It can then be configured to protect virtual and physical data center workloads that expand, contract, or shift their location over time. Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96qsg/asavaws.html

Question: 50

Which statement describes a traffic profile on a Cisco Next Generation Intrusion Prevention System?

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

Answer: B

Explanation:

Question: 51

Which statement about IOS zone-based firewalls is true?

A. An unassigned interface can communicate with assigned interfaces
B. Only one interface can be assigned to a zone.
C. An interface can be assigned to multiple zones.
D. An interface can be assigned only to one zone.

Answer: D

Explanation:

Question: 52

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

A. It tracks flow-create, flow-teardown, and flow-denied events.
B. It provides stateless IP flow tracking that exports all records of a specific flow.
C. It tracks the flow continuously and provides updates every 10 seconds.
D. Its events match all traffic classes in parallel.

Answer: A

Explanation:

The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs).
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.html

Question: 53

Which CLI command is used to register a Cisco FirePower sensor to Firepower Management Center?

A. configure system add <host><key>
B. configure manager <key> add host
C. configure manager delete
D. configure manager add <host><key

Answer: D

Explanation:

Question: 54

Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention
System?

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

Answer: D

Explanation:

The Firepower System uses network discovery and identity policies to collect host, application, and user data
for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive
map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and
respond to the vulnerabilities and exploits to which your organization is susceptible.
You can configure your network discovery policy to perform host and application detection.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.html

Question: 55

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

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

Answer: C

Explanation:

Question: 56

Refer to the exhibit.

```
Gateway of last resort is 1.1.1.1 to network 0.0.0.0

S*   0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C        1.1.1.0 255.255.255.0 is directly connect, outside
S        172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C        192.168.100.0 255.255.255.0 is directly connected, inside
C        172.16.10.0 255.255.255.0 is directly connected, dmz
S          10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz

---------------------------------------------------------------

access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
 match access-list redirect-acl

policy-map inside-policy
 class redirect-class
 sfr fail-open

service-policy inside-policy global
```


What is a result of the configuration?

A. Traffic from the DMZ network isredirected
B. Trafficfrom the inside network is redirected
C. All TCP traffic is redirected
D. Traffic from the inside and DMZ networks is redirected

Answer: D

Explanation:

The purpose of above commands is to redirect traffic that matches the ACL "redirect-acl" to the Cisco FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and
any other actions that are applied by policy are performed, the traffic is returned to the ASA for further
processing and ultimate transmission.
The command "service-policy global_policy global" applies the policy to all of the interfaces.
Reference: https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.html

Question: 57

Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?

A. Group Policy
B. Access Control Policy
C. Device Management Policy
D. Platform Service Policy

Answer: D

Explanation:

Cisco Firepower deployments can take advantage of platform settings policies. A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. Examples of these platform settings policies are time and date settings, external authentication, and other common
administrative features.
A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device. For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/platform_settings_policies_for_managed_devices.html
Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best
answer here so we have to choose it.

Question: 58

Which two tasks allow NetFlow on a Cisco ASA 5500 Series firewall? (Choose two)

A. Enable NetFlow Version 9.
B. Create an ACL to allow UDP traffic on port 9996.
C. Apply NetFlow Exporter to the outside interface in the inbound direction.
D. Create a class map to match interesting traffic.
E. Define a NetFlow collector by using the flow-export command

Answer: C, E

Explanation:

Question: 59

A mall provides security services to customers with a shared appliance. The mall wants separation of management on the shared appliance. Which ASA deployment mode meets these needs?

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

Answer: C

Explanation:

Question: 60

What is a characteristic of Firepower NGIPS inline deployment mode?

A. ASA with Firepower module cannot be deployed.
B. It cannot take actions such as blocking traffic.
C. It is out-of-band from traffic.
D. It must have inline interface pairs configured.

Answer: D

Explanation:

Question: 61

An engineer wants to generate NetFlow records on traffic traversing the Cisco AS
A. Which Cisco ASA
command must be used?
A. flow-export destination inside 1.1.1.1 2055
B. ip flow monitor input
C. ip flow-export destination 1.1.1.1 2055
D. flow exporter

Answer: A

Explanation:

The syntax of this command is: flow-export destination interface-name ipv4-address | hostname udp-port
This command is used on Cisco ASA to configure Network Secure Event Logging (NSEL) collector to which
NetFlow packets are sent. The destination keyword indicates that a NSEL collector is being

configured.
+ The interface-name argument is the name of the ASA and ASA Services Module interface through which the
collector is reached.
+ The ipv4-address argument is the IP address of the machine running the collector application.
+ The hostname argument is the destination IP address or name of the collector.
+ The udp-port argument is the UDP port number to which NetFlow packets are sent.
You can configure a maximum of five collectors. After a collector is configured, template records are automatically sent to all configured NSEL collectors.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_nsel.html

Question: 62

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

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

Answer: B

Explanation:

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

Question: 63

Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention
System? (Choose two)

A. packet decoder
B. SIP
C. modbus
D. inline normalization
E. SSL

Answer: B, E

Explanation:

Application layer protocols can represent the same data in a variety of ways. The Firepower System provides
application layer protocol decoders that normalize specific types of packet data into formats that the intrusion
rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively
apply the same content-related rules to packets whose data is represented differently and obtain meaningful
results.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Application_Layer_Preprocessors.html#ID-2244-0000080c
FirePower uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

Question: 64

Which two features of Cisco Email Security can protect your organization against email threats? (Choose two)

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

Answer: B, D

Explanation:

Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution.
Cisco Email Security appliance can now handle incoming mail connections and incoming messages from
specific geolocations and perform appropriate actions on them, for example:
– Prevent email threats coming from specific geographic regions.
– Allow or disallow emails coming from specific geographic regions.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_00.html

Question: 65

Why would a user choose an on-premises ESA versus the CES solution?

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

Answer: A

Explanation:

Question: 66

Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware?
(Choose two)

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

Answer: A, D

Explanation:

Question: 67

What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?

A. It decrypts HTTPS application traffic for unauthenticated users.
B. It alerts users when the WSA decrypts their traffic.
C. It decrypts HTTPS application traffic for authenticated users.
D. It provides enhanced HTTPS application detection for AsyncOS.

Answer: D

Explanation:

Question: 68

Which two statements about a Cisco WSA configured in Transparent mode are true? (Choose two)

A. It can handle explicit HTTP requests.
B. It requires a PAC file for the client web browser.
C. It requires a proxy for the client web browser.
D. WCCP v2-enabled devices can automatically redirect traffic destined to port 80.
E. Layer 4 switches can automatically redirect traffic destined to port 80.

Answer: D, E

Explanation:

Question: 69

Which action controls the amount of URI text that is stored in Cisco WSA logs files?

A. Configure the datasecurityconfig command
B. Configure the advancedproxyconfig command with the HTTPS subcommand
C. Configure a small log-entry size.
D. Configure a maximum packet size.

Answer: B

Explanation:

Question: 70

An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a
recipient address. Which list contains the allowed recipient addresses?

A. SAT
B. BAT
C. HAT
D. RAT

Answer: D

Explanation:

Question: 71

Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two)

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

Answer: D, E

Explanation:

Cisco Hybrid Email Security is a unique service offering that combines a cloud-based email security deployment

with an appliance-based email security deployment (on premises) to provide maximum choice and control for
your organization. The cloud-based infrastructure is typically used for inbound email cleansing, while the onpremises appliances provide granular control – protecting sensitive information with data loss prevention (DLP) and encryption technologies.
Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

Question: 72

Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?

A. IP Blacklist Center
B. File Reputation Center
C. AMP Reputation Center
D. IP and Domain Reputation Center

Answer: D

Explanation:

Question: 73

Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

A. transparent
B. redirection
C. forward
D. proxy gateway

Answer: A

Explanation:

There are two possible methods to accomplish the redirection of traffic to Cisco WSA: transparent proxy mode and explicit proxy mode.
In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to Cisco WSA, without any configuration on the client. The transparent proxy
deployment is used in this design, and the Cisco ASA firewall is used to redirect traffic to the appliance because all of the outbound web traffic passes through the device and is generally managed by the same operations staff who manage Cisco WSA.
Reference:
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesignGuide-AUG13.pdf

Question: 74

After deploying a Cisco ESA on your network, you notice that some messages fail to reach their destinations.
Which task can you perform to determine where each message was lost?

A. Configure the trackingconfig command to enable message tracking.
B. Generate a system report.
C. Review the log files.
D. Perform a trace.

Answer: A

Explanation:

Message tracking helps resolve help desk calls by giving a detailed view of message flow. For example, if a message was not delivered as expected, you can determine if it was found to contain a virus or placed in a spam quarantine — or if it is located somewhere else in the mail stream.
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_12_0_chapter_011110.html

Question: 75

What is the primary benefit of deploying an ESA in hybrid mode?

A. You can fine-tune its settings to provide the optimum balance between security and performance for your environment
B. It provides the lowest total cost of ownership by reducing the need for physical appliances
C. It provides maximum protection and control of outbound messages
D. It provides email security while supporting the transition to the cloud

Answer: D

Explanation:

Cisco Hybrid Email Security is a unique service offering that facilitates the deployment of your email security
infrastructure both on premises and in the cloud. You can change the number of on-premises versus cloud
users at any time throughout the term of your contract, assuming the total number of users does not change.
This allows for deployment flexibility as your organization's needs change.

Question: 76

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

A. Mail Submission Agent

B. Mail Transfer Agent
C. Mail Delivery Agent
D. Mail User Agent

Answer: B

Explanation:

Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work
by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing
email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within
the email-delivery chain. Another name for an MTA is a mail relay.
Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/
Cisco_SBA_BN_EmailSecurityUsingCiscoESADeploymentGuide-Feb2013.pdf

Question: 77

Which technology is used to improve web traffic performance by proxy caching?

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

Answer: A

Explanation:

Question: 78

In which two ways does a system administrator send web traffic transparently to the Web Security Appliance?
(Choose two)

A. configure Active Directory Group Policies to push proxy settings
B. configure policy-based routing on the network infrastructure
C. reference a Proxy Auto Config file
D. configure the proxy IP address in the web-browser settings
E. use Web Cache Communication Protocol

Answer: C, E

Explanation:

Question: 79

Which technology reduces data loss by identifying sensitive information stored in public computing environments?

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

Answer: D

Explanation:

Question: 80

Which deployment model is the most secure when considering risks to cloud adoption?

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

Answer: D

Explanation:

Question: 81

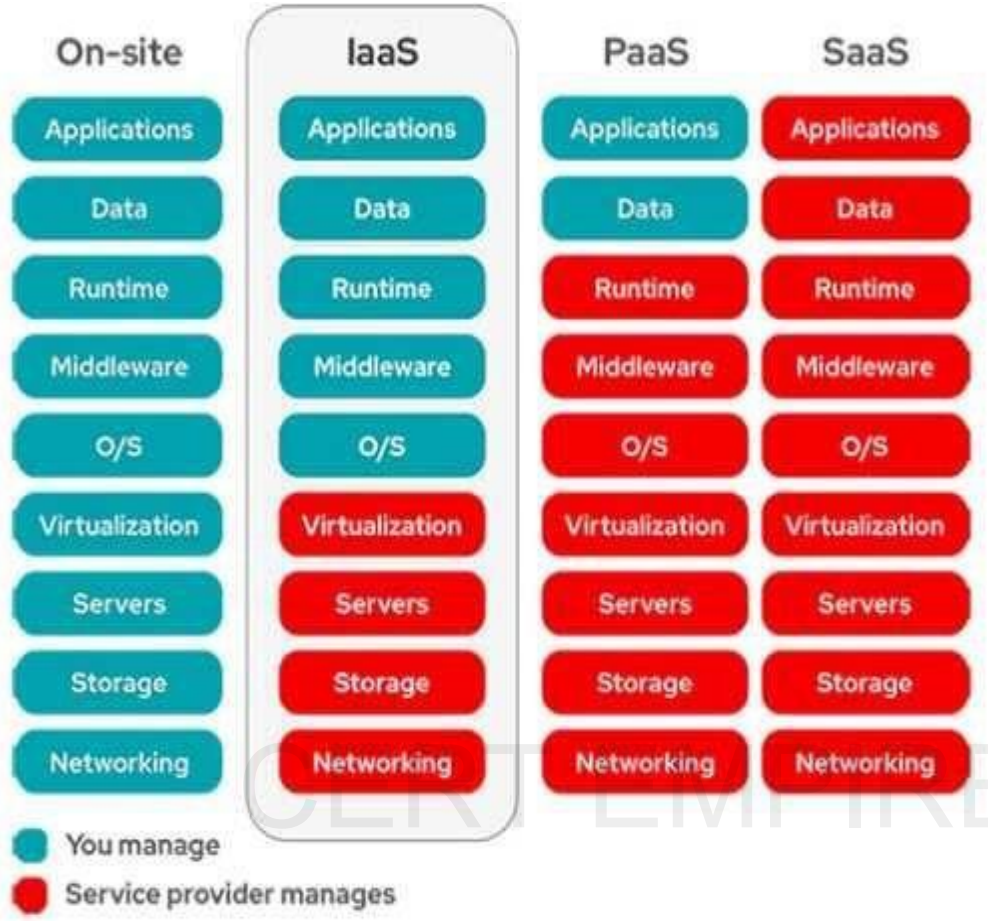
In which cloud services model is the tenant responsible for virtual machine OS patching?

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

Answer: A

Explanation:

Only in On-site (on-premises) and IaaS we (tenant) manage O/S (Operating System).



Question: 82

Which cloud service model offers an environment for cloud consumers to develop and deploy applications
without needing to manage or maintain the underlying cloud infrastructure?

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

Answer: A

Explanation:

Cloud computing can be broken into the following three basic models:
+ Infrastructure as a Service (IaaS): IaaS describes a cloud solution where you are renting infrastructure. You purchase virtual power to execute your software as needed. This is much like running a virtual server on your own equipment, except you are now running a virtual server on a virtual disk. This model is similar to a utility company model because you pay for what you use.
+ Platform as a Service (PaaS): PaaS provides everything except applications. Services provided by this

model include all phases of the system development life cycle (SDLC) and can use application programming interfaces (APIs), website portals, or gateway software. These solutions tend to be proprietary, which can cause problems if the customer moves away from the provider's platform.
+ Software as a Service (SaaS): SaaS is designed to provide a complete packaged solution. The software is rented out to the user. The service is usually provided through some type of front end or web portal. While the end user is free to use the service from anywhere, the company pays a peruse fee.
Reference: CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide

Question: 83

What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?

A. It allows the administrator to quarantine malicious files so that the application can function, just not
maliciously.
B. It discovers and controls cloud apps that are connected to a company's corporate environment.
C. It deletes any application that does not belong in the network.
D. It sends the application information to an administrator to act on.

Answer: B

Explanation:

Question: 84

Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

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

Answer: D

Explanation:

Question: 85

In a PaaS model, which layer is the tenant responsible for maintaining and patching?

A. hypervisor
B. virtual machine
C. network
D. application

Answer: D

Explanation:

Question: 86

On which part of the IT environment does DevSecOps focus?

A. application development
B. wireless network
C. data center
D. perimeter network

Answer: A

Explanation:

Question: 87

What is the function of Cisco Cloudlock for data security?

A. data loss prevention
B. controls malicious cloud apps
C. detects anomalies
D. user and entity behavior analytics

Answer: A

Explanation:

Question: 88

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

Answer: A

Explanation:

Question: 89

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

Answer: C

Explanation:

Question: 90

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

Answer: A, C

Explanation:

Question: 91

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

Answer: C

Explanation:

Question: 92

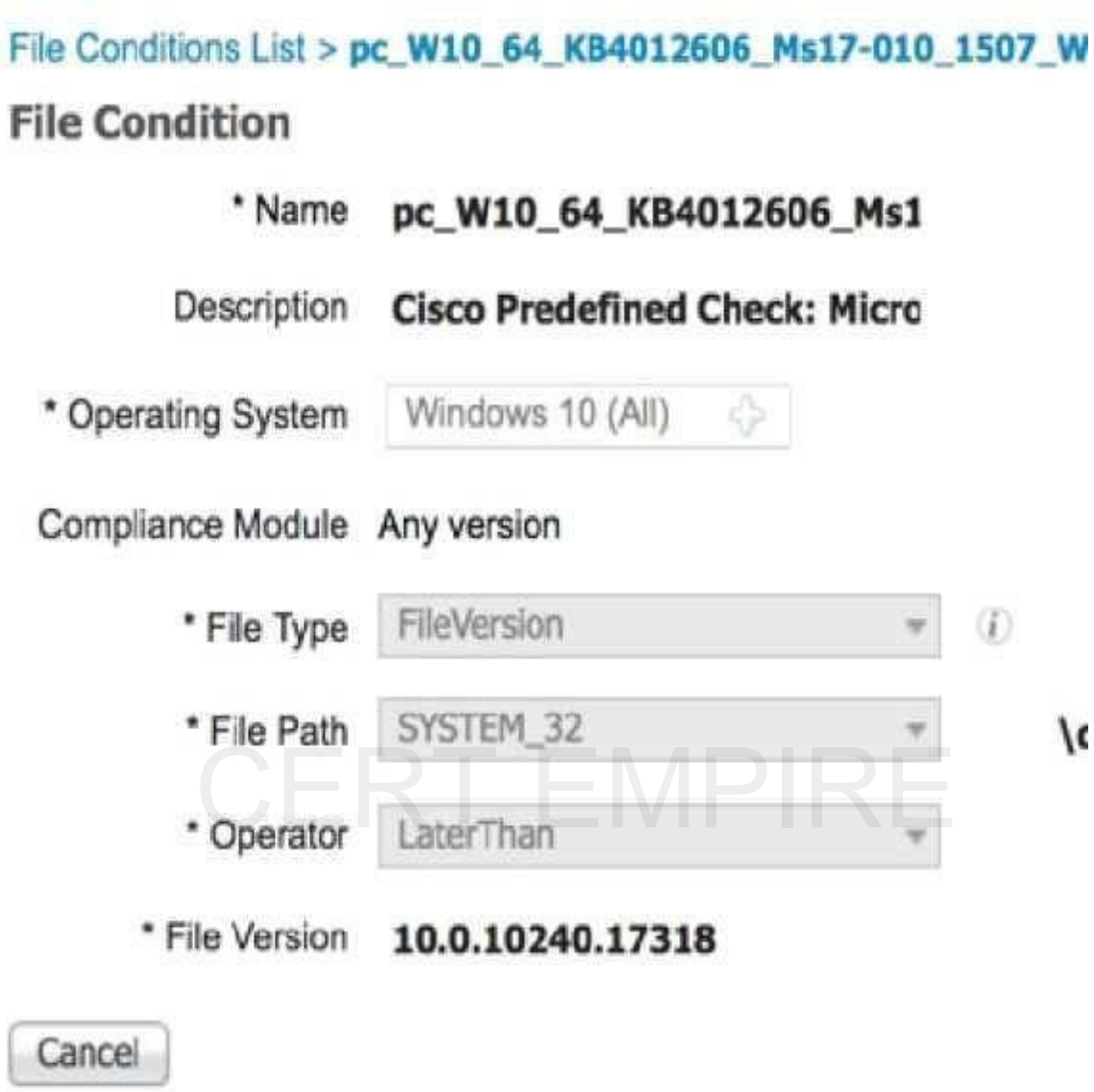
An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch
was not installed, which left the endpoint vulnerable to WannaCry ransomware. Which two solutions mitigate
the risk of this ransom ware infection? (Choose two)

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.

Answer: A, C

Explanation:

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



Question: 93

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

Answer: A

Explanation:

Question: 94

What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services?
(Choose two)

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

Answer: B, D

Explanation:

Question: 95

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

Answer: A, D

Explanation:

Question: 96

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

A. compliant
B. unknown
C. authorized
D. noncompliant

Answer: D

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: 97

Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?

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

Answer: A

Explanation:

Question: 98

Which IPS engine detects ARP spoofing?

A. Atomic ARP Engine
B. Service Generic Engine
C. ARP Inspection Engine
D. AIC Engine

Answer: A

Explanation:

Question: 99

What is a characteristic of Dynamic ARP Inspection?

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

snooping binding database.
B. In a typical network, make all ports as trusted except for the ports connecting to switches, which are
untrusted
C. DAI associates a trust state with each switch.
D. DAI intercepts all ARP requests and responses on trusted ports only.

Answer: A

Explanation:

Question: 100

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.

Answer: A

Explanation:

Question: 101

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

Answer: A, E

Explanation:

Question: 102

Which command enables 802.1X globally on a Cisco switch?

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

Answer: A

Explanation:

Question: 103

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

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

Answer: C

Explanation:

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-based-networkingservices/config_guide_c17-663759.html

Question: 104

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

Answer: D

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: 105

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

Answer: D

Explanation:

Question: 106

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

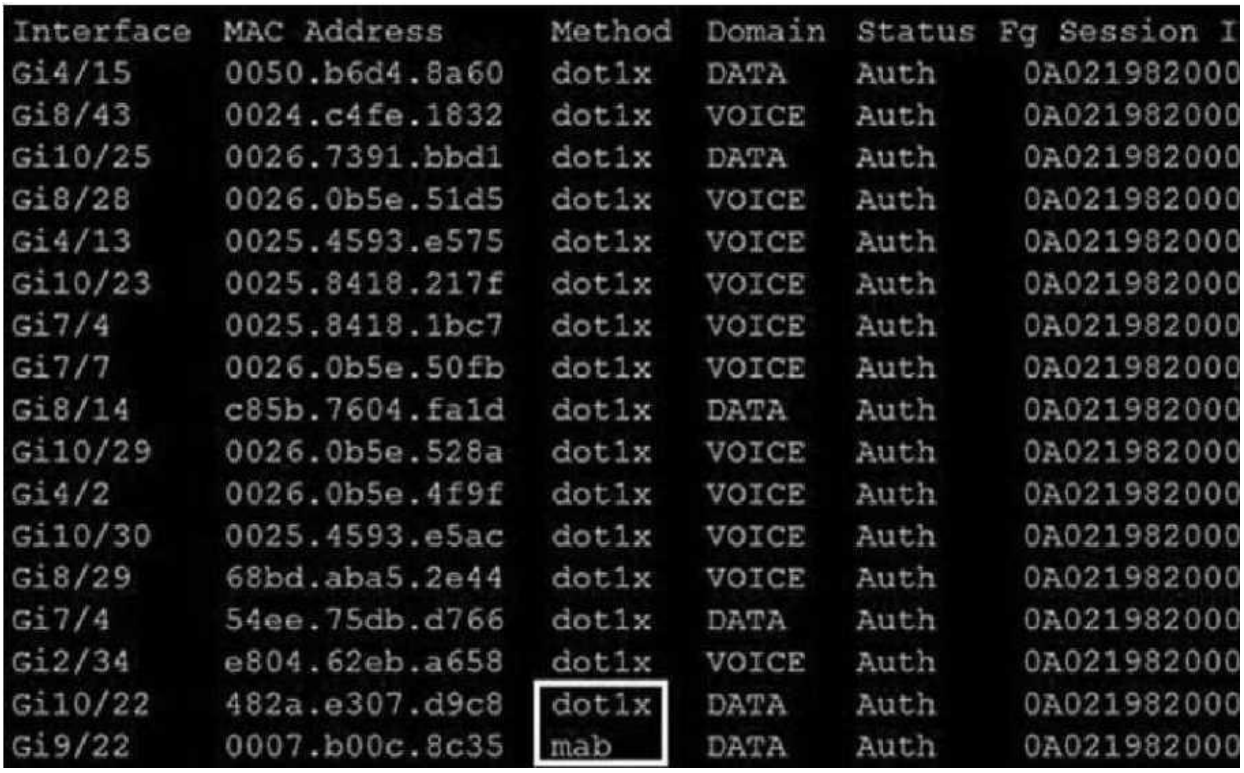
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXX
asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
D. asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX
asa-host(config)#snmp-server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

Answer: D

Explanation:

Question: 107

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

Answer: D

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#wp3404908137
Displaying the Summary of All Auth Manager Sessions on the Switch
Enter 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: 108

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

Answer: B

Explanation:

Question: 109

Refer to the exhibit.

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

What does the number 15 represent in this configuration?
A. privilege level for an authorized user to this router
B. access list that identifies the SNMP devices that can access the router
C. interval in seconds between SNMPv3 authentication attempts
D. number of possible failed attempts until the SNMPv3 user is locked out

Answer: B

Explanation:

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

Question: 110

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

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

Answer: B, D

Explanation:

The profiling service issues the change of authorization in the following cases:
– Endpoint deleted—When an endpoint is deleted from the Endpoints page and the endpoint is disconnected
or removed from the network.
An exception action is configured—If you have an exception action configured per profile that leads to an
unusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to the
corresponding static profile by issuing a CoA.
– An endpoint is profiled for the first time—When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.
+ An endpoint identity group has changed—When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.
The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:
++ The endpoint identity group changes for endpoints when they are dynamically profiled
++ The endpoint identity group changes when the static assignment flag is set to true for a dynamic endpoint – An endpoint profiling policy has changed and the policy is used in an authorization policy—When an endpoint profiling policy changes, and the policy is included in a logical profile that is used in an authorization policy. The endpoint profiling policy may change due to the profiling policy match or when an endpoint is statically assigned to an endpoint profiling policy, which is associated to a logical profile. In both the cases, the profiling service issues a CoA, only when the endpoint profiling policy is used in an authorization policy.
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: 111

Refer to the exhibit.

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

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

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

Answer: B

Explanation:

The user "admin5" was configured with privilege level 5. In order to allow configuration (enter 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: 112

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

Answer: A

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: 113

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

Answer: A

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: 114

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

Answer: C

Explanation:

Question: 115

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

Answer: A

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: 116

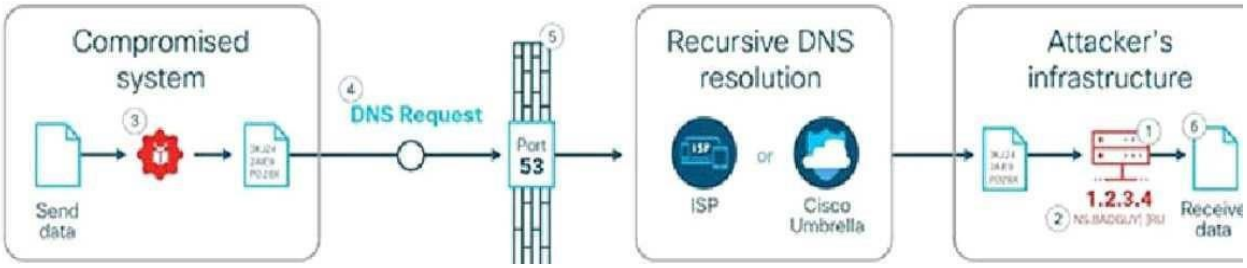
How is DNS tunneling used to exfiltrate data out of a corporate network?

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.

Answer: B

Explanation:

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



The attacker incorporates one of many open-source DNS tunneling kits into an authoritative 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: 117

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

Answer: C, E

Explanation:

Question: 118

Which Cisco AMP file disposition valid?

A. pristine
B. malware
C. dirty
D. non malicious

Answer: B

Explanation:

Question: 119

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

Answer: B

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-config-guidev60/Reference_a_wrapper_Chapter_topic_here.html
-> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload the
whole 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: 120

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

Answer: C

Explanation:

Question: 121

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

Answer: B

Explanation:

Question: 122

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

Answer: C

Explanation:

Question: 123

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

Answer: C

Explanation:

Question: 124

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

Answer: B, D

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: 125

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.

Answer: D

Explanation:

Question: 126

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

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

Answer: A, C

Explanation:

Question: 127

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

Answer: A

Explanation:

Question: 128

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

Answer: C

Explanation:

This command uses RADIUS which combines authentication and authorization in one function (packet).

Question: 129

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

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

Answer: B

Explanation:

Question: 130

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

Answer: B

Explanation:

Question: 131

An MDM provides which two advantages to an organization with regards to device management? (Choose two)

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

Answer: A, B

Explanation:

Question: 132

Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the
deployment?

A. NGFW
B. AMP
C. WSA
D. ESA

Answer: B

Explanation:

Question: 133

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

A. It streamlines the incident response process to automatically perform digital forensics on the endpoint.

B. It allows the organization to mitigate web-based attacks as long as the user is active in the domain.
C. It allows the organization to detect and respond to threats at the edge of the network.
D. It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.

