

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

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



NEW QUESTION 1

- (Exam Topic 3)

Drag and drop the Cisco CWS redirection options from the left onto the capabilities on the right.

Cisco AnyConnect client	location-independent, bandwidth-efficient option
ISR with CWS connector	extends identity information and on-premises features to the cloud
NGFW with CWS connector	provides user-group granularity and supports cloud-based scanning
WSAv with CWS connector	supports cached credentials and makes directory information available off-premises

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://www.westconcomstor.com/medias/CWS-data-sheet-c78-729637-1-.pdf?context=bWFzdGVyfHJvb3R8M>

NEW QUESTION 2

- (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 3

- (Exam Topic 3)

Which Cisco cloud security software centrally manages policies on multiple platforms such as Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS?

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

Answer: A

NEW QUESTION 4

- (Exam Topic 3)

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

- A. Cisco ASA because it enables URL filtering and blocks malicious URLs by default, whereas Cisco FTD does not
- B. Cisco ASA because it includes URL filtering in the access control policy capabilities, whereas Cisco FTD does not
- C. Cisco FTD because it includes URL filtering in the access control policy capabilities, whereas Cisco ASA does not
- D. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not

Answer: C

NEW QUESTION 5

- (Exam Topic 3)

What is a difference between GETVPN and IPsec?

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

Answer: C

NEW QUESTION 6

- (Exam Topic 3)

What is the purpose of the Cisco Endpoint IoC feature?

- A. It provides stealth threat prevention.
- B. It is a signature-based engine.
- C. It 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_Manageable_Protocol_Security_Architecture.pdf

NEW QUESTION 7

- (Exam Topic 3)

Which function is performed by certificate authorities but is a limitation of registration authorities?

- A. accepts enrollment requests
- B. certificate re-enrollment
- C. verifying user identity
- D. CRL publishing

Answer: C

NEW QUESTION 8

- (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 9

- (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. It 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 10

- (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. ???-???
- D. CoA-ACK

Answer: D

NEW QUESTION 10

- (Exam Topic 3)

What are two facts about WSA HTTP proxy configuration with a PAC file? (Choose two.)

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

Answer: CD

NEW QUESTION 13

- (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 Cisco FMC

- D. FMC
- E. Cisco Firepower NGFW Virtual appliance with Cisco FMC

Answer: B

NEW QUESTION 18

- (Exam Topic 3)

What is a benefit of using Cisco Umbrella?

- A. DNS queries are resolved faster.
- B. Attacks can be mitigated before the application connection occurs.
- C. Files are scanned for viruses before they are allowed to run.
- D. It prevents malicious inbound traffic.

Answer: B

NEW QUESTION 23

- (Exam Topic 3)

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

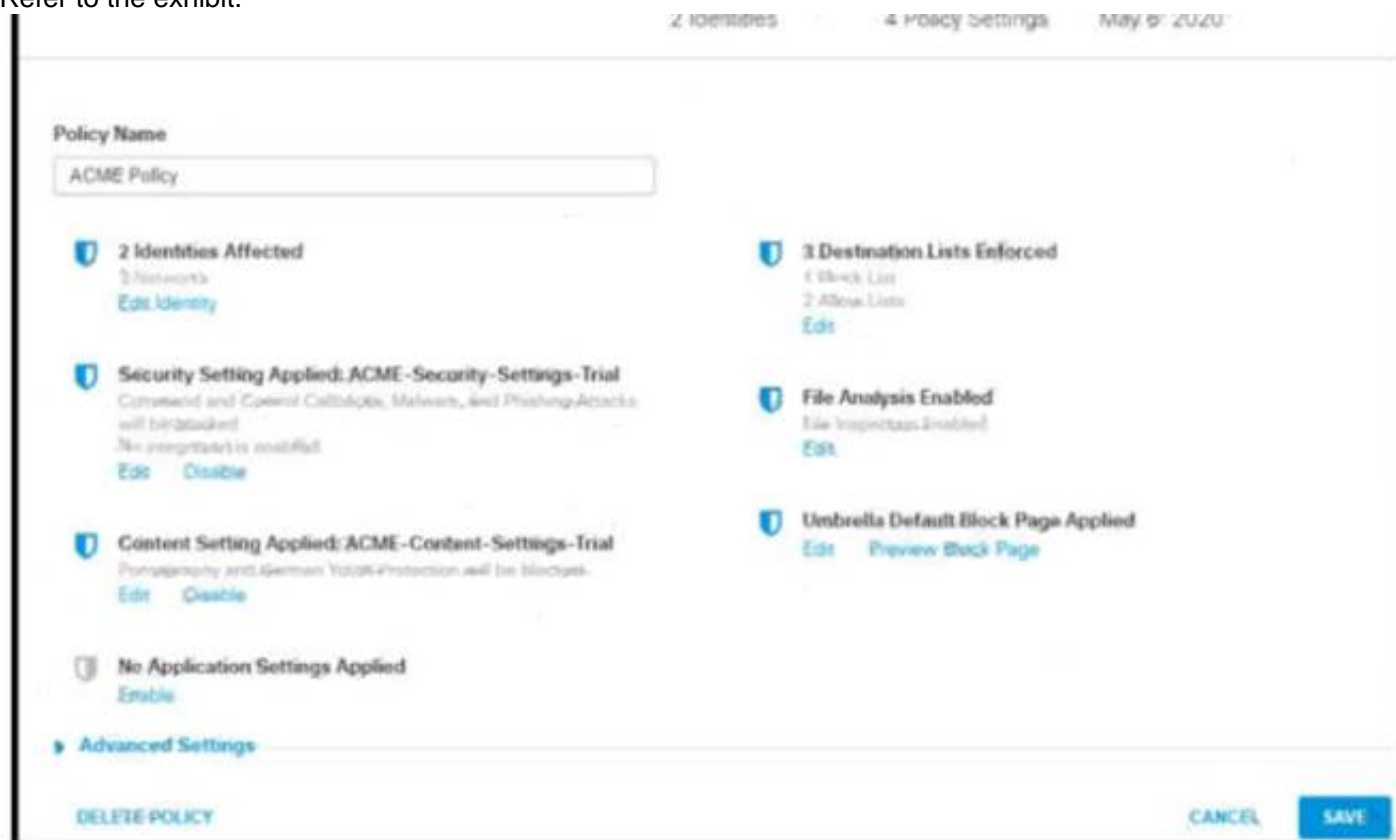
- A. CiscoASA(config-pmap-c)#flow-export event-type flow-update destination 209.165.201.10
- B. CiscoASA(config-cmap)# flow-export event-type all destination 209.165.201.
- C. CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.10
- D. CiscoASA(config-cmap)#flow-export event-type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

Answer: C

NEW QUESTION 27

- (Exam Topic 3)

Refer to the exhibit.



