Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

https://www.2passeasy.com/dumps/350-701/

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

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

Answer: B

NEW QUESTION 2
- (Exam Topic 2)
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:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advance

NEW QUESTION 3
- (Exam Topic 2)
An attacker needs to perform reconnaissance on a target system to help gain access to it. The system has weak passwords, no encryption on the VPN links, and software bugs on the system’s applications. Which
vulnerability allows the attacker to see the passwords being transmitted in clear text?

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

Answer: B

NEW QUESTION 4
- (Exam Topic 2)
What is a benefit of conducting device compliance checks?

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

Answer: B

NEW QUESTION 5
- (Exam Topic 2)
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: AC

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-configguide-v623/secu

NEW QUESTION 6
- (Exam Topic 2)
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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A picture containing table Description automatically generated

NEW QUESTION 7
- (Exam Topic 2)
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:
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technoteesa-00.htmlIn this question, it stated “the network is congested” (not the file analysis server was overloaded) so theappliance will not try to upload the file again.

NEW QUESTION 8
- (Exam Topic 2)
What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?

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

Answer: A

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

NEW QUESTION 9
- (Exam Topic 2)
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

NEW QUESTION 10
- (Exam Topic 2)
What is managed by Cisco Security Manager?

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

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/products/security/security-manager/index.html

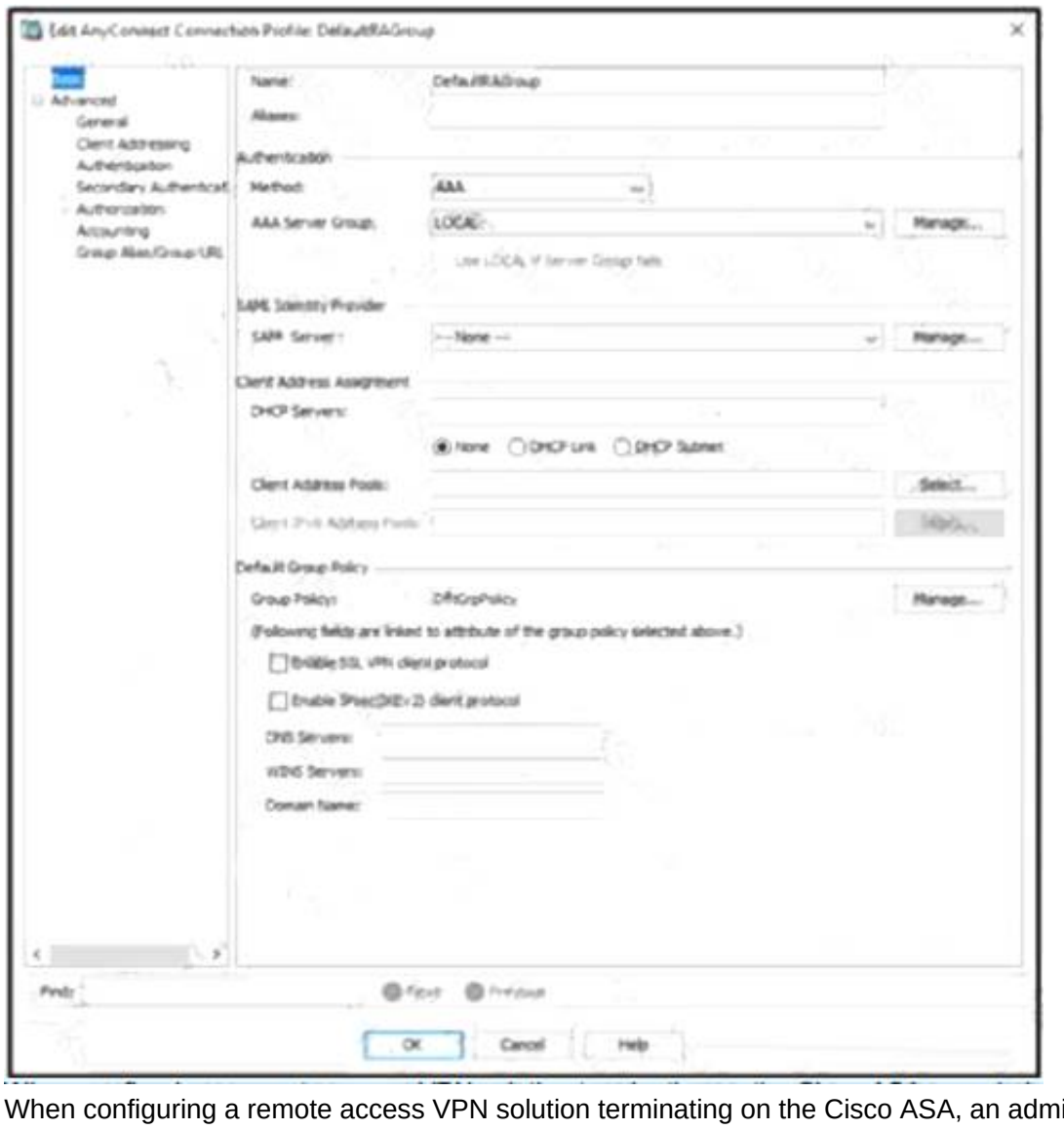
NEW QUESTION 10
- (Exam Topic 2)
What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group?

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

Answer: B

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

NEW QUESTION 11
- (Exam Topic 2)
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” inthe Authentication.

NEW QUESTION 14
- (Exam Topic 2)
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 differentpermutations of common username. Its easy for attackers to get hold of a valid email address if yourorganization uses standard format for official e-mail alias (for example: jsmith@example.com). We canconfigure 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.

NEW QUESTION 16
- (Exam Topic 2)
An organization is trying to implement micro-segmentation on the network and wants to be able to gain visibility on the applications within the network. The solution must be able to maintain and force compliance. Which product should be used to meet these requirements?

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

Answer: D

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

NEW QUESTION 19
- (Exam Topic 2)
In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint Protection Platform?

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

Answer: D

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

NEW QUESTION 24
- (Exam Topic 2)
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

NEW QUESTION 25
- (Exam Topic 2)
What is a benefit of using Cisco FMC over Cisco ASDM?

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

Answer: B

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

NEW QUESTION 29
- (Exam Topic 2)
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:
Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide

NEW QUESTION 32
- (Exam Topic 2)
A Cisco Firepower administrator needs to configure a rule to allow a new application that has never been seen on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose
two)

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

Answer: BE

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

NEW QUESTION 36
- (Exam Topic 1)
What is a commonality between DMVPN and FlexVPN technologies?

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

Answer: D

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

NEW QUESTION 38
- (Exam Topic 1)
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

NEW QUESTION 42
- (Exam Topic 1)
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 instancefamily.+ 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-96 qsg/asavaws.html

NEW QUESTION 44
- (Exam Topic 1)
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

NEW QUESTION 45
- (Exam Topic 1)
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: AD

Explanation:
Reference: https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.htmlThe two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint,face, and retina scans. Biometrics is used commonly in mobile devices).

NEW QUESTION 50
- (Exam Topic 1)
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

NEW QUESTION 53
- (Exam Topic 1)
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: AC

NEW QUESTION 58
- (Exam Topic 1)
Which two key and block sizes are valid for AES? (Choose two)

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

Answer: CD

Explanation:

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

NEW QUESTION 59
- (Exam Topic 1)
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: AD

NEW QUESTION 62
- (Exam Topic 1)
Refer to the exhibit.

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

What does the number 15 represent in this configuration?

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

Answer: B

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

NEW QUESTION 65
- (Exam Topic 1)
What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?

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

Answer: A

NEW QUESTION 70
- (Exam Topic 1)
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 is redirected
B. Traffic from the inside network is redirected
C. All TCP traffic is redirected

D. Traffic from the inside and DMZ networks is redirected

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.htm

NEW QUESTION 74
- (Exam Topic 1)
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.

NEW QUESTION 79
- (Exam Topic 1)
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

NEW QUESTION 82
- (Exam Topic 1)
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.

NEW QUESTION 85
- (Exam Topic 1)
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: AD

Explanation:
Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using asecond factor (like your phone or other mobile device) prevents anyone but you from logging in, even if theyknow your password.Note: Single sign-on (SSO) is a property of identity and access management that enables users to securelyauthenticate 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 atrusted third party to verify that users are who they say they are.

NEW QUESTION 89
- (Exam Topic 1)
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: B

NEW QUESTION 92
- (Exam Topic 1)
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:
Reference: https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_oveviw.html

NEW QUESTION 93
- (Exam Topic 1)
When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

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

Answer: B

NEW QUESTION 97
- (Exam Topic 1)
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

NEW QUESTION 101
- (Exam Topic 1)
What are two rootkit types? (Choose two)

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

Answer: CD

Explanation:
The term 'rootkit' originally comes from the Unix world, where the word 'root' is used to describe a user with thehighest possible level of access privileges, similar to an 'Administrator' in Windows. The word 'kit' refers to thesoftware that grants root-level access to the machine. Put the two together and you get 'rootkit', a program thatgives 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

NEW QUESTION 104
- (Exam Topic 1)
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

NEW QUESTION 107
- (Exam Topic 1)
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.

NEW QUESTION 111
- (Exam Topic 1)
Which RADIUS attribute can you use to filter MAB requests in an 802.1 x deployment?

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

Answer: C

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

NEW QUESTION 113
- (Exam Topic 1)
Which deployment model is the most secure when considering risks to cloud adoption?

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

Answer: D

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

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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

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

response_json = response.json()

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

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

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

Answer: D

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

NEW QUESTION 120

- (Exam Topic 1)
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

NEW QUESTION 123
- (Exam Topic 1)
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

NEW QUESTION 126
- (Exam Topic 1)
Which two characteristics of messenger protocols make data exfiltration difficult to detect and prevent? (Choose two)

A. Outgoing traffic is allowed so users can communicate with outside organizations.
B. Malware infects the messenger application on the user endpoint to send company data.
C. Traffic is encrypted, which prevents visibility on firewalls and IPS systems.
D. An exposed API for the messaging platform is used to send large amounts of data.
E. Messenger applications cannot be segmented with standard network controls

Answer: CE

NEW QUESTION 129
- (Exam Topic 1)
Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

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

Answer: D

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

NEW QUESTION 132
- (Exam Topic 1)
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

NEW QUESTION 137
- (Exam Topic 1)
Which two fields are defined in the NetFlow flow? (Choose two)

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

Answer: AD

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

NEW QUESTION 139
- (Exam Topic 1)
What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services? (Choose two)

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

Answer: BD

NEW QUESTION 143
- (Exam Topic 1)
An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA. Which Cisco ASA command must be used?