Answer: D

Explanation:

Question: 134

What are the two most commonly used authentication factors in multifactor authentication? (Choose two)

A. biometric factor
B. time factor
C. confidentiality factor
D. knowledge factor
E. encryption factor

Answer: A, D

Explanation:

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more
verification factors to gain access to a resource. MFA requires means of verification that unauthorized users
won't have.
Proper multi-factor authentication uses factors from at least two different categories.
MFA methods:
+ Knowledge – usually a password – is the most commonly used tool in MFA solutions. However, despite their
simplicity, passwords have become a security problem and slow down productivity.
+ Physical factors – also called possession factors–use tokens, such as a USB dongle or a portable device,
that generate a temporary QR (quick response) code. Mobile phones are commonly used, as they have the
advantage of being readily available in most situations.
+ Inherent – This category includes biometrics like fingerprint, face, and retina scans. As technology advances,
it may also include voice ID or other behavioral inputs like keystroke metrics. Because inherent factors are
reliably unique, always present, and secure, this category shows promise.
+ Location-based and time-based – Authentication systems can use GPS coordinates, network

parameters,
and metadata for the network in use, and device recognition for MFA. Adaptive authentication combines these
data points with historical or contextual user data.
A time factor in conjunction with a location factor could detect an attacker attempting to authenticate in Europe
when the user was last authenticated in California an hour prior, for example.
+ Time-based one-time password (TOTP) – This is generally used in 2FA but could apply to any MFA method where a second step is introduced dynamically at login upon completing a first step. The wait for a
second step–in which temporary passcodes are sent by SMS or email–is usually brief, and the process is easy
to use for a wide range of users and devices. This method is currently widely used.
+ Social media – In this case a user grants permission for a website to use their social media username and
password for login. This provide an easy login process, and one generally available to all users.
+ Risk-based authentication – Sometimes called adaptive multi-factor authentication, this method combines
adaptive authentication and algorithms that calculate risk and observe the context of specific login requests.
The goal of this method is to reduce redundant logins and provide a more user-friendly workflow.
+ Push-based 2FA – Push-based 2FA improves on SMS and TOTP 2FA by adding additional layers of security
while improving ease of use. It confirms a user's identity with multiple factors of authentication that other
methods cannot. Because push-based 2FA sends notifications through data networks like cellular or Wi-Fi,
users must have data access on their mobile devices to use the 2FA functionality.
Reference: https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html
The two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint,
face, and retina scans. Biometrics is used commonly in mobile devices).

Question: 135

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

A. phishing
B. brute force
C. man-in-the-middle
D. DDOS
E. teardrop

Answer: B, C

Explanation:

Question: 136

What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and
Response?

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

Answer: A

Explanation:

Question: 137

An engineer wants to automatically assign endpoints that have a specific OUI into a new endpoint group. Which
probe must be enabled for this type of profiling to work?

A. NetFlow
B. NMAP
C. SNMP
D. DHCP

Answer: B

Explanation:

Cisco ISE can determine the type of device or endpoint connecting to the network by performing "profiling."
Profiling is done by using DHCP, SNMP, Span, NetFlow, HTTP, RADIUS, DNS, or NMAP scans to collect as
much metadata as possible to learn the device fingerprint.
NMAP ("Network Mapper") is a popular network scanner which provides a lot of features. One of them is the
OUI (Organizationally Unique Identifier) information. OUI is the first 24 bit or 6 hexadecimal value of the MAC
address.
Note: DHCP probe cannot collect OUIs of endpoints. NMAP scan probe can collect these endpoint attributes:
+ EndPointPolicy
+ LastNmapScanCount
+ NmapScanCount
+ OUI
+ Operating-system

Reference: http://www.network-node.com/blog/2016/1/2/ise-20-profiling

Question: 138

What are two reasons for implementing a multifactor authentication solution such as Duo Security provide to an
organization? (Choose two)

A. flexibility of different methods of 2FA such as phone callbacks, SMS passcodes, and push notifications
B. single sign-on access to on-premises and cloud applications
C. integration with 802.1x security using native Microsoft Windows supplicant
D. secure access to on-premises and cloud applications
E. identification and correction of application vulnerabilities before allowing access to resources

Answer: A, D

Explanation:

Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a
second factor (like your phone or other mobile device) prevents anyone but you from logging in, even if they
know your password.
Note: Single sign-on (SSO) is a property of identity and access management that enables users to securely
authenticate with multiple applications and websites by logging in only once with just one set of credentials
(username and password). With SSO, the application or website that the user is trying to access relies on a
trusted third party to verify that users are who they say they are.

Question: 139

An engineer configured a new network identity in Cisco Umbrella but must verify that traffic is being routed
through the Cisco Umbrella network. Which action tests the routing?

A. Ensure that the client computers are pointing to the on-premises DNS servers.
B. Enable the Intelligent Proxy to validate that traffic is being routed correctly.
C. Add the public IP address that the client computers are behind to a Core Identity.
D. Browse to http://welcome.umbrella.com/ to validate that the new identity is working.

Answer: D

Explanation:

Question: 140

Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

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

Answer: C

Explanation:

SSL Decryption is an important part of the Umbrella Intelligent Proxy. he feature allows the Intelligent Proxy to go beyond simply inspecting normal URLs and actually proxy and inspect traffic that's sent over HTTPS. The SSL Decryption feature does require the root certificate be installed.
Reference: https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-IntelligentProxy

Question: 141

How is Cisco Umbrella configured to log only security events?

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

Answer: A

Explanation:

The logging of your identities' activities is set per-policy when you first create a policy. By default, logging is on and set to log all requests an identity makes to reach destinations. At any time after you create a policy, you can change what level of identity activity Umbrella logs.
From the Policy wizard, log settings are:
Log All Requests—For full logging, whether for content, security or otherwise
Log Only Security Events—For security logging only, which gives your users more privacy—a good setting for people with the roaming client installed on personal devices
Don't Log Any Requests—Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on.
Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management

Question: 142

How does Cisco Umbrella archive logs to an enterprise owned storage?

A. by using the Application Programming Interface to fetch the logs
B. by sending logs via syslog to an on-premises or cloud-based syslog server
C. by the system administrator downloading the logs from the Cisco Umbrella web portal

D. by being configured to send logs to a self-managed AWS S3 bucket

Answer: D

Explanation:

The Cisco Umbrella Multi-Org console has the ability to upload, store, and archive traffic activity logs from your organizations' Umbrella dashboards to the cloud through Amazon S3. CSV formatted Umbrella logs are compressed (gzip) and uploaded every ten minutes so that there's a minimum of delay between traffic from the organization's Umbrella dashboard being logged and then being available to download from an S3 bucket.
By having your organizations' logs uploaded to an S3 bucket, you can then download logs automatically to keep in perpetuity in backup storage.
Reference: https://docs.umbrella.com/deployment-umbrella/docs/manage-logs

Question: 143

When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are
blocked when they host malware, command and control, phishing, and more threats?

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

Answer: B

Explanation:

Question: 144

Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

A. AMP
B. AnyConnect
C. DynDNS
D. Talos

Answer: D

Explanation:

When Umbrella receives a DNS request, it uses intelligence to determine if the request is safe, malicious or risky — meaning the domain contains both malicious and legitimate content. Safe and

malicious requests are routed as usual or blocked, respectively. Risky requests are routed to our cloud-based proxy for deeper inspection. The Umbrella proxy uses Cisco Talos web reputation and other third-party feeds to determine if a URL is malicious.

Question: 145

Where are individual sites specified to be blacklisted in Cisco Umbrella?

A. application settings
B. content categories
C. security settings
D. destination lists

Answer: D

Explanation:

A destination list is a list of internet destinations that can be blocked or allowed based on the administrative
preferences for the policies applied to the identities within your organization. A destination is an IP address
(IPv4), URL, or fully qualified domain name. You can add a destination list to Umbrella at any time; however, a
destination list does not come into use until it is added to a policy.
Reference: https://docs.umbrella.com/deployment-umbrella/docs/working-with-destination-lists

Question: 146

Which Cisco security solution protects remote users against phishing attacks when they are not connected to
the VPN?

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

Answer: B

Explanation:

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

Question: 147

How does Cisco Stealthwatch Cloud provide security for cloud environments?

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

Answer: A

Explanation:

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

Question: 148

What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two)

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

Answer: A, B

Explanation:

Cisco Cognitive Threat Analytics helps you quickly detect and respond to sophisticated, clandestine attacks that are already under way or are attempting to establish a presence within your environment. The solution automatically identifies and investigates suspicious or malicious web-based traffic. It identifies both potential and confirmed threats, allowing you to quickly remediate the infection and reduce the scope and damage of an attack, whether it's a known threat campaign that has spread across multiple organizations or a unique threat you've never seen before.
Detection and analytics features provided in Cognitive Threat Analytics are shown below:
+ Data exfiltration: Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content
+ Command-and-control (C2) communication: Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPSencoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad
range of threats
…
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-

analytics/at-aglance-c45-736555.pdf

Question: 149

Which network monitoring solution uses streams and pushes operational data to provide a near real-time view
of activity?

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

Answer: D

Explanation:

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.
Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming.
Reference: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide

Question: 150

What provides visibility and awareness into what is currently occurring on the network?

A. CMX
B. WMI
C. Prime Infrastructure
D. Telemetry

Answer: D

Explanation:

Telemetry – Information and/or data that provides awareness and visibility into what is occurring on the network

at any given time from networking devices, appliances, applications or servers in which the core function of the
device is not to generate security alerts designed to detect unwanted or malicious activity from computer
networks.
Reference:
https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/active threat-analytics-premier.pdf

Question: 151

What can be integrated with Cisco Threat Intelligence Director to provide information about security threats,
which allows the SOC to proactively automate responses to those threats?

A. Cisco Umbrella
B. External Threat Feeds
C. Cisco Threat Grid
D. Cisco Stealthwatch

Answer: C

Explanation:

Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically.
Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector

Question: 152

Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application traffic?

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

Answer: B

Explanation:

The Cisco Application Visibility and Control (AVC) solution leverages multiple technologies to recognize,

analyze, and control over 1000 applications, including voice and video, email, file sharing, gaming, peer-to-peer
(P2P), and cloud-based applications. AVC combines several Cisco IOS/IOS XE components, as well as communicating with external tools, to integrate the following functions into a powerful solution…
Reference: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/guide/avc-user-guide/avc_tech_overview.html

Question: 153

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

A. DHCP
B. Design
C. Accounting
D. DNS
E. Provision

Answer: B, E

Explanation:

Cisco DNA Center has four general sections aligned to IT workflows:
Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller
Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site.
Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains
threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need.
Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task.
The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity—greatly

facilitating remote office setups.
Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation
automates resolution to keep your network performing at its optimal with less mundane troubleshooting work.
The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks.
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- dna-center-so-cte-en.html

Question: 154

What must be used to share data between multiple security products?

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

Answer: B

Explanation:

Question: 155

Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from
Cisco and other vendors to share data and interoperate with each other?

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

Answer: B

Explanation:

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

Question: 156

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

A. intent-based APIs

B. automation adapters
C. domain integration
D. application adapters

Answer: A

Explanation:

Question: 157

What is the function of the Context Directory Agent?

A. maintains users' group memberships
B. relays user authentication requests from Web Security Appliance to Active Directory
C. reads the Active Directory logs to map IP addresses to usernames
D. accepts user authentication requests on behalf of Web Security Appliance for user identification

Answer: C

Explanation:

Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow
security gateways to understand which user is using which IP Address in the network, so those security
gateways can now make decisions based on those users (or the groups to which the users belong to).
CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_oveviw.html

Question: 158

What is a characteristic of a bridge group in ASA Firewall transparent mode?

A. It includes multiple interfaces and access rules between interfaces are customizable
B. It is a Layer 3 segment and includes one port and customizable access rules
C. It allows ARP traffic with a single access rule
D. It has an IP address on its BVI interface and is used for management traffic

Answer: A

Explanation:

A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place.
Each bridge group includes a Bridge Virtual Interface (BVI). The ASA uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.
You can include multiple interfaces per bridge group. If you use more than 2 interfaces per bridge group, you can control communication between multiple segments on the same network, and not just between inside and outside. For example, if you have three inside segments that you do not want to communicate with each other, you can put each segment on a separate interface, and only allow them to communicate with the outside interface. Or you can customize the access rules between interfaces to allow only as much access as desired.
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.html
Note: BVI interface is not used for management purpose. But we can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA.

Question: 159

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

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

Answer: B

Explanation:

Vendors, security researchers, and vulnerability coordination centers typically assign vulnerabilities an identifier that's disclosed to the public. This identifier is known as the Common Vulnerabilities and Exposures (CVE).
CVE is an industry-wide standard. CVE is sponsored by US-CERT, the office of Cybersecurity and Communications at the U.S. Department of Homeland Security.
The goal of CVE is to make it's easier to share data across tools, vulnerability repositories, and security
services.
Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide

Question: 160

Which two fields are defined in the NetFlow flow? (Choose two)

A. type of service byte

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

Answer: A, D

Explanation:

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

Question: 161

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

A. NetFlow
B. desktop client
C. ASDM
D. API

Answer: D

Explanation:

Question: 162

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

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

Answer: D

Explanation:

Question: 163

An organization is trying to improve their Defense in Depth by blocking malicious destinations prior to a
connection being established. The solution must be able to block certain applications from being used within the network. Which product should be used to accomplish this goal?

A. Cisco Firepower
B. Cisco Umbrella
C. ISE
D. AMP

Answer: B

Explanation:

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

Question: 164

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

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

Answer: B

Explanation:

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

Question: 165

An engineer is trying to securely connect to a router and wants to prevent insecure algorithms from being used.
However, the connection is failing. Which action should be taken to accomplish this goal?

A. Disable telnet using the no ip telnet command.
B. Enable the SSH server using the ip ssh server command.
C. Configure the port using the ip ssh port 22 command.
D. Generate the RSA key using the crypto key generate rsa command.

Answer: D

Explanation:

In this question, the engineer was trying to secure the connection so maybe he was trying to allow SSH to the device. But maybe something went wrong so the connection was failing (the connection used to be good). So maybe he was missing the "crypto key generate rsa" command.

Question: 166

A network administrator is using the Cisco ESA with AMP to upload files to the cloud for analysis. The network
is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?

A. AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.
B. The file is queued for upload when connectivity is restored.
C. The file upload is abandoned.
D. The ESA immediately makes another attempt to upload the file.

Answer: C

Explanation:

The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.
Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technoteesa-00.html
In this question, it stated "the network is congested" (not the file analysis server was overloaded) so the
appliance will not try to upload the file again.

Question: 167

Which type of algorithm provides the highest level of protection against brute-force attacks?

A. PFS
B. HMAC
C. MD5
D. SHA

Answer: D

Explanation:

Question: 168

What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is
deleted from an identity group?

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

Answer: B

Explanation:

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration
page that enables the profiling service with more control over endpoints that are already authenticated.
One of the settings to configure the CoA type is "Reauth". This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.
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_010101.html

Question: 169

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?

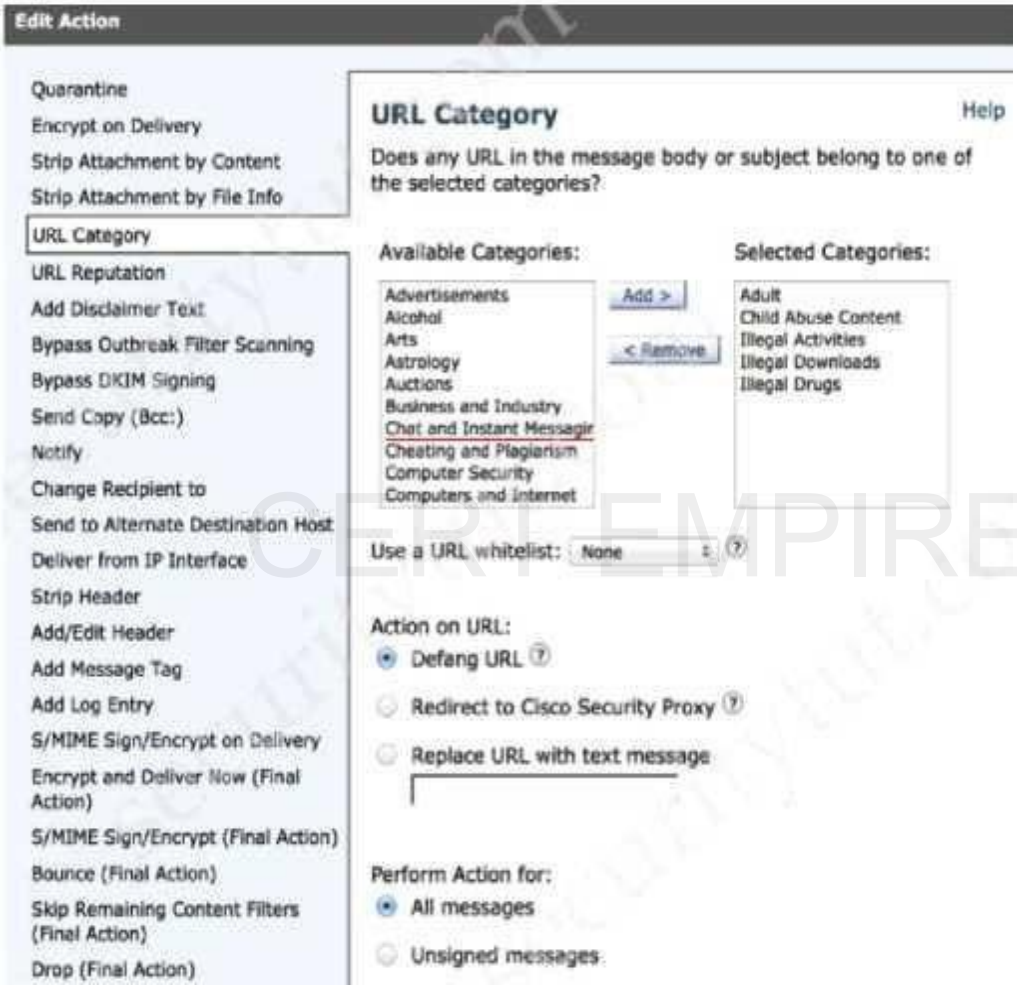
A. 1
B. 3
C. 5

D. 10

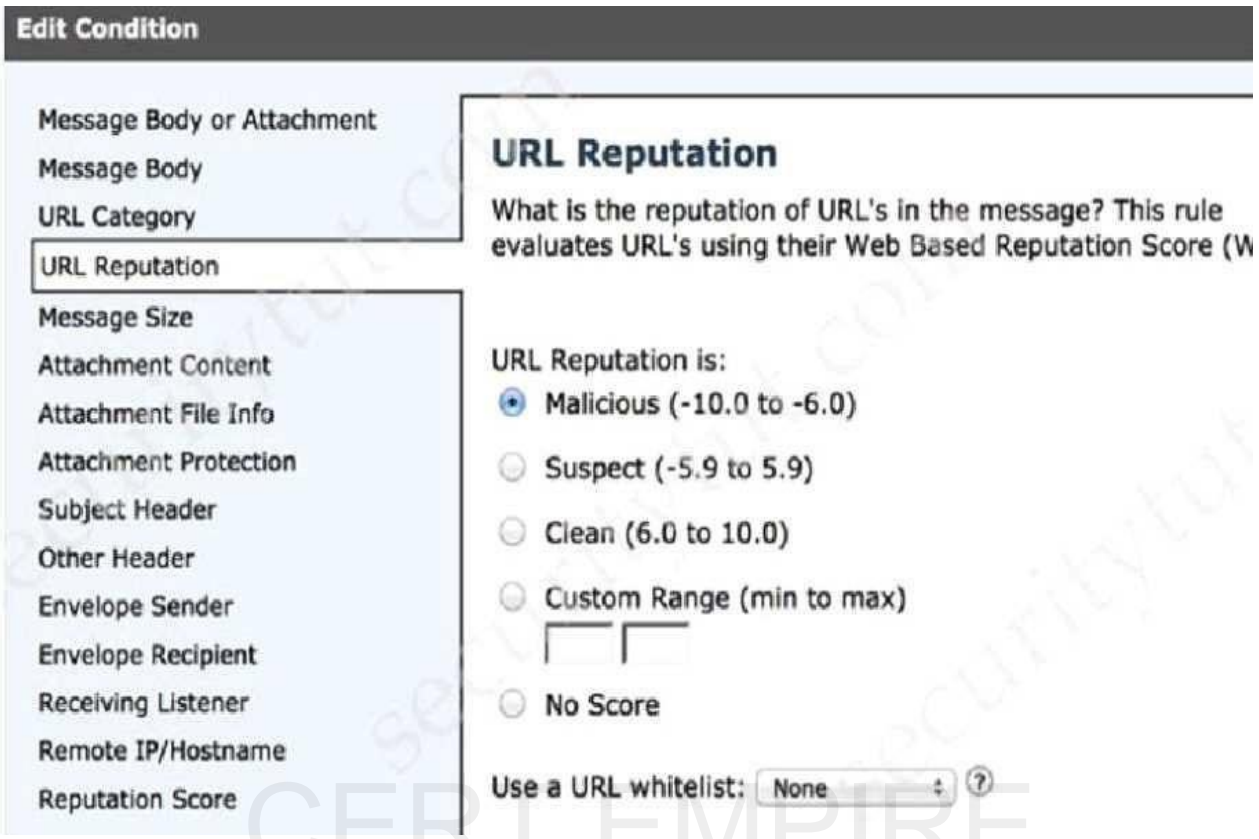
Answer: D

Explanation:

We choose “Chat and Instant Messaging” category in “URL Category”:



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



Question: 170

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

Answer: B

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: 171

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

Answer: E

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.pdf
The Cisco Intercloud Fabric architecture provides two product configurations to address the following two
consumption 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: 172

What are two DDoS attack categories? (Choose two)

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

Answer: B, D

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-ddos-attacks/

Question: 173

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

Answer: D

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.html
The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

Question: 174

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

Answer: D

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: 175

Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?

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

Answer: B

Explanation:

Question: 176

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.

Answer: D, E

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-communications-protocol-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: 177

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

Answer: A

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-config-guidev60/Access_Control_Rules URL_Filtering.html

Question: 178

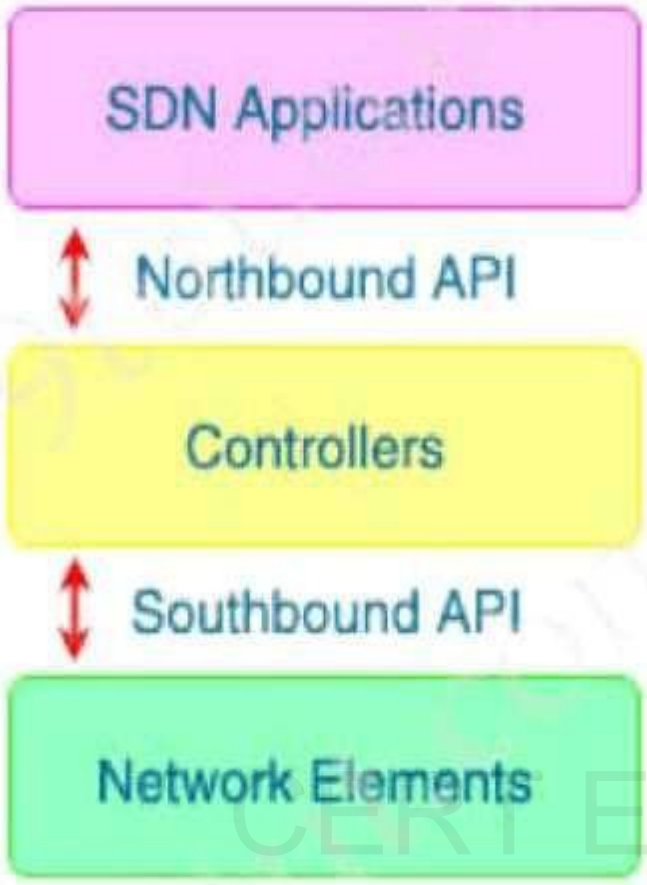
What is the function of SDN southbound API protocols?

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

Answer: B

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: 179

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.

Answer: B

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-ike-protocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html

Question: 180

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

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

Answer: B

Explanation:

Question: 181

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

Answer: A, C

Explanation:

Security Intelligence Sources
...
Custom 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/fpmc-configguide-v623/security_intelligence_blacklisting.html

Question: 182

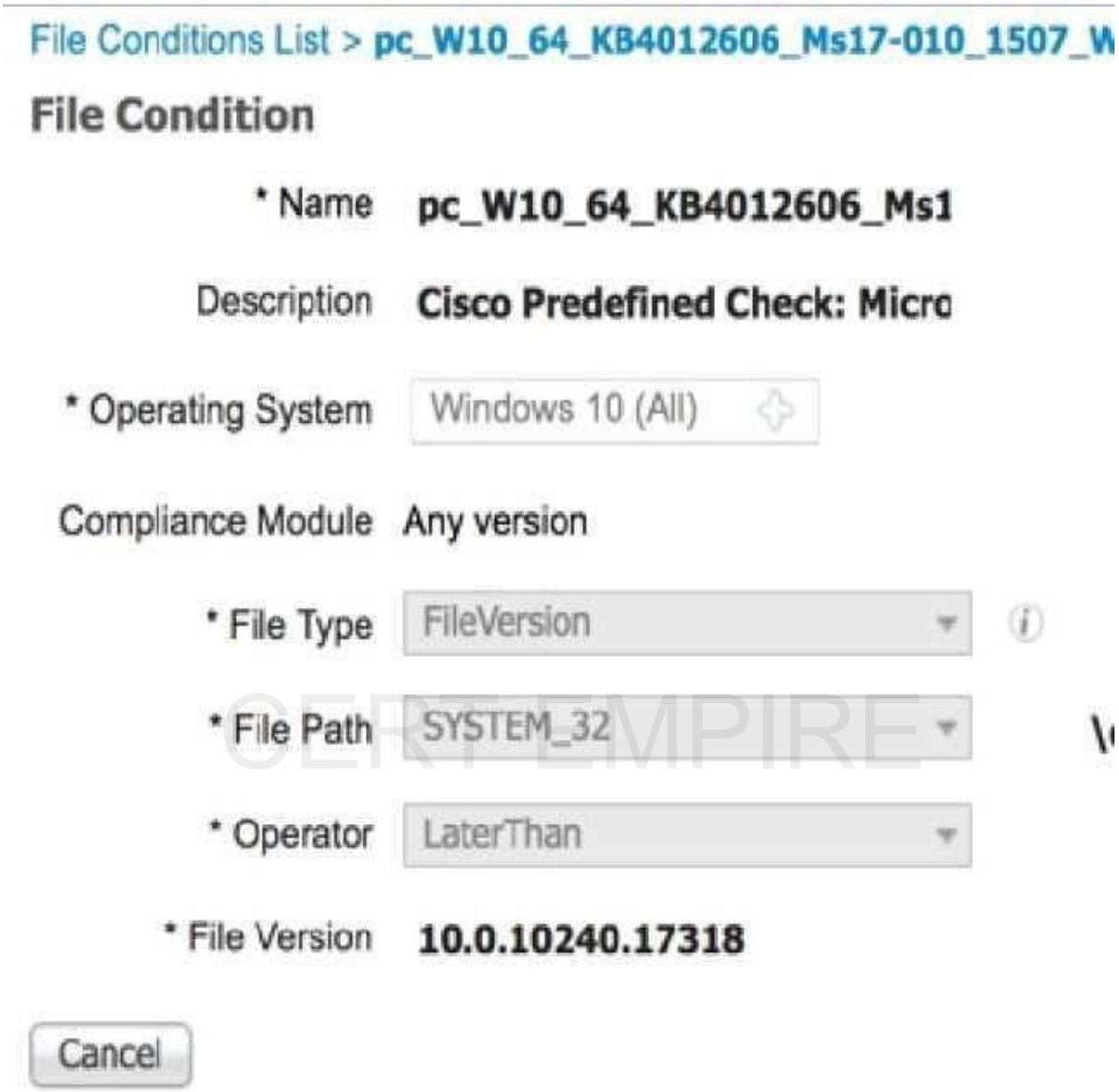
Which Cisco platform ensures that machines that connect to organizational networks have the recommended
antivirus definitions and patches to help prevent an organizational malware outbreak?

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

Answer: C

Explanation:

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



Question: 183

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

Answer: A, C

Explanation:

NetFlow is typically used for several key customer applications, including the following:
…
Billing 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.html
If the predefined Flexible NetFlow records are not suitable for your traffic requirements, you can create 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#wp1057997
Note: Traditional NetFlow allows us to monitor from Layer 2 to 4 but Flexible NetFlow goes beyond these
layers.