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

- A. Traffic is proxied 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 32

- (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 33

- (Exam Topic 3)

An engineer recently completed the system setup on a Cisco WSA Which URL information does the system send to SensorBase Network servers?

- A. Summarized server-name information and MD5-hashed path information
- B. complete URL,without obfuscating the path segments
- C. URL information collected from clients that connect to the Cisco WSA using Cisco AnyConnect
- D. none because SensorBase Network Participation is disabled by default

Answer: B

NEW QUESTION 35

- (Exam Topic 3)

Why is it important to patch endpoints consistently?

- A. Patching reduces the attack surface of the infrastructure.
- B. Patching helps to mitigate vulnerabilities.
- C. Patching is required per the vendor contract.
- D. Patching allows for creating a honeypot.

Answer: B

NEW QUESTION 39

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 43

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 44

- (Exam Topic 3)

An administrator configures new authorization policies within Cisco ISE and has difficulty profiling the devices. Attributes for the new Cisco IP phones that are profiled based on the RADIUS authentication are seen however the attributes for CDP or DHCP are not. What should the administrator do to address this issue?

- A. Configure the ip dhcp snooping trust command on the DHCP interfaces to get the information to Cisco ISE
- B. Configure the authentication port-control auto feature within Cisco ISE to identify the devices that are trying to connect
- C. Configure a service template within the switch to standardize the port configurations so that the correct information is sent to Cisco ISE
- D. Configure the device sensor feature within the switch to send the appropriate protocol information

Answer: D

Explanation:

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-ConfigureDevice-Sensor>

NEW QUESTION 45

- (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 48

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 49

- (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 53

- (Exam Topic 3)

What is a function of the Layer 4 Traffic Monitor on a Cisco WSA?

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

Answer: C

NEW QUESTION 58

- (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 62

- (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 64

- (Exam Topic 3)

Which Cisco DNA Center Intent API action is used to retrieve the number of devices known to a DNA Center?

- A. GET <https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/network-device/count>
- B. GET <https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/network-device>
- C. GET <https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/networkdevice?parameter1=value¶meter2=v>
- D. GET <https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/networkdevice/startIndex/recordsToReturn>

Answer: A

NEW QUESTION 69

- (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 71

- (Exam Topic 3)

What is a description of microsegmentation?

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

Answer: B

NEW QUESTION 75

- (Exam Topic 3)

Which MDM configuration provides scalability?

- A. pushing WPA2-Enterprise settings automatically to devices
- B. enabling use of device features such as camera use
- C. BYOD support without extra appliance or licenses
- D. automatic device classification with level 7 fingerprinting

Answer: C

NEW QUESTION 80

- (Exam Topic 3)

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

- A. posture assessment
- B. aaa authorization exec default local
- C. tacacs-server host 10.1.1.250 key password
- D. aaa server radius dynamic-author
- E. CoA

Answer: DE

NEW QUESTION 83

- (Exam Topic 3)

What does endpoint isolation in Cisco AMP for Endpoints security protect from?

- A. an infection spreading across the network E
- B. a malware spreading across the user device
- C. an infection spreading across the LDAP or Active Directory domain from a user account
- D. a malware spreading across the LDAP or Active Directory domain from a user account

Answer: C

Explanation:

<https://community.cisco.com/t5/endpoint-security/amp-endpoint-isolation/td-p/4086674#:~:text=Isolating%20an>

NEW QUESTION 84

- (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 IP addresses to a host interface.
- D. Enable flagged message handling

Answer: D

NEW QUESTION 86

- (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 89

- (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 91

- (Exam Topic 3)

An organization has DHCP servers set up to allocate IP addresses to clients on the LAN. What must be done to ensure the LAN switches prevent malicious DHCP traffic while also distributing IP addresses to the correct endpoints?

- A. Configure Dynamic ARP inspection and add entries in the DHCP snooping database.
- B. Configure DHCP snooping and set trusted interfaces for all client connections.
- C. Configure Dynamic ARP inspection and antispoofing ACLs in the DHCP snooping database.
- D. Configure DHCP snooping and set a trusted interface for the DHCP server.

Answer: B

Explanation:

Reference: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuratio

NEW QUESTION 94

- (Exam Topic 3)

Which characteristic is unique to a Cisco WSAv as compared to a physical appliance?

- A. supports VMware vMotion on VMware ESXi
- B. requires an additional license
- C. performs transparent redirection
- D. supports SSL decryption

Answer: A

NEW QUESTION 95

- (Exam Topic 3)

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

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

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_client_posture_Mandatory_Requirements During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings

NEW QUESTION 99

- (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 104

- (Exam Topic 3)

Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?

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

Answer: C

NEW QUESTION 107

- (Exam Topic 3)

Which solution is made from a collection of secure development practices and guidelines that developers must follow to build secure applications?

- A. AFL
- B. Fuzzing Framework
- C. Radamsa
- D. OWASP

Answer: D

NEW QUESTION 108

- (Exam Topic 3)

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

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

Answer: CD

NEW QUESTION 109

- (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 113

- (Exam Topic 3)

What is the recommendation in a zero-trust model before granting access to corporate applications and resources?

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

Answer: A

NEW QUESTION 114

- (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 117

- (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:

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

NEW QUESTION 120

- (Exam Topic 3)

What is a benefit of using Cisco Tetration?

- A. It collects telemetry data from servers and then uses software sensors to analyze flow information.
 B. It collects policy compliance data and process details.
 C. It collects enforcement data from servers and collects interpacket variation.
 D. It collects near-real time data from servers and inventories the software packages that exist on servers.

Answer: C

NEW QUESTION 124

- (Exam Topic 3)

Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks? (Choose two.)

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

Answer: CE

NEW QUESTION 128

- (Exam Topic 3)

What are two security benefits of an MDM deployment? (Choose two.)

- A. robust security policy enforcement
 B. privacy control checks
 C. on-device content management
 D. distributed software upgrade
 E. distributed dashboard

Answer: AC

NEW QUESTION 132

- (Exam Topic 3)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 137

- (Exam Topic 3)

What is the term for when an endpoint is associated to a provisioning WLAN that is shared with guest access, and the same guest portal is used as the BYOD portal?

- A. single-SSID BYOD
- B. multichannel GUI
- C. dual-SSID BYOD
- D. streamlined access

Answer: C

NEW QUESTION 140

- (Exam Topic 3)

How does Cisco Umbrella protect clients when they operate outside of the corporate network?

- A. by modifying the registry for DNS lookups
- B. by using Active Directory group policies to enforce Cisco Umbrella DNS servers
- C. by using the Cisco Umbrella roaming client
- D. by forcing DNS queries to the corporate name servers

Answer: C

NEW QUESTION 141

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 145

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 149

- (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 150

- (Exam Topic 3)

Email security has become a high priority task for a security engineer at a large multi-national organization due to ongoing phishing campaigns. To help control

this, the engineer has deployed an Incoming Content Filter with a URL reputation of (-10 00 to -6 00) on the Cisco ESA Which action will the system perform to disable any links in messages that match the filter?