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

Answer: A

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

NEW QUESTION 145
- (Exam Topic 1)
What must be used to share data between multiple security products?

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

Answer: B

NEW QUESTION 148
- (Exam Topic 1)
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

NEW QUESTION 152
- (Exam Topic 1)
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: BE

NEW QUESTION 157
- (Exam Topic 1)
Refer to the exhibit.

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

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-c 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

NEW QUESTION 158
- (Exam Topic 1)
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.

NEW QUESTION 162
- (Exam Topic 1)
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: DE

NEW QUESTION 163
- (Exam Topic 1)
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

NEW QUESTION 164
- (Exam Topic 1)
Which benefit does endpoint security provide the overall security posture of an organization?

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

Answer: D

NEW QUESTION 166
- (Exam Topic 1)
Which functions of an SDN architecture require southbound APIs to enable communication?

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

Answer: A

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

NEW QUESTION 168
- (Exam Topic 1)
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: CD

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/firewall/asa-firewall-asdm/modules-sfr.html

NEW QUESTION 171
- (Exam Topic 1)
Which SNMPv3 configuration must be used to support the strongest security possible?

A. asa-host(config)#snmp-server group myv3 v3 privasa-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 noauthasa-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 noauthasa-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 privasa-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

NEW QUESTION 174
- (Exam Topic 1)
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:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesign

NEW QUESTION 177
- (Exam Topic 1)
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:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.h 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.

NEW QUESTION 181
- (Exam Topic 1)
Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?

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

Answer: B

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

NEW QUESTION 183
- (Exam Topic 1)
Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

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

Answer: D

NEW QUESTION 186
- (Exam Topic 1)
Which IPS engine detects ARP spoofing?

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

Answer: A

NEW QUESTION 188
- (Exam Topic 1)
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

NEW QUESTION 193
- (Exam Topic 1)

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

A. cross-site scripting
B. water holing
C. DDoS
D. buffer overflow

Answer: D

Explanation:

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

NEW QUESTION 196
- (Exam Topic 1)
What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?

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

Answer: A

Explanation:

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

NEW QUESTION 198
- (Exam Topic 1)
Which command enables 802.1X globally on a Cisco switch?

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

Answer: A

NEW QUESTION 200
- (Exam Topic 1)
Which two behavioral patterns characterize a ping of death attack? (Choose two)

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

Answer: BD

Explanation:
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 documentedLike other large but well-formed packets, a ping of death is fragmented into groups of 8 octets beforetransmission. 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.

NEW QUESTION 205
- (Exam Topic 1)
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

NEW QUESTION 210
- (Exam Topic 1)
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: AB

NEW QUESTION 214
- (Exam Topic 1)
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

NEW QUESTION 218
- (Exam Topic 1)
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

NEW QUESTION 223
- (Exam Topic 1)
How is Cisco Umbrella configured to log only security events?

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

Answer: A

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

NEW QUESTION 226
- (Exam Topic 1)
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

NEW QUESTION 227
- (Exam Topic 1)
Which API is used for Content Security?

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

Answer: D

NEW QUESTION 231
- (Exam Topic 1)
What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?

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

Answer:

A

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

NEW QUESTION 235
- (Exam Topic 1)
Which type of attack is social engineering?

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

Answer: B

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

NEW QUESTION 240
- (Exam Topic 1)
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

NEW QUESTION 245
- (Exam Topic 1)
Which two capabilities does TAXII support? (Choose two)

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

Answer: AB

Explanation:
The Trusted Automated eXchangeof Indicator Information (TAXII) specifies mechanisms for exchangingstructured 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 capabilitiesthat 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.

NEW QUESTION 246
- (Exam Topic 1)
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.

NEW QUESTION 250
- (Exam Topic 1)
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

NEW QUESTION 254
- (Exam Topic 1)
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 credentialsleaks, unauthorized access, data theft and DDoS attacks.

NEW QUESTION 258
- (Exam Topic 1)
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

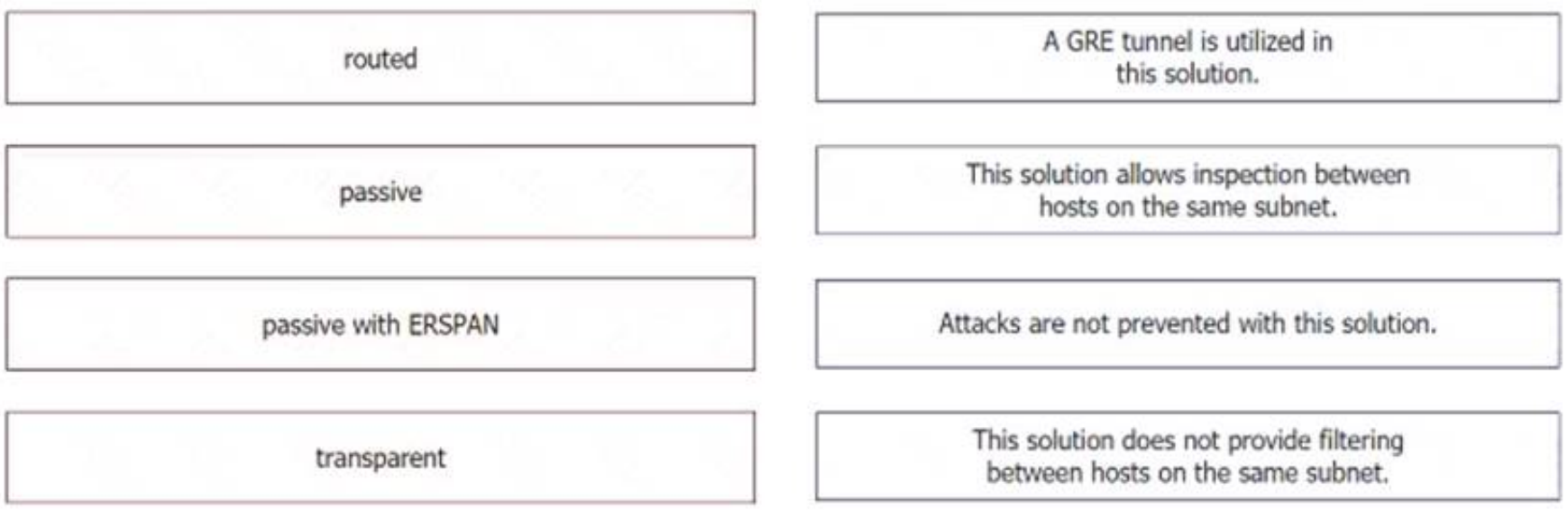
Explanation:
Reference: https://docs.umbrella.com/deployment-umbrella/docs/working-with-destination-lists

NEW QUESTION 262
- (Exam Topic 3)
Which command is used to log all events to a destination colector 209.165.201.107?

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

Answer: C

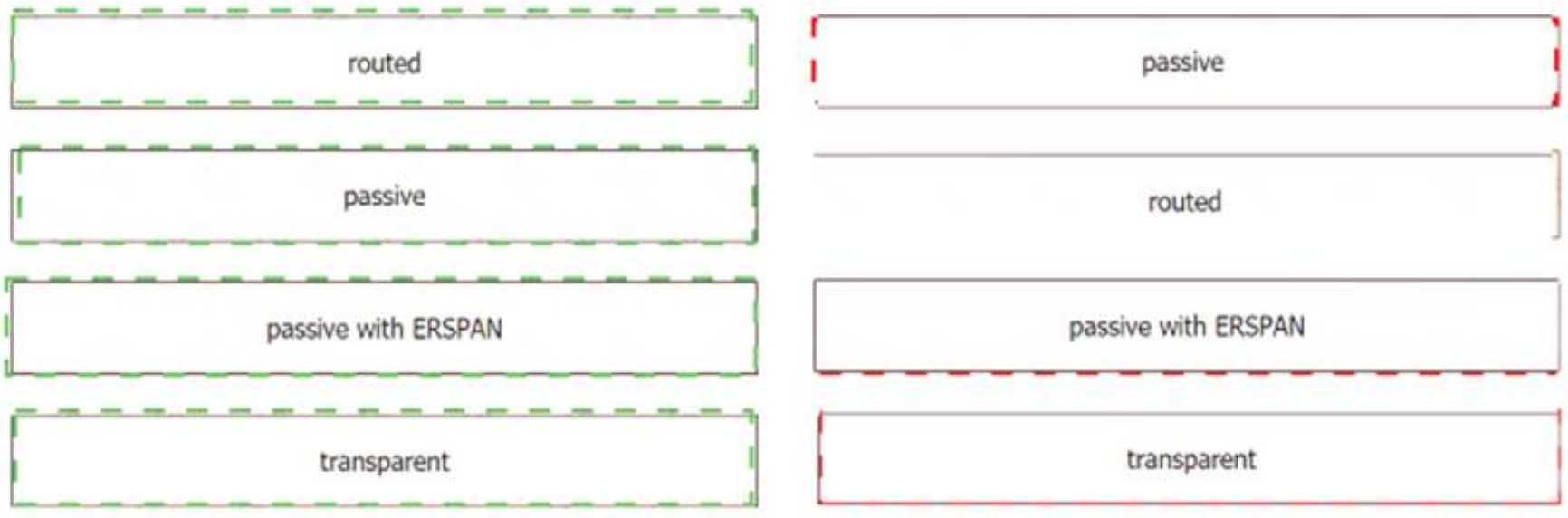
NEW QUESTION 265
- (Exam Topic 3)
Drag and drop the deployment models from the left onto the explanations on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 267
- (Exam Topic 3)
Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)

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

Answer: AB

NEW QUESTION 270
- (Exam Topic 3)
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

NEW QUESTION 275
- (Exam Topic 3)
Which algorithm is an NGE hash function?