Question: 184

How does DNS Tunneling exfiltrate data?

A. An attacker registers a domain that a client connects to based on DNS records and sends malware through
that connection.
B. An attacker opens a reverse DNS shell to get into the client's system and install malware on it.
C. An attacker uses a non-standard DNS port to gain access to the organization's DNS servers in order to
poison the resolutions.
D. An attacker sends an email to the target with hidden DNS resolvers in it to redirect them to a malicious
domain.

Answer: A

Explanation:

Question: 185

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

A. phishing
B. slowloris

C. pharming
D. SYN flood

Answer: D

Explanation:

Question: 186

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

Answer: A

Explanation:

Question: 187

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

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

Answer: B, E

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: 188

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

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

Answer: C

Explanation:

Question: 189

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

Answer: C

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: 190

What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

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

Answer: D

Explanation:

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: 191

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

Answer: B

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: 192

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

Answer: D

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-virtual-appliance-asav/ white-paper-c11-740505.html

Question: 193

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

Answer: A

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: 194

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

Answer: D

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: 195

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

Answer: B

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: 196

What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?

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

Answer: A

Explanation:

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

Question: 197

What is managed by Cisco Security Manager?

A. access point
B. WSA
C. ASA
D. ESA

Answer: C

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: 198

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.

Answer: D

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: 199

What is a benefit of using Cisco FMC over Cisco ASDM?

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

Answer: B

Explanation:

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/firepower-compatibility.html
The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management.
Reference: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheetc78-736775.html

Question: 200

What is a key difference between Cisco Firepower and Cisco ASA?

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

Answer: C

Explanation:

Question: 201

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

Answer: A

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.
…
Umbrella'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-import-information

Question: 202

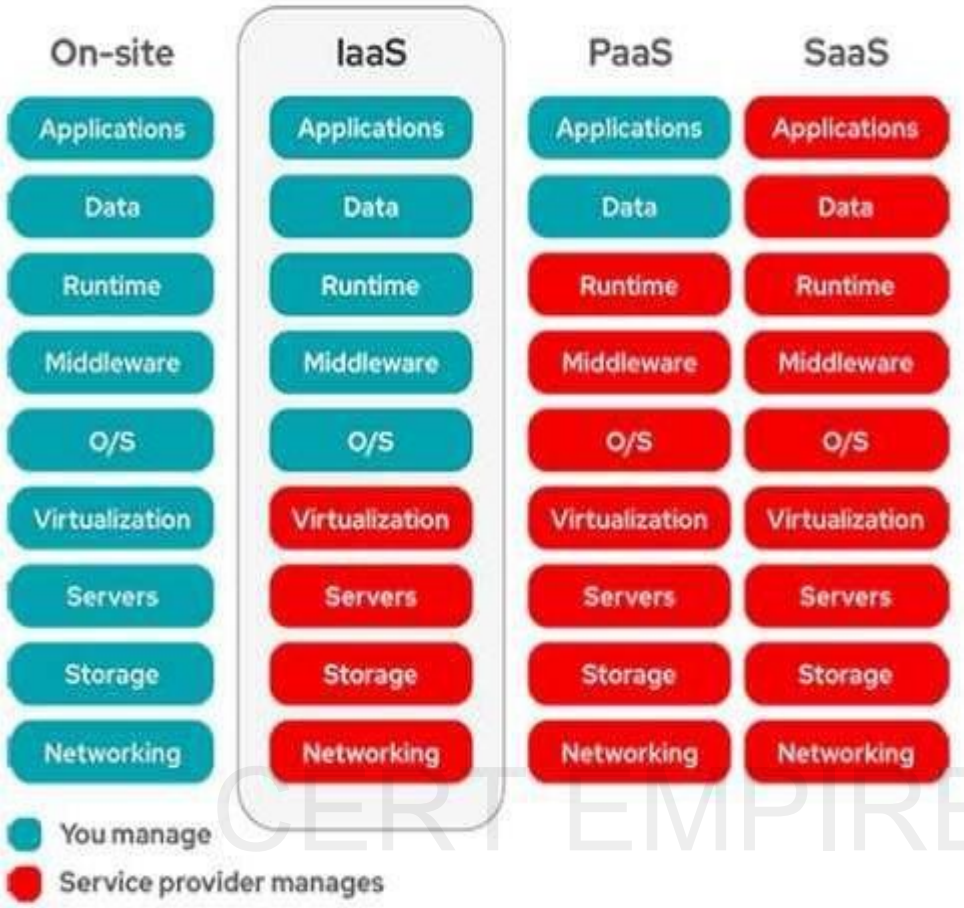
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two)

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

Answer: D, E

Explanation:

Customers must manage applications and data in PaaS.



Question: 203

What is an attribute of the DevSecOps process?

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

Answer: C

Explanation:

DevSecOps (development, security, and operations) is a concept used in recent years to describe how to 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: 204

An engineer notices traffic interruption on the network. Upon further investigation, it is learned that broadcast
packets have been flooding the network. What must be configured, based on a predefined threshold, to
address this issue?

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

Answer: C

Explanation:

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

Question: 205

Which two cryptographic algorithms are used with IPsec? (Choose two)

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

Answer: C, E

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: 206

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

Answer: B

Explanation:

Question: 207

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

A. smurf
B. MITM
C. teardrop
D. LAND

Answer: C

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: 208

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

Answer: D

Explanation:

Question: 209

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

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

Answer: B, C

Explanation:

Question: 210

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.

Answer: B

Explanation:

Question: 211

Which algorithm provides asymmetric encryption?

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

Answer: C

Explanation:

Question: 212

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

Answer: B, D

Explanation:

Question: 213

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

Answer: B, E

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: 214

Which attack type attempts to shut down a machine or network so that users are not able to access it?

A. smurf
B. bluesnarfing

C. MAC spoofing
D. IP spoofing

Answer: A

Explanation:

Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to 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: 215

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.

Answer: B

Explanation:

Question: 216

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

Answer: D

Explanation:

Question: 217

In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint

Protection Platform?

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

Answer: D

Explanation:

Endpoint protection platforms (EPP) prevent endpoint security threats like known and unknown malware.
Endpoint detection and response (EDR) solutions can detect and respond to threats that your EPP and other security tools did not catch.
EDR and EPP have similar goals but are designed to fulfill different purposes. EPP is designed to 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: 218

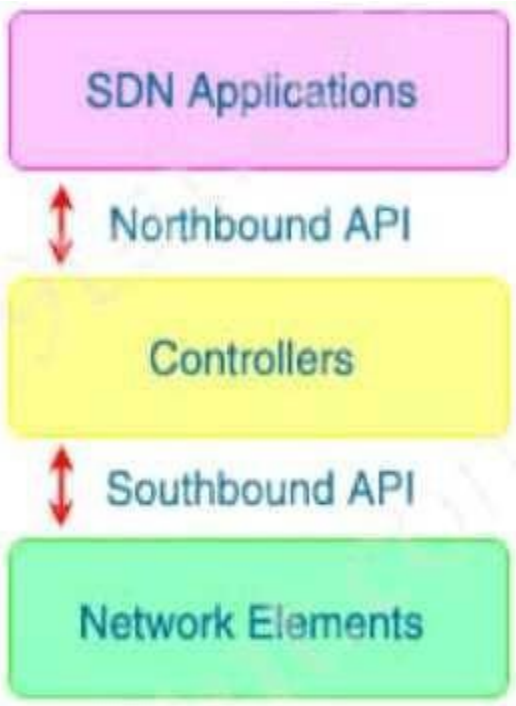
Which type of API is being used when a controller within a software-defined network architecture dynamically
makes configuration changes on switches within the network?

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

Answer: B

Explanation:

Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and
scalability needs.



Question: 219

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

Answer: A

Explanation:

Question: 220

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

Answer: C

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: 221

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

A. integrity
B. key exchange
C. encryption
D. authentication

Answer: A

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). HMAC-SHA-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: 222

A network engineer is deciding whether to use stateful or stateless failover when configuring two ASAs for high availability. What is the connection status in both cases?

A. need to be reestablished with stateful failover and preserved with stateless failover
B. preserved with stateful failover and need to be reestablished with stateless failover
C. preserved with both stateful and stateless failover
D. need to be reestablished with both stateful and stateless failover

Answer: B

Explanation:

Question: 223

Which type of protection encrypts RSA keys when they are exported and imported?

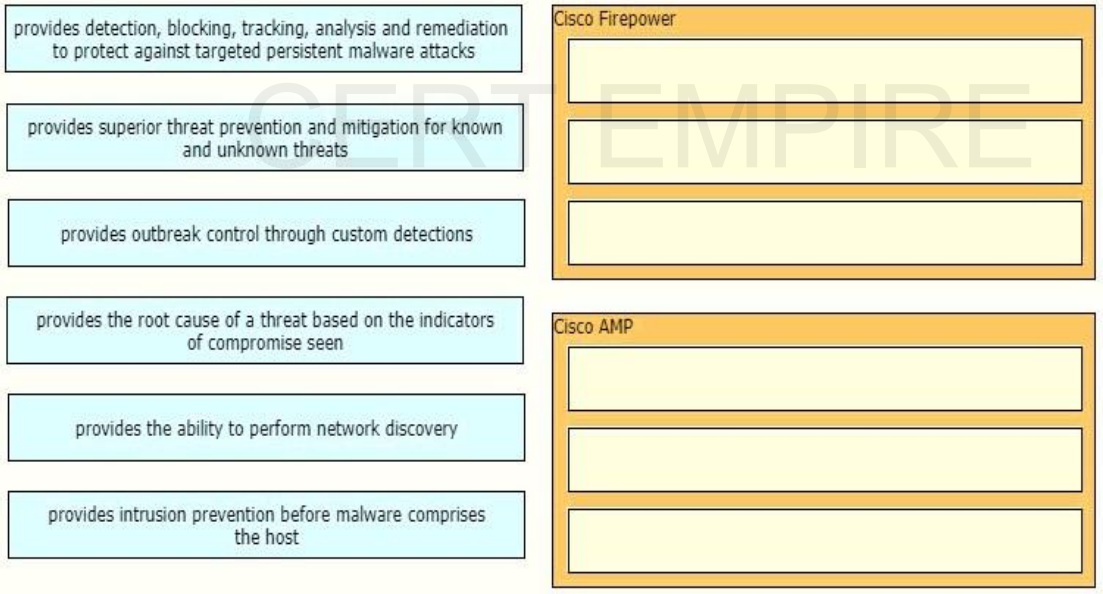
A. file
B. passphrase
C. NGE
D. nonexportable

Answer: B

Explanation:

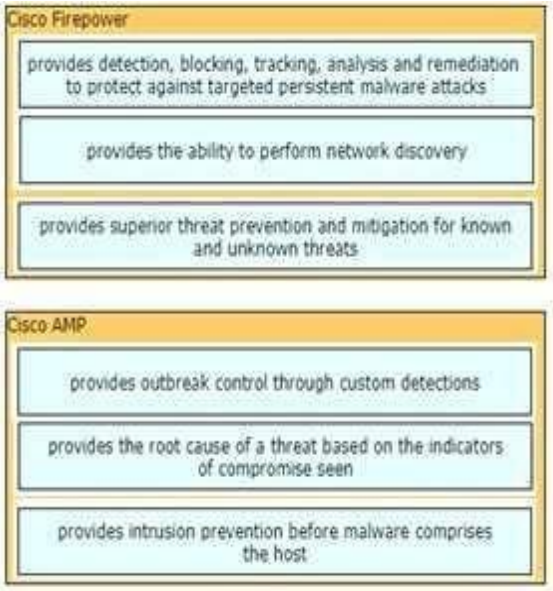
Question: 224

DRAG DROP
Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.



Answer:

Explanation:



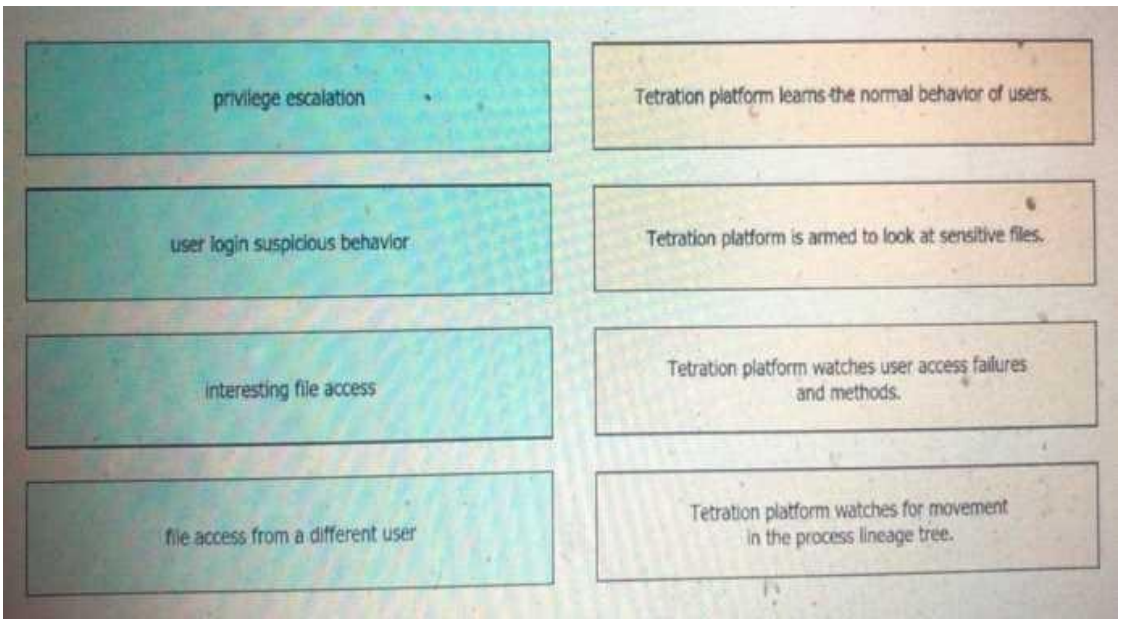
The Firepower System uses network discovery and identity policies to collect host, application, and user data for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible.

The Cisco Advanced Malware Protection (AMP) solution enables you to detect and block malware, continuously analyze for malware, and get retrospective alerts. AMP for Networks delivers network-based advanced malware protection that goes beyond point-in-time detection to protect your organization across the entire attack continuum – before, during, and after an attack. Designed for Cisco Firepower® network threat appliances, AMP for Networks detects, blocks, tracks, and contains malware threats across multiple threat vectors within a single system. It also provides the visibility and control necessary to protect your organization against highly sophisticated, targeted, zero-day, and persistent advanced malware threats.

Question: 225

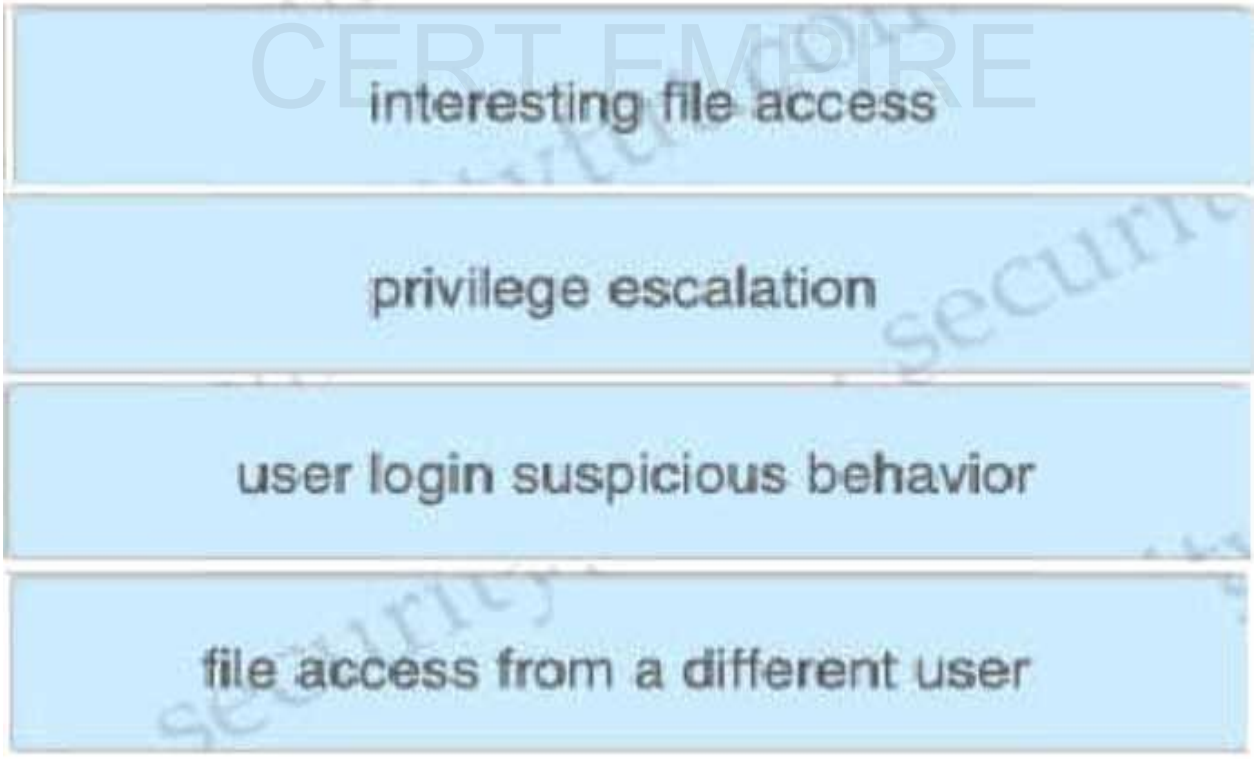
DRAG DROP

Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.



Answer:

Explanation:

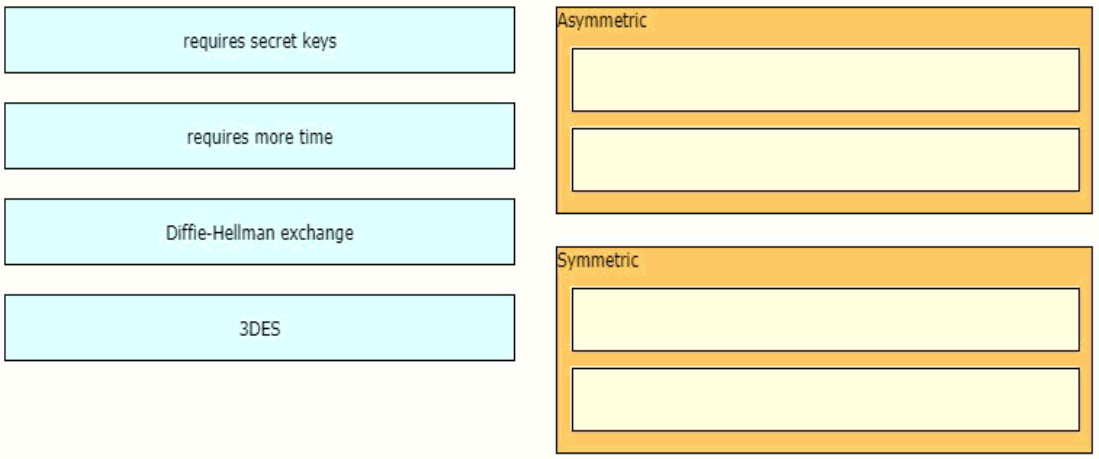


Cisco Tetration platform studies the behavior of the various processes and applications in the workload,
measuring them against known bad behavior sequences. It also factors in the process hashes it collects. By
studying various sets of malwares, the Tetration Analytics engineering team deconstructed it back into its basic
building blocks. Therefore, the platform understands clear and crisp definitions of these building blocks and

watches for them.
The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:
+ Shell code execution: Looks for the patterns used by shell code.
+ Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process
lineage tree.
+ Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts.
Using these, it can detect Meltdown, Spectre, and other cache-timing attacks.
+ Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping).
+ User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods.
+ Interesting file access: Cisco Tetration platform can be armed to look at sensitive files.
+ File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user.
+ Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage
of each command over time. Any new command or command with a different lineage triggers the interest of the
Tetration Analytics platform.
Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html

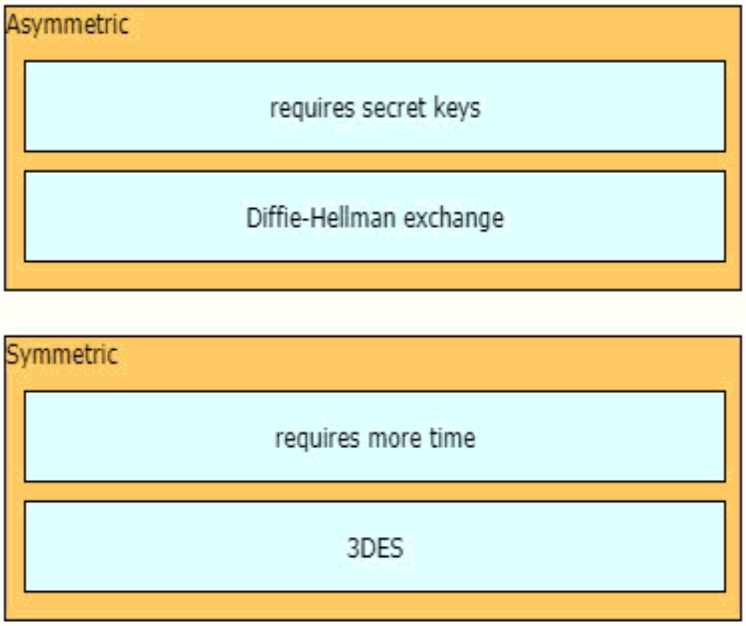
Question: 226

DRAG DROP
Drag and drop the descriptions from the left onto the encryption algorithms on the right.



Answer:

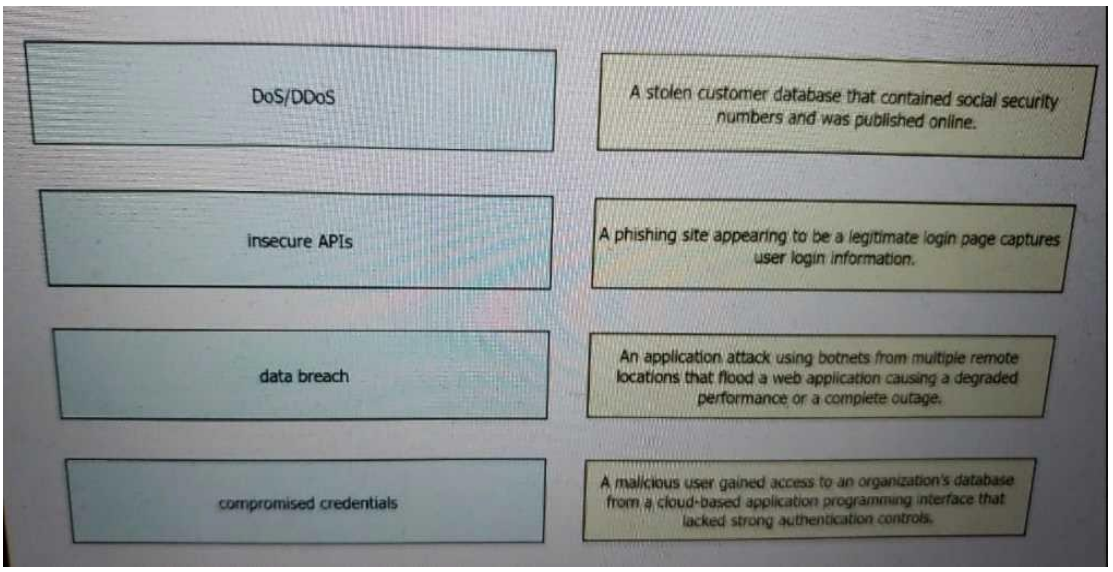
Explanation:



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

Question: 227

DRAG DROP
Drag and drop the threats from the left onto examples of that threat on the right



Answer:

Explanation:

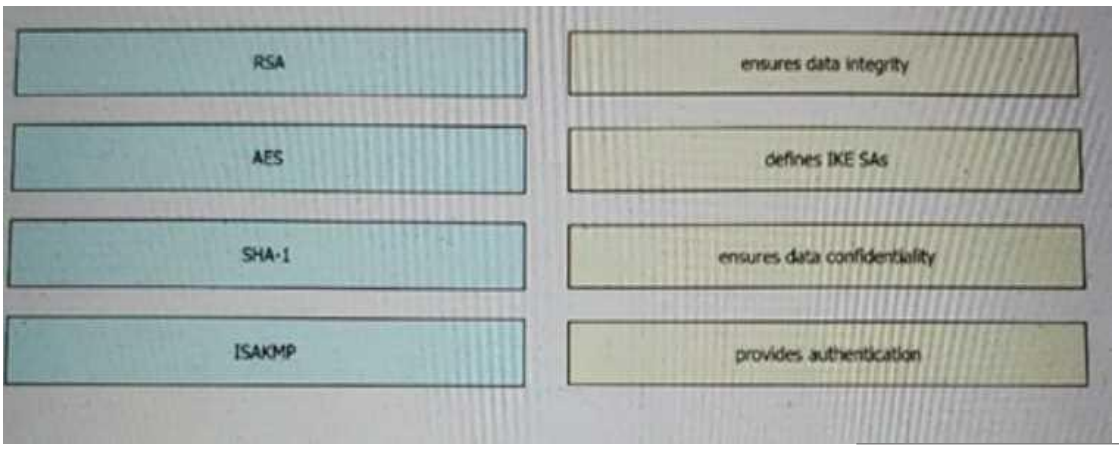
Correct Answer:

A data breach is the intentional or unintentional release of secure or private/confidential information to an
untrusted environment.
When your credentials have been compromised, it means someone other than you may be in possession of your account information, such as your username and/or password.

Question: 228

DRAG DROP

Drag and drop the VPN functions from the left onto the description on the right.



Answer:

Explanation:

The purpose of message integrity algorithms, such as Secure Hash Algorithm (SHA-1), ensures data has not
been changed in transit. They use one way hash functions to determine if data has been changed.
SHA-1, which is also known as HMAC-SHA-1 is a strong cryptographic hashing algorithm, stronger than
another popular algorithm known as Message Digest 5 (MD5). SHA-1 is used to provide data integrity (to
guarantee data has not been altered in transit) and authentication (to guarantee data came from the source it
was supposed to come from). SHA was produced to be used with the digital signature standard.
A VPN uses groundbreaking 256-bit AES encryption technology to secure your online connection against
cyberattacks that can compromise your security. It also offers robust protocols to combat malicious attacks and reinforce your online identity.
IKE SAs describe the security parameters between two IKE devices, the first stage in establishing IPSec

Question: 229

DRAG DROP
Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.

PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

Answer:

Explanation:

Distributed PortScan

Decoy PortScan

Port Sweep

PortScan Detection

Question: 230

DRAG DROP

Drag and drop the capabilities from the left onto the correct technologies on the right.