- A. Defang
- B. Quarantine
- C. FilterAction
- D. ScreenAction

Answer: B

Explanation:

Reference: <https://www.cisco.com/c/dam/en/us/products/collateral/security/esa-content-filters.pdf>

NEW QUESTION 154

- (Exam Topic 3)

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

- A. Use DNSSEC between the endpoints and Cisco Umbrella DNS servers.
- B. Modify the Cisco Umbrella configuration to pass queries only to non-DNSSEC capable zones.
- C. Integrate Cisco Umbrella with Cisco CloudLock to ensure that DNSSEC is functional.
- D. Configure Cisco Umbrella and use DNSSEC for domain authentication to authoritative servers.

Answer: D

NEW QUESTION 155

- (Exam Topic 3)

How does the Cisco WSA enforce bandwidth restrictions for web applications?

- A. It implements a policy route to redirect application traffic to a lower-bandwidth link.
- B. It dynamically creates a scavenger class QoS policy and applies it to each client that connects through the WSA.
- C. It sends commands to the uplink router to apply traffic policing to the application traffic.
- D. It simulates a slower link by introducing latency into application traffic.

Answer: C

NEW QUESTION 160

- (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 165

- (Exam Topic 3)

Refer to the exhibit.

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

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

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

Answer: B

NEW QUESTION 170

- (Exam Topic 3)

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

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

Answer: AE

NEW QUESTION 173

- (Exam Topic 3)
Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

What function does the API key perform while working with <https://api.amp.cisco.com/v1/computers?>

- A. imports requests
- B. HTTP authorization
- C. HTTP authentication
- D. plays dent ID

Answer: C

NEW QUESTION 176

- (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 180

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 183

- (Exam Topic 3)

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

- A. The Umbrella Roaming client stops and tracks malicious activity on hosts, and AMP for Endpoints tracks only URL-based threats.
- B. The Umbrella Roaming Client authenticates users and provides segmentation, and AMP for Endpoints allows only for VPN connectivity.
- C. AMP for Endpoints authenticates users and provides segmentation, and the Umbrella Roaming Client allows only for VPN connectivity.
- D. AMP for Endpoints stops and tracks malicious activity on hosts, and the Umbrella Roaming Client tracks only URL-based threats.

Answer: D

NEW QUESTION 188

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 192

- (Exam Topic 3)

An engineer is configuring Cisco WSA and needs to deploy it in transparent mode. Which configuration component must be used to accomplish this goal?

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

Answer: C

NEW QUESTION 195

- (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 197

- (Exam Topic 3)

What is a feature of container orchestration?

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

Answer: C

NEW QUESTION 199

- (Exam Topic 3)

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

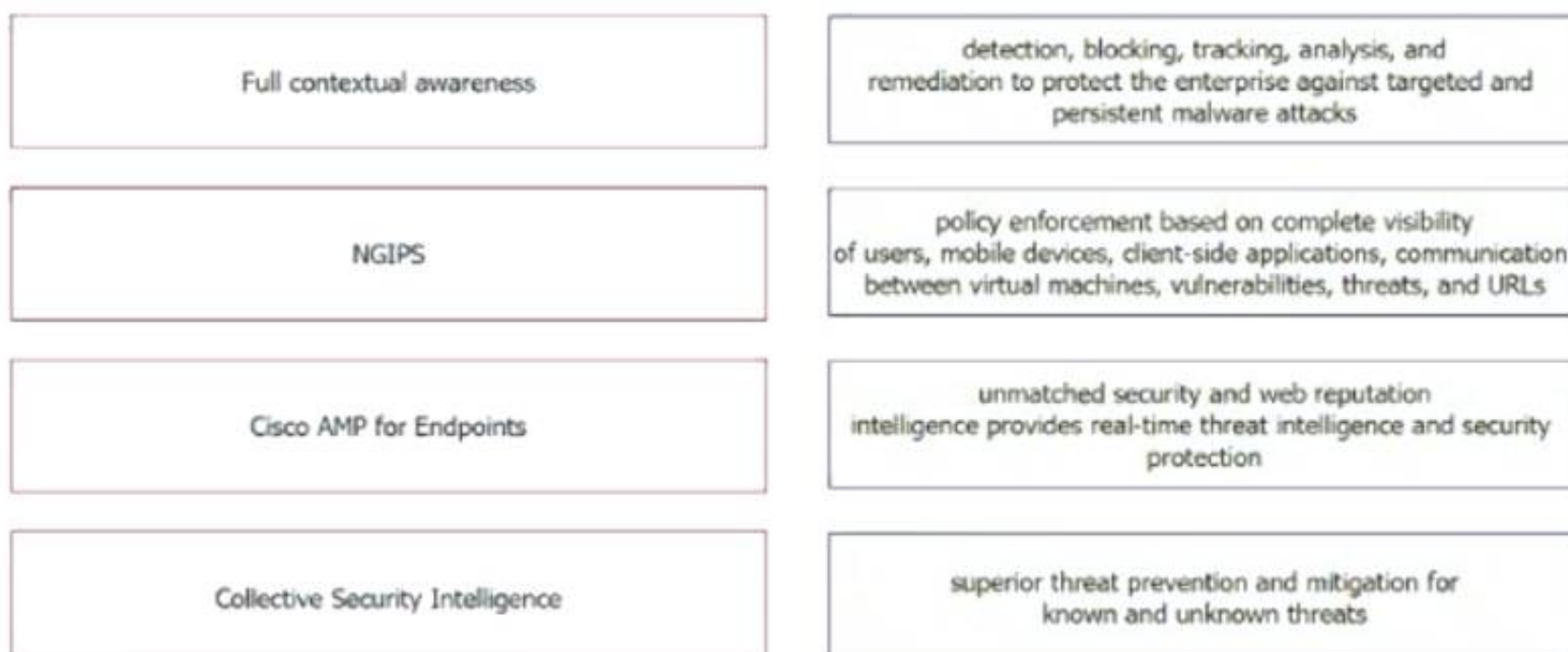
- A. Change the IP address of the new Cisco ISE node to the same network as the others.
- B. Make the new Cisco ISE node a secondary PAN before registering it with the primary.
- C. Open port 8905 on the firewall between the Cisco ISE nodes
- D. Add the DNS entry for the new Cisco ISE node into the DNS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

Answer: D

NEW QUESTION 203

- (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 206

- (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 the 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 210

- (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 the 10.0.0.0/24 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 214

- (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 216

- (Exam Topic 3)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 220

- (Exam Topic 3)

Why should organizations migrate to a multifactor authentication strategy?