A. HMAC
B. SHA-1
C. MD5
D. SISHA-2

Answer: D

NEW QUESTION 278
- (Exam Topic 3)
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

NEW QUESTION 280
- (Exam Topic 3)
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

NEW QUESTION 285
- (Exam Topic 3)

Refer to the exhibit,

```
*Jul  1 15:33:50.027: ISAKMP: (0):Enqueued KEY_MGR_SESSION_CLOSED for Tunnel0 deletion
*Jul  1 15:33:50.027: ISAKMP: (0):Deleting peer node by peer_reap for 2.2.2.2: D1250B0
*Jul  1 15:33:50.029: ISAKMP: (1001):peer does not do paranoid keepalives.
*Jul  1 15:33:54.781: ISAKMP-PAK: (0):received packet from 2.2.2.2 dport 500 sport 500 Global (N) NEW SA
*Jul  1 15:33:54.781: ISAKMP: (0):Created a peer struct for 2.2.2.2, peer port 500
*Jul  1 15:33:54.781: ISAKMP: (0):New peer created peer = 0x11026528 peer_handle = 0x80000004
*Jul  1 15:33:54.781: ISAKMP: (0):Locking peer struct 0x11026528, refcount 1 for crypto_isakmp_process_block
*Jul  1 15:33:54.782: ISAKMP: (0):local port 500, remote port 500
*Jul  1 15:33:54.782: ISAKMP: (0):Find a dup sa in the avl tree during calling isadb_insert sa = 104E3C68
*Jul  1 15:33:54.782: ISAKMP: (0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jul  1 15:33:54.782: ISAKMP: (0):Old State = IKE_READY  New State = IKE_R_MM1
```

which command results in these messages when attempting to troubleshoot an iPsec VPN connection?

A. debug crypto isakmp
B. debug crypto ipsec endpoint
C. debug crypto Ipsec
D. debug crypto isakmp connection

Answer: A

NEW QUESTION 289
- (Exam Topic 3)
Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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

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

Answer: D

NEW QUESTION 294
- (Exam Topic 3)
A customer has various external HTTP resources available including Intranet. Extranet, and Internet, with a proxy configuration running in explicit mode Which method allows the client desktop browsers to be configured to select when to connect direct or when to use the proxy?

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

Answer: C

NEW QUESTION 295
- (Exam Topic 3)
An engineer is configuring Cisco Umbrella and has an identity that references two different policies. Which action ensures that the policy that the identity must use takes precedence over the second one?

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

Answer: D

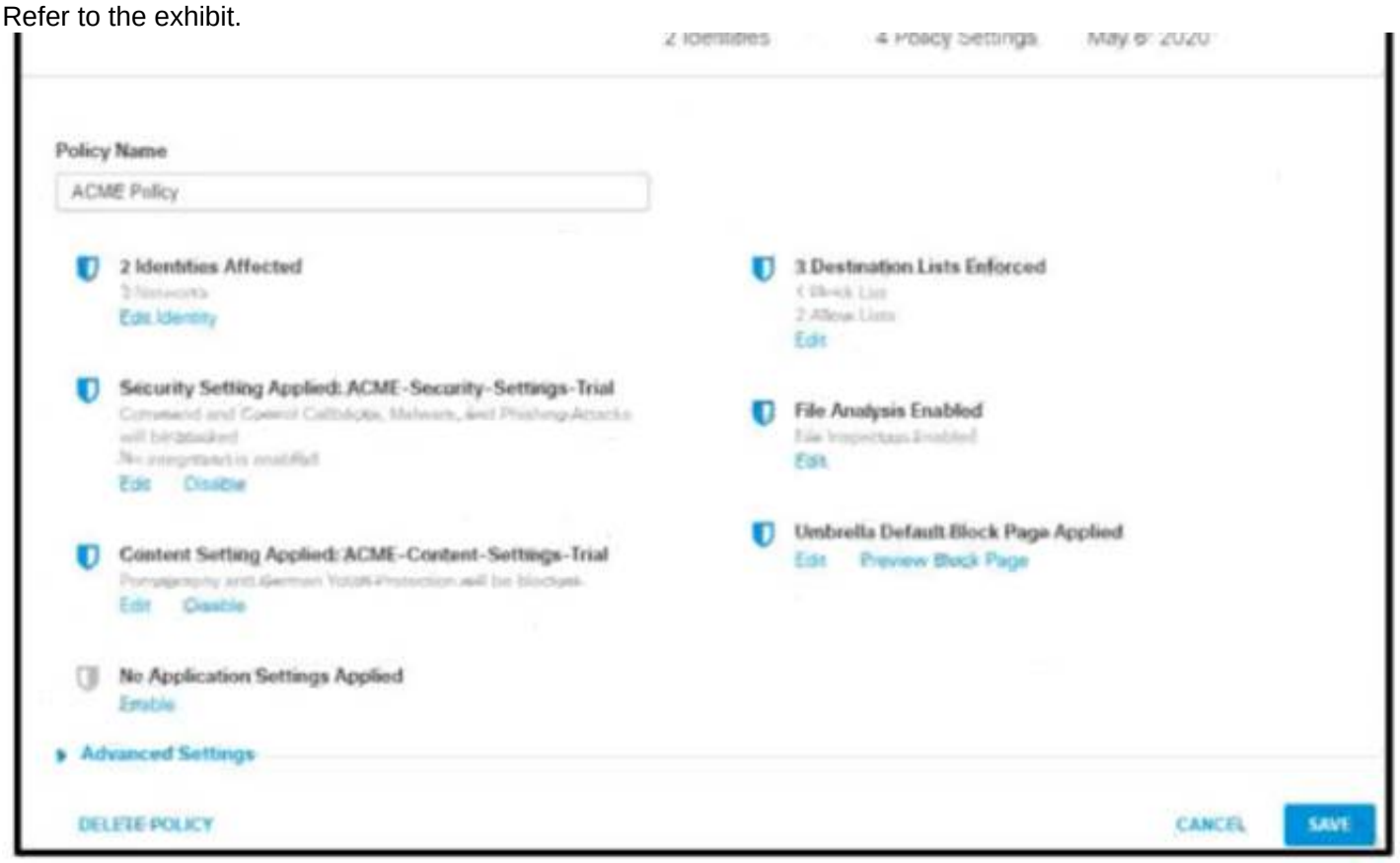
NEW QUESTION 298
- (Exam Topic 3)
When a transparent authentication fails on the Web Security Appliance, which type of access does the end user get?

A. guest

B. limited Internet
C. blocked
D. full Internet

Answer: C

NEW QUESTION 303
- (Exam Topic 3)
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

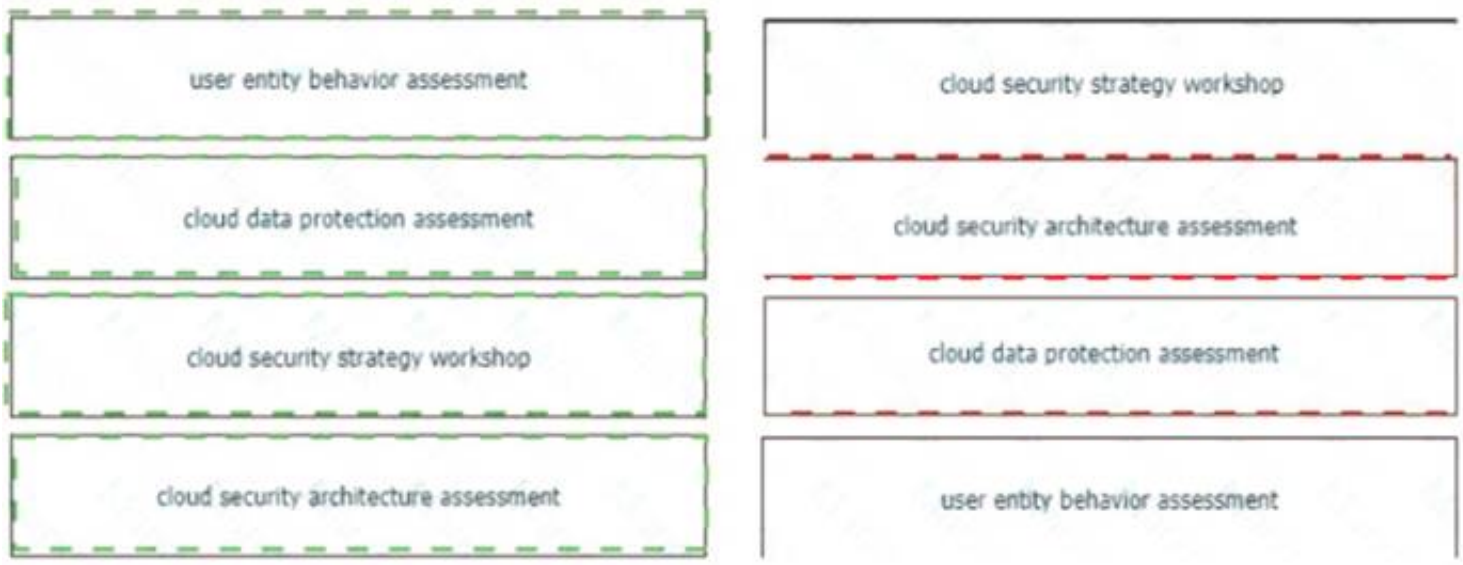
NEW QUESTION 307
- (Exam Topic 3)
Drag and drop the cloud security assessment components from the left onto the definitions on the right.

user entity behavior assessment	develop a cloud security strategy and roadmap aligned to business priorities
cloud data protection assessment	identify strengths and areas for improvement in the current security architecture during onboarding
cloud security strategy workshop	understand the security posture of the data or activity taking place in public cloud deployments
cloud security architecture assessment	detect potential anomalies in user behavior that suggest malicious behavior in a Software-as-a-Service application

A. Mastered
B. Not Mastered

Answer: A

Explanation:

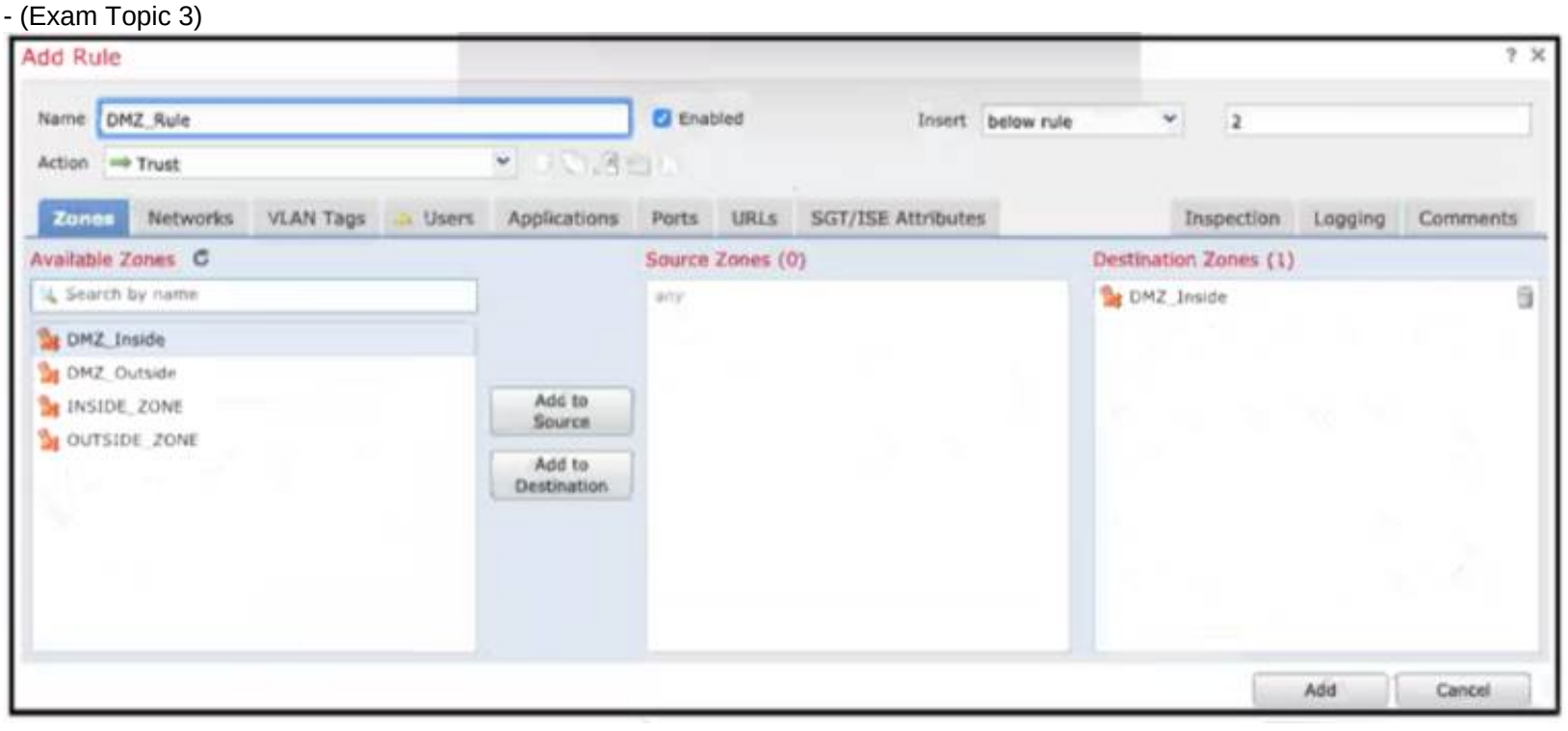


NEW QUESTION 308
- (Exam Topic 3)
Which two capabilities does an MDM provide? (Choose two.)

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: BC

NEW QUESTION 313
- (Exam Topic 3)



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

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

Answer: A

NEW QUESTION 314
- (Exam Topic 3)
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

NEW QUESTION 316
- (Exam Topic 3)
An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices. The default management port conflicts with other communications on the network and must be changed. What must be done to ensure that all devices can communicate together?

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

Answer: A

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

NEW QUESTION 319
- (Exam Topic 3)
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

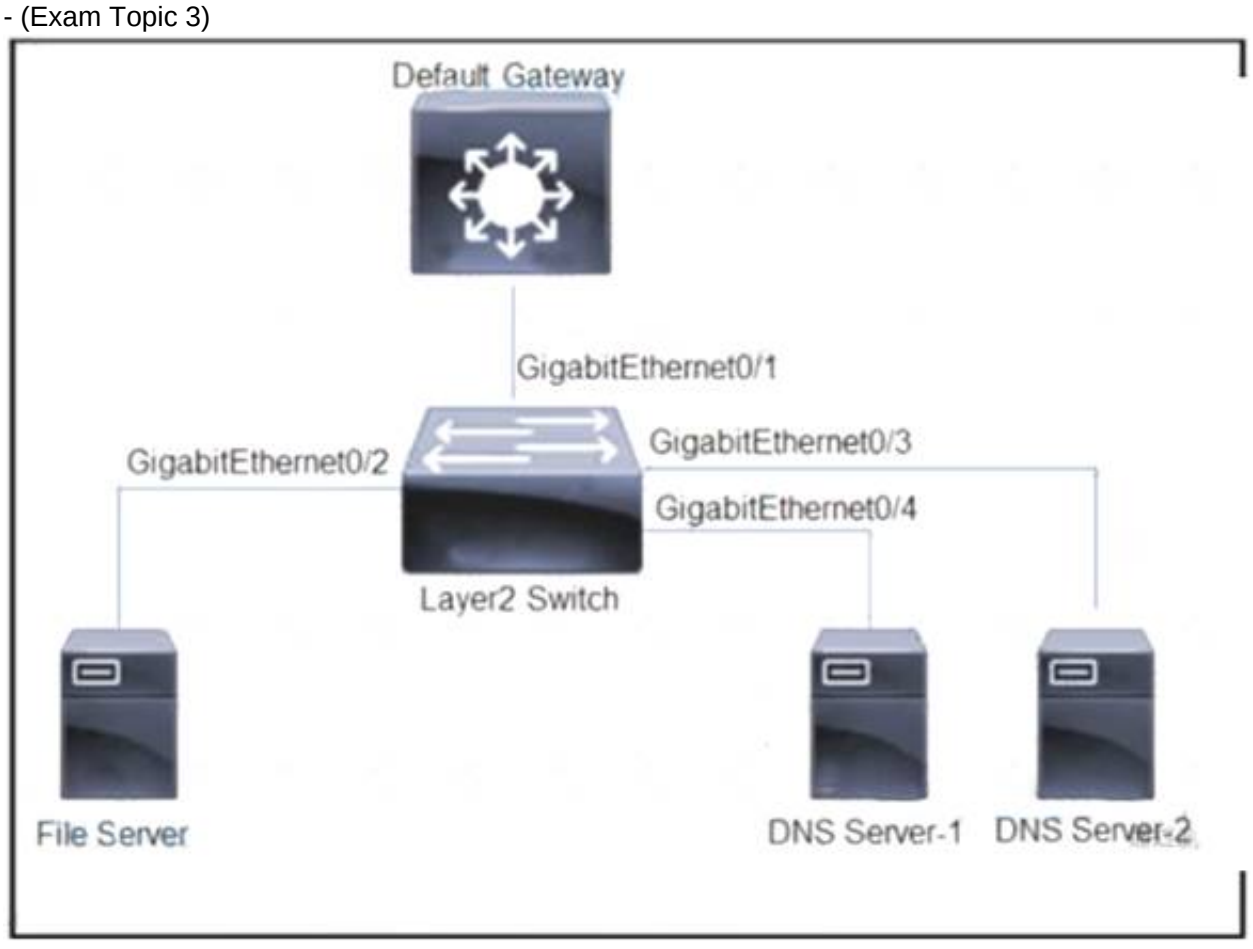
Answer: A

NEW QUESTION 320
- (Exam Topic 3)
Which ESA implementation method segregates inbound and outbound email?

A. one listener on a single physical Interface
B. pair of logical listeners on a single physical interface with two unique logical IPv4 addresses and one IPv6 address
C. pair of logical IPv4 listeners and a pair Of IPv6 listeners on two physically separate interfaces
D. one listener on one logical IPv4 address on a single logical interface

Answer: D

NEW QUESTION 323
- (Exam Topic 3)



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 all servers must communicate with default gateway multilayer switch. Which type of private VLAN ports should be configured to prevent communication between DNS servers and the file server?

A. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as isolated port, and GigabitEthernet0/3 and GigabitEthernet0/4 as promiscuous ports.
B. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as promiscuous port, Gigabit Ethernet0/3 and GigabitEthernet0/4 as isolated ports
C. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as isolated port and GigabitEthernet0/3 and GrgabitEthernet0/4 as community ports
D. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as community port, and GigabitEthernet0/3 and GrgabitEthernet0/4 as isolated ports.

Answer: C

NEW QUESTION 325

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

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

Answer: BC

NEW QUESTION 327
- (Exam Topic 3)
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

NEW QUESTION 329
- (Exam Topic 3)
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

NEW QUESTION 333
- (Exam Topic 3)
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: AB

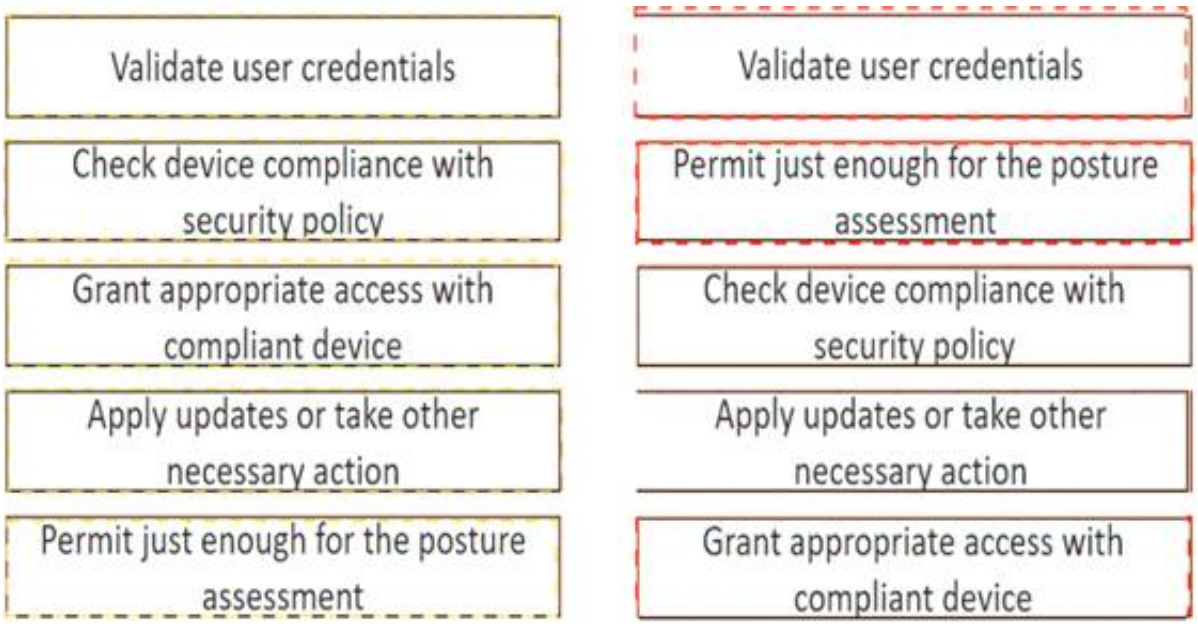
NEW QUESTION 335
- (Exam Topic 3)
Drag and drop the posture assessment flow actions from the left into a sequence on the right.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 339
- (Exam Topic 3)
An engineer is adding a Cisco DUO solution to the current TACACS+ deployment using Cisco ISE. The engineer wants to authenticate users using their account when they log into network devices. Which action accomplishes this task?