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

Answer:

Explanation:

superior threat prevention and mitigation for known and unknown threats

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks

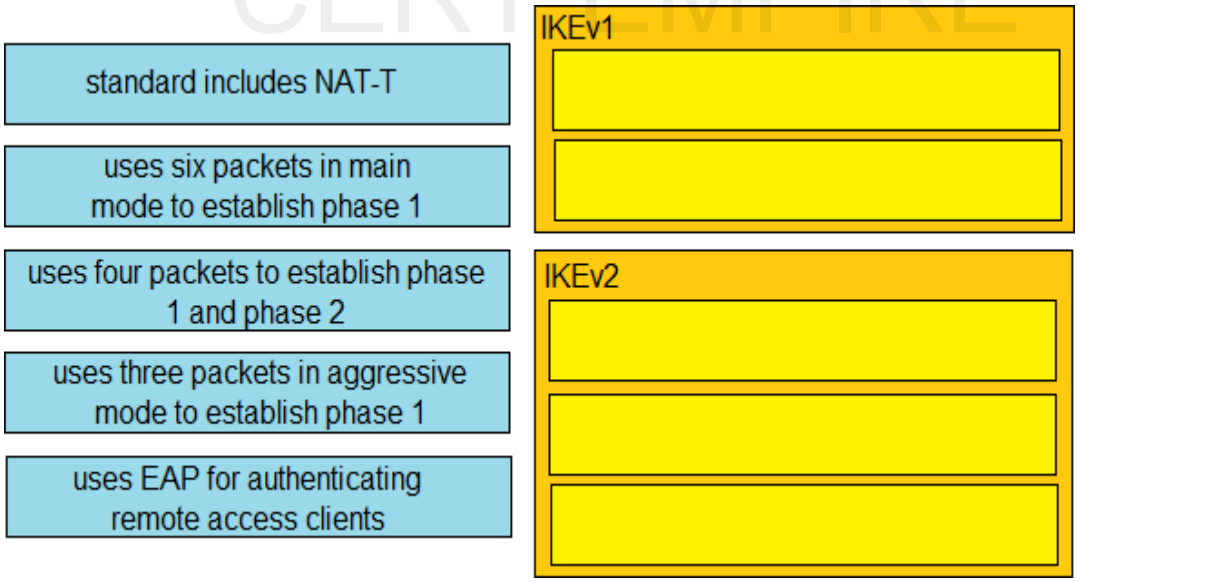
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs

combined integrated solution of strong defense and web protection, visibility, and controlling solutions

Question: 231

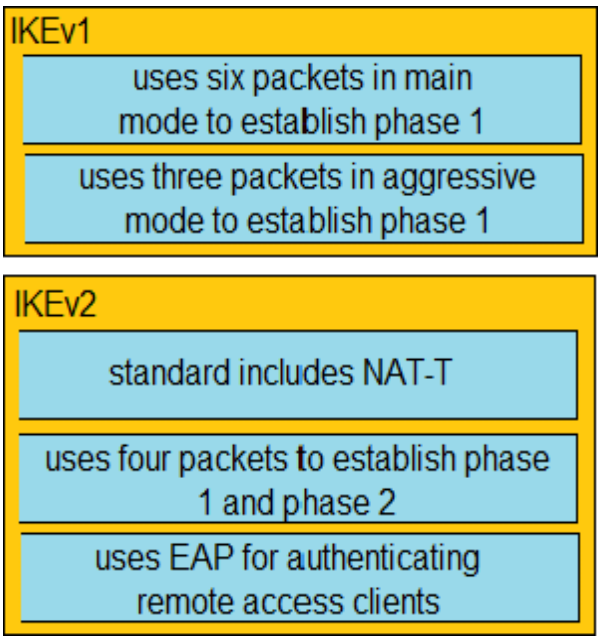
DRAG DROP

Drag and drop the descriptions from the left onto the correct protocol versions on the right.



Answer:

Explanation:



Question: 232

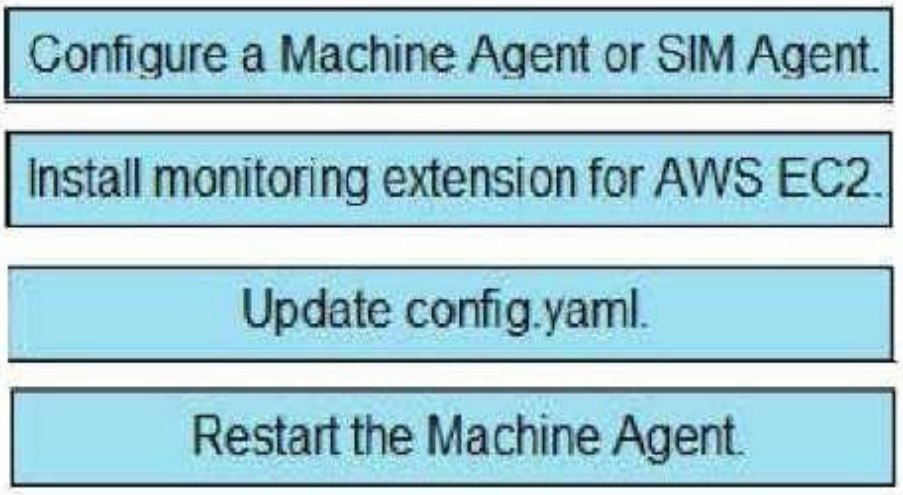
DRAG DROP

Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.

Install monitoring extension for AWS EC2.	step 1
Restart the Machine Agent.	step 2
Update config.yaml.	step 3
Configure a Machine Agent or SIM Agent.	step 4

Answer:

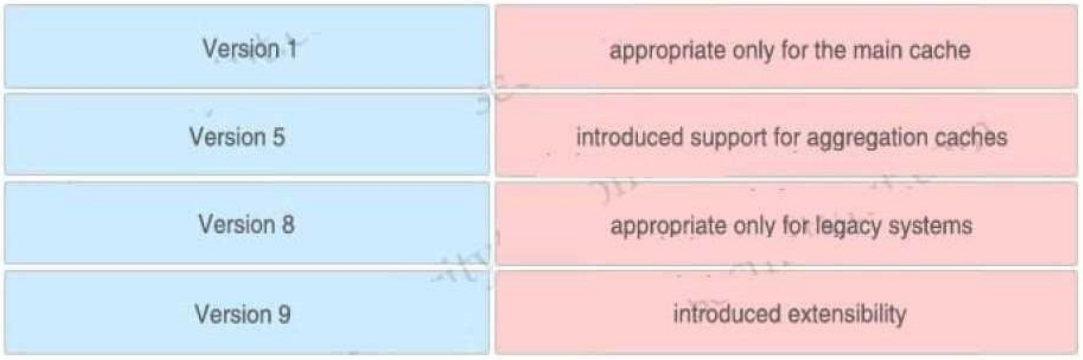
Explanation:



Question: 233

DRAG DROP

Drag and drop the NetFlow export formats from the left onto the descriptions on the right.



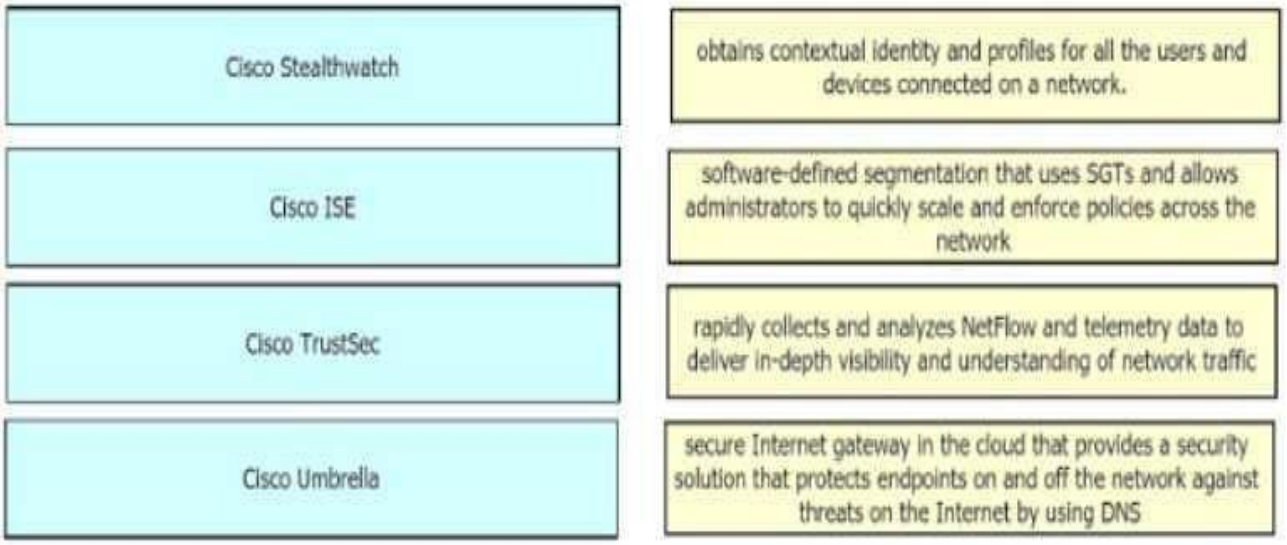
Answer:

Explanation:

The Version 1 format was the initially released version. Do not use the Version 1 format unless you are using a legacy collection system that requires it. Use Version 9 or Version 5 export format.
Version 5 export format is suitable only for the main cache; it cannot be expanded to support new features.
Version 8 export format is available only for aggregation caches; it cannot be expanded to support new
features.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgnflow-data-expt.html

Question: 234

DRAG DROP
Drag and drop the solutions from the left onto the solution's benefits on the right.

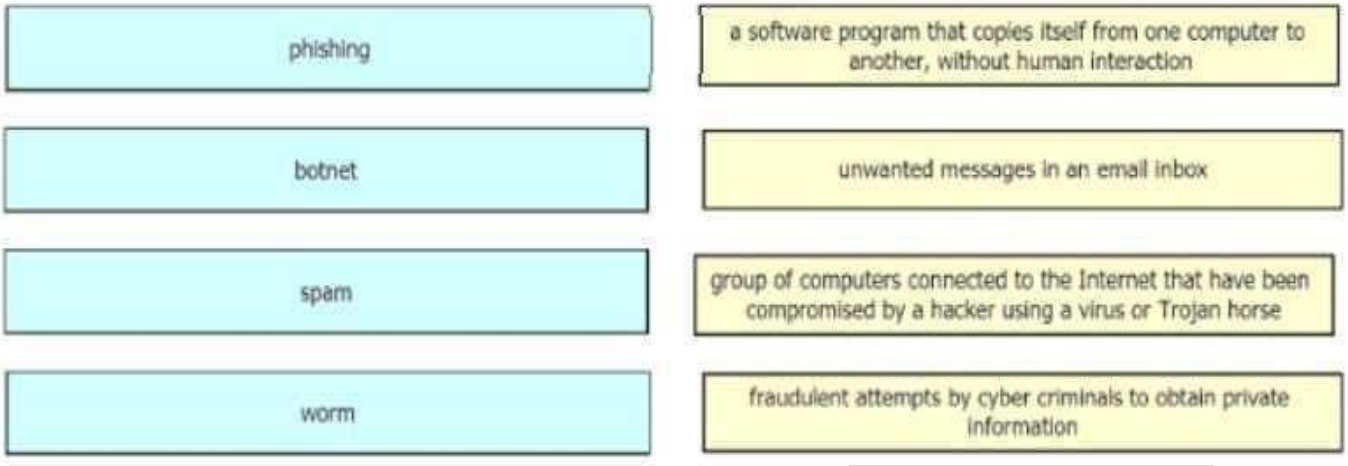


Answer:

Explanation:
Cisco Stealthwatch - rapidly collects and analyzes netflow and telementy data to deliver in-depth visibility and understanding of network traffic
Cisco ISE – obtains contextual identity and profiles for all users and device
Cisco TrustSec – software defined segmentation that uses SGTs
Cisco Umbrella – secure internet gateway ion the cloud that provides a security solution

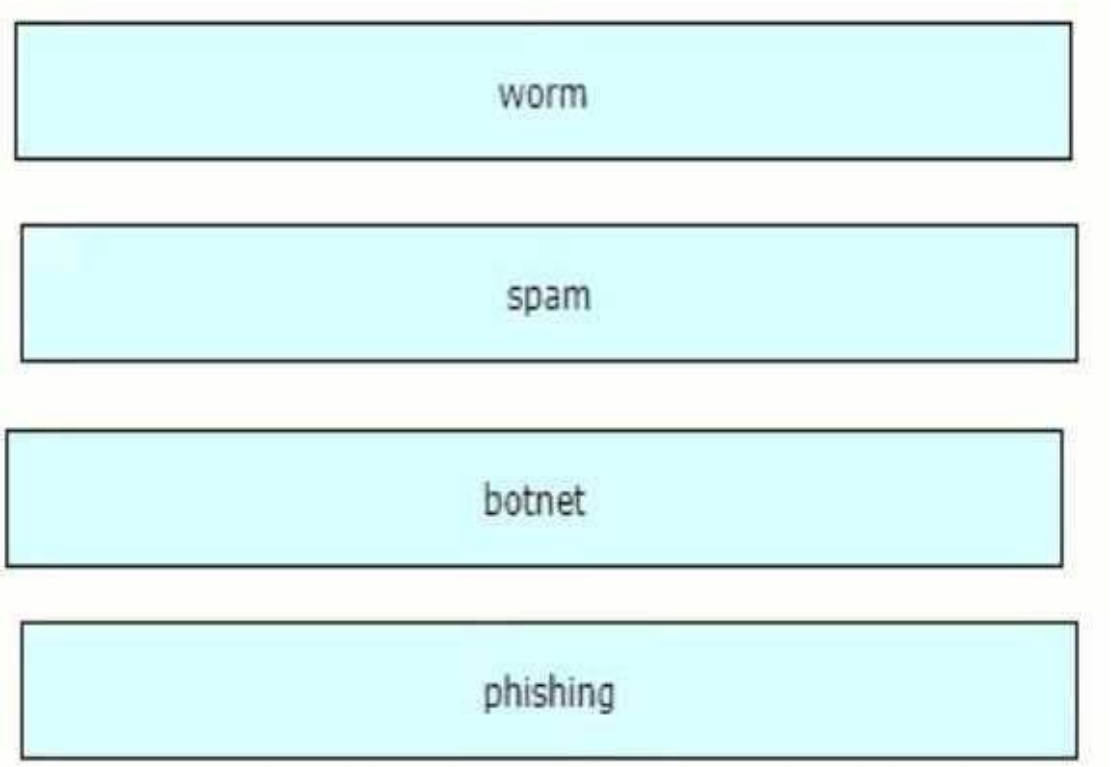
Question: 235

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



Answer:

Explanation:



Question: 236

A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based
on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an
undetermined verdict. What is causing this issue?

A. The policy was created to send a message to quarantine instead of drop
B. The file has a reputation score that is above the threshold
C. The file has a reputation score that is below the threshold
D. The policy was created to disable file analysis

Answer: D

Explanation:

Maybe the "newly installed service" in this Qmentions about Advanced Malware Protection (AMP) which can be used along with ESA. AMP allows superior protection across the attack continuum.
+ File Reputation – captures a fingerprint of each file as it traverses the ESA and sends it to AMP's cloudbased intelligence network for a reputation verdict. Given these results, you can automatically block malicious files and apply administrator-defined policy.
+ File Analysis – provides the ability to analyze unknown files that are traversing the ESA. A highly secure sandbox environment enables AMP to glean precise details about the file's behavior and to combine that data with detailed human and machine analysis to determine the file's threat level.

This disposition is then fed into AMP cloud-based intelligence network and used to dynamically update and expand the AMP cloud data set for enhanced protection

Question: 237

An administrator is trying to determine which applications are being used in the network but does not want the
network devices to send metadata to Cisco Firepower. Which feature should be used to accomplish this?

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

Answer: C

Explanation:

NetFlow is a network protocol developed by Cisco for the collection and monitoring of network traffic flow data
generated by NetFlow-enabled routers and switches. The flows do not contain actual packet data, but rather the
metadata for communications. It is a standard form of session data that details who, what, when, and where of
network traffic -> Answer A is not correct.
Reference: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/
white-paper-c11-736595.html

Question: 238

Which attack is preventable by Cisco ESA but not by the Cisco WSA?

A. buffer overflow
B. DoS
C. SQL injection
D. phishing

Answer: D

Explanation:

The following are the benefits of deploying Cisco Advanced Phishing Protection on the Cisco Email

Security
Gateway:
Prevents the following:
+ Attacks that use compromised accounts and social engineering.
+ Phishing, ransomware, zero-day attacks and spoofing.
+ BEC with no malicious payload or URL.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html

Question: 239

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

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

Answer: A, E

Explanation:

We should scan emails using AntiVirus signatures to make sure there are no viruses attached in emails.
Note: A virus signature is the fingerprint of a virus. It is a set of unique data, or bits of code, that allow it to be identified. Antivirus software uses a virus signature to find a virus in a computer file system, allowing to detect, quarantine, and remove the virus.
SenderBase is an email reputation service designed to help email administrators research senders, identify legitimate sources of email, and block spammers. When the Cisco ESA receives messages from known or highly reputable senders, it delivers them directly to the end user without any content scanning. However, when the Cisco ESA receives email messages from unknown or less reputable senders, it performs antispam and antivirus scanning.
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_12_0_chapter_0100100.html
-> Therefore Outbreak filters can be used to block emails from bad mail servers.
Web servers and email gateways are generally located in the DMZ so
Note: The recipient access table (RAT), not to be confused with remote-access Trojan (also RAT), is a Cisco ESA term that defines which recipients are accepted by a public listener.

Question: 240

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

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

Answer: B

Explanation:

Cisco's DNA Center is the only centralized network management system to bring all of this functionality into a single pane of glass.
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- dna-center-faq-cte-en.html

Question: 241

In an IaaS cloud services model, which security function is the provider responsible for managing?

A. Internet proxy
B. firewalling virtual machines
C. CASB
D. hypervisor OS hardening

Answer: B

Explanation:

In this IaaS model, cloud providers offer resources to users/machines that include computers as virtual
machines, raw (block) storage, firewalls, load balancers, and network devices.
Note: Cloud access security broker (CASB) provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware such as ransomware.

Question: 242

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

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

Answer: A

Explanation:

As the new device does not have a supplicant, we cannot use 802.1X.
MAC Authentication Bypass (MAB) is a fallback option for devices that don't support 802.1x. It is virtually
always used in deployments in some way shape or form. MAB works by having the authenticator take the
connecting device's MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or Access-Reject just like it would with 802.1x.
Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the
network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network
endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so
on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles.
Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their corporate workstation but be granted limited network access when accessing the network from their personal iPhone.
Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/tap/3739456

Question: 243

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

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

Answer: B

Explanation:

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

Question: 244

What is the role of an endpoint in protecting a user from a phishing attack?

A. Use Cisco Stealthwatch and Cisco ISE Integration.
B. Utilize 802.1X network security to ensure unauthorized access to resources.
C. Use machine learning models to help identify anomalies and determine expected sending behavior.
D. Ensure that antivirus and anti malware software is up to date

Answer: C

Explanation:

Question: 245

An organization has noticed an increase in malicious content downloads and wants to use Cisco Umbrella to prevent this activity for suspicious domains while allowing normal web traffic. Which action will accomplish this task?

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

Answer: B

Explanation:

Obviously, if you allow all traffic to these risky domains, users might access malicious content, resulting in an infection or data leak. But if you block traffic, you can expect false positives, an increase in support inquiries, and thus, more headaches. By only proxying risky domains, the intelligent proxy delivers more granular visibility and control.
The intelligent proxy bridges the gap by allowing access to most known good sites without being proxied and only proxying those that pose a potential risk. The proxy then filters and blocks against specific URLs hosting malware while allowing access to everything else.
Reference: https://docs.umbrella.com/deployment-umbrella/docs/what-is-the-intelligent-proxy

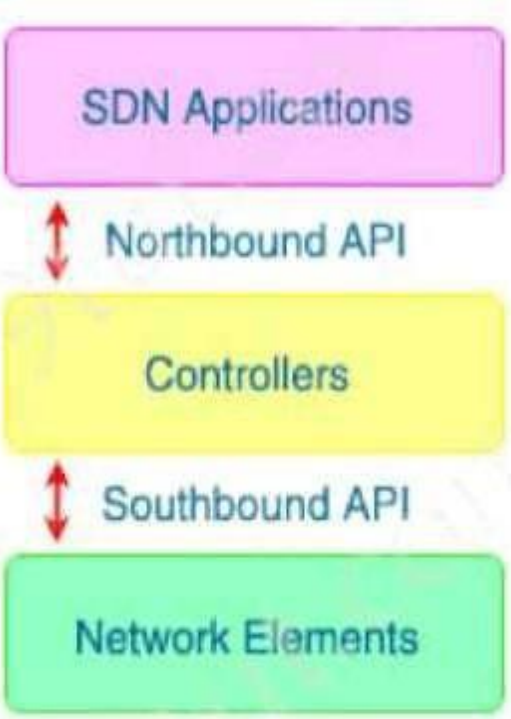
Question: 246

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

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

Answer: D

Explanation:



The Southbound API is used to communicate between Controllers and network devices.

Question: 247

A network administrator needs to find out what assets currently exist on the network. Third-party systems need to be able to feed host data into Cisco Firepower. What must be configured to accomplish this?

A. a Network Discovery policy to receive data from the host
B. a Threat Intelligence policy to download the data from the host
C. a File Analysis policy to send file data into Cisco Firepower
D. a Network Analysis policy to receive NetFlow data from the host

Answer: A

Explanation:

You can configure discovery rules to tailor the discovery of host and application data to your needs. The Firepower System can use data from NetFlow exporters to generate connection and discovery events, and to add host and application data to the network map.
A network analysis policy governs how traffic is decoded and preprocessed so it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt -> Answer D is not correct.

Question: 248

When configuring ISAKMP for IKEv1 Phase1 on a Cisco IOS router, an administrator needs to input the
command crypto isakmp key cisco address 0.0.0.0. The administrator is not sure what the IP addressing in this command issued for. What would be the effect of changing the IP address from 0.0.0.0 to 1.2.3.4?

A. The key server that is managing the keys for the connection will be at 1.2.3.4
B. The remote connection will only be allowed from 1.2.3.4
C. The address that will be used as the crypto validation authority
D. All IP addresses other than 1.2.3.4 will be allowed

Answer: B

Explanation:

The command crypto isakmp key cisco address 1.2.3.4 authenticates the IP address of the 1.2.3.4 peer by using the key cisco. The address of "0.0.0.0" will authenticate any address with this key

Question: 249

Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?

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

D. privilege escalation

Answer: C

Explanation:

The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:
+ Shell code execution: Looks for the patterns used by shell code.
+ Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.
+ Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts.
Using these, it can detect Meltdown, Spectre, and other cache-timing attacks.
+ Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping).
+ User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods.
+ Interesting file access: Cisco Tetration platform can be armed to look at sensitive files.
+ File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user.
+ Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform.
Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html

Question: 250

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

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

Answer: C, E

Explanation:

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

Question: 251

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

A. Cross-site Scripting is an attack where code is injected into a database, whereas SQL Injection is an attack where code is injected into a browser.
B. Cross-site Scripting is a brute force attack targeting remote sites, whereas SQL Injection is a social engineering attack.
C. Cross-site Scripting is when executives in a corporation are attacked, whereas SQL Injection is when a
database is manipulated.
D. Cross-site Scripting is an attack where code is executed from the server side, whereas SQL Injection is an attack where code is executed from the client side.

Answer: A

Explanation:

Answer B is not correct because Cross-site Scripting (XSS) is not a brute force attack.
Answer C is not correct because the statement "Cross-site Scripting is when executives in a corporation are attacked" is not true. XSS is a client-side vulnerability that targets other application users.
Answer D is not correct because the statement "Cross-site Scripting is an attack where code is executed from the server side". In fact, XSS is a method that exploits website vulnerability by injecting scripts that will run at client's side.
Therefore only answer A is left. In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites where
attackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POST
parameters.
Note: The main difference between a SQL and XSS injection attack is that SQL injection attacks are used to steal information from databases whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

Question: 252

A network administrator is configuring a switch to use Cisco ISE for 802.1X. An endpoint is failing

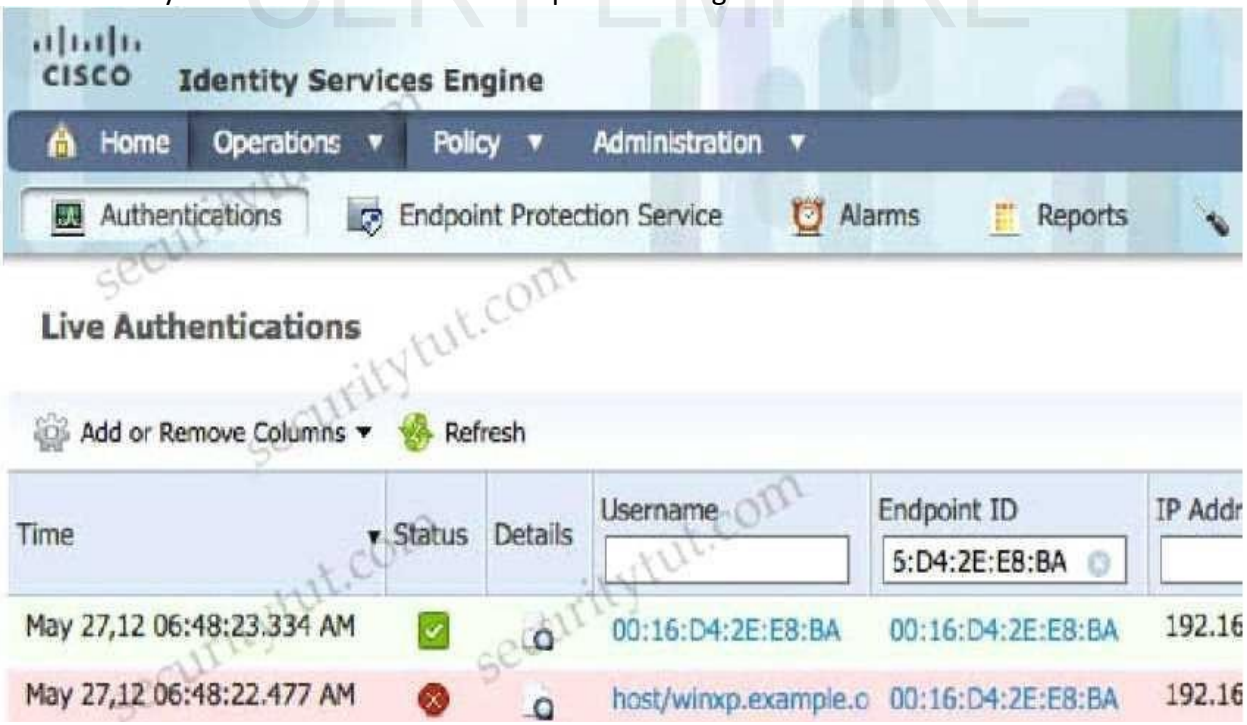
authentication and is unable to access the network. Where should the administrator begin troubleshooting to verify the authentication details?

A. Adaptive Network Control Policy List
B. Context Visibility
C. Accounting Reports
D. RADIUS Live Logs

Answer: D

Explanation:

How To Troubleshoot ISE Failed Authentications & Authorizations
Check the ISE Live Logs
Login to the primary ISE Policy Administration Node (PAN).
Go to Operations > RADIUS > Live Logs
(Optional) If the event is not present in the RADIUS Live Logs, go to Operations > Reports > Reports > Endpoints and Users > RADIUS Authentications
Check for Any Failed Authentication Attempts in the Log



Reference: https://community.cisco.com/t5/security-documents/how-to-troubleshoot-ise-failed-authenticationsamp/ta-p/3630960

Question: 253

What is a prerequisite when integrating a Cisco ISE server and an AD domain?

A. Place the Cisco ISE server and the AD server in the same subnet
B. Configure a common administrator account

C. Configure a common DNS server
D. Synchronize the clocks of the Cisco ISE server and the AD server

Answer: D

Explanation:

The following are the prerequisites to integrate Active Directory with Cisco ISE.
+ Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server
and Active Directory. You can configure NTP settings from Cisco ISE CLI.
+ If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that trust
relationships exist between the domain to which Cisco ISE is connected and the other domains that have user
and machine information to which you need access. For more information on establishing trust relationships,
refer to Microsoft Active Directory documentation.
+ You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to
which you are joining Cisco ISE.
Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F

Question: 254

An organization recently installed a Cisco WSA and would like to take advantage of the AVC engine to allow the organization to create a policy to control application specific activity. After enabling the AVC engine, what must be done to implement this?

A. Use security services to configure the traffic monitor, .
B. Use URL categorization to prevent the application traffic.
C. Use an access policy group to configure application control settings.
D. Use web security reporting to validate engine functionality

Answer: C

Explanation:

The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or

allow applications individually or according to application type. You can also apply controls to particular application types.

Question: 255

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

A. BYOD on boarding
B. Simple Certificate Enrollment Protocol
C. Client provisioning
D. MAC authentication bypass

Answer: A

Explanation:

When supporting personal devices on a corporate network, you must protect network services and enterprise
data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE
provides the tools you need to allow employees to securely use personal devices on a corporate network.
Guests can add their personal devices to the network by running the native supplicant provisioning (Network
Setup Assistant), or by adding their devices to the My Devices portal.
Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add
these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices.
Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_byod.html

Question: 256

Refer to the exhibit.

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

What will happen when this Python script is run?