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

Answer: D

NEW QUESTION 225

- (Exam Topic 3)

Which technology enables integration between Cisco ISE and other platforms to gather and share network and vulnerability data and SIEM and location information?

- A. pxGrid
- B. NetFlow
- C. SNMP
- D. Cisco Talos

Answer: A

NEW QUESTION 227

- (Exam Topic 3)
Refer to the exhibit.

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

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

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

Answer: A

NEW QUESTION 228

- (Exam Topic 3)
What are two features of NetFlow flow monitoring? (Choose two)

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

Answer: AE

Explanation:

Reference:
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow>

NEW QUESTION 232

- (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 233

- (Exam Topic 3)
An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users.

- A. Upload the organization root CA to the Umbrella admin portal
- B. Modify the user's browser settings to suppress errors from Umbrella.
- C. Restrict access to only websites with trusted third-party signed certificates.
- D. Import the Umbrella root CA into the trusted root store on the user's device.

Answer: A

NEW QUESTION 237

- (Exam Topic 3)
Which feature must be configured before implementing NetFlow on a router?

- A. SNMPv3
- B. syslog
- C. VRF
- D. IP routing

Answer: D

NEW QUESTION 242

- (Exam Topic 3)
In which scenario is endpoint-based security the solution?

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

Answer: C

NEW QUESTION 246

- (Exam Topic 3)

Which capability is provided by application visibility and control?

- A. reputation filtering
- B. data obfuscation
- C. data encryption
- D. deep packet inspection

Answer: D

NEW QUESTION 249

- (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 254

- (Exam Topic 3)

What is the most common type of data exfiltration that organizations currently experience?

- A. HTTPS file upload site
- B. Microsoft Windows network shares
- C. SQL database injections
- D. encrypted SMTP

Answer: B

Explanation:

Reference: <https://blogs.cisco.com/security/sensitive-data-exfiltration-and-the-insider>

NEW QUESTION 256

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 259

- (Exam Topic 2)

Refer to the exhibit.

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

What will happen when the Python script is executed?

- A. The hostname will be translated to an IP address and printed.
- B. The hostname will be printed for the client in the client ID field.

- C. The script will pull all computer hostnames and print them.
- D. The script will translate the IP address to FODN and print it

Answer: C

NEW QUESTION 264

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 268

- (Exam Topic 2)

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

- A. TCP 6514
- B. UDP 1700
- C. TCP 49
- D. UDP 1812

Answer: B

Explanation:

CoA Messages are sent on two different udp ports depending on the platform. Cisco standardizes on UDP port1700, while the actual RFC calls out using UDP port 3799.

NEW QUESTION 269

- (Exam Topic 2)

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

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

Answer: BD

NEW QUESTION 273

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 275

- (Exam Topic 2)

Refer to the exhibit.


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

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

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

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

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

- A. No split-tunnel policy is defined on the Firepower Threat Defense appliance.
- B. The access control policy is not allowing VPN traffic in.
- C. Site-to-site VPN peers are using different encryption algorithms.
- D. Site-to-site VPN preshared keys are mismatched.

Answer: A

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 278

- (Exam Topic 2)

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

- A. It forwards the packet after validation by using the MAC Binding Table.
- B. It drops the packet after validation by using the IP & MAC Binding Table.
- C. It forwards the packet without validation.
- D. It drops the packet without validation.

Answer: B

NEW QUESTION 279

- (Exam Topic 2)

Refer to the exhibit.

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

What will happen when this Python script is run?

- A. The compromised computers and malware trajectories will be received from Cisco AMP
- B. The list of computers and their current vulnerabilities will be received from Cisco AMP

- C. The compromised computers and what compromised them will be received from Cisco AMP
D. The list of computers, policies, and connector statuses will be received from Cisco AMP

Answer: D

Explanation:

Reference:

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

NEW QUESTION 283

- (Exam Topic 2)

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

- A. Public managed
B. Service Provider managed
C. Enterprise managed
D. User managed
E. Hybrid managed

Answer: BC

Explanation:

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

NEW QUESTION 285

- (Exam Topic 2)

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

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

Answer: CE

Explanation:

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

NEW QUESTION 287

- (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 290

- (Exam Topic 2)

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

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

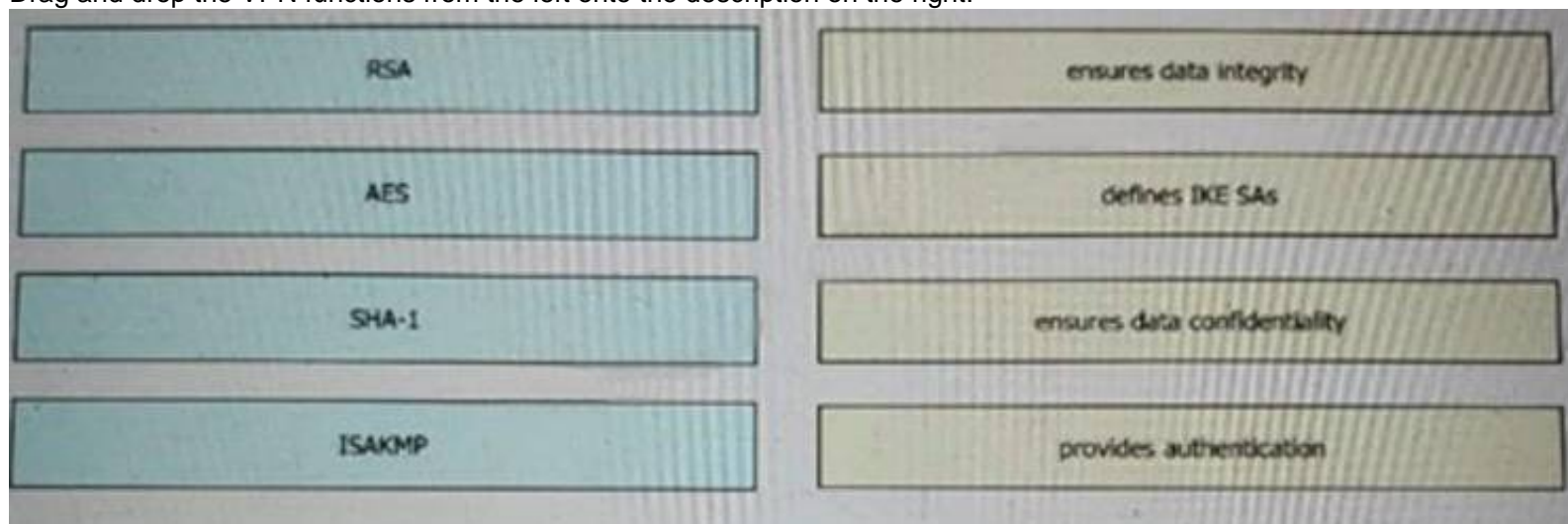
Reference:

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

NEW QUESTION 293

- (Exam Topic 2)

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 294

- (Exam Topic 2)

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

- A. Ethos Engine to perform fuzzy fingerprinting
- B. Tetra Engine to detect malware when the endpoint is connected to the cloud
- C. Clam AV Engine to perform email scanning
- D. Spero Engine with machine learning to perform dynamic analysis

Answer: A

Explanation:

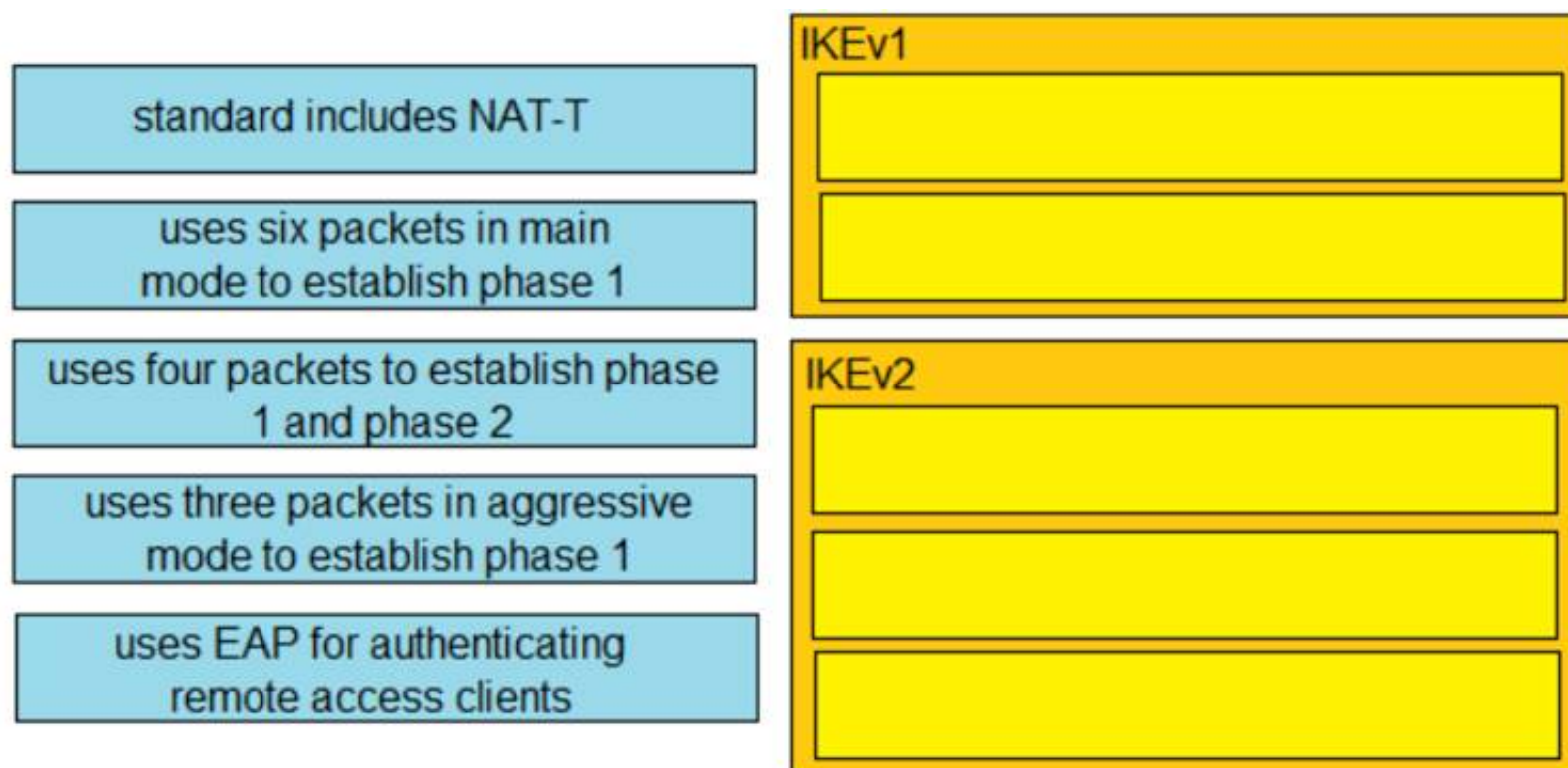
Reference: <https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf> ETHOS = Fuzzy Fingerprinting using static/passive heuristics

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/BRKSEC-2139.pdf>

NEW QUESTION 297

- (Exam Topic 2)

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated with low confidence

NEW QUESTION 298

- (Exam Topic 2)

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

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 300

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 303

- (Exam Topic 2)

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

- A. Google Cloud Platform
- B. Red Hat Enterprise Visualization
- C. VMware ESXi
- D. Amazon Web Services

Answer: D

Explanation:

Reference:

<https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html>

NEW QUESTION 306

- (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 311

- (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 315

- (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.html>In this question, it stated “the network is congested” (not the file analysis server was overloaded) so the appliance will not try to upload the file again.

NEW QUESTION 318

- (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 319

- (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 320

- (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 324

- (Exam Topic 2)

How does Cisco Advanced Phishing Protection protect users?

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

Answer: D

Explanation:

Reference: <https://docs.ces.cisco.com/docs/advanced-phishing-protection>

NEW QUESTION 326

- (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 327

- (Exam Topic 2)