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

Answer: B

NEW QUESTION 342
- (Exam Topic 3)
Which solution supports high availability in routed or transparent mode as well as in northbound and southbound deployments?

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

Answer: B

NEW QUESTION 344
- (Exam Topic 3)
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

NEW QUESTION 346
- (Exam Topic 3)
Which Cisco security solution stops exfiltration using HTTPS?

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

Answer: C

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

NEW QUESTION 351
- (Exam Topic 3)
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 an 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.

NEW QUESTION 352
- (Exam Topic 3)
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: C

Explanation:
Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or microsegmented (uSeg) EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another.

NEW QUESTION 357
- (Exam Topic 3)
Which type of data exfiltration technique encodes data in outbound DNS requests to specific servers and can be stopped by Cisco Umbrella?

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

Answer: A

NEW QUESTION 358
- (Exam Topic 3)
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

NEW QUESTION 360
- (Exam Topic 3)
Which DevSecOps implementation process gives a weekly or daily update instead of monthly or quarterly in the applications?

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

Answer: B

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

NEW QUESTION 363
- (Exam Topic 3)
What is an advantage of the Cisco Umbrella roaming client?

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

Answer: C

NEW QUESTION 365
- (Exam Topic 3)
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: A

NEW QUESTION 368
- (Exam Topic 3)
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

NEW QUESTION 369
- (Exam Topic 3)
Refer to the exhibit.

```
ASA#  show  service-policy sfr

Global policy:
  Service-policy:  global_policy
    Class-map:  SFR
      SFR:  card status Up,  mode fail-open monitor-only
        Packet input 0, packet output [redacted]  drop 0,  reset-drop 0
```

What are two indications of the Cisco Firepower Services Module configuration? (Choose two.)

A. The module is operating in IDS mode.
B. Traffic is blocked if the module fails.
C. The module fails to receive redirected traffic.
D. The module is operating in IPS mode.
E. Traffic continues to flow if the module fails.

Answer: AE

Explanation:
sfr {fail-open | fail-close [monitor-only]} <- There's a couple different options here. The first one is fail-open which means that if the Firepower software module is unavailable, the ASA will continue to forward traffic. fail-close means that if the Firepower module fails, the traffic will stop flowing. While this doesn't seem ideal, there might be a use case for it when securing highly regulated environments. The monitor-only switch can be used with both and basically puts the Firepower services into IDS-mode only. This might be useful for initial testing or setup.

NEW QUESTION 373
- (Exam Topic 3)
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

NEW QUESTION 375
- (Exam Topic 3)
When MAB is configured for use within the 802.1X environment, an administrator must create a policy that allows the devices onto the network. Which information is used for the username and password?

A. The MAB uses the IP address as username and password.
B. The MAB uses the call-station-ID as username and password.
C. Each device must be set manually by the administrator.
D. The MAB uses the MAC address as username and password.

Answer: D

NEW QUESTION 380
- (Exam Topic 3)
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: BC

NEW QUESTION 382
- (Exam Topic 3)
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

NEW QUESTION 384
- (Exam Topic 3)
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: A

NEW QUESTION 388
- (Exam Topic 3)
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

NEW QUESTION 393
- (Exam Topic 3)
Drag and drop the exploits from the left onto the type of security vulnerability on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 394
- (Exam Topic 3)
What is the purpose of the Cisco Endpoint loC feature?

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

Answer: C

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

NEW QUESTION 398
- (Exam Topic 3)
An engineer must configure Cisco AMP for Endpoints so that it contains a list of files that should not be executed by users. These files must not be quarantined.
Which action meets this configuration requirement?

A. Identity the network IPs and place them in a blocked list.
B. Modify the advanced custom detection list to include these files.
C. Create an application control blocked applications list.
D. Add a list for simple custom detection.

Answer: C

NEW QUESTION 403
- (Exam Topic 3)
What is a difference between a DoS attack and a DDoS attack?

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

Answer: A

NEW QUESTION 405
- (Exam Topic 3)
An engineer needs to add protection for data in transit and have headers in the email message Which
configuration is needed to accomplish this goal?

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

Answer: D

NEW QUESTION 406
- (Exam Topic 3)
Which VMware platform does Cisco ACI integrate with to provide enhanced visibility, provide policy integration and deployment, and implement security policies with access lists?

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

Answer: B

NEW QUESTION 410
- (Exam Topic 3)
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

NEW QUESTION 414
- (Exam Topic 3)
Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

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

Answer: D

NEW QUESTION 415
- (Exam Topic 3)
Which API method and required attribute are used to add a device into Cisco DNA Center with the native API?

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

Answer: A

NEW QUESTION 419
- (Exam Topic 3)
What are two workloaded security models? (Choose two)

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

Answer: CD

NEW QUESTION 424
- (Exam Topic 3)
What is a benefit of flexible NetFlow records?

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

Answer: D

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

NEW QUESTION 425
- (Exam Topic 3)
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 (ISE)
B. Cisco Enterprise Security Appliance (ESA)
C. Cisco Web Security Appliance (WSA)
D. Cisco Advanced Stealthwatch Appliance (ASA)

Answer:

C

NEW QUESTION 426
- (Exam Topic 3)
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: B

NEW QUESTION 427
- (Exam Topic 3)
With regard to RFC 5176 compliance, how many IETF attributes are supported by the RADIUS CoA feature?

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

Answer: D

NEW QUESTION 430
- (Exam Topic 3)
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 Compliance Solution

Answer: D

NEW QUESTION 433
- (Exam Topic 3)
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: BE

NEW QUESTION 438
- (Exam Topic 3)
What is the most commonly used protocol for network telemetry?

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

Answer: D

NEW QUESTION 443
- (Exam Topic 3)
An engineer musí set up 200 new laptops on a network and wants to prevent the users from moving their laptops around to simplify administration Which switch port MAC address security setting must be used?

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

Answer: A

NEW QUESTION 448
- (Exam Topic 3)
For a given policy in Cisco Umbrella, how should a customer block website based on a custom list?

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

Answer: C

NEW QUESTION 449
- (Exam Topic 3)
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

NEW QUESTION 451
- (Exam Topic 3)
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

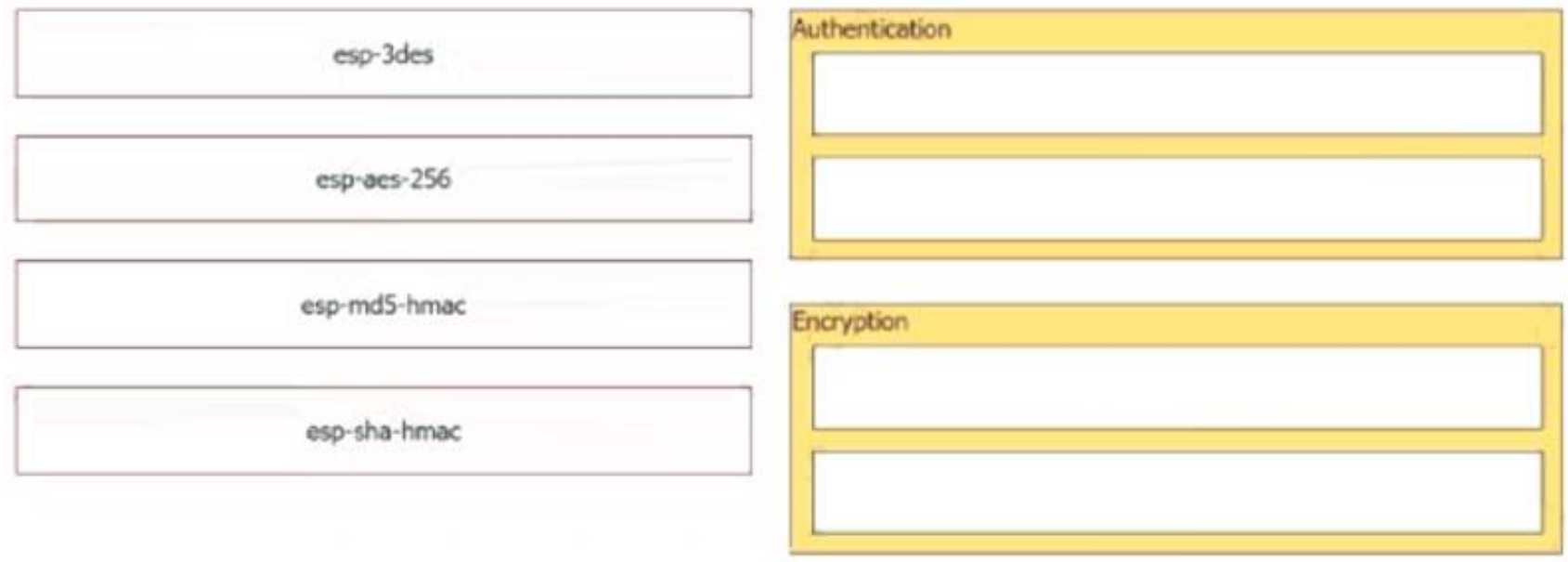
Answer: C

NEW QUESTION 452
- (Exam Topic 3)
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: D

NEW QUESTION 456
- (Exam Topic 3)
Drag and drop the cryptographic algorithms for IPsec from the left onto the cryptographic processes on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 459
- (Exam Topic 3)
A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to
ensure that bandwidth is available for VPN users needing access to corporate resources on the10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the
network?

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

Answer: A

NEW QUESTION 463
- (Exam Topic 3)
A university policy must allow open access to resources on the Internet for research, but internal workstations are exposed to malware. Which Cisco AMP feature allows the engineering team to determine whether a file is installed on a selected few workstations?

A. file prevalence
B. file discovery
C. file conviction
D. file manager

Answer: A

NEW QUESTION 464
- (Exam Topic 3)
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:
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

NEW QUESTION 466
- (Exam Topic 3)
Which two protocols must be configured to authenticate end users to the Cisco WSA? (Choose two.)

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

Answer: AD

NEW QUESTION 471
- (Exam Topic 3)
What is the purpose of the Cisco Endpoint IoC feature?

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

Answer: A

Explanation:
Reference: https://docs.amp.cisco.com/Cisco%20Endpoint%20IOC%20Attributes.pdf
The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

NEW QUESTION 476
- (Exam Topic 3)
What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?