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

Answer: D

Explanation:

The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across 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: 257

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

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

Answer: D

Explanation:

Micro-segmentation secures applications by expressly allowing particular application traffic and, by default,
denying all other traffic. Micro-segmentation is the foundation for implementing a zero-trust security model for
application workloads in the data center and cloud.
Cisco Tetration is an application workload security platform designed to secure your compute instances across
any infrastructure and any cloud. To achieve this, it uses behavior and attribute-driven microsegmentation
policy generation and enforcement. It enables trusted access through automated, exhaustive context from
various systems to automatically adapt security policies.
To generate accurate microsegmentation policy, Cisco Tetration performs application dependency mapping to
discover the relationships between different application tiers and infrastructure services. In addition, the
platform supports "what-if" policy analysis using real-time data or historical data to assist in the validation and risk assessment of policy application pre-enforcement to ensure ongoing application availability. The
normalized microsegmentation policy can be enforced through the application workload itself for a consistent approach to workload microsegmentation across any environment, including virtualized, bare-metal, and container workloads running in any public cloud or any data center. Once the microsegmentation policy is enforced, Cisco Tetration continues to monitor for compliance deviations, ensuring the segmentation policy is up to date as the application behavior change.
Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf

Question: 258

Which factor must be considered when choosing the on-premise solution over the cloud-based one?

A. With an on-premise solution, the provider is responsible for the installation and maintenance of the product, whereas with a cloud-based solution, the customer is responsible for it
B. With a cloud-based solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.
C. With an on-premise solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.
D. With an on-premise solution, the customer is responsible for the installation and maintenance of the
product, whereas with a cloud-based solution, the provider is responsible for it.

Answer: D

Explanation:

Question: 259

Which term describes when the Cisco Firepower downloads threat intelligence updates from Cisco

Talos?

A. consumption
B. sharing
C. analysis
D. authoring

Answer: A

Explanation:

…we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's Firepower Management Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector

Question: 260

An organization has a Cisco Stealthwatch Cloud deployment in their environment. Cloud logging is working as expected, but logs are not being received from the on-premise network, what action will resolve this issue?

A. Configure security appliances to send syslogs to Cisco Stealthwatch Cloud
B. Configure security appliances to send NetFlow to Cisco Stealthwatch Cloud
C. Deploy a Cisco FTD sensor to send events to Cisco Stealthwatch Cloud
D. Deploy a Cisco Stealthwatch Cloud sensor on the network to send data to Cisco Stealthwatch Cloud

Answer: D

Explanation:

You can also monitor on-premises networks in your organizations using Cisco Stealthwatch Cloud. In order to do so, you need to deploy at least one Cisco Stealthwatch Cloud Sensor appliance (virtual or physical appliance).
Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide

Question: 261

What does Cisco AMP for Endpoints use to help an organization detect different families of malware?

A. Ethos Engine to perform fuzzy fingerprinting
B. Tetra Engine to detect malware when me endpoint is connected to the cloud

C. Clam AV Engine to perform email scanning
D. Spero Engine with machine learning to perform dynamic analysis

Answer: A

Explanation:

ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of
a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected.
Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf
ETHOS = Fuzzy Fingerprinting using static/passive heuristics
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/BRKSEC-2139.pdf

Question: 262

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

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

Answer: D, E

Explanation:

Question: 263

What is a benefit of conducting device compliance checks?

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

Answer: B

Explanation:

Question: 264

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).

Answer: C, E

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/enterprise-networks/trustsec/trustsec-witheasy-connect-configuration-guide.pdf

Question: 265

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

Answer: D

Explanation:

Question: 266

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?

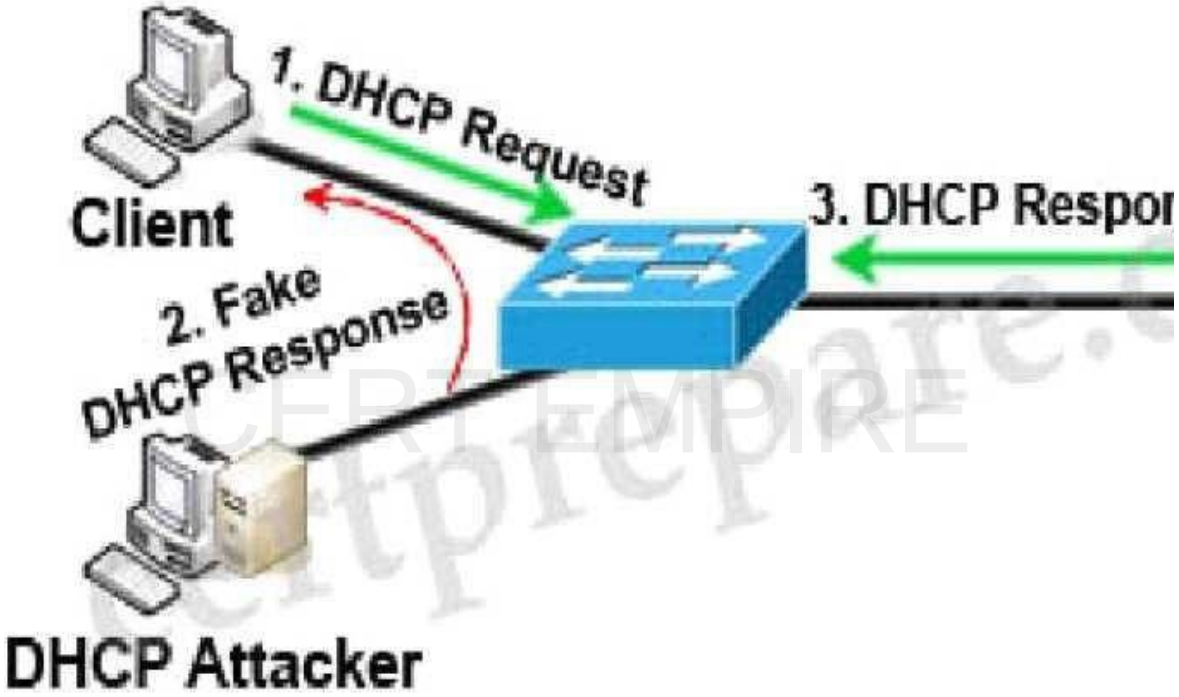
A. Set a trusted interface for the DHCP server
B. Set the DHCP snooping bit to 1

C. Add entries in the DHCP snooping database
D. Enable ARP inspection for the required VLAN

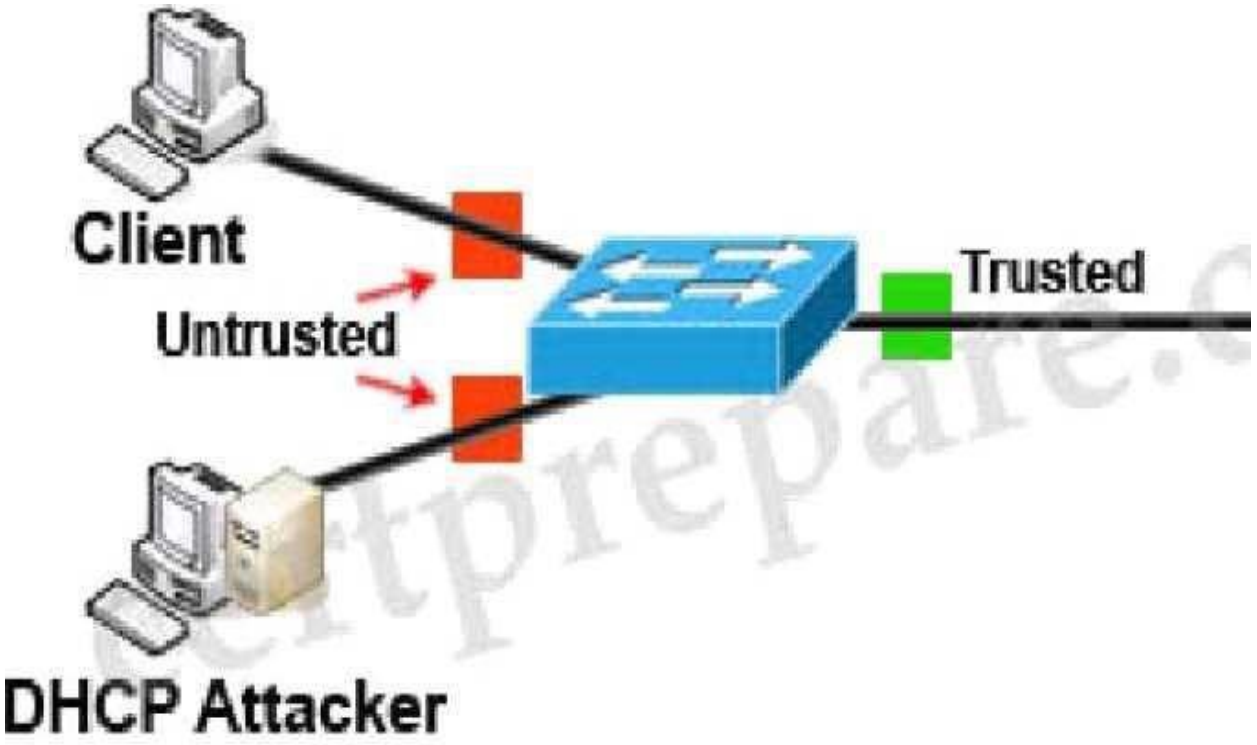
Answer: A

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.

Question: 267

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?

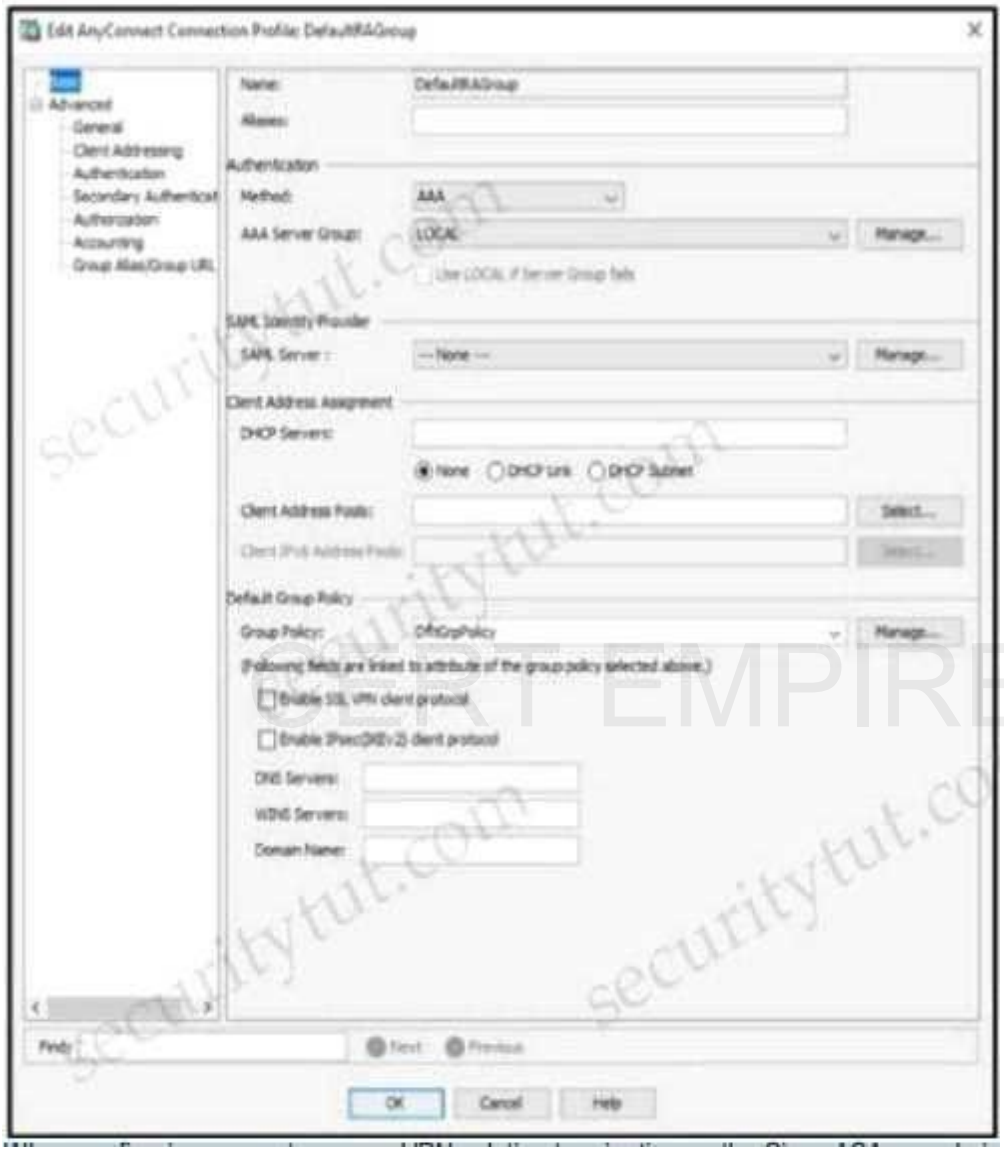
A. The hostname will be translated to an IP address and printed.
B. The hostname will be printed for the client in the client ID field.
C. The script will pull all computer hostnames and print them.
D. The script will translate the IP address to FODN and print it

Answer: C

Explanation:

Question: 268

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

Answer: B

Explanation:

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

Question: 269

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

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

Answer: D

Explanation:

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-web-security/at-a-glance-c45- 738565.pdf

Question: 270

An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with
other cloud solutions via an API. Which solution should be used to accomplish this goal?

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

Answer: D

Explanation:

+ 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/endpoints
Note:
+ 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: 271

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.

Answer: C

Explanation:

Question: 272

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

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

Answer: B

Explanation:

Question: 273

An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to

centrally
manage cloud policies across these platforms. Which software should be used to accomplish this goal?

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

Answer: A

Explanation:

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/defense-orchestrator/datasheet-c78-736847.html

Question: 274

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

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

Answer: C

Explanation:

Question: 275

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

Answer: C

Explanation:

Question: 276

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

Answer: D

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: 277

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>

Answer: D

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: 278

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.

Answer: C

Explanation:

Question: 279

What is a functional difference between a Cisco ASA and a Cisco IOS router with Zone-based policy firewall?

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

Answer: A

Explanation:

Question: 280

What is a benefit of performing device compliance?

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

Answer: A

Explanation:

Question: 281

Which cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several
organizations from a specific group?

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

Answer: B

Explanation:

Community Cloud allows system and services to be accessible by group of organizations. It shares the infrastructure between several organizations from a specific community. It may be managed internally by
organizations or by the third-party.

Question: 282

Which cryptographic process provides origin confidentiality, integrity, and origin authentication for packets?

A. IKEv1
B. AH
C. ESP
D. IKEv2

Answer: C

Explanation:

Question: 283

An organization wants to secure users, data, and applications in the cloud. The solution must be API-based and
operate as a cloud-native CASB. Which solution must be used for this implementation?

A. Cisco Cloudlock
B. Cisco Cloud Email Security
C. Cisco Firepower Next-Generation Firewall
D. Cisco Umbrella

Answer: A

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-web-security/at-a-glance-c45-738565.pdf

Question: 284

What are two Trojan malware attacks? (Choose two)

A. Frontdoor
B. Rootkit
C. Smurf
D. Backdoor
E. Sync

Answer: B, D

Explanation:

Question: 285

What is the role of Cisco Umbrella Roaming when it is installed on an endpoint?

A. To protect the endpoint against malicious file transfers
B. To ensure that assets are secure from malicious links on and off the corporate network
C. To establish secure VPN connectivity to the corporate network
D. To enforce posture compliance and mandatory software

Answer: B

Explanation:

Umbrella Roaming is a cloud-delivered security service for Cisco's next-generation firewall. It protects your employees even when they are off the VPN.

Question: 286

What is a capability of Cisco ASA Netflow?

A. It filters NSEL events based on traffic

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

Answer: A

Explanation:

Question: 287

Which component of Cisco umbrella architecture increases reliability of the service?

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

Answer: D

Explanation:

Question: 288

What is the benefit of integrating Cisco ISE with a MDM solution?

A. It provides compliance checks for access to the network
B. It provides the ability to update other applications on the mobile device
C. It provides the ability to add applications to the mobile device through Cisco ISE
D. It provides network device administration access

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperability_mdm.html

Question: 289

An administrator configures a new destination list in Cisco Umbrella so that the organization can block specific domains for its devices. What should be done to ensure that all subdomains of domain.com are blocked?

A. Configure the *.com address in the block list.
B. Configure the *.domain.com address in the block list
C. Configure the *.domain.com address in the block list

D. Configure the domain.com address in the block list

Answer: C

Explanation:

Question: 290

An organization wants to provide visibility and to identify active threats in its network using a VM. The
organization wants to extract metadata from network packet flow while ensuring that payloads are not retained
or transferred outside the network. Which solution meets these requirements?

A. Cisco Umbrella Cloud
B. Cisco Stealthwatch Cloud PNM
C. Cisco Stealthwatch Cloud PCM
D. Cisco Umbrella On-Premises

Answer: B

Explanation:

Private Network Monitoring (PNM) provides visibility and threat detection for the on-premises network, delivered from the cloud as a SaaS solution. It is the perfect solution for organizations who prefer SaaS products and desire better awareness and security in their on-premises environments while reducing capital expenditure and
operational overhead. It works by deploying lightweight software in a virtual machine or server that can
consume a variety of native sources of telemetry or extract metadata from network packet flow. It encrypts this metadata and sends it to the Stealthwatch Cloud analytics platform for analysis. Stealthwatch Cloud consumes metadata only. The packet payloads are never retained or transferred outside the network.
This lab focuses on how to configure a Stealthwatch Cloud Private Network Monitoring (PNM) Sensor, in order to provide visibility and effectively identify active threats, and monitors user and device behavior within onpremises networks.
The Stealthwatch Cloud PNM Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. –VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf

Question: 291

An organization deploys multiple Cisco FTD appliances and wants to manage them using one

centralized
solution. The organization does not have a local VM but does have existing Cisco ASAs that must migrate over
to Cisco FTDs. Which solution meets the needs of the organization?

A. Cisco FMC
B. CSM
C. Cisco FDM
D. CDO

Answer: A

Explanation:

Question: 292

An organization wants to secure data in a cloud environment. Its security model requires that all users be
authenticated and authorized. Security configuration and posture must be continuously validated before access is granted or maintained to applications and dat
a. There is also a need to allow certain application traffic and deny all other traffic by default. Which technology must be used to implement these requirements?
A. Virtual routing and forwarding
B. Microsegmentation
C. Access control policy
D. Virtual LAN

Answer: B

Explanation:

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.
The Zero Trust model uses microsegmentation — a security technique that involves dividing perimeters into small zones to maintain separate access to every part of the network — to contain attacks.

Question: 293

A Cisco FTD engineer is creating a new IKEv2 policy called s2s00123456789 for their organization to allow for additional protocols to terminate network devices with. They currently only have one policy established and need the new policy to be a backup in case some devices cannot support the stronger algorithms listed in the primary policy. What should be done in order to support this?

A. Change the integrity algorithms to SHA* to support all SHA algorithms in the primary policy
B. Make the priority for the new policy 5 and the primary policy 1
C. Change the encryption to AES* to support all AES algorithms in the primary policy
D. Make the priority for the primary policy 10 and the new policy 1

Answer: B

Explanation:

All IKE policies on the device are sent to the remote peer regardless of what is in the selected policy section.
The first IKE Policy matched by the remote peer will be selected for the VPN connection. Choose which policy is sent first using the priority field. Priority 1 will be sent first.
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html

Question: 294

Which type of encryption uses a public key and private key?

A. Asymmetric
B. Symmetric
C. Linear
D. Nonlinear

Answer: A

Explanation:

Question: 295

What are two features of NetFlow flow monitoring? (Choose two)

A. Can track ingress and egress information
B. Include the flow record and the flow importer
C. Copies all ingress flow information to an interface
D. Does not required packet sampling on interfaces
E. Can be used to track multicast, MPLS, or bridged traffic

Answer: A, E

Explanation:

The following are restrictions for Flexible NetFlow:
+ Traditional NetFlow (TNF) accounting is not supported.
+ Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported.

+ Both ingress and egress NetFlow accounting is supported.
+ Microflow policing feature shares the NetFlow hardware resource with FNF.
+ Only one flow monitor per interface and per direction is supported.
Reference: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html
When configuring NetFlow, follow these guidelines and restrictions:
+ Except in PFC3A mode, NetFlow supports bridged IP traffic. PFC3A mode does not support NetFlow bridged IP traffic.
+ NetFlow supports multicast IP traffic.
Reference: https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.html
The Flexible NetFlow – MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow.html

Question: 296

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

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

Answer: C

Explanation:

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

Question: 297

Which Talos reputation center allows for tracking the reputation of IP addresses for email and web traffic?

A. IP and Domain Reputation Center
B. File Reputation Center
C. IP Slock List Center
D. AMP Reputation Center

Answer: A

Explanation:

Question: 298

An engineer is configuring IPsec VPN and needs an authentication protocol that is reliable and supports ACK
and sequence. Which protocol accomplishes this goal?

A. AES-192
B. IKEv1
C. AES-256
D. ESP

Answer: D

Explanation:

Question: 299

An administrator is establishing a new site-to-site VPN connection on a Cisco IOS router. The organization
needs to ensure that the ISAKMP key on the hub is used only for terminating traffic from the IP address of
172.19.20.24. Which command on the hub will allow the administrator to accomplish this?

A. crypto ca identity 172.19.20.24
B. crypto isakmp key Cisco0123456789 172.19.20.24
C. crypto enrollment peer address 172.19.20.24
D. crypto isakmp identity address 172.19.20.24

Answer: B

Explanation:

The command “crypto isakmp identity address 172.19.20.24” is not valid. We can only use “crypto

isakmp
identity {address | hostname}. The following example uses preshared keys at two peers and sets both their
ISAKMP identities to the IP address.
At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified:
crypto isakmp identity address
crypto isakmp key sharedkeystring address 192.168.1.33
At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified:
crypto isakmp identity address
crypto isakmp key sharedkeystring address 10.0.0.1
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp3880782430
The command "crypto enrollment peer address" is not valid either.
The command "crypto ca identity ..." is only used to declare a trusted CA for the router and puts you in the caidentity configuration mode. Also it should be followed by a name, not an IP address. For example: "crypto ca
identity CA-Server" -> Answer A is not correct.
Only answer B is the best choice left.

Question: 300

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

A. SQL injection is a hacking method used to attack SQL databases, whereas XSS attacks can exist in many differenttypes of applications
B. XSS is a hacking method used to attack SQL databases, whereas SQL injection attacks can exist in many differenttypes of applications
C. SQL injection attacks are used to steal information from databases whereas XSS attacks are used to redirect users to websites where attackers can steal data from them
D. XSS attacks are used to steal information from databases whereas SQL injection attacks are used to redirect users to websites where attackers can steal data from them

Answer: C

Explanation:

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

Question: 301

An engineer has been tasked with configuring a Cisco FTD to analyze protocol fields and detect anomalies in
the traffic from industrial systems. What must be done to meet these requirements?

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

Answer: A

Explanation:

The Modbus, DNP3, and CIP SCADA preprocessors detect traffic anomalies and provide data to intrusion
rules. Therefore in this question only answer A or answer C is correct.
The DNP3 preprocessor detects anomalies in DNP3 traffic and decodes the DNP3 protocol for processing by
the rules engine, which uses DNP3 keywords to access certain protocol fields.
The Common Industrial Protocol (CIP) is a widely used application protocol that supports industrial automation
applications. EtherNet/IP is an implementation of CIP that is used on Ethernet-based networks.The CIP
preprocessor detects CIP and ENIP traffic running on TCP or UDP and sends it to the intrusion rules engine.
You can use CIP and ENIP keywords in custom intrusion rules to detect attacks in CIP and ENIP traffic.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-configguide-v63/scada_preprocessors.html
Both DNP3 and CIP preprocessors can be used to detect traffic anomalies but we choose CIP as it is widely used in industrial applications.
Note:
+ An intrusion rule is a specified set of keywords and arguments that the system uses to detect attempts to exploit vulnerabilities in your network. As the system analyzes network traffic, it compares packets against the conditions specified in each rule, and triggers the rule if the data packet meets all the conditions specified in the rule. + Preprocessor rules, which are rules associated with preprocessors and packet decoder detection options in the network analysis policy. Most preprocessor rules are disabled by default.

Question: 302

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

Answer: A

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: 303

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

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

Answer: B

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: 304

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

Answer: A

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: 305

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

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

Answer: C

Explanation:

Question: 306

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

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

Answer: C

Explanation:

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

Question: 307

How does Cisco Workload Optimization Manager help mitigate application performance issues?

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

Answer: C

Explanation:

Cisco Workload Optimization Manager provides specific real-time actions that ensure workloads get the
resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software).
Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf

Question: 308

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

Answer: D

Explanation:

Question: 309

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

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

Answer: A

Explanation:

Question: 310

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

A. Automatically deploy new virtual routers
B. Upgrade software on switches and routers
C. Application monitors for power utilization of devices and IoT sensors
D. Connect to Information Technology Service Management Platforms
E. Create new SSIDs on a wireless LAN controller

Answer: C, D

Explanation:

Integration API (Westbound)
Integration capabilities are part of Westbound interfaces. To meet the need to scale and accelerate operations
in modern data centers, IT operators require intelligent, end-to-end work flows built with open APIs. The Cisco
DNA Center platform provides mechanisms for integrating Cisco DNA Assurance workflows and data with thirdparty IT Service Management (ITSM) solutions.
Reference: https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/events-andnotifications-eastbound
-> Therefore answer D is correct.
Westbound—Integration APIs

Cisco DNA Center platform can power end-to-end IT processes across the value chain by integrating various
domains such as ITSM, IPAM, and reporting. By leveraging the REST-based Integration Adapter APIs, bidirectional interfaces can be built to allow the exchange of contextual information between Cisco DNA Center
and the external, third-party IT systems. The westbound APIs provide the capability to publish the network data,
events and notifications to the external systems and consume information in Cisco DNA Center from the
connected systems.
Reference: https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitiveadvantage
Therefore the most suitable choice is Integration APIs can monitor for power utilization of devices and IoT
sensors -> Answer C is correct.

Question: 311

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

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

Answer: B

Explanation:

Question: 312

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

Answer: A

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-in-pki/

Question: 313

Which DevSecOps implementation process gives a weekly or daily update instead of monthly or quarterly in the applications?

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

Answer: B

Explanation:

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: 314

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

Answer: C

Explanation:

An example of configuring a NetFlow exporter is shown below:
flow exporter Exporter
destination 192.168.100.22
transport udp 2055

Question: 315

Which category includes DoS Attacks?

A. Virus attacks
B. Trojan attacks
C. Flood attacks
D. Phishing attacks

Answer: C

Explanation:

Question: 316

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

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

Answer: C, E

Explanation:

Question: 317

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

Answer: D

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: 318

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

Answer: D

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: 319

What is a difference between GETVPN and IPsec?

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

Answer: A

Explanation:

Question: 320

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

Answer: D

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-start-guide/streaming telemetry

Question: 321

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

Answer: C

Explanation:

Question: 322

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

Answer: A

Explanation:

Question: 323

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

Answer: D

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

Question: 324

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

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

D. Configure a Cisco FMC to send NetFlow to Cisco Stealthwatch Cloud

Answer: B

Explanation:

The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology,
capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete
Ubuntu based virtual appliance on different hypervisors (e.g. –VMware, VirtualBox). It can be deployed on
hardware running a number of different Linux-based operating systems.
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf

Question: 325

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

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

Answer: A

Explanation:

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

Question: 326

Which service allows a user export application usage and performance statistics with Cisco

Application Visibility
and control?

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

Answer: B

Explanation:

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

Question: 327

An engineer adds a custom detection policy to a Cisco AMP deployment and encounters issues with the
configuration. The simple detection mechanism is configured, but the dashboard indicates that the hash is not 64 characters and is non-zero. What is the issue?

A. The engineer is attempting to upload a hash created using MD5 instead of SHA-256
B. The file being uploaded is incompatible with simple detections and must use advanced detections
C. The hash being uploaded is part of a set in an incorrect format
D. The engineer is attempting to upload a file instead of a hash

Answer: A

Explanation:

Question: 328

Refer to the exhibit.

```
interface GigabitEthernet1/0/18
switchport access vlan 41
switchport mode access
switchport voice vlan 44
device-tracking attach-policy IPDT_MAX_10
authentication periodic
authentication timer reauthenticate server
access-session host-mode multi-domain
access-session port-control auto
dot1x pae authenticator
dot1x timeout tx-period 7
dot1x max-reauth-req 3
spanning-tree portfast
```

Refer to the exhibit. A Cisco ISE administrator adds a new switch to an 802.1X deployment and has difficulty with some endpoints gaining access.
Most PCs and IP phones can connect and authenticate using their machine certificate credentials. However printer and video cameras cannot base d on the interface configuration provided, what must be to get these devices on to the network using Cisco ISE for authentication and authorization while maintaining security controls?

