

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)

What limits communication between applications or containers on the same node?

- A. microsegmentation
- B. container orchestration
- C. microservicing
- D. Software-Defined Access

Answer: D

NEW QUESTION 4

- (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_Endpoint_IoC_Feature.pdf

NEW QUESTION 5

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 6

- (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 7

- (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 8

- (Exam Topic 3)

What is a benefit of using GET VPN over FlexVPN within a VPN deployment?

- A. GET VPN supports Remote Access VPNs
- B. GET VPN natively supports MPLS and private IP networks
- C. GET VPN uses multiple security associations for connections
- D. GET VPN interoperates with non-Cisco devices

Answer: B

NEW QUESTION 9

- (Exam Topic 3)

When a next-generation endpoint security solution is selected for a company, what are two key deliverables that help justify the implementation? (Choose two.)

- A. signature-based endpoint protection on company endpoints
- B. macro-based protection to keep connected endpoints safe
- C. continuous monitoring of all files that are located on connected endpoints
- D. email integration to protect endpoints from malicious content that is located in email
- E. real-time feeds from global threat intelligence centers

Answer: CE

NEW QUESTION 10

- (Exam Topic 3)

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

- A. Malware installation
- B. Command-and-control communication
- C. Network footprinting
- D. Data exfiltration

Answer: D

Explanation:

Reference: <https://www.netsurion.com/articles/5-types-of-dns-attacks-and-how-to-detect-them>

NEW QUESTION 10

- (Exam Topic 3)

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

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

Answer: AD

NEW QUESTION 12

- (Exam Topic 3)

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

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

Answer: AD

NEW QUESTION 16

- (Exam Topic 3)

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

- A. Define MAC-to-IP address mappings in the switch to ensure that rogue devices cannot get an IP address
- B. Use DHCP option 82 to ensure that the request is from a legitimate endpoint and send the information to Cisco ISE
- C. Modify the DHCP relay and point the IP address to Cisco ISE.
- D. Configure DHCP snooping on the switch VLANs and trust the necessary interfaces

Answer: D

NEW QUESTION 20

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 23

- (Exam Topic 3)

Which two commands are required when configuring a flow-export action on a Cisco ASA? (Choose two.)

- A. flow-export event-type
- B. policy-map
- C. access-list
- D. flow-export template timeout-rate 15
- E. access-group

Answer: AB

NEW QUESTION 26

- (Exam Topic 3)

Which solution supports high availability in routed or transparent mode as well as in northbound and southbound deployments?

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

Answer: B

NEW QUESTION 30

- (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 31

- (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 35

- (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 38

- (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 43

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 48

- (Exam Topic 3)

An engineer must set up 200 new laptops on a network and wants to prevent the users from moving their laptops around to simplify administration Which switch port MAC address security setting must be used?

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

Answer: A

NEW QUESTION 53

- (Exam Topic 3)

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

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

Answer: B

Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/vpn/ipsec-negotiation-ike-protocols/215470-site-to-site-vpn-configuration-on-ftd-ma.html>

NEW QUESTION 57

- (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 61

- (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 65

- (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 66

- (Exam Topic 3)

A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address <https://<FMC IP>/capture/CAP/pcap/test.pcap>, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

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

Answer: D

NEW QUESTION 69

- (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 74

- (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 78

- (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 80

- (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 85

- (Exam Topic 3)

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

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

Answer: AE

NEW QUESTION 90

- (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 91

- (Exam Topic 3)

In which two ways does the Cisco Advanced Phishing Protection solution protect users? (Choose two.)

- A. It prevents use of compromised accounts and social engineering.
- B. It prevents all zero-day attacks coming from the Internet.
- C. It automatically removes malicious emails from users' inbox.
- D. It prevents trojan horse malware using sensors.
- E. It secures all passwords that are shared in video conferences.

Answer: BC

NEW QUESTION 96

- (Exam Topic 3)

A hacker initiated a social engineering attack and stole username and passwords of some users within a company. Which product should be used as a solution to this problem?

- A. Cisco NGFW
- B. Cisco AnyConnect
- C. Cisco AMP for Endpoints
- D. Cisco Duo

Answer: D

NEW QUESTION 98

- (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 102

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 106

- (Exam Topic 3)

Refer to the exhibit.

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

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

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

Answer: B

NEW QUESTION 110

- (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 115

- (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 120

- (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 122

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 125

- (Exam Topic 3)

What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.)

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

Answer: AC

NEW QUESTION 130

- (Exam Topic 3)

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

- A. using Cisco Umbrella
- B. using Cisco ESA
- C. using Cisco FTD
- D. using an inline IPS/IDS in the network
- E. using Cisco ISE

Answer: AB

NEW QUESTION 131

- (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 135

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 140

- (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 142

- (Exam Topic 3)

What are two recommended approaches to stop DNS tunneling for data exfiltration and command and control call backs? (Choose two.)

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

Answer: CE

NEW QUESTION 146

- (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 148

- (Exam Topic 3)

Which feature does the IaaS model provide?

- A. granular control of data
- B. dedicated, restricted workstations
- C. automatic updates and patching of software
- D. software-defined network segmentation

Answer: C

NEW QUESTION 150

- (Exam Topic 3)

Drag and drop the exploits from the left onto the type of security vulnerability on the right.

causes memory access errors	path transversal
makes the client the target of attack	cross-site request forgery
gives unauthorized access to web server files	SQL injection
accesses or modifies application data	buffer overflow

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 155

- (Exam Topic 3)

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

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

Answer: D

Explanation:

<