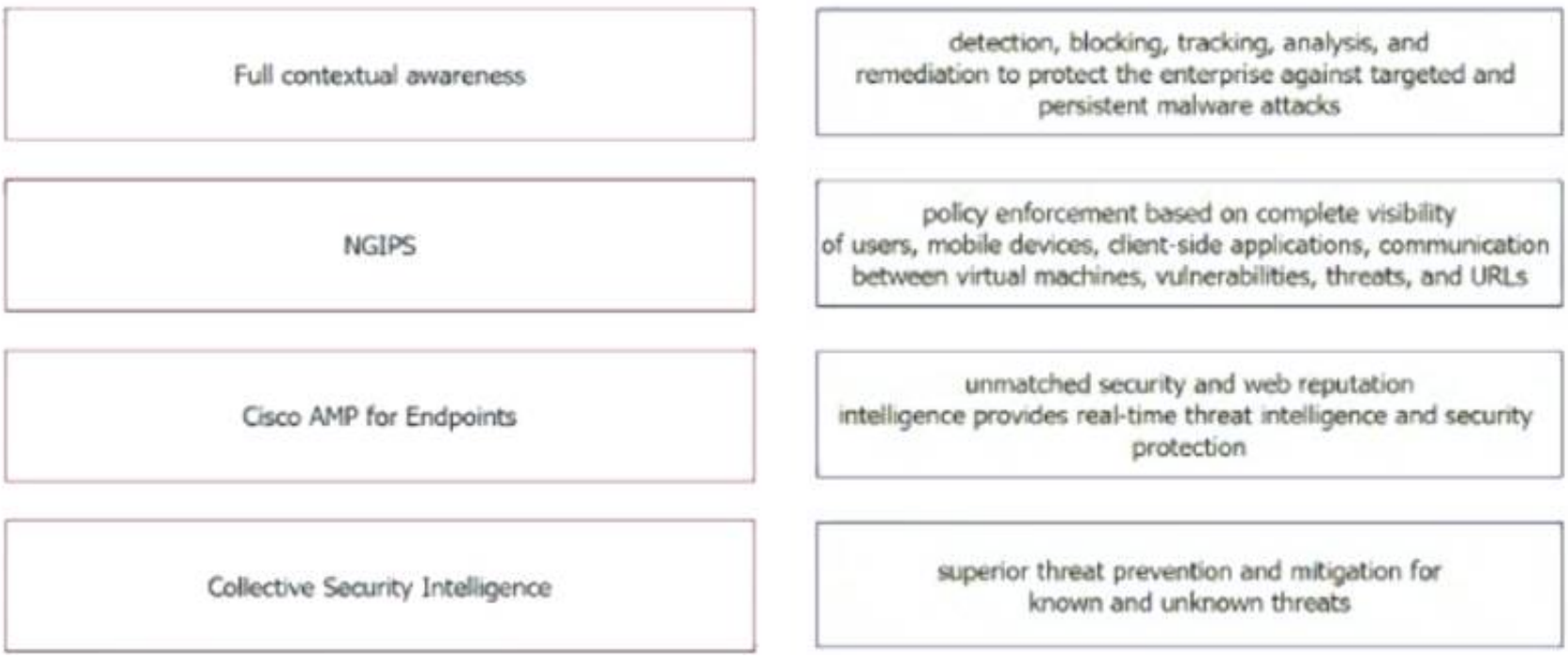
A. Telemetry uses a pull mehod, which makes it more reliable than SNMP
B. Telemetry uses push and pull, which makes it more scalable than SNMP
C. Telemetry uses push and pull which makes it more secure than SNMP
D. Telemetry uses a push method which makes it faster than SNMP

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

NEW QUESTION 480
- (Exam Topic 3)
Drag and drop the security solutions from the left onto the benefits they provide on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 483
- (Exam Topic 3)
Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using higher-level protocols without readdressing the network?

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

Answer: B

NEW QUESTION 485
- (Exam Topic 3)
An engineer is trying to decide whether to use Cisco Umbrella, Cisco CloudLock, Cisco Stealthwatch, or Cisco AppDynamics Cloud Monitoring for visibility into data transfers as well as protection against data exfiltration Which solution best meets these requirements?

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

Answer: D

NEW QUESTION 490
- (Exam Topic 3)
Which direction do attackers encode data in DNS requests during exfiltration using DNS tunneling?

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

Answer: D

NEW QUESTION 492
- (Exam Topic 3)
Which type of encryption uses a public key and private key?

A. Asymmetric
B. Symmetric
C. Linear

D. Nonlinear

Answer: A

NEW QUESTION 493
- (Exam Topic 3)
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: D

NEW QUESTION 497
- (Exam Topic 3)
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: CD

NEW QUESTION 501
- (Exam Topic 3)
A large organization wants to deploy a security appliance in the public cloud to form a site-to-site VPN and link the public cloud environment to the private cloud in the headquarters data center. Which Cisco security appliance meets these requirements?

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

Answer: B

NEW QUESTION 504
- (Exam Topic 3)
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:
Reference: https://cheapsslsecurity.com/blog/understanding-the-role-of-certificate-authorities-in-pki/

NEW QUESTION 507
- (Exam Topic 3)
A network engineer must monitor user and device behavior within the on-premises network. This data must be sent to the Cisco Stealthwatch Cloud analytics platform for analysis. What must be done to meet this
requirement using the Ubuntu-based VM appliance deployed in a VMware-based hypervisor?

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

Answer: B

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

NEW QUESTION 510
- (Exam Topic 3)
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: A

NEW QUESTION 512
- (Exam Topic 3)
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

NEW QUESTION 517
- (Exam Topic 3)
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

NEW QUESTION 522
- (Exam Topic 3)
Which threat intelligence standard contains malware hashes?

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

Answer: A

NEW QUESTION 526
- (Exam Topic 3)
Which type of data does the Cisco Stealthwatch system collect and analyze from routers, switches, and firewalls?

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

Answer: D

NEW QUESTION 529
- (Exam Topic 3)
Which encryption algorithm provides highly secure VPN communications?

A. 3DES
B. AES 256
C. AES 128
D. DES

Answer: B

NEW QUESTION 533
- (Exam Topic 3)
Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?

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

Answer: B

NEW QUESTION 538
- (Exam Topic 3)

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

NEW QUESTION 541
- (Exam Topic 3)
What are two functions of IKEv1 but not IKEv2? (Choose two)

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

Answer: CE

NEW QUESTION 542
- (Exam Topic 3)
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

NEW QUESTION 544
- (Exam Topic 3)
Which Cisco security solution secures public, private, hybrid, and community clouds?

A. Cisco ISE
B. Cisco ASAv
C. Cisco Cloudlock
D. Cisco pxGrid

Answer: C

NEW QUESTION 545
- (Exam Topic 3)
An organization is implementing AAA for their users. They need to ensure that authorization is verified for every command that is being entered by the network administrator. Which protocol must be configured in order to provide this capability?

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

Answer: D

NEW QUESTION 546
- (Exam Topic 3)
What are two workload security models? (Choose two.)

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

Answer: CD

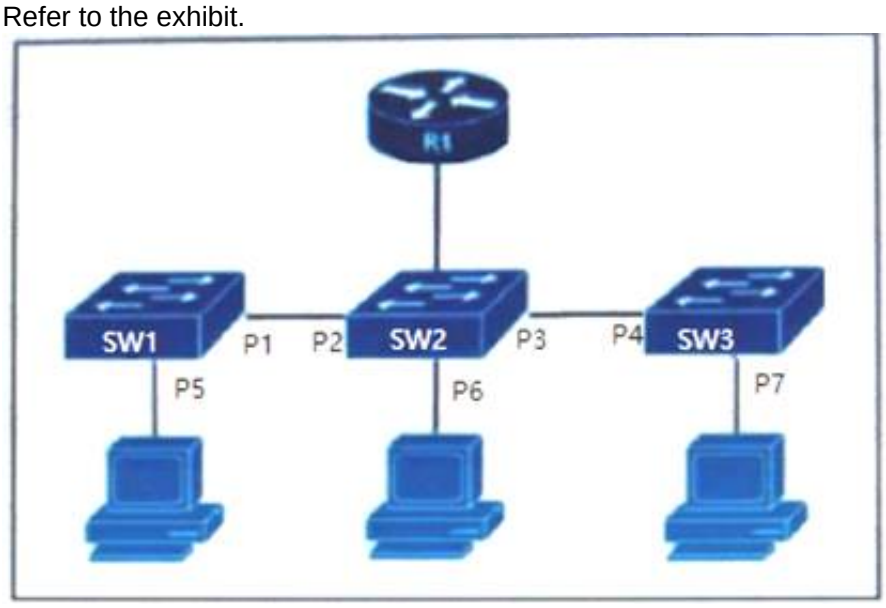
NEW QUESTION 551
- (Exam Topic 3)
An engineer needs to configure an access control policy rule to always send traffic for inspection without using the default action. Which action should be configured for this rule?

A. monitor
B. allow
C. block
D. trust

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/acce the first three access control rules in the policy—Monitor, Trust, and Block—cannot inspect matching
traffic. Monitor rules track and log but do not inspect network traffic, so the system continues to match traffic
against additional rules to determine whether to permit or deny it
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/acce

NEW QUESTION 553
- (Exam Topic 3)
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

NEW QUESTION 556
- (Exam Topic 3)
Which two capabilities of Integration APIs are utilized with Cisco DNA center? (Choose two)

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

Answer: BC

Explanation:
Reference:
https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/integration-api-westbound

NEW QUESTION 561
- (Exam Topic 3)
Which industry standard is used to integrate Cisco ISE and pxGrid to each other and with other interoperable security platforms?

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

Answer: B

NEW QUESTION 562
- (Exam Topic 3)
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

NEW QUESTION 567
- (Exam Topic 3)
An organization wants to secure data in a cloud environment. Its security model requires that all users be authenticated and authorized. Security configuration and posture must be continuously validated before access is granted or maintained to applications and data. There is also a need to allow certain application traffic and deny all other traffic by default. Which technology must be used to implement these requirements?

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

Answer: C

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

NEW QUESTION 570
- (Exam Topic 3)
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: CE

NEW QUESTION 572
- (Exam Topic 3)
What is a function of Cisco AMP for Endpoints?

A. It detects DNS attacks
B. It protects against web-based attacks
C. It blocks email-based attacks
D. It automates threat responses of an infected host

Answer: D

NEW QUESTION 575
- (Exam Topic 3)
What is an advantage of network telemetry over SNMP pulls?

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

Answer: D

NEW QUESTION 577
- (Exam Topic 3)
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

NEW QUESTION 579
- (Exam Topic 3)
What is the function of the crypto is a kmp key cisc406397954 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel?