A. Change the default policy in Cisco ISE to allow all devices not using machine authentication .
B. Enable insecure protocols within Cisco ISE in the allowed protocols configuration.
C. Configure authentication event fail retry 2 action authorize vlan 41 on the interface
D. Add mab to the interface configuration.

Answer: A

Explanation:

Question: 329

An administrator is adding a new switch onto the network and has configured AAA for network access control. When testing the configuration, the RADIUS authenticates to Cisco ISE but is being rejected. Why is the ip radius source-interface command needed for this configuration?

A. Only requests that originate from a configured NAS IP are accepted by a RADIUS server
B. The RADIUS authentication key is transmitted only from the defined RADIUS source interface
C. RADIUS requests are generated only by a router if a RADIUS source interface is defined.
D. Encrypted RADIUS authentication requires the RADIUS source interface be defined

Answer: B

Explanation:

Question: 330

A customer has various external HTTP resources available including Intranet. Extranet, and Internet, with a proxy configuration running in explicit mode Which method allows the client desktop

browsers to be configured to select when to connect direct or when to use the proxy?

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

Answer: C

Explanation:

Question: 331

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

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

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

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

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

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

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

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

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

A. It allows authentication with TLSv1 SSL protocol
B. It authenticates to a Cisco ISE with an SSH connection.
C. lt authenticates to a Cisco ISE server using the username of ersad

Answer: C

Explanation:

Question: 332

Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-

based container?

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

Answer: B

Explanation:

Question: 333

Which feature is leveraged by advanced antimalware capabilities to be an effective endpomt protection platform?

A. big data
B. storm centers
C. sandboxing
D. blocklisting

Answer: C

Explanation:

Question: 334

An organization wants to implement a cloud-delivered and SaaS-based solution to provide visibility and threat detection across the AWS network. The solution must be deployed without software agents and rely on AWS VPC flow logs instead. Which solution meets these requirements?

A. Cisco Stealthwatch Cloud
B. Cisco Umbrella
C. NetFlow collectors
D. Cisco Cloudlock

Answer: A

Explanation:

Question: 335

What is the difference between a vulnerability and an exploit?

A. A vulnerability is a hypothetical event for an attacker to exploit
B. A vulnerability is a weakness that can be exploited by an attacker

C. An exploit is a weakness that can cause a vulnerability in the network
D. An exploit is a hypothetical event that causes a vulnerability in the network

Answer: B

Explanation:

Question: 336

Cisco SensorBase gaihers threat information from a variety of Cisco products and services and performs analytics to find patterns on threats Which term describes this process?

A. deployment
B. consumption
C. authoring
D. sharing

Answer: A

Explanation:

Question: 337

An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1 1 11 using the flow record Stea!thwatch406397954 command Which additional command is required to complete the flow record?

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

Answer: B

Explanation:

Question: 338

Which Cisco platform processes behavior baselines, monitors for deviations, and reviews for malicious processes in data center traffic and servers while performing software vulnerability detection?

A. Cisco Tetration
B. Cisco ISE?
C. Cisco AMP for Network
D. Cisco AnyConnect

Answer: C

Explanation:

Question: 339

How is data sent out to the attacker during a DNS tunneling attack?

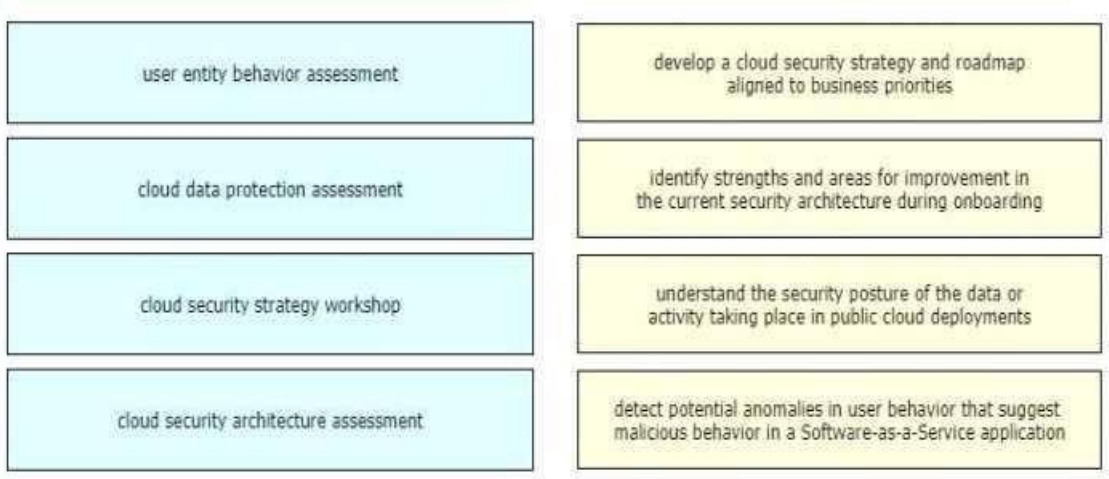
A. as part of the UDP'53 packet payload
B. as part of the domain name
C. as part of the TCP/53 packet header
D. as part of the DNS response packet

Answer: B

Explanation:

Question: 340

DRAG DROP
Drag and drop the cloud security assessment components from the left onto the definitions on the right.



Answer:

Explanation:

Question: 341

An engineer is adding a Cisco DUO solution to the current TACACS+ deployment using Cisco ISE. The engineer wants to authenticate users using their account when they log into network devices. Which action accomplishes this task?

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

Answer: C

Explanation:

Question: 342

A Cisco AMP for Endpoints administrator configures a custom detection policy to add specific MD5 signatures The configuration is created in the simple detection policy section, but it does not work What is the reason for this failure?

A. The administrator must upload the file instead of the hash for Cisco AMP to use.
B. The MD5 hash uploaded to the simple detection policy is in the incorrect format
C. The APK must be uploaded for the application that the detection is intended
D. Detections for MD5 signatures must be configured in the advanced custom detection policies

Answer: D

Explanation:

Question: 343

An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems. Why should the organization select either Platform as a Service or Infrastructure as a Service for this environment?

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

Answer: B

Explanation:

Question: 344

An administrator is adding a new Cisco ISE node to an existing deployment. What must be done to ensure that the addition of the node will be successful when inputting the FQDN?

A. Change the IP address of the new Cisco ISE node to the same network as the others.
B. Make the new Cisco ISE node a secondary PAN before registering it with the primary.
C. Open port 8905 on the firewall between the Cisco ISE nodes
D. Add the DNS entry for the new Cisco ISE node into the DNS server

Answer: B

Explanation:

Question: 345

Refer to the exhibit.

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

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

A. 802.1X will not work, but MAB will start and allow the device on the network.
B. 802.1X will not work and the device will not be allowed network access
C. 802 1X will work and the device will be allowed on the network

D. 802 1X and MAB will both be used and ISE can use policy to determine the access level

Answer: D

Explanation:

Question: 346

A network engineer must configure a Cisco ESA to prompt users to enter two forms of information before gaining access The Cisco ESA must also join a cluster machine using preshared keys What must be configured to meet these requirements?

A. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA CLI.
B. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA GUI
C. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA GUI.
D. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA CLI

Answer: D

Explanation:

Question: 347

Which portion of the network do EPP solutions solely focus on and EDR solutions do not?

A. server farm
B. perimeter
C. core
D. East-West gateways

Answer: B

Explanation:

Question: 348

Refer to the exhibit.

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

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

A. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.
B. Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully
C. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER
D. The OU of the IKEv2 peer certificate is set to MANGLER

Answer: A

Explanation:

Question: 349

What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?

A. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not
B. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA.
C. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA
D. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA

Answer: D

Explanation:

Question: 350

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

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

Answer: B

Explanation:

Question: 351

An organization has a requirement to collect full metadata information about the traffic going through their AWS cloud services They want to use this information for behavior analytics and

statistics Which two actions must be taken to implement this requirement? (Choose two.)

A. Configure Cisco ACI to ingest AWS information.
B. Configure Cisco Thousand Eyes to ingest AWS information.
C. Send syslog from AWS to Cisco Stealthwatch Cloud.
D. Send VPC Flow Logs to Cisco Stealthwatch Cloud.
E. Configure Cisco Stealthwatch Cloud to ingest AWS information

Answer: D, E

Explanation:

Question: 352

What is the function of the crypto is a kmp key cisc406397954 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel?

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

Answer: B

Explanation:

Question: 353

An organization wants to improve its cybersecurity processes and to add intelligence to its data The organization wants to utilize the most current intelligence data for URL filtering, reputations, and vulnerability information that can be integrated with the Cisco FTD and Cisco WSA What must be done to accomplish these objectives?

A. Create a Cisco pxGrid connection to NIST to import this information into the security products for policy use
B. Create an automated download of the Internet Storm Center intelligence feed into the Cisco FTD and Cisco WSA databases to tie to the dynamic access control policies.
C. Download the threat intelligence feed from the IETF and import it into the Cisco FTD and Cisco WSA databases
D. Configure the integrations with Talos Intelligence to take advantage of the threat intelligence that it provides.

Answer: B

Explanation:

Question: 354

Refer to the exhibit.

```
ntp authentication-key 10 md5 cisco123
ntp trusted-key 10
```

A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced What is the cause of this issue?

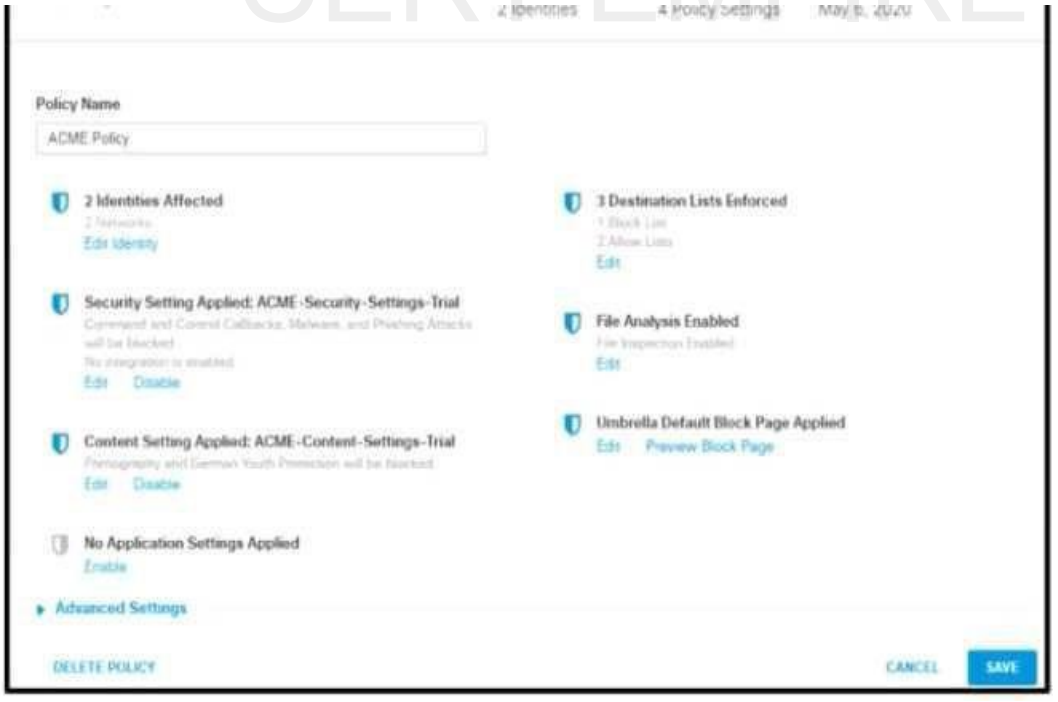
A. The key was configured in plain text.
B. NTP authentication is not enabled.
C. The hashing algorithm that was used was MD5. which is unsupported.
D. The router was not rebooted after the NTP configuration updated.

Answer: D

Explanation:

Question: 355

Refer to the exhibit.



How does Cisco Umbrella manage traffic that is directed toward risky domains?

A. Traffic is proximed through the intelligent proxy.
B. Traffic is managed by the security settings and blocked.
C. Traffic is managed by the application settings, unhandled and allowed.
D. Traffic is allowed but logged.

Answer: B

Explanation:

Question: 356

An engineer needs to add protection for data in transit and have headers in the email message
Which configuration is needed to accomplish this goal?

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

Answer: B

Explanation:

Question: 357

How does a cloud access security broker function?

A. It is an authentication broker to enable single sign-on and multi-factor authentication for a cloud solution
B. lt integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution
C. It acts as a security information and event management solution and receives syslog from other cloud solutions.
D. It scans other cloud solutions being used within the network and identifies vulnerabilities

Answer: B

Explanation:

Question: 358

An engineer integrates Cisco FMC and Cisco ISE using pxGrid Which role is assigned for Cisco FMC?

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

Answer: D

Explanation:

Question: 359

A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address Error! Hyperlink reference not valid. IP>/capure/CAPI/pcap/test.pcap, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

A. Disable the proxy setting on the browser
B. Disable the HTTPS server and use HTTP instead
C. Use the Cisco FTD IP address as the proxy server setting on the browser
D. Enable the HTTPS server for the device platform policy

Answer: D

Explanation:

Question: 360

What is a description of microsegmentation?

A. Environments apply a zero-trust model and specify how applications on different servers or containers can communicate
B. Environments deploy a container orchestration platform, such as Kubernetes, to manage the application delivery
C. Environments implement private VLAN segmentation to group servers with similar applications.
D. Environments deploy centrally managed host-based firewall rules on each server or container

Answer: A

Explanation:

Question: 361

What must be enabled to secure SaaS-based applications?

A. modular policy framework
B. two-factor authentication
C. application security gateway
D. end-to-end encryption

Answer: D

Explanation:

Question: 362

What are two ways a network administrator transparently identifies users using Active Directory on

the Cisco WSA? (Choose two.) The eDirectory client must be installed on each client workstation.

A. Create NTLM or Kerberos authentication realm and enable transparent user identification
B. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.
C. Create an LDAP authentication realm and disable transparent user identification.
D. Deploy a separate eDirectory server: the client IP address is recorded in this server

Answer: B, C

Explanation:

Question: 363

Which method of attack is used by a hacker to send malicious code through a web application to an unsuspecting user to request that the victim's web browser executes the code?

A. buffer overflow
B. browser WGET
C. SQL injection
D. cross-site scripting

Answer: D

Explanation:

Question: 364

An administrator enables Cisco Threat Intelligence Director on a Cisco FMC. Which process uses STIX and allows uploads and downloads of block lists?

A. consumption
B. sharing
C. editing
D. authoring

Answer: C

Explanation:

Question: 365

Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

A. OpenC2
B. OpenIOC

C. CybOX
D. STIX

Answer: B

Explanation:

Question: 366

What are two functionalities of SDN Northbound APIs? (Choose two.)

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

Answer: A, B

Explanation:

Question: 367

What is an advantage of network telemetry over SNMP pulls?

A. accuracy
B. encapsulation
C. security
D. scalability

Answer: C

Explanation:

Question: 368

What are two functions of TAXII in threat intelligence sharing? (Choose two.)

A. determines the "what" of threat intelligence
B. Supports STIX information
C. allows users to describe threat motivations and abilities
D. exchanges trusted anomaly intelligence information
E. determines how threat intelligence information is relayed

Answer: B, D

Explanation:

Question: 369

A network engineer must migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vMotion. What is a requirement for both physical hosts?

A. The hosts must run Cisco AsyncOS 10.0 or greater.
B. The hosts must run different versions of Cisco AsyncOS.
C. The hosts must have access to the same defined network.
D. The hosts must use a different datastore than the virtual appliance.

Answer: A

Explanation:

Question: 370

What is a difference between Cisco AMP for Endpoints and Cisco Umbrella?

A. Cisco AMP for Endpoints is a cloud-based service, and Cisco Umbrella is not.
B. Cisco AMP for Endpoints prevents connections to malicious destinations, and C malware.
C. Cisco AMP for Endpoints automatically researches indicators of compromise ..
D. Cisco AMP for Endpoints prevents, detects, and responds to attacks before and against Internet threats.

Answer: C

Explanation:

Question: 371

What is the result of the ACME-Router(config)#login block-for 100 attempts 4 within 60 command on a Cisco IOS router?

A. If four log in attempts fail in 100 seconds, wait for 60 seconds to next log in prompt.
B. After four unsuccessful log in attempts, the line is blocked for 100 seconds and only permit IP addresses are permitted in ACL
C. After four unsuccessful log in attempts, the line is blocked for 60 seconds and only permit IP addresses are permitted in ACL1
D. If four failures occur in 60 seconds, the router goes to quiet mode for 100 seconds.

Answer: A

Explanation:

Question: 372

An engineer is implementing Cisco CES in an existing Microsoft Office 365 environment and must route inbound email to Cisco CE.. record must be modified to accomplish this task?

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

Answer: B

Explanation:

Question: 373

What are two functionalities of northbound and southbound APIs within Cisco SDN architecture? (Choose two.)

A. Southbound APIs are used to define how SDN controllers integrate with applications.
B. Southbound interfaces utilize device configurations such as VLANs and IP addresses.
C. Northbound APIs utilize RESTful API methods such as GET, POST, and DELETE.
D. Southbound APIs utilize CLI, SNMP, and RESTCONF.
E. Northbound interfaces utilize OpenFlow and OpFlex to integrate with network devices.

Answer: B, D

Explanation:

Question: 374

Refer to the exhibit. Which configuration item makes it possible to have the AAA session on the network?

A. aaa authentication login console ise
B. aaa authentication enable default enable
C. aaa authorization network default group ise
D. aaa authorization exec default ise

Answer: B

Explanation:

Question: 375

Refer to the exhibit. What is the function of the Python script code snippet for the Cisco ASA REST API?

A. adds a global rule into policies
B. changes the hostname of the Cisco ASA
C. deletes a global rule from policies
D. obtains the saved configuration of the Cisco ASA firewall

Answer: A

Explanation:

Question: 376

An engineer must modify a policy to block specific addresses using Cisco Umbrell
a. The policy is created already and is actively u: of the default policy elements. What else must be done to accomplish this task?
A. Add the specified addresses to the identities list and create a block action.
B. Create a destination list for addresses to be allowed or blocked.
C. Use content categories to block or allow specific addresses.
D. Modify the application settings to allow only applications to connect to required addresses.

Answer: D

Explanation:

Question: 377

An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation. What must be un solution?

A. L2TP is an IP packet encapsulation protocol, and GRE over IPsec is a tunneling protocol.
B. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701.
C. GRE over IPsec adds its own header, and L2TP does not.
D. GRE over IPsec cannot be used as a standalone protocol, and L2TP can.

Answer: A

Explanation:

Question: 378

What is a benefit of using a multifactor authentication strategy?

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

Answer: D

Explanation:

Question: 379

A Cisco ISE engineer configures Central Web Authentication (CWA) for wireless guest access and must have the guest endpoints redirect to the guest portal for authentication and authorization. While testing the policy, the engineer notices that the device is not redirected and instead gets full guest access. What must be done for the redirect to work?

A. Tag the guest portal in the CWA part of the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.
B. Use the track movement option within the authorization profile for the authorization policy line that the unauthenticated devices hit.
C. Create an advanced attribute setting of Cisco:cisco-gateway-id=guest within the authorization profile for the authorization policy line that the unauthenticated devices hit.
D. Add the DACL name for the Airespace ACL configured on the WLC in the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.

Answer: C

Explanation:

Question: 380

Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)

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

Answer: A, E

Explanation:

Question: 381

Which role is a default guest type in Cisco ISE?

A. Monthly
B. Yearly
C. Contractor
D. Full-Time

Answer: B

Explanation:

Question: 382

Which two methods must be used to add switches into the fabric so that administrators can control how switches are added into DCNM for private cloud management? (Choose two.)

A. Cisco Cloud Director
B. Cisco Prime Infrastructure
C. PowerOn Auto Provisioning
D. Seed IP
E. CDP AutoDiscovery

Answer: C, D

Explanation:

Question: 383

Refer to the exhibit. All servers are in the same VLAN/Subnet. DNS Server-1 and DNS Server-2 must communicate with each other, and communicate with default gateway multilayer switch. Which type of private VLAN ports should be configured to prevent communication and the file server?

A. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as isolated port, and GigabitEthernet0/3 and GigabitEthernet... ports.
B. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as promiscuous port, GigabitEthernet0/3 and GigabitEthernet...0/
C. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as community port, and GigabitEthernet0/3 and GigabitEthen... ports.
D. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as isolated port, and GigabitEthernet0/3 and GigabitEthernet...OA ports.

Answer: C

Explanation:

Question: 384

Refer to the exhibit. When creating an access rule for URL filtering, a network engineer adds certain categories and individual URLs to block. What is the result of the configuration?

A. Only URLs for botnets with reputation scores of 1-3 will be blocked.
B. Only URLs for botnets with a reputation score of 3 will be blocked.
C. Only URLs for botnets with reputation scores of 3-5 will be blocked.
D. Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked.

Answer: A

Explanation:

Question: 385

Why is it important to have a patching strategy for endpoints?

A. to take advantage of new features released with patches
B. so that functionality is increased on a faster scale when it is used
C. so that known vulnerabilities are targeted and having a regular patch cycle reduces risks
D. so that patching strategies can assist with disabling nonsecure protocols in applications

Answer: C

Explanation:

Question: 386

An engineer is configuring Cisco Umbrella and has an identity that references two different policies. Which action ensures that the..... use takes precedence over the second one?

A. Configure only the policy with the most recently changed timestamp.
B. Make the correct policy first in the policy order.
C. Place the policy with the most-specific configuration last in the policy order.
D. Configure the default policy to redirect the requests to the correct policy.

Answer: D

Explanation:

Question: 387

Which security product enables administrators to deploy Kubernetes clusters in air-gapped sites without needing Internet access?

A. Cisco Content Platform
B. Cisco Container Controller
C. Cisco Container Platform
D. Cisco Cloud Platform

Answer: C

Explanation:

Question: 388

What is the intent of a basic SYN flood attack?

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

Answer: B

Explanation:

Question: 389

An engineer configures new features within the Cisco Umbrella dashboard and wants to identify and proxy traffic that is categorized as risky domains and may contain safe and malicious content. Which action accomplishes these objectives?

A. Configure URL filtering within Cisco Umbrella to track the URLs and proxy the requests for those categories and below.
B. Configure intelligent proxy within Cisco Umbrella to intercept and proxy the requests for only those categories.
C. Upload the threat intelligence database to Cisco Umbrella for the most current information on reputations and to have the destination lists block them.
D. Create a new site within Cisco Umbrella to block requests from those categories so they can be sent to the proxy device.

Answer: B

Explanation:

Question: 390

Which endpoint solution protects a user from a phishing attack?

A. Cisco Identity Services Engine

B. Cisco AnyConnect with ISE Posture module
C. Cisco AnyConnect with Network Access Manager module
D. Cisco AnyConnect with Umbrella Roaming Security module

Answer: D

Explanation:

Question: 391

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

A. Cisco Identity Services Engine
B. Cisco Enterprise Security Appliance
C. Cisco Web Security Appliance
D. Cisco Advanced Stealthwatch Appliance

Answer: C

Explanation:

Question: 392

What are two things to consider when using PAC files with the Cisco WSA? (Choose two.)

A. If the WSA host port is changed, the default port redirects web traffic to the correct port automatically.
B. PAC files use if-else statements to determine whether to use a proxy or a direct connection for traffic between the PC and the host.
C. The WSA hosts PAC files on port 9001 by default.
D. The WSA hosts PAC files on port 6001 by default.
E. By default, they direct traffic through a proxy when the PC and the host are on the same subnet.

Answer: BC

Explanation:

Question: 393

Which IETF attribute is supported for the RADIUS CoA feature?

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

Answer: A

Explanation:

Question: 394

When a transparent authentication fails on the Web Security Appliance, which type of access does the end user get?

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

Answer: C

Explanation:

Question: 395

What are two ways that Cisco Container Platform provides value to customers who utilize cloud service providers? (Choose two.)

A. Allows developers to create code once and deploy to multiple clouds
B. helps maintain source code for cloud deployments
C. manages Docker containers
D. manages Kubernetes clusters
E. Creates complex tasks for managing code

Answer: AE

Explanation:

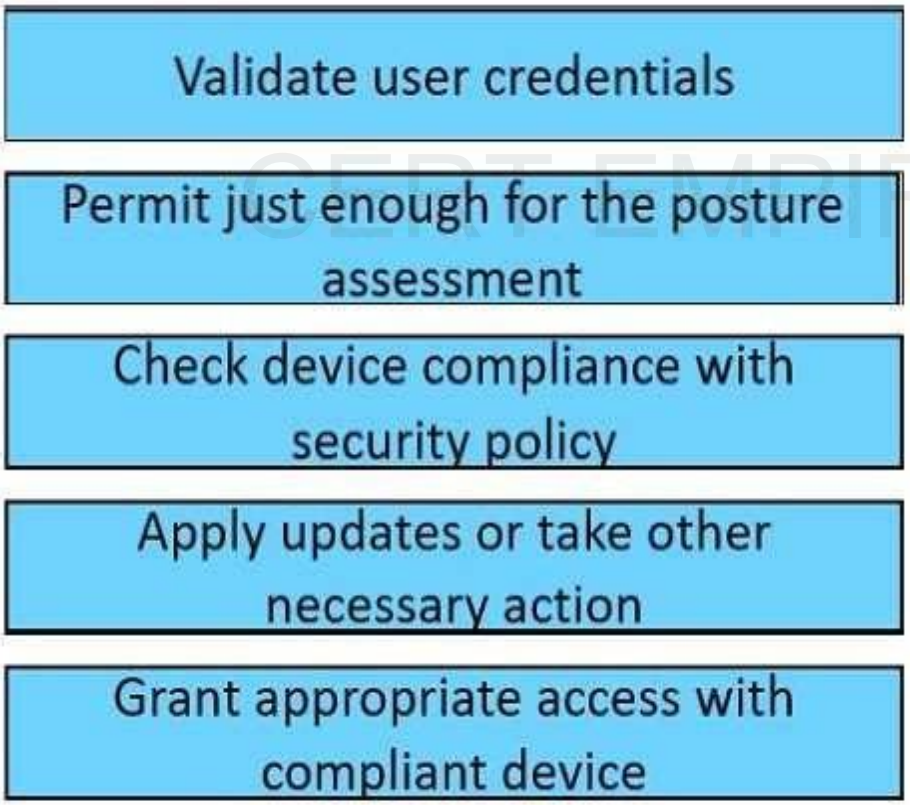
Question: 396

DRAG DROP
Drag and drop the posture assessment flow actions from the left into a sequence on the right.

Validate user credentials	step 1
Check device compliance with security policy	step 2
Grant appropriate access with compliant device	step 3
Apply updates or take other necessary action	step 4
Permit just enough for the posture assessment	step 5

Answer:

Explanation:



Question: 397

Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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

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

Answer: C

Explanation:

Question: 398

Which statement describes a serverless application?

A. The application delivery controller in front of the server farm designates on which server the application runs each time.
B. The application runs from an ephemeral, event-triggered, and stateless container that is fully managed by a cloud provider.
C. The application is installed on network equipment and not on physical servers.
D. The application runs from a containerized environment that is managed by Kubernetes or Docker Swarm.

Answer: B

Explanation:

Question: 399

What is a description of microsegmentation?

A. Environments deploy a container orchestration platform, such as Kubernetes, to manage the application delivery.
B. Environments apply a zero-trust model and specify how applications on different servers or containers can communicate.
C. Environments deploy centrally managed host-based firewall rules on each server or container.
D. Environments implement private VLAN segmentation to group servers with similar applications.

Answer: B

Explanation:

Question: 400

Which Cisco WSA feature supports access control using URL categories?

A. transparent user identification
B. SOCKS proxy services
C. web usage controls
D. user session restrictions

Answer: A

Explanation:

Question: 401

Which technology limits communication between nodes on the same network segment to individual applications?

A. serverless infrastructure
B. microsegmentation
C. SaaS deployment
D. machine-to-machine firewalling

Answer: B

Explanation:

Question: 402

An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users. Which action accomplishes this goal?

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

Answer: D

Explanation:

Question: 403

What is the purpose of joining Cisco WSAs to an appliance group?

A. All WSAs in the group can view file analysis results.
B. The group supports improved redundancy
C. It supports cluster operations to expedite the malware analysis process.
D. It simplifies the task of patching multiple appliances.

Answer: B

Explanation:

Question: 404

Why should organizations migrate to an MFA strategy for authentication?

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

Answer: A

Explanation:

Question: 405

Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?