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

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

Answer: C

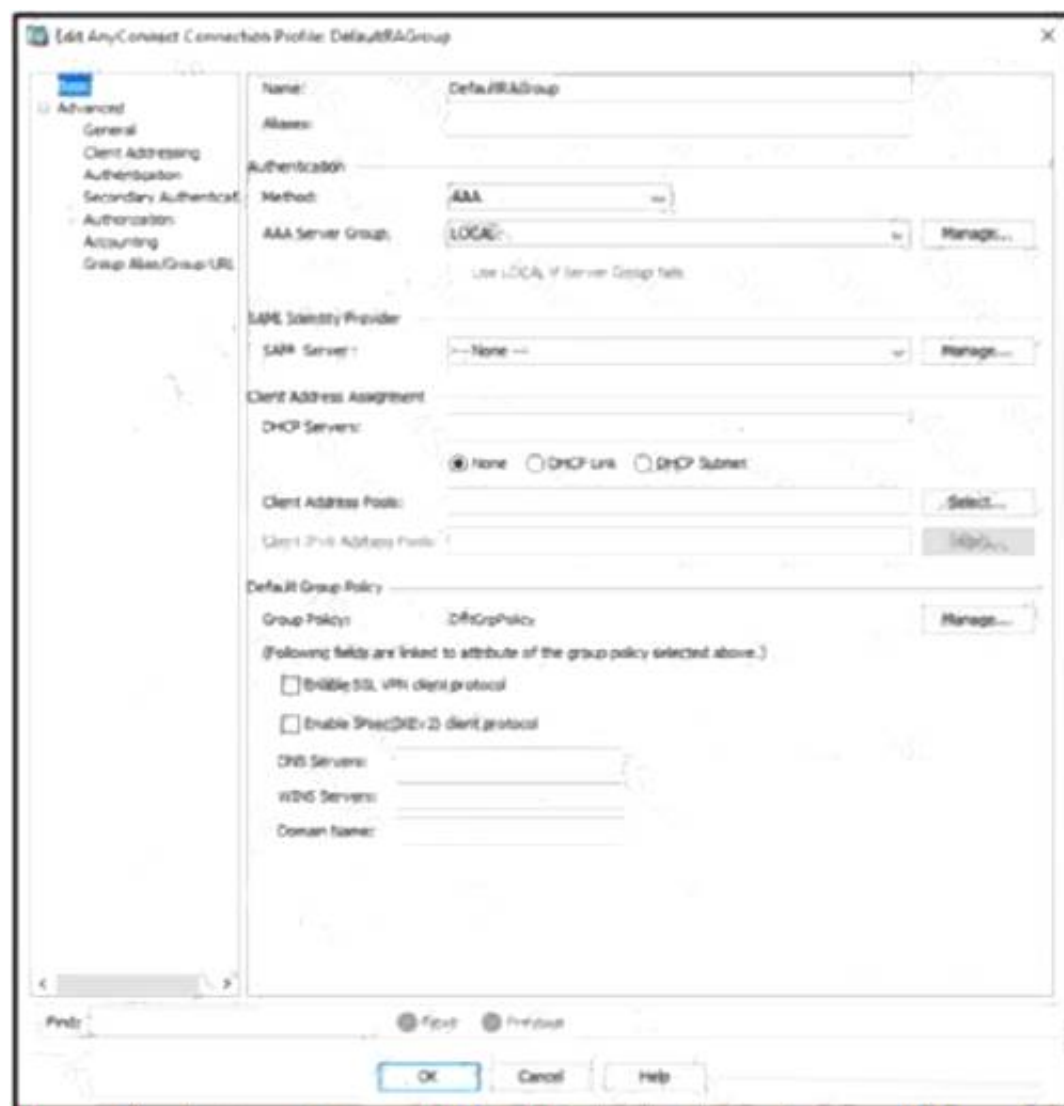
Explanation:

The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or allow applications individually or according to application type. You can also apply controls to particular application types.

NEW QUESTION 332

- (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" in the Authentication.

NEW QUESTION 336

- (Exam Topic 2)

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

- A. To prevent man-the-middle attacks from being successful.
- B. To prevent DoS attacks from being successful.
- C. To prevent brute force attacks from being successful.
- D. To prevent phishing attacks from being successful.

Answer: C

NEW QUESTION 337

- (Exam Topic 2)

What are two DDoS attack categories? (Choose two)

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

Answer: BD

Explanation:

There are three basic categories of attack: + volume-based attacks, which use high traffic to inundate the network bandwidth + protocol attacks, which focus on exploiting server resources + application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks

Reference: <https://www.esecurityplanet.com/networks/types-of-ddos-attacks/>

NEW QUESTION 342

- (Exam Topic 2)

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

- A. Use MAB with profiling

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

Answer: A

Explanation:

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

NEW QUESTION 343

- (Exam Topic 2)

Refer to the exhibit.

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

- A. configure manager add DONTRESOLVE kregistration key>
- B. configure manager add <FMC IP address> <registration key> 16
- C. configure manager add DONTRESOLVE <registration key> FTD123
- D. configure manager add <FMC IP address> <registration key>

Answer: D

Explanation:

Reference: <https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/>

NEW QUESTION 348

- (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 provide device-level protection by identifying malicious files, detecting potentially malicious activity, and providing tools for incident investigation and response. The preventative nature of EPP complements proactive EDR. EPP acts as the first line of defense, filtering out attacks that can be detected by the organization's deployed security solutions. EDR acts as a second layer of protection, enabling security analysts to perform threat hunting and identify more subtle threats to the endpoint. Effective endpoint defense requires a solution that integrates the capabilities of both EDR and EPP to provide protection against cyber threats without overwhelming an organization's security team.

NEW QUESTION 349

- (Exam Topic 1)

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

- A. Mail Submission Agent
- B. Mail Transfer Agent
- C. Mail Delivery Agent
- D. Mail User Agent

Answer: B

Explanation:

Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/Cisco_SBA_BN_EmailSecurityUsing

NEW QUESTION 350

- (Exam Topic 2)

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 355

- (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 358

- (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 363

- (Exam Topic 1)

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

- A. Port Bounce
- B. CoA Terminate
- C. CoA Reauth
- D. CoA Session Query

Answer: C

NEW QUESTION 366

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 368

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

NEW QUESTION 371

- (Exam Topic 1)

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

- A. aaa server radius dynamic-author
- B. aaa new-model
- C. auth-type all
- D. ip device-tracking

Answer: D

NEW QUESTION 372

- (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 375

- (Exam Topic 1)

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

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

Answer: D

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/platfo> the answer should be “Platform Settings Policy”, not “Platform Service Policy” but it is the best answer here so we have to choose it.

NEW QUESTION 378

- (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 383

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 385

- (Exam Topic 1)

Refer to the exhibit.

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

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

- A. The authentication request contains only a password
- B. The authentication request contains only a username
- C. The authentication and authorization requests are grouped in a single packet
- D. There are separate authentication and authorization request packets

Answer: C

Explanation:

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

NEW QUESTION 387

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 392

- (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 397

- (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 398

- (Exam Topic 1)

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

- A. cloud web services
- B. network AMP
- C. private cloud
- D. public cloud

Answer: C

NEW QUESTION 400

- (Exam Topic 1)