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

Answer: B

NEW QUESTION 583

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

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

Answer: B

NEW QUESTION 584
- (Exam Topic 3)
A security engineer must add destinations into a destination list in Cisco Umbrella. What describes the application of these changes?

A. The changes are applied immediately it the destination list is part or a policy.
B. The destination list must be removed from the policy before changes are made to It.
C. The changes are applied only after the configuration is saved in Cisco Umbrella.
D. The user role of Block Page Bypass or higher is needed to perform these changes.

Answer: A

NEW QUESTION 587
- (Exam Topic 3)
Which kind of API that is used with Cisco DNA Center provisions SSIDs, QoS policies, and update software versions on switches?

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

Answer: B

NEW QUESTION 590
- (Exam Topic 3)
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: A

NEW QUESTION 591
- (Exam Topic 3)
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: CD

NEW QUESTION 593
- (Exam Topic 3)
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

NEW QUESTION 598
- (Exam Topic 3)
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

NEW QUESTION 603
- (Exam Topic 3)
What is a benefit of using a multifactor authentication strategy?

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

Answer: D

NEW QUESTION 606
- (Exam Topic 3)
An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices The default management port conflicts with other communications on the network and must be changed What must be done to ensure that all devices can communicate together?

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

Answer: D

NEW QUESTION 609
- (Exam Topic 3)
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-ACK

Answer: D

NEW QUESTION 610
- (Exam Topic 3)
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

NEW QUESTION 612
- (Exam Topic 3)
Which category includes DoS Attacks?

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

Answer: C

NEW QUESTION 617
- (Exam Topic 3)
What is a feature of NetFlow Secure Event Logging?

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

Answer: A

NEW QUESTION 620
- (Exam Topic 3)
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

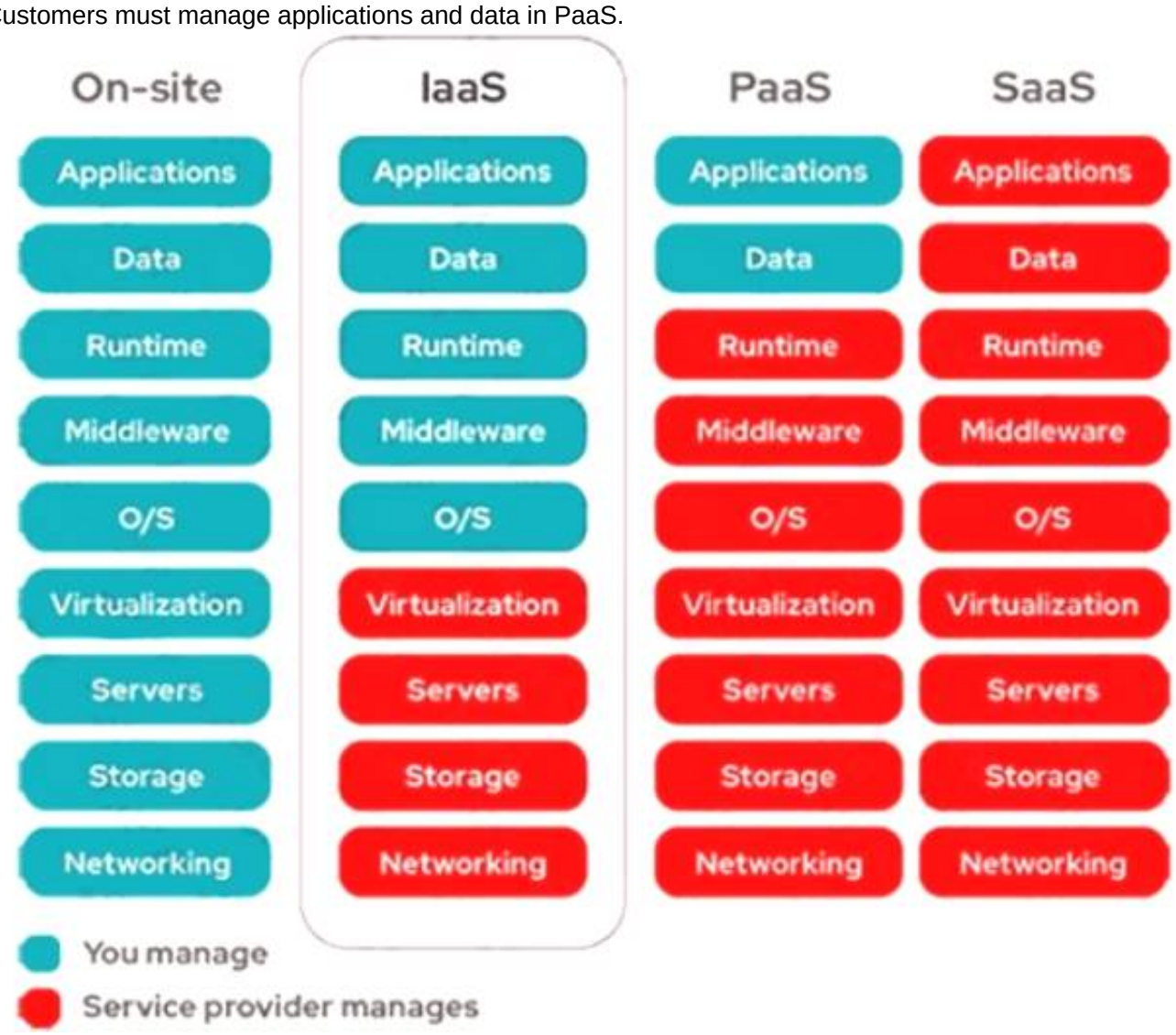
Answer: D

NEW QUESTION 625
- (Exam Topic 2)
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two)

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

Answer: DE

Explanation:
Customers must manage applications and data in PaaS.



NEW QUESTION 630
- (Exam Topic 2)
What is a prerequisite when integrating a Cisco ISE server and an AD domain?

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

Answer: D

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

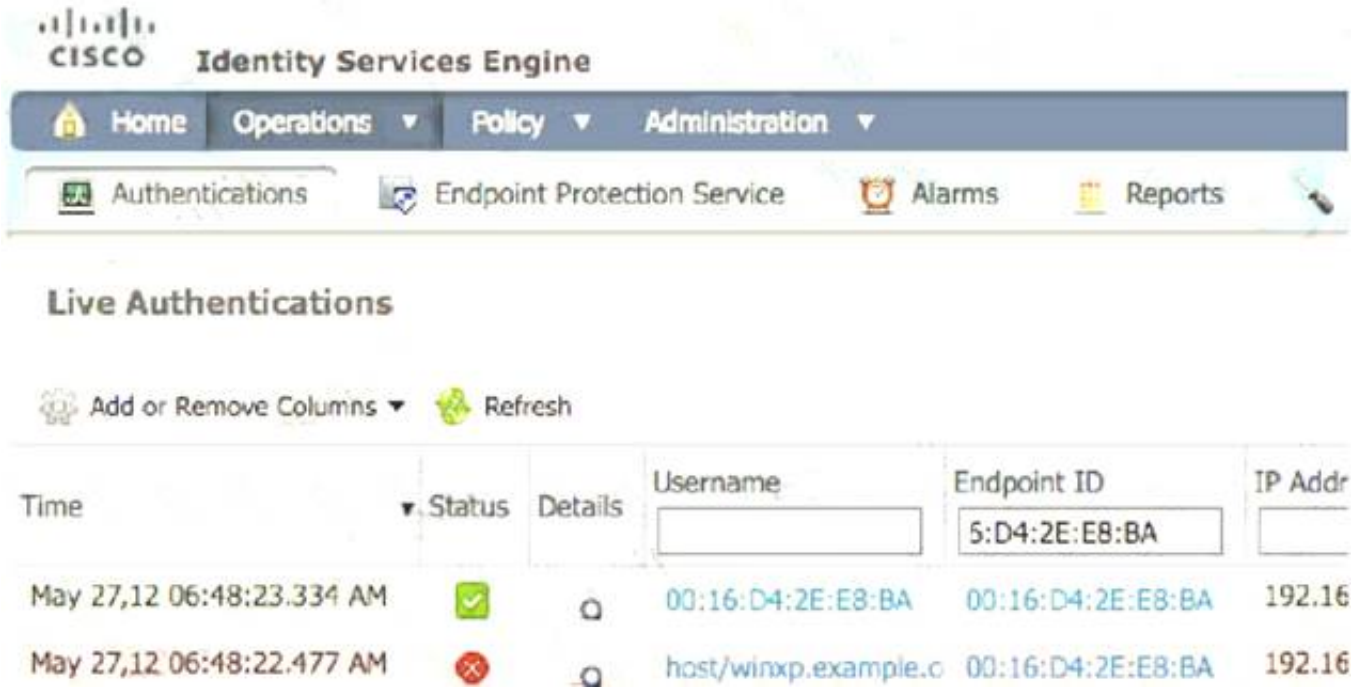
NEW QUESTION 631
- (Exam Topic 2)
A network administrator is configuring a switch to use Cisco ISE for 802.1X. An endpoint is failing authentication and is unable to access the network. Where should the administrator begin troubleshooting to verify the authentication details?