A. RADIUS-based REAP
B. fingerprinting
C. Dynamic ARP Inspection
D. multifactor authentication

Answer: A

Explanation:

Question: 406

Which type of attack is MFA an effective deterrent for?

A. ping of death
B. phishing

C. teardrop
D. syn flood

Answer: B

Explanation:

Question: 407

Which solution for remote workers enables protection, detection, and response on the endpoint against known and unknown threats?

A. Cisco AMP for Endpoints
B. Cisco AnyConnect
C. Cisco Umbrella
D. Cisco Duo

Answer: A

Explanation:

Question: 408

Which two actions does the Cisco Identity Services Engine posture module provide that ensures endpoint security? (Choose two.)

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

Answer: A, D

Explanation:

Question: 409

What is an advantage of the Cisco Umbrella roaming client?

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

Answer: C

Explanation:

Question: 410

Which Cisco platform provides an agentless solution to provide visibility across the network including encrypted traffic analytics to detect malware in encrypted traffic without the need for decryption?

A. Cisco Advanced Malware Protection
B. Cisco Stealthwatch
C. Cisco Identity Services Engine
D. Cisco AnyConnect

Answer: B

Explanation:

Question: 411

Which two Cisco ISE components must be configured for BYOD? (Choose two.)

A. local WebAuth
B. central WebAuth
C. null WebAuth
D. guest
E. dual

Answer: B, D

Explanation:

Question: 412

Which system performs compliance checks and remote wiping?

A. MDM
B. ISE
C. AMP
D. OTP

Answer: A

Explanation:

Question: 413

An engineer is configuring Cisco WSA and needs to enable a separated email transfer flow from the Internet and from the LAN. Which deployment mode must be used to accomplish this goal?

A. single interface
B. multi-context
C. transparent
D. two-interface

Answer: D

Explanation:

Question: 414

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

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

Answer: B, C

Explanation:

Question: 415

Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or Microsoft vSwitch?

A. inter-EPG isolation
B. inter-VLAN security
C. intra-EPG isolation
D. placement in separate EPGs

Answer: B

Explanation:

Question: 416

What are two ways a network administrator transparently identifies users using Active Directory on

the Cisco WSA? (Choose two.)

A. Create an LDAP authentication realm and disable transparent user identification.
B. Create NTLM or Kerberos authentication realm and enable transparent user identification.
C. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.
D. The eDirectory client must be installed on each client workstation.
E. Deploy a separate eDirectory server; the dent IP address is recorded in this server.

Answer: A, C

Explanation:

Question: 417

Which baseline form of telemetry is recommended for network infrastructure devices?

A. SDNS
B. NetFlow
C. passive taps
D. SNMP

Answer: D

Explanation:

Question: 418

In which scenario is endpoint-based security the solution?

A. inspecting encrypted traffic
B. device profiling and authorization
C. performing signature-based application control
D. inspecting a password-protected archive

Answer: C

Explanation:

Question: 419

```
def dnac_login(host, username, password):
    url = "https://{}/api/system/v1/auth/token".format(host)
    response = requests.request("POST", url,
auth=HTTPBasicAuth(username, password),
                                headers=headers, verify=False)
    return response.json() ["Token"]
```

Refer to the exhibit. What is the result of the Python script?

A. It uses the POST HTTP method to obtain a username and password to be used for authentication.
B. It uses the POST HTTP method to obtain a token to be used for authentication.
C. It uses the GET HTTP method to obtain a token to be used for authentication.
D. It uses the GET HTTP method to obtain a username and password to be used for authentication

Answer: B

Explanation:

Question: 420

Why is it important to patch endpoints consistently?

A. Patching reduces the attack surface of the infrastructure.
B. Patching helps to mitigate vulnerabilities.
C. Patching is required per the vendor contract.
D. Patching allows for creating a honeypot.

Answer: B

Explanation:

Question: 421

Which two parameters are used for device compliance checks? (Choose two.)

A. endpoint protection software version
B. Windows registry values
C. DHCP snooping checks
D. DNS integrity checks
E. device operating system version

Answer: C, E

Explanation:

Question: 422

Which Cisco cloud security software centrally manages policies on multiple platforms such as Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS?

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

Answer: A

Explanation:

Question: 423

Which Cisco security solution determines if an endpoint has the latest OS updates and patches installed on the system?

A. Cisco Endpoint Security Analytics
B. Cisco AMP for Endpoints
C. Endpoint Compliance Scanner
D. Security Posture Assessment Service

Answer: D

Explanation:

Question: 424

A network administrator is configuring a role 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?

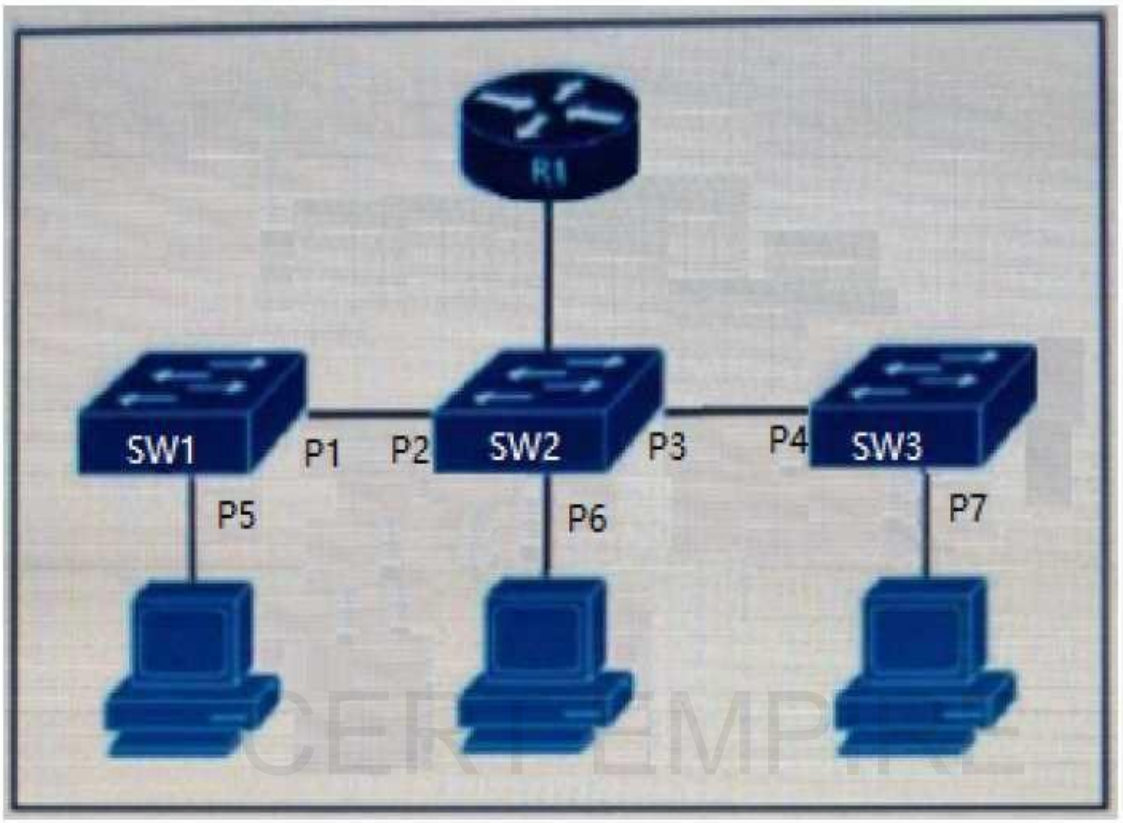
A. 3
B. 5
C. 10
D. 1

Answer: C

Explanation:

Question: 425

Refer to the exhibit.



The DHCP snooping database resides on router R1, and dynamic ARP inspection is configured only on switch SW2. Which ports must be configured as untrusted so that dynamic ARP inspection operates normally?

A. P2 and P3 only
B. P5, P6, and P7 only
C. P1, P2, P3, and P4 only
D. P2, P3, and P6 only

Answer: D

Explanation:

Question: 426

An engineer is configuring device-hardening on a router in order to prevent credentials from being seen
if the router configuration was compromised. Which command should be used?

A. service password-encryption
B. username <username> privilege 15 password <password>
C. service password-recovery
D. username < username> password <password>

Answer: A

Explanation:

Question: 427

Which security solution protects users leveraging DNS-layer security?

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

Answer: C

Explanation:

Question: 428

Which CoA response code is sent if an authorization state is changed successfully on a Cisco IOS device?

A. CoA-NCL
B. CoA-NAK
C. CoA-MAB
D. CoA-ACK

Answer: D

Explanation:

Question: 429

Which security solution uses NetFlow to provide visibility across the network, data center, branch offices, and cloud?

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

Answer: B

Explanation:

Question: 430

How does a WCCP-configured router identify if the Cisco WSA is functional?

A. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the router.

B. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the WSA.
C. The WSA sends a Here-I-Am message every 10 seconds, and the router acknowledges with an ISee-You message.
D. The router sends a Here-I-Am message every 10 seconds, and the WSA acknowledges with an ISee-You message.

Answer: C

Explanation:

Question: 431

Which solution supports high availability in routed or transparent mode as well as in northbound and southbound deployments?

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

Answer: B

Explanation:

Question: 432

Which Cisco ASA Platform mode disables the threat detection features except for Advanced Threat Statistics?

A. cluster
B. transparent
C. routed
D. multiple context

Answer: B

Explanation:

Question: 433

Which benefit does DMVPN provide over GETVPN?

A. DMVPN supports QoS, multicast, and routing, and GETVPN supports only QoS.
B. DMVPN is a tunnel-less VPN, and GETVPN is tunnel-based.
C. DMVPN supports non-IP protocols, and GETVPN supports only IP protocols.
D. DMVPN can be used over the public Internet, and GETVPN requires a private network.

Answer: D

Explanation:

Question: 434

An organization has DHCP servers set up to allocate IP addresses to clients on the LAN. What must be done to ensure the LAN switches prevent malicious DHCP traffic while also distributing IP addresses to
the correct endpoints?

A. Configure Dynamic ARP Inspection and add entries in the DHCP snooping database
B. Configure DHCP snooping and set an untrusted interface for all clients
C. Configure Dynamic ARP Inspection and antispoofing ACLs in the DHCP snooping database
D. Configure DHCP snooping and set a trusted interface for the DHCP server

Answer: A

Explanation:

Question: 435

Which two parameters are used to prevent a data breach in the cloud? (Choose two.)

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

Answer: A, B

Explanation:

Question: 436

Which technology enables integration between Cisco ISE and other platforms to gather and share network and vulnerability data and SIEM and location information?

A. pxGrid
B. NetFlow
C. SNMP
D. Cisco Talos

Answer: A

Explanation:

Question: 437

Which Cisco DNA Center Intent API action is used to retrieve the number of devices known to a DNA

Center?

A. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/network-device/count
B. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/network-device
C. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/networkdevice?parameter1=value&parameter2=value&....
D. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/networkdevice/startIndex/recordsToReturn

Answer: A

Explanation:

Question: 438

An organization must add new firewalls to its infrastructure and wants to use Cisco ASA or Cisco FTD. The chosen firewalls must provide methods of blocking traffic that include offering the user the option to bypass the block for certain sites after displaying a warning page and to reset the connection. Which solution should the organization choose?

A. Cisco FTD because it supports system rate level traffic blocking, whereas Cisco ASA does not
B. Cisco ASA because it allows for interactive blocking and blocking with reset to be configured via the GUI, whereas Cisco FTD does not.
C. Cisco FTD because it enables interactive blocking and blocking with reset natively, whereas Cisco ASA does not
D. Cisco ASA because it has an additional module that can be installed to provide multiple blocking capabilities, whereas Cisco FTD does not.

Answer: C

Explanation:

Question: 439

An engineer is configuring web filtering for a network using Cisco Umbrella Secure Internet Gateway. The requirement is that all traffic needs to be filtered. Using the SSL decryption feature, which type of certificate should be presented to the end-user to accomplish this goal?

A. third-party
B. self-signed
C. organization owned root
D. SubCA

Answer: C

Explanation:

Question: 440

An engineer needs to configure an access control policy rule to always send traffic for inspection without
using the default action. Which action should be configured for this rule?

A. monitor
B. allow
C. block
D. trust

Answer: A

Explanation:

Question: 441

When NetFlow is applied to an interface, which component creates the flow monitor cache that is used
to collect traffic based on the key and nonkey fields in the configured record?

A. records
B. flow exporter
C. flow sampler
D. flow monitor

Answer: B

Explanation:

Question: 442

Which encryption algorithm provides highly secure VPN communications?

A. 3DES
B. AES 256
C. AES 128
D. DES

Answer: B

Explanation:

Question: 443

An administrator needs to configure the Cisco ASA via ASDM such that the network management system
can actively monitor the host using SNMPv3. Which two tasks must be performed for this

configuration?
(Choose two.)

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

Answer: D, E

Explanation:

Question: 444

Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using
higher-level protocols without readdressing the network?

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

Answer: B

Explanation:

Question: 445

Which function is performed by certificate authorities but is a limitation of registration authorities?

A. accepts enrollment requests
B. certificate re-enrollment
C. verifying user identity
D. CRL publishing

Answer: C

Explanation:

Question: 446

Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect
from phishing attacks? (Choose two.)

A. blocks malicious websites and adds them to a block list
B. does a real-time user web browsing behavior analysis

C. provides a defense for on-premises email deployments
D. uses a static algorithm to determine malicious
E. determines if the email messages are malicious

Answer: C, E

Explanation:

Question: 447

What is a feature of NetFlow Secure Event Logging?

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

Answer: A

Explanation:

Question: 448

A hacker initiated a social engineering attack and stole username and passwords of some users within a
company. Which product should be used as a solution to this problem?

A. Cisco NGFW
B. Cisco AnyConnect
C. Cisco AMP for Endpoints
D. Cisco Duo

Answer: D

Explanation:

Question: 449

Which technology provides the benefit of Layer 3 through Layer 7 innovative deep packet inspection, enabling the platform to identify and output various applications within the network traffic flows?

A. Cisco NBAR2
B. Cisco ASAV
C. Account on Resolution
D. Cisco Prime Infrastructure

Answer: A

Explanation:

Question: 450

Which RADIUS feature provides a mechanism to change the AAA attributes of a session after it is authenticated?

A. Authorization
B. Accounting
C. Authentication
D. CoA

Answer: D

Explanation:

Question: 451

Which type of data exfiltration technique encodes data in outbound DNS requests to specific servers and can be stopped by Cisco Umbrella?

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

Answer: A

Explanation:

Question: 452

A large organization wants to deploy a security appliance in the public cloud to form a site-to-site VPN
and link the public cloud environment to the private cloud in the headquarters data center. Which Cisco
security appliance meets these requirements?

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

Answer: B

Explanation:

Question: 453

Which CLI command is used to enable URL filtering support for shortened URLs on the Cisco ESA?

A. webadvancedconfig
B. websecurity advancedconfig
C. outbreakconfig
D. websecurity config

Answer: B

Explanation:

Question: 454

Which standard is used to automate exchanging cyber threat information?

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

Answer: A

Explanation:

Question: 455

What is a function of the Layer 4 Traffic Monitor on a Cisco WSA?

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

Answer: C

Explanation:

Question: 456

A network engineer entered the snmp-server user asmith myv7 auth sha cisco priv aes 256 cisc0xxxxxxxxx command and needs to send SNMP information to a host at 10.255.255.1. Which command achieves this goal?

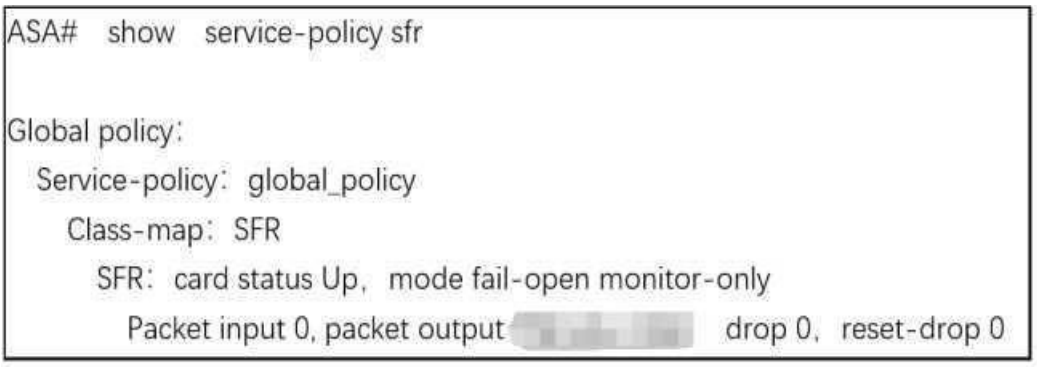
A. snmp-server host inside 10.255.255.1 version 3 myv7
B. snmp-server host inside 10.255.255.1 snmpv3 myv7
C. snmp-server host inside 10.255.255.1 version 3 asmith
D. snmp-server host inside 10.255.255.1 snmpv3 asmith

Answer: C

Explanation:

Question: 457

Refer to the exhibit.



What are two indications of the Cisco Firepower Services Module configuration? (Choose two.)

A. The module is operating in IDS mode.
B. The module fails to receive redirected traffic
C. Traffic is blocked if the module fails.
D. Traffic continues to flow if the module fails.
E. The module is operating in IPS mode.

Answer: AD

Explanation:

Question: 458

Why is it important for the organization to have an endpoint patching strategy?

A. so the organization can identify endpoint vulnerabilities
B. so the internal PSIRT organization is aware of the latest bugs
C. so the network administrator is notified when an existing bug is encountered
D. so the latest security fixes are installed on the endpoints

Answer: C

Explanation:

Question: 459

An email administrator is setting up a new Cisco ES
A. The administrator wants to enable the blocking of
greymail for the end user. Which feature must the administrator enable first?
A. File Analysis
B. IP Reputation Filtering
C. Intelligent Multi-Scan
D. Anti-Virus Filtering

Answer: C

Explanation:

Question: 460

What limits communication between applications or containers on the same node?

A. microsegmentation
B. container orchestration
C. microservicing
D. Software-Defined Access

Answer: D

Explanation:

Question: 461

Which open source tool does Cisco use to create graphical visualizations of network telemetry on Cisco IOS XE devices?

A. InfluxDB
B. Splunk
C. SNMP
D. Grafana

Answer: D

Explanation:

Question: 462

How does the Cisco WSA enforce bandwidth restrictions for web applications?

A. It implements a policy route to redirect application traffic to a lower-bandwidth link.
B. It dynamically creates a scavenger class QoS policy and applies it to each client that connects through the WSA.
C. It sends commands to the uplink router to apply traffic policing to the application traffic.
D. It simulates a slower link by introducing latency into application traffic.

Answer: C

Explanation:

Question: 463

Which two components do southbound APIs use to communicate with downstream devices? (Choose two.)

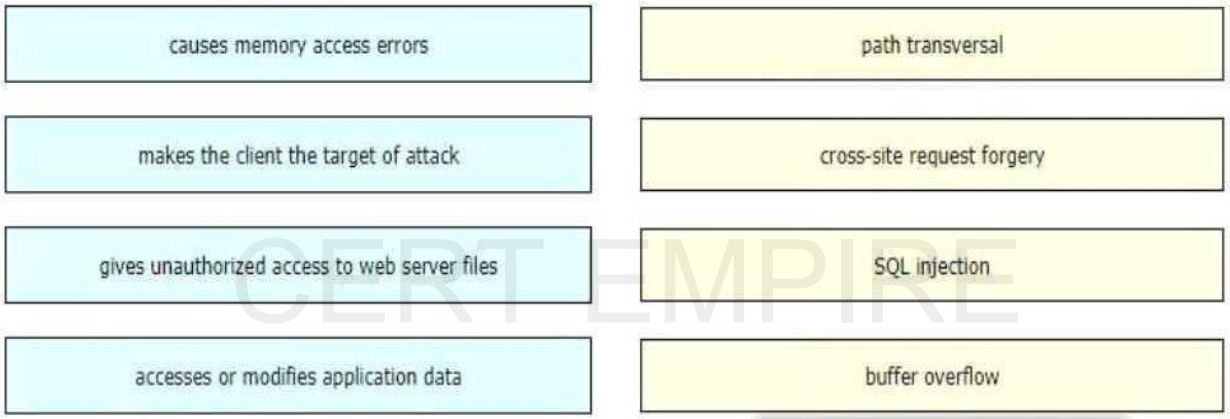
A. services running over the network
B. OpenFlow
C. external application APIs
D. applications running over the network
E. OpFlex

Answer: B, E

Explanation:

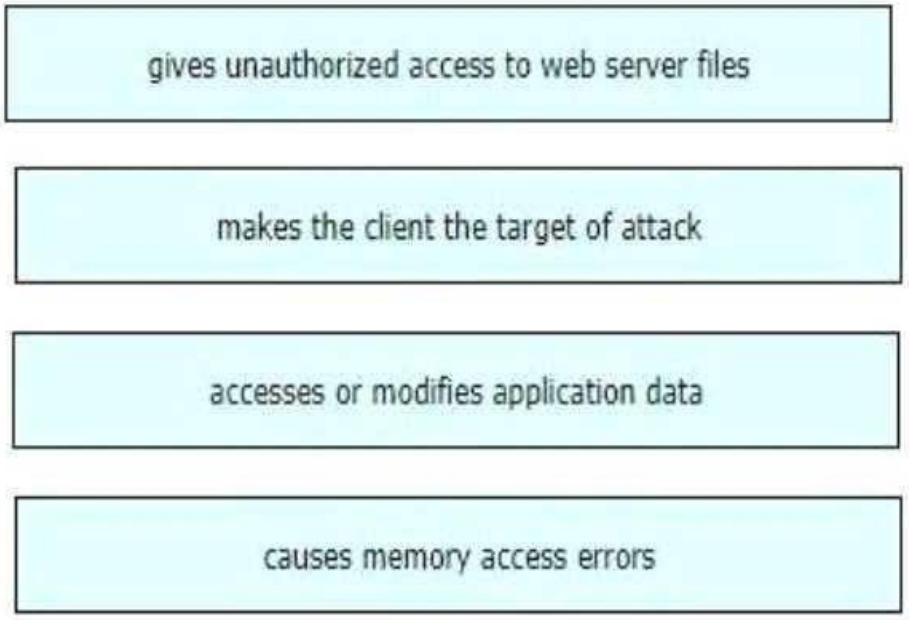
Question: 464

DRAG DROP
Drag and drop the exploits from the left onto the type of security vulnerability on the right.



Answer:

Explanation:



Question: 465

What is the term for when an endpoint is associated to a provisioning WLAN that is shared with guest

access, and the same guest portal is used as the BYOD portal?

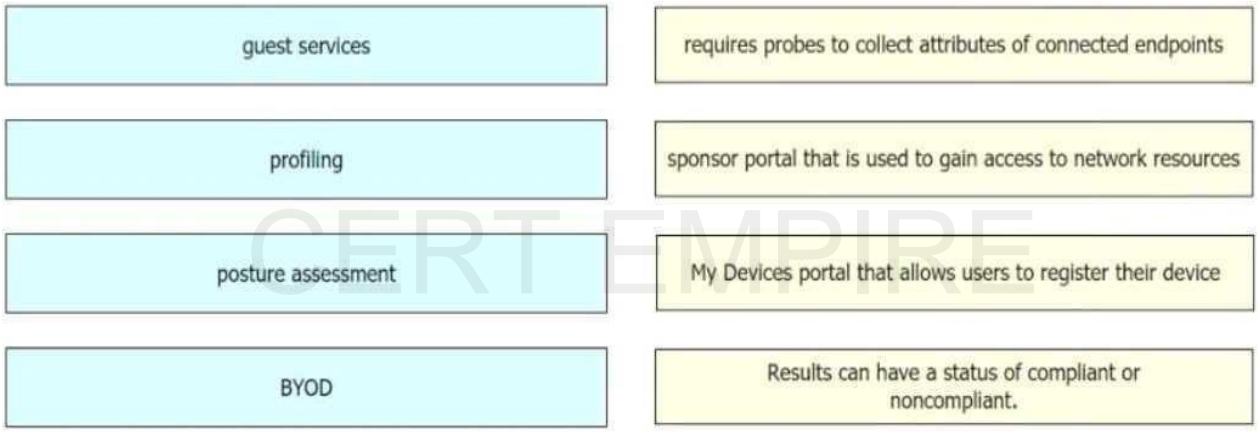
A. single-SSID BYOD
B. multichannel GUI
C. dual-SSID BYOD
D. streamlined access

Answer: C

Explanation:

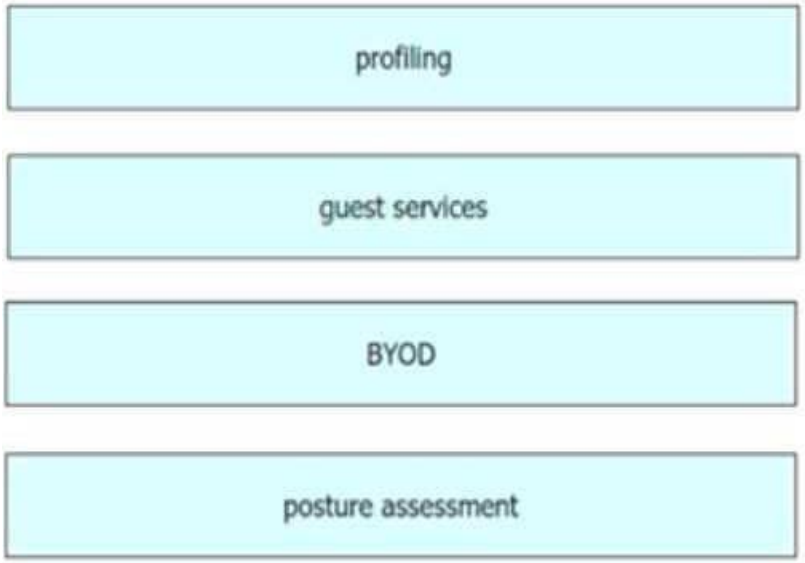
Question: 466

DRAG DROP
Drag and drop the concepts from the left onto the correct descriptions on the right



Answer:

Explanation:



Question: 467

Which feature within Cisco ISE verifies the compliance of an endpoint before providing access to the network?

A. Posture
B. Profiling
C. pxGrid
D. MAB

Answer: A

Explanation:

Question: 468

Which MDM configuration provides scalability?

A. pushing WPA2-Enterprise settings automatically to devices
B. enabling use of device features such as camera use
C. BYOD support without extra appliance or licenses
D. automatic device classification with level 7 fingerprinting

Answer: C

Explanation:

Question: 469

Which Cisco ISE service checks the compliance of endpoints before allowing the endpoints to connect to
the network?

A. posture
B. profiler
C. Cisco TrustSec
D. Threat Centric NAC

Answer: A

Explanation:

Question: 470

Which endpoint protection and detection feature performs correlation of telemetry, files, and intrusion
events that are flagged as possible active breaches?

A. retrospective detection
B. indication of compromise
C. file trajectory
D. elastic search

Answer: D

Explanation:

Question: 471

Which feature enables a Cisco ISR to use the default bypass list automatically for web filtering?

A. filters
B. group key
C. company key
D. connector

Answer: D

Explanation:

Question: 472

A network engineer has configured a NTP server on a Cisco AS
A. The Cisco ASA has IP reachability to the
NTP server and is not filtering any traffic. The show ntp association detail command indicates that
the
configured NTP server is unsynchronized and has a stratum of 16. What is the cause of this issue?
A. Resynchronization of NTP is not forced
B. NTP is not configured to use a working server.
C. An access list entry for UDP port 123 on the inside interface is missing.
D. An access list entry for UDP port 123 on the outside interface is missing.

Answer: B

Explanation:

Question: 473

When a next-generation endpoint security solution is selected for a company, what are two key deliverables that help justify the implementation? (Choose two.)

A. signature-based endpoint protection on company endpoints
B. macro-based protection to keep connected endpoints safe
C. continuous monitoring of all files that are located on connected endpoints
D. email integration to protect endpoints from malicious content that is located in email
E. real-time feeds from global threat intelligence centers

Answer: C, E

Explanation:

Question: 474

What is the process of performing automated static and dynamic analysis of files against preloaded behavioral indicators for threat analysis?

A. deep visibility scan
B. point-in-time checks
C. advanced sandboxing
D. advanced scanning

Answer: C

Explanation:

Question: 475

Which solution is made from a collection of secure development practices and guidelines that developers must follow to build secure applications?

A. AFL
B. Fuzzing Framework
C. Radamsa
D. OWASP

Answer: D

Explanation:

Question: 476

What do tools like Jenkins, Octopus Deploy, and Azure DevOps provide in terms of application and infrastructure automation?

A. continuous integration and continuous deployment
B. cloud application security broker
C. compile-time instrumentation
D. container orchestration

Answer: A

Explanation:

Question: 477

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

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

Answer: D

Explanation:

Question: 478

Which technology provides a combination of endpoint protection endpoint detection, and response?

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

Answer: A

Explanation:

Question: 479

What is a feature of container orchestration?

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

Answer: C

Explanation:

Question: 480

What are two security benefits of an MDM deployment? (Choose two.)

A. robust security policy enforcement
B. privacy control checks
C. on-device content management
D. distributed software upgrade
E. distributed dashboard

Answer: A,C

Explanation:

Question: 481

Refer to the exhibit.

Consider that any feature of DNS requests, such as the length off the domain name and the number of subdomains, can be used to construct models of expected behavior to which observed values can be compared. Which type of malicious attack are these values associated with?

A. Spectre Worm
B. Eternal Blue Windows
C. Heartbleed SSL Bug
D. W32/AutoRun worm

Answer: D

Explanation:

Question: 482

What is the recommendation in a zero-trust model before granting access to corporate applications and
resources?

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

Answer: A

Explanation:

Question: 483

Which Cisco AMP feature allows an engineer to look back to trace past activities, such as file and process
activity on an endpoint?

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

Answer: D

Explanation:

Question: 484

Which solution stops unauthorized access to the system if a user's password is compromised?

A. VPN
B. MFA
C. AMP
D. SSL

Answer: B

Explanation:

Question: 485

What is a benefit of using Cisco Tetration?

A. It collects telemetry data from servers and then uses software sensors to analyze flow information.
B. It collects policy compliance data and process details.
C. It collects enforcement data from servers and collects interpacket variation.
D. It collects near-real time data from servers and inventories the software packages that exist on servers.

Answer: A

Explanation:

Question: 486

How does Cisco Umbrella protect clients when they operate outside of the corporate network?

A. by modifying the registry for DNS lookups
B. by using Active Directory group policies to enforce Cisco Umbrella DNS servers
C. by using the Cisco Umbrella roaming client
D. by forcing DNS queries to the corporate name servers

Answer: C

Explanation:

Question: 487

Which industry standard is used to integrate Cisco ISE and pxGrid to each other and with other interoperable security platforms?

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

Answer: B

Explanation:

Question: 488

What are two facts about WSA HTTP proxy configuration with a PAC file? (Choose two.)

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

Answer: C, D

Explanation:

Question: 489

Which solution should be leveraged for secure access of a CI/CD pipeline?

A. Duo Network Gateway
B. remote access client
C. SSL WebVPN
D. Cisco FTD network gateway

Answer: A

Explanation:

Question: 490

Which function is included when Cisco AMP is added to web security?

A. multifactor, authentication-based user identity
B. detailed analytics of the unknown file's behavior
C. phishing detection on emails
D. threat prevention on an infected endpoint

Answer: B

Explanation:

Question: 491

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

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

Answer: A

Explanation:

Question: 492

Which solution detects threats across a private network, public clouds, and encrypted traffic?

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

Answer: A

Explanation:

Question: 493

Which Cisco security solution integrates with cloud applications like Dropbox and Office 365 while protecting data from being exfiltrated?

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

Answer: C

Explanation:

Question: 494

Which two actions does the Cisco Identity Services Engine posture module provide that ensures endpoint security?(Choose two.)

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

Answer: AD

Explanation:

Question: 495

Which two authentication protocols are supported by the Cisco WSA? (Choose two.)

A. WCCP
B. NTLM
C. TLS
D. SSL
E. LDAP

Answer: BE

Explanation:

Question: 496

When a Cisco WSA checks a web request, what occurs if it is unable to match a user-defined policy?

A. It blocks the request.
B. It applies the global policy.
C. It applies the next identification profile policy.
D. It applies the advanced policy.

Answer: B

Explanation:

Question: 497

Which Cisco solution extends network visibility, threat detection, and analytics to public cloud environments?

A. Cisco Umbrella
B. Cisco Stealthwatch Cloud
C. Cisco Appdynamics
D. Cisco CloudLock

Answer: B

Explanation:

Question: 498

Which metric is used by the monitoring agent to collect and output packet loss and jitter information?

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

Answer: B

Explanation:

Question: 499

Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)

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

Answer: A, B

Explanation:

Question: 500

DRAG DROP

Drag and drop the features of Cisco ASA with Firepower from the left onto the benefits on the right.

Answer:

Explanation:

Question: 501

What are two benefits of using Cisco Duo as an MFA solution? (Choose two.)

A. grants administrators a way to remotely wipe a lost or stolen device

B. provides simple and streamlined login experience for multiple applications and users
C. native integration that helps secure applications across multiple cloud platforms or on-premises environments
D. encrypts data that is stored on endpoints
E. allows for centralized management of endpoint device applications and configurations

Answer: B, C

Explanation:

Question: 502

How does Cisco Workload Optimization portion of the network do EPP solutions solely performance issues?

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

Answer: B

Explanation:

Question: 503

What are two benefits of using an MDM solution? (Choose two.)

A. grants administrators a way to remotely wipe a lost or stolen device
B. provides simple and streamlined login experience for multiple applications and users
C. native integration that helps secure applications across multiple cloud platforms or on-premises environments
D. encrypts data that is stored on endpoints
E. allows for centralized management of endpoint device applications and configurations

Answer: A, E

Explanation:

Question: 504

A company has 5000 Windows users on its campus. Which two precautions should IT take to prevent WannaCry ransomware from spreading to all clients? (Choose two.)

A. Segment different departments to different IP blocks and enable Dynamic ARp inspection on all

VLANs
B. Ensure that noncompliant endpoints are segmented off to contain any potential damage.
C. Ensure that a user cannot enter the network of another department.
D. Perform a posture check to allow only network access to (hose Windows devices that are already patched.
E. Put all company users in the trusted segment of NGFW and put all servers to the DMZ segment of the Cisco NGFW. ni

Answer: B, D

Explanation:

Question: 505

What provides total management for mobile and PC including managing inventory and device tracking, remote view, and live troubleshooting using the included native remote desktop support?

A. mobile device management
B. mobile content management
C. mobile application management
D. mobile access management

Answer: A

Explanation:

Question: 506

What is the process In DevSecOps where all changes In the central code repository are merged and synchronized?

A. CD
B. EP
C. CI
D. QA

Answer: C

Explanation:

Question: 507

Based on the NIST 800-145 guide, which cloud architecture may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises?

A. hybrid cloud
B. private cloud

C. public cloud
D. community cloud

Answer: D

Explanation:

Question: 508

Which type of data does the Cisco Stealthwatch system collect and analyze from routers, switches, and firewalls?

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

Answer: D

Explanation:

Question: 509

What is the most common type of data exfiltration that organizations currently experience?

A. HTTPS file upload site
B. Microsoft Windows network shares
C. SQL database injections
D. encrypted SMTP

Answer: A

Explanation:

Question: 510

Which security solution is used for posture assessment of the endpoints in a BYOD solution?

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

Answer: D

Explanation:

Question: 511

An engineer is configuring Dropbox integration with Cisco Cloudlock. Which action must be taken before granting API access in the Dropbox admin console?

A. Authorize Dropbox within the Platform settings in the Cisco Cloudlock portal.
B. Add Dropbox to the Cisco Cloudlock Authentication and API section in the Cisco Cloudlock portal.
C. Send an API request to Cisco Cloudlock from Dropbox admin portal.
D. Add Cisco Cloudlock to the Dropbox admin portal.

Answer: A

Explanation:

Question: 512

How does Cisco AMP for Endpoints provide next-generation protection?

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

Answer: B

Explanation:

Question: 513

Which two protocols must be configured to authenticate end users to the Web Security Appliance? (Choose two.)

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

Answer: A,B

Explanation:

Question: 514

Which API method and required attribute are used to add a device into DNAC with the native API?

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

Answer: B

Explanation:

Question: 515

What is a benefit of using Cisco Umbrella?

A. DNS queries are resolved faster.
B. Attacks can be mitigated before the application connection occurs.
C. Files are scanned for viruses before they are allowed to run.
D. It prevents malicious inbound traffic.

Answer: B

Explanation:

Question: 516

Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?

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

Answer: C

Explanation:

Question: 517

What is the term for the concept of limiting communication between applications or containers on the same node?

A. container orchestration
B. software-defined access
C. microservicing
D. microsegmentation

Answer: D

Explanation:

Question: 518

Which Cisco platform onboards the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing the endpoint to gain network access?

A. Cisco ISE
B. Cisco NAC
C. Cisco TACACS+
D. Cisco WSA

Answer: A

Explanation:

Question: 519

What are two characteristics of the RESTful architecture used within Cisco DNA Center? (Choose two.)

A. REST uses methods such as GET, PUT, POST, and DELETE.
B. REST codes can be compiled with any programming language.
C. REST is a Linux platform-based architecture.
D. The POST action replaces existing data at the URL path.
E. REST uses HTTP to send a request to a web service.

Answer: A, E

Explanation:

Question: 520

Which cloud service offering allows customers to access a web application that is being hosted, managed, and maintained by a cloud service provider?

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

Answer: B

Explanation:

Question: 521

Which characteristic is unique to a Cisco WSAv as compared to a physical appliance?

A. supports VMware vMotion on VMware ESXi
B. requires an additional license
C. performs transparent redirection
D. supports SSL decryption

Answer: A

Explanation:

Question: 522

An administrator is configuring N I P on Cisco ASA via ASDM and needs to ensure that rogue NTP servers cannot insert themselves as the authoritative time source Which two steps must be taken to accomplish this task? (Choose two)

A. Specify the NTP version
B. Configure the NTP stratum
C. Set the authentication key
D. Choose the interface for syncing to the NTP server
E. Set the NTP DNS hostname

Answer: C, E

Explanation:

Question: 523

What is a characteristic of an EDR solution and not of an EPP solution?

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

Answer: B

Explanation:

Question: 524

Email security has become a high priority task for a security engineer at a large multi-national

organization due to ongoing phishing campaigns. To help control this, the engineer has deployed an Incoming Content Filter with a URL reputation of (-10 00 to -6 00) on the Cisco ESA Which action will the system perform to disable any links in messages that match the filter?

A. Defang
B. Quarantine
C. FilterAction
D. ScreenAction

Answer: A

Explanation:

Question: 525

What are two workloaded security models? (Choose two)

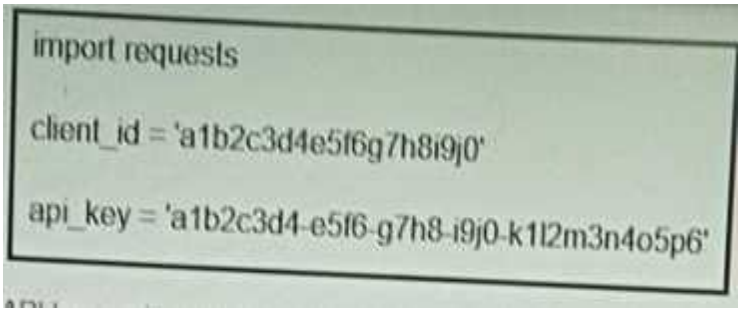
A. SaaS
B. IaaS
C. on-premises
D. off-premises
E. PaaS

Answer: C,D

Explanation:

Question: 526

Refer to the exhibit.



Refer to the exhibit. What function does the API key perform while working with https://api.amp.cisco.com/v1/computers?

A. imports requests
B. HTTP authorization
C. HTTP authentication
D. plays dent ID

Answer: C

Explanation:

Question: 527

What is a benefit of using GET VPN over FlexVPN within a VPN deployment?

A. GET VPN supports Remote Access VPNs
B. GET VPN natively supports MPLS and private IP networks
C. GET VPN uses multiple security associations for connections
D. GET VPN interoperates with non-Cisco devices

Answer: B

Explanation:

Question: 528

An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users.

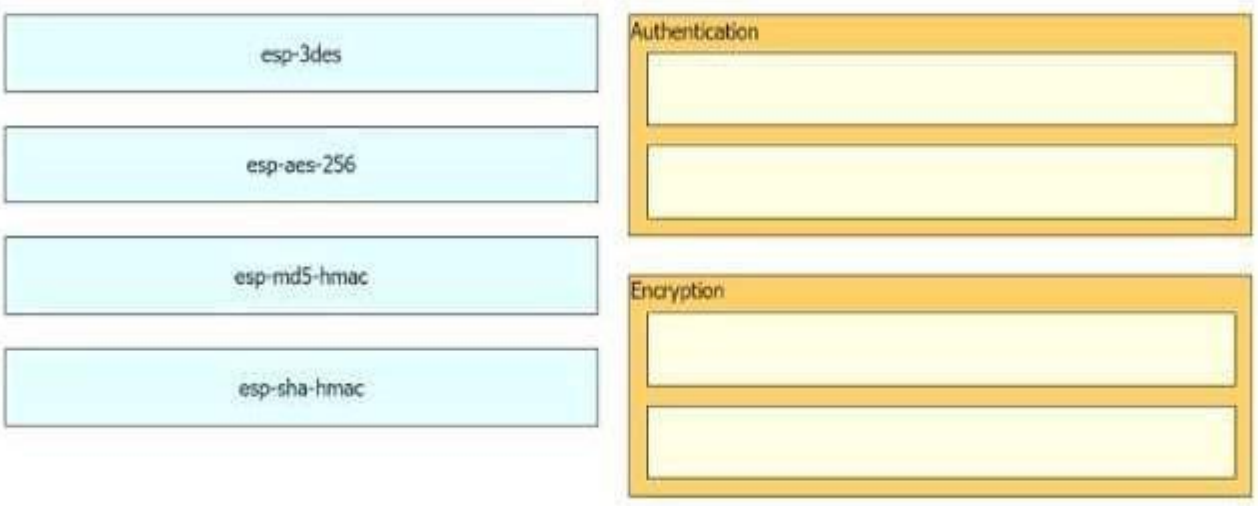
A. Upload the organization root CA to the Umbrella admin portal
B. Modify the user's browser settings to suppress errors from Umbrella.
C. Restrict access to only websites with trusted third-party signed certificates.
D. Import the Umbrella root CA into the trusted root store on the user's device.

Answer: A

Explanation:

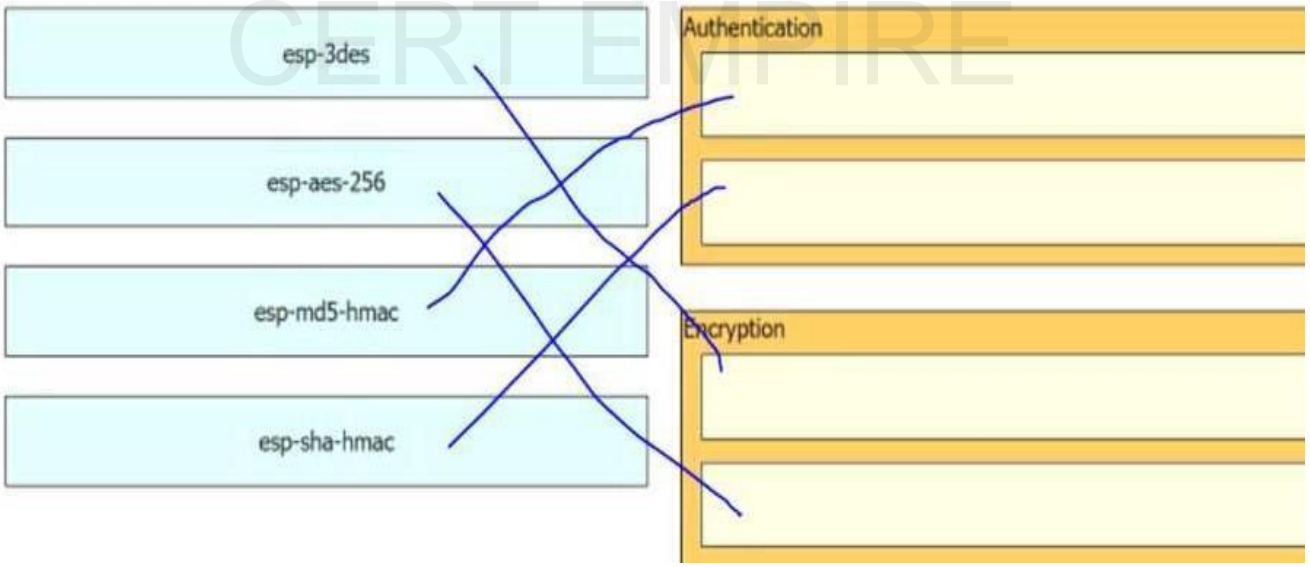
Question: 529

DRAG DROP
Drag and drop the cryptographic algorithms for IPsec from the left onto the cryptographic processes on the right.



Answer:

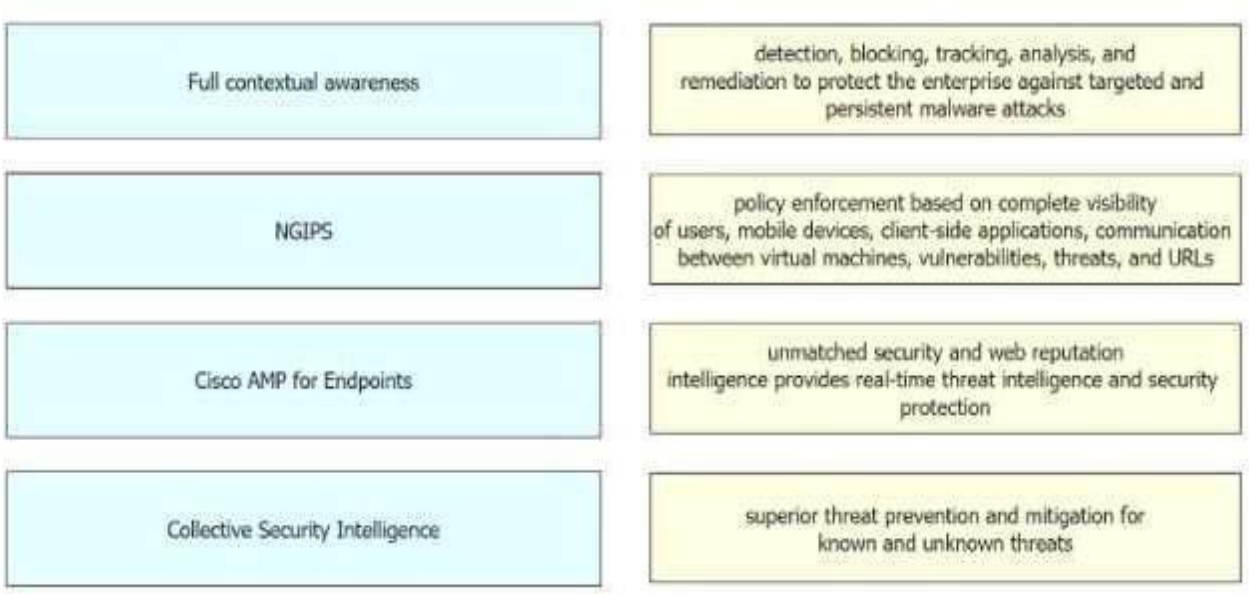
Explanation:



Question: 530

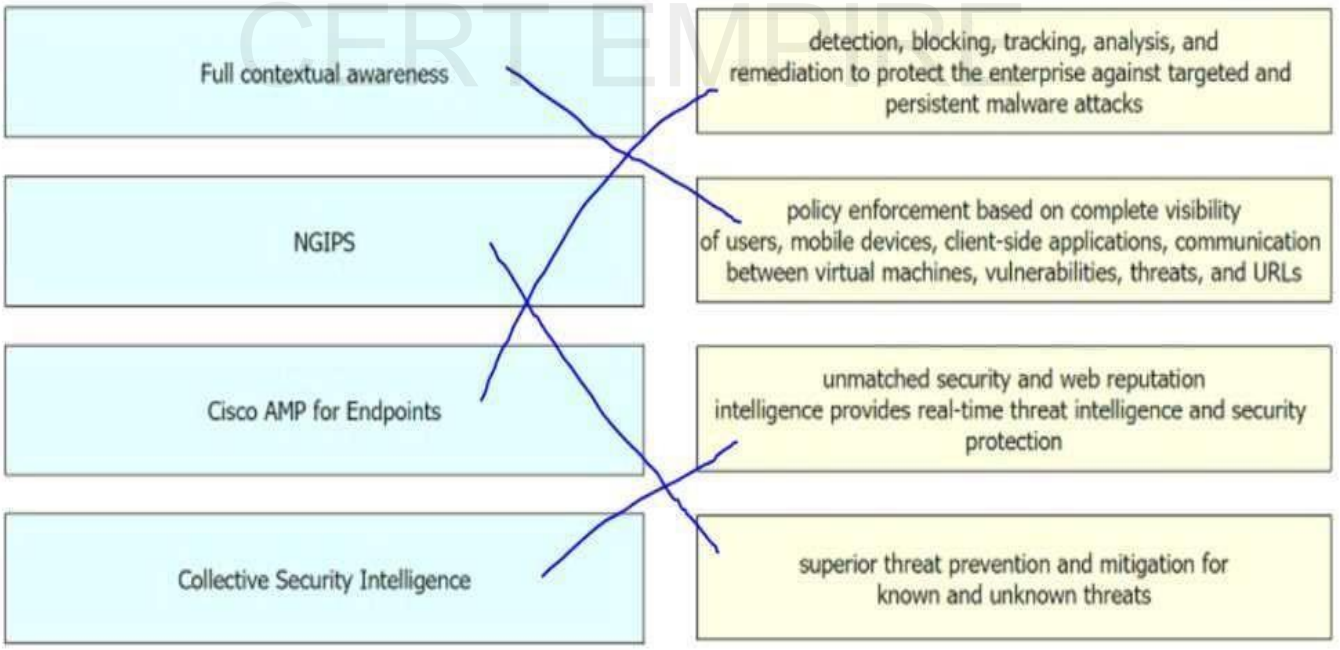
DRAG DROP

Drag and drop the security solutions from the left onto the benefits they provide on the right.



Answer:

Explanation:



Question: 531

DoS attacks are categorized as what?

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

Answer: B

Question: 532

Which Cisco DNA Center RESTful PNP API adds and claims a device into a workflow?
A.api/v1/fie/config
B.api/v1/onboarding/pnp-device/import
C.api/v1/onboarding/pnp-device
D.api/v1/onboarding/workflow

Answer: A

Explanation:

Question: 533

What is the purpose of a NetFlow version 9 template record?
A. It specifies the data format of NetFlow processes.
B. It provides a standardized set of information about an IP flow.
C. It defines the format of data records.
D. It serves as a unique identification number to distinguish individual data records

Answer: B

Explanation:

Question: 534

Which Cisco solution integrates Encrypted Traffic Analytics to perform enhanced visibility,promote compliance,shorten response times, and provide administrators with the information needed to provide educated and automated decisions to secure the environment?

A. Cisco DNA Center
B. Cisco SDN
C. Cisco ISE
D. Cisco Security Compiance Solution

Answer: D

Explanation:

Question: 535

Which feature does the laaS model provide?

A. granular control of data
B. dedicated, restricted workstations
C. automatic updates and patching of software
D. software-defined network segmentation

Answer: C

Explanation:

Question: 536

What is a benefit of flexible NetFlow records?

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

Answer: D

Explanation:

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

Question: 537

What is the purpose of the Cisco Endpoint IoC feature?

A. It provides stealth threat prevention.
B. It is a signature-based engine. W
C. It is an incident response tool 6W
D. It provides precompromise detection.

Answer: C

Explanation:

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Secure_Managed_Endpoint.pdf

Question: 538

An engineer recently completed the system setup on a Cisco WSA Which URL information does the system send to SensorBase Network servers?

A. Summarized server-name information and MD5-hashed path information
B. complete URL,without obfuscating the path segments
C. URL information collected from clients that connect to the Cisco WSA using Cisco AnyConnect
D. none because SensorBase Network Participation is disabled by default

Answer: A

Explanation:

Question: 539

What does endpoint isolation in Cisco AMP for Endpoints security protect from?

A. an infection spreading across the network E
B. a malware spreading across the user device
C. an infection spreading across the LDAP or Active Directory domain from a user account
D. a malware spreading across the LDAP or Active Directory domain from a user account

Answer: C

Explanation:

https://community.cisco.com/t5/endpoint-security/amp-endpoint-isolation/td-p/4086674#:~:text=Isolating%20an%20endpoint%20blocks%20all,your%20IP%20isolation%20allow%20list

Question: 540

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

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

Answer: D

Explanation:

Question: 541

Which Cisco security solution stops exfiltration using HTTPS?

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

Answer: C

Explanation:

https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf

Question: 542

What is a functional difference between Cisco AMP for Endpoints and Cisco Umbrella Roaming Client?

A. The Umbrella Roaming client stops and tracks malicious activity on hosts, and AMP for Endpoints tracks only URL-based threats.
B. The Umbrella Roaming Client authenticates users and provides segmentation, and AMP for Endpoints allows only for VPN connectivity
C. AMP for Endpoints authenticates users and provides segmentation, and the Umbrella Roaming Client allows only for VPN connectivity.
D. AMP for Endpoints stops and tracks malicious activity on hosts, and the Umbrella Roaming Client tracks only URL-based threats.

Answer: B

Explanation:

Question: 543

What is the difference between EPP and EDR?

A. EPP focuses primarily on threats that have evaded front-line defenses that entered the environment.
B. Having an EPP solution allows an engineer to detect, investigate, and remediate modern threats.
C. EDR focuses solely on prevention at the perimeter.
D. Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior.

Answer: B

Question: 544

Which algorithm is an NGE hash function?

A. HMAC
B. SHA-1
C. MD5
D. SISHA-2

Answer: D

Question: 545

What are two recommended approaches to stop DNS tunneling for data exfiltration and command and control call backs? (Choose two.)

A. Use intrusion prevention system.

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

Answer: C, E

Question: 546

Which two capabilities does an MDM provide? (Choose two.)

A. delivery of network malware reports to an inbox in a schedule
B. unified management of mobile devices, Macs, and PCs from a centralized dashboard
C. enforcement of device security policies from a centralized dashboard
D. manual identification and classification of client devices
E. unified management of Android and Apple devices from a centralized dashboard

Answer: B, C

Question: 547

DRAG DROP
Drag and drop the deployment models from the left onto the explanations on the right.

routed	A GRE tunnel is utilized in this solution.
passive	This solution allows inspection between hosts on the same subnet.
passive with ERSPAN	Attacks are not prevented with this solution.
transparent	This solution does not provide filtering between hosts on the same subnet.

Answer:

passive	
routed	
passive with ERSPAN	
transparent	

Question: 548

Which VMware platform does Cisco ACI integrate with to provide enhanced visibility, provide policy integration and deployment, and implement security policies with access lists?

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

Answer: B

Question: 549

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

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

Answer: C

Question: 550

Which capability is provided by application visibility and control?

A. reputation filtering
B. data obfuscation
C. data encryption
D. deep packet inspection

Answer: D

Question: 551

When network telemetry is implemented, what is important to be enabled across all network infrastructure devices to correlate different sources?

A. CDP
B. NTP
C. syslog
D. DNS

Answer: B

Question: 552

In which two ways does the Cisco Advanced Phishing Protection solution protect users? (Choose two.)

A. It prevents use of compromised accounts and social engineering.
B. It prevents all zero-day attacks coming from the Internet.
C. It automatically removes malicious emails from users' inbox.
D. It prevents trojan horse malware using sensors.
E. It secures all passwords that are shared in video conferences.

Answer: B, C

Question: 553

An engineer is adding a Cisco router to an existing environment. NTP authentication is configured on all devices in the environment with the command ntp authentication-key 1 md5 Clsc427128380. There are two routers on the network that are configured as NTP servers for redundancy, 192.168.1.110 and 192.168.1.111. 192.168.1.110 is configured as the authoritative time source. What command must be configured on the new router to use 192.168.1.110 as its primary time source without the new router attempting to offer time to existing devices?

A. ntp server 192.168.1.110 primary key 1
B. ntp peer 192.168.1.110 prefer key 1
C. ntp server 192.168.1.110 key 1 prefer
D. ntp peer 192.168.1.110 key 1 primary

Answer: A

Thank You for your purchase

Cisco 350-701 Exam Question & Answers Implementing and Operating Cisco Security Core Technologies Exam