Refer to the exhibit.

```

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

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

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

- A. hashing algorithm mismatch
- B. encryption algorithm mismatch
- C. authentication key mismatch
- D. interesting traffic was not applied

Answer: C

NEW QUESTION 402

- (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 406

- (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 409

- (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 411

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 415

- (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 418

- (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 421

- (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 422

- (Exam Topic 1)

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

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

Answer: D

Explanation:

Reference:

https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_

NEW QUESTION 426

- (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 430

- (Exam Topic 1)

A network engineer is configuring DMVPN and entered the crypto isakmp key cisc0380739941 address 1.1.1.1 command on hostA. The tunnel is not being established to hostB. What action is needed to authenticate the VPN?

- A. Change isakmp to ikev2 in the command on hostA.
- B. Enter the command with a different password on hostB.
- C. Enter the same command on hostB.
- D. Change the password on hostA to the default password.

Answer: C

NEW QUESTION 431

- (Exam Topic 1)

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

- A. DNS tunneling
- B. DNSCrypt
- C. DNS security
- D. DNSSEC

Answer: A

Explanation:

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

NEW QUESTION 434

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 439

- (Exam Topic 1)

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

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

Answer: AB

NEW QUESTION 442

- (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 443

- (Exam Topic 1)

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

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

Answer: AB

NEW QUESTION 447

- (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 449

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 452

- (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 454

- (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 455

- (Exam Topic 1)

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

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

Answer: BC

NEW QUESTION 456

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 459

- (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 Service Note: A flow is a unidirectional series of packets between a given source and destination.

NEW QUESTION 460

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 463

- (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 465

- (Exam Topic 1)

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

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

Answer: DE

Explanation:

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

NEW QUESTION 467

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide

NEW QUESTION 468

- (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 472

- (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 475

- (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 479

- (Exam Topic 1)

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

- A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.
- B. Set up a profiling policy in Cisco Identity Service Engine to check and endpoint patch level before allowing access on the network.
- C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.
- D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.
- E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.

Answer: AC

Explanation:

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

[File Conditions List > pc_W10_64_KB4012606_Ms17-010_1507_W](#)

File Condition

* Name	pc_W10_64_KB4012606_Ms1
Description	Cisco Predefined Check: Micro
* Operating System	Windows 10 (All)
Compliance Module	Any version
* File Type	FileVersion
* File Path	SYSTEM_32
* Operator	LaterThan
* File Version	10.0.10240.17318
<input type="button" value="Cancel"/>	

NEW QUESTION 481

- (Exam Topic 1)

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

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

Answer: BD

Explanation:

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

<https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf>

NEW QUESTION 483

- (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 486

- (Exam Topic 1)

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

- A. url
- B. terminal
- C. profile
- D. selfsigned

Answer: C

Explanation:

Reference:

<https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/211333-IOSPKI-Deploy>

NEW QUESTION 488

- (Exam Topic 1)

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

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

Answer: CE

NEW QUESTION 489

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 490

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 491

- (Exam Topic 1)

What is a characteristic of Firepower NGIPS inline deployment mode?

- A. ASA with Firepower module cannot be deployed.
- B. It cannot take actions such as blocking traffic.

- C. It is out-of-band from traffic.
- D. It must have inline interface pairs configured.

Answer: D

NEW QUESTION 493

- (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 495

- (Exam Topic 1)

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

- A. RADIUS Change of Authorization
- B. device tracking
- C. DHCP snooping
- D. VLAN hopping

Answer: A

NEW QUESTION 498

- (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.html> 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 499

- (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 502

- (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 506

- (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 allotted memory space. This happens quite frequently in the case of arrays.

NEW QUESTION 511

- (Exam Topic 1)

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

- A. DHCP Snooping
- B. 802.1AE MacSec
- C. Port security
- D. IP Device track
- E. Dynamic ARP inspection
- F. Private VLANs

Answer: AE

NEW QUESTION 515

- (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. dot1x reauthentication
- C. cisp enable
- D. dot1x pae authenticator

Answer: D

NEW QUESTION 520

- (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 521

- (Exam Topic 1)

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

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

Answer: AC

Explanation:

The ASA REST API gives you programmatic access to managing individual ASAs through a Representational State Transfer (REST) API. The API allows external clients to perform CRUD (Create, Read, Update, Delete) operations on ASA resources; it is based on the HTTPS protocol and REST methodology. All API requests are sent over HTTPS to the ASA, and a response is returned. Request Structure Available request methods are: GET – Retrieves data from the specified object. PUT

– Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist. POST – Creates the object with the supplied information. DELETE – Deletes the specified object
 Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html>

NEW QUESTION 523

- (Exam Topic 1)

Refer to the exhibit.

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

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

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

Answer: B

NEW QUESTION 527

- (Exam Topic 1)

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

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

Answer: BD

Explanation:

The profiling service issues the change of authorization in the following cases:– Endpoint deleted—When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network. An exception action is configured—If you have an exception action configured per profile that leads to an unusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to the corresponding static profile by issuing a CoA.– An endpoint is profiled for the first time—When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.+ An endpoint identity group has changed—When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy. The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:

Reference:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide

NEW QUESTION 532

- (Exam Topic 1)

Which statement about IOS zone-based firewalls is true?

- A. An unassigned interface can communicate with assigned interfaces
- B. Only one interface can be assigned to a zone.

- C. An interface can be assigned to multiple zones.
- D. An interface can be assigned only to one zone.

Answer: D

NEW QUESTION 537

- (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 541

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 544

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 548

- (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 550

- (Exam Topic 1)

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

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

Answer: BE

Explanation:

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

NEW QUESTION 555

- (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 documented. Like other large but well-formed packets, a ping of death is fragmented into groups of 8 octets before transmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code.

NEW QUESTION 557

- (Exam Topic 1)

Refer to the exhibit.

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

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

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

Answer: B

Explanation:

The user "admin5" was configured with privilege level 5. In order to allow configuration (enter global configuration mode), we must type this command: (config)#privilege exec level 5 configure terminal. Without this command, this user cannot do any configuration. Note: Cisco IOS supports privilege levels from 0 to 15, but the privilege levels which are used by default are privilege level 1 (user EXEC) and level privilege 15 (privilege EXEC).

NEW QUESTION 560

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 565

- (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 566

- (Exam Topic 1)

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

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

Answer: AC

NEW QUESTION 571

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 576

- (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 580

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 582

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 584

- (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 588

- (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 591

- (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 596

- (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 or financial institution that requests account information, often suggesting that there is a problem.

NEW QUESTION 599

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 602

- (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 607

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 610

- (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 615

- (Exam Topic 1)

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

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

Answer: DE

Explanation:

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

NEW QUESTION 617

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 618

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 622

- (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 626

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 631

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 636

- (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 641

- (Exam Topic 3)

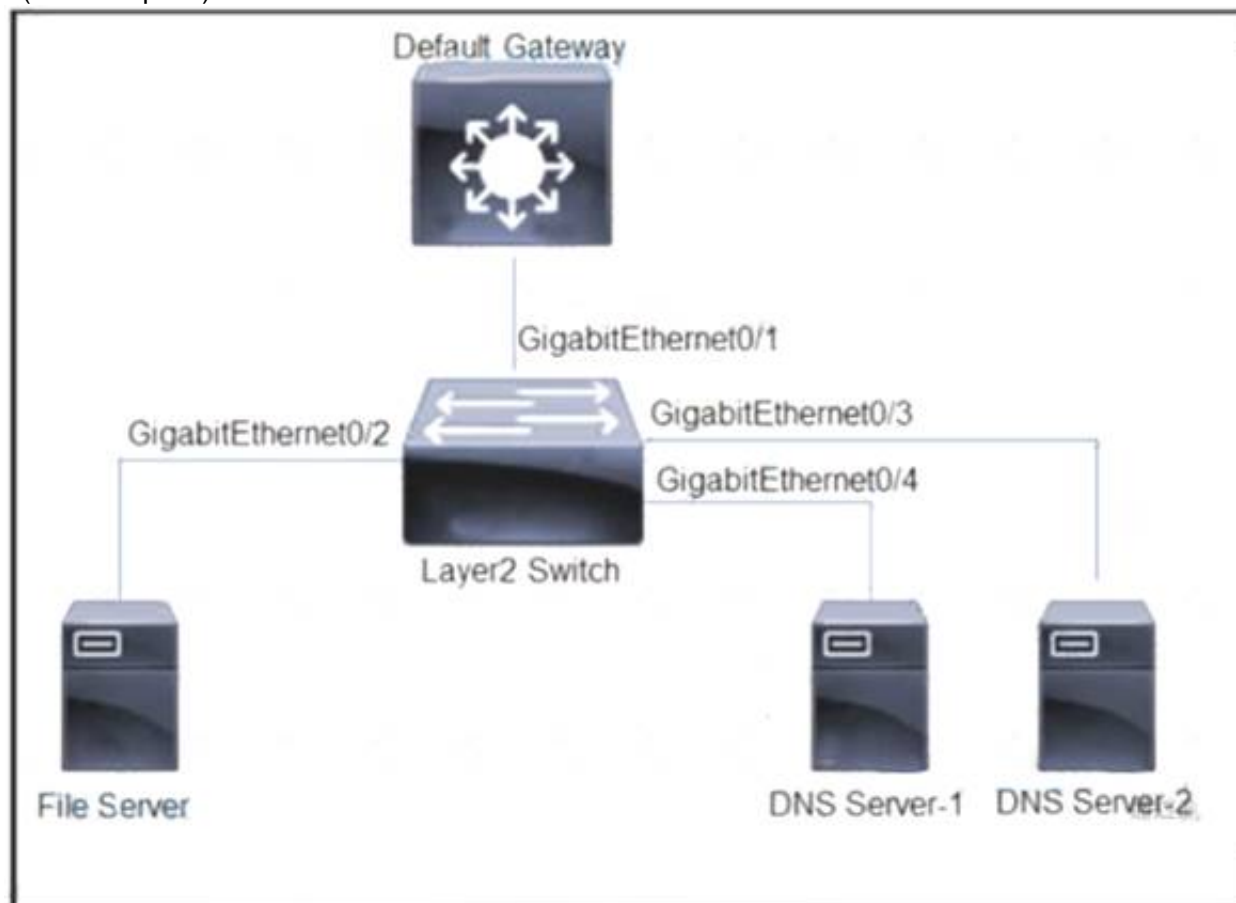
What is a characteristic of an EDR solution and not of an EPP solution?

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

Answer: B

NEW QUESTION 645

- (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 648

- (Exam Topic 3)

What is the process In DevSecOps where all changes In the central code repository are merged and synchronized?

- A. CD

- B. EP
- C. CI
- D. QA

Answer: C

NEW QUESTION 649

- (Exam Topic 3)

Which system performs compliance checks and remote wiping?

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

Answer: A

NEW QUESTION 651

- (Exam Topic 3)

Which CLI command is used to enable URL filtering support for shortened URLs on the Cisco ESA?

- A. webadvancedconfig
- B. websecurity advancedconfig
- C. outbreakconfig
- D. websecurity config

Answer: B

NEW QUESTION 655

- (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 657

- (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 659

- (Exam Topic 3)

What is the difference between EPP and EDR?

- A. EPP focuses primarily on threats that have evaded front-line defenses that entered the environment.
- B. Having an EPP solution allows an engineer to detect, investigate, and remediate modern threats.
- C. EDR focuses solely on prevention at the perimeter.
- D. Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior.

Answer: B

NEW QUESTION 664

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 665

- (Exam Topic 3)

What are two characteristics of the RESTful architecture used within Cisco DNA Center? (Choose two.)

- A. REST uses methods such as GET, PUT, POST, and DELETE.
- B. REST codes can be compiled with any programming language.
- C. REST is a Linux platform-based architecture.
- D. The POST action replaces existing data at the URL path.
- E. REST uses HTTP to send a request to a web service.

Answer: AE

NEW QUESTION 668

- (Exam Topic 3)

What is the concept of CI/CD pipelining?

- A. The project is split into several phases where one phase cannot start before the previous phase finishes successfully.
- B. The project code is centrally maintained and each code change should trigger an automated build and test sequence
- C. The project is split into time-limited cycles and focuses on pair programming for continuous code review
- D. Each project phase is independent from other phases to maintain adaptiveness and continual improvement

Answer: A

NEW QUESTION 669

- (Exam Topic 3)

What is the purpose of a NetFlow version 9 template record?

- A. It specifies the data format of NetFlow processes.
- B. It provides a standardized set of information about an IP flow.
- C. It defines the format of data records.
- D. It serves as a unique identification number to distinguish individual data records

Answer: C

NEW QUESTION 670

- (Exam Topic 3)

An organization has a requirement to collect full metadata information about the traffic going through their AWS cloud services They want to use this information for behavior analytics and statistics Which two actions must be taken to implement this requirement? (Choose two.)

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

Answer: BE

NEW QUESTION 673

- (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 676

- (Exam Topic 3)

Which Cisco security solution determines if an endpoint has the latest OS updates and patches installed on the system?

- A. Cisco Endpoint Security Analytics
- B. Cisco AMP for Endpoints
- C. Endpoint Compliance Scanner
- D. Security Posture Assessment Service

Answer: A

NEW QUESTION 680

- (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 682

- (Exam Topic 3)

Which solution stops unauthorized access to the system if a user's password is compromised?

- A. VPN
- B. MFA
- C. AMP
- D. SSL

Answer: B

NEW QUESTION 683

- (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 684

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 686

- (Exam Topic 3)

Which two components do southbound APIs use to communicate with downstream devices? (Choose two.)

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

Answer: BE

NEW QUESTION 687

- (Exam Topic 3)

Which Cisco DNA Center RESTful PNP API adds and claims a device into a workflow?

- A. api/v1/fie/config
- B. api/v1/onboarding/pnp-device/import
- C. api/v1/onboarding/pnp-device
- D. api/v1/onboarding/workflow

Answer: B

NEW QUESTION 688

- (Exam Topic 3)

Which type of attack is MFA an effective deterrent for?

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

Answer: B

NEW QUESTION 691

- (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 695

.....

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