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 & AuthorizationsCheck the ISE Live LogsLogin 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 AuthenticationsCheck for Any Failed Authentication Attempts in the Log



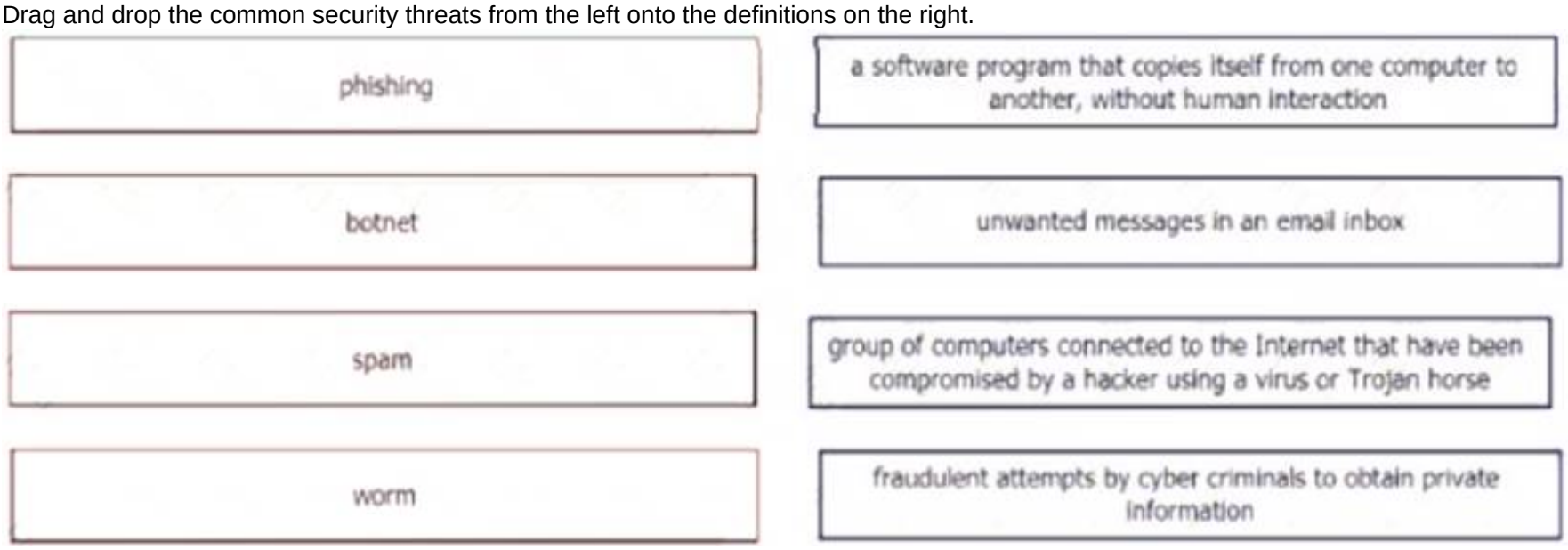
Reference:
https://community.cisco.com/t5/security-documents/how-to-troubleshoot-ise-failed-authenticationsamp/ta-p/363

NEW QUESTION 632
- (Exam Topic 2)
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

NEW QUESTION 636
- (Exam Topic 2)
Drag and drop the common security threats from the left onto the definitions on the right.



A. Mastered
B. Not Mastered

Answer: A

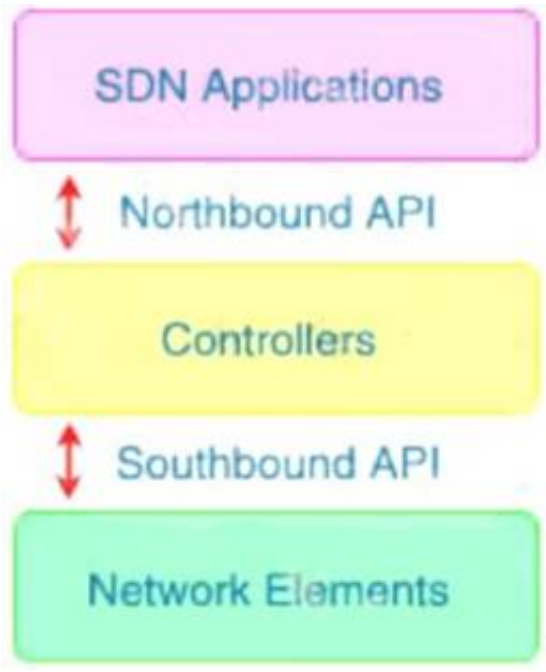
Explanation:
A picture containing application Description automatically generated

NEW QUESTION 641
- (Exam Topic 2)
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:



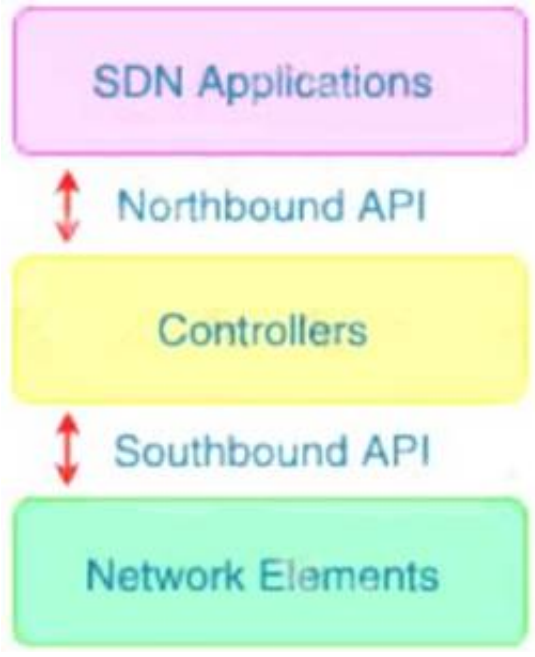
The Southbound API is used to communicate between Controllers and network devices.

NEW QUESTION 644
- (Exam Topic 2)
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 andscalability needs.



NEW QUESTION 646
- (Exam Topic 2)
How does DNS Tunneling exfiltrate data?

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

Answer: A

NEW QUESTION 649
- (Exam Topic 2)
Which attack type attempts to shut down a machine or network so that users are not able to access it?

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

Answer: A

Explanation:
Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to itsintended users.The Smurf attack is a DDoS attack in which

large numbers of Internet Control Message Protocol (ICMP)packets with the intended victim's spoofed source IP are broadcast to a computer network using an IPbroadcast address.

NEW QUESTION 651
- (Exam Topic 2)
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

NEW QUESTION 655
- (Exam Topic 2)
Which type of API is being used when a security application notifies a controller within a software-defined network architecture about a specific security threat?

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

Answer: C

NEW QUESTION 659
- (Exam Topic 2)
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.

NEW QUESTION 664
- (Exam Topic 2)
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: DE

NEW QUESTION 669
- (Exam Topic 2)
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated

NEW QUESTION 673
- (Exam Topic 2)
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:
Reference:
https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45-738565.pdf

NEW QUESTION 675
- (Exam Topic 2)
An engineer is implementing NTP authentication within their network and has configured both the client and server devices with the command ntp authentication-key 1 md5 Cisc392368270. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however it is unable to do so. Which command is required to enable the client to accept the server's authentication key?

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

Answer: B

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

NEW QUESTION 680
- (Exam Topic 2)
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 virtualmachines, 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.

NEW QUESTION 685
- (Exam Topic 2)
Which type of protection encrypts RSA keys when they are exported and imported?

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

Answer: B

NEW QUESTION 688
- (Exam Topic 2)
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

NEW QUESTION 690
- (Exam Topic 2)
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

NEW QUESTION 694
- (Exam Topic 2)
Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?

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

Answer: B

NEW QUESTION 699
- (Exam Topic 2)
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 thatdetermines 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.

NEW QUESTION 702
- (Exam Topic 2)
Which Dos attack uses fragmented packets to crash a target machine?

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

Answer: C

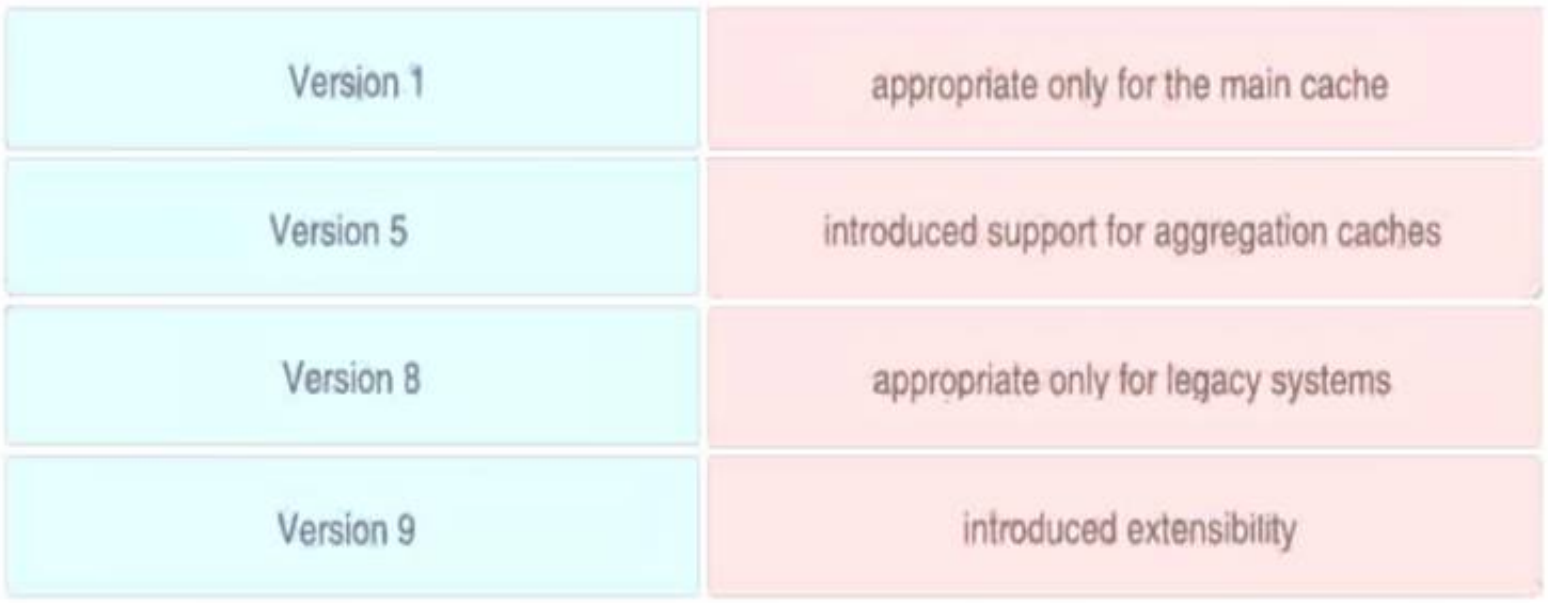
Explanation:
A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a targetmachine. Since the machine receiving such packets cannot reassemble them due
to a bug in TCP/IPfragmentation reassembly, the packets overlap one another, crashing the target network 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.

NEW QUESTION 705
- (Exam Topic 2)
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

NEW QUESTION 706
- (Exam Topic 2)
Drag and drop the NetFlow export formats from the left onto the descriptions on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgnflow-data-e

NEW QUESTION 711
- (Exam Topic 2)
A user has a device in the network that is receiving too many connection requests from multiple machines. Which type of attack is the device undergoing?

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

Answer: D

NEW QUESTION 713
- (Exam Topic 2)
A Cisco ESA administrator has been tasked with configuring the Cisco ESA to ensure there are no viruses before quarantined emails are delivered. In addition, delivery of mail from known bad mail servers must be prevented. Which two actions must be taken in order to meet these requirements? (Choose two)

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

Answer: AE

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

NEW QUESTION 715
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 350-701 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 350-701 Product From:

https://www.2passeasy.com/dumps/350-701/

Money Back Guarantee

350-701 Practice Exam Features:

* 350-701 Questions and Answers Updated Frequently

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

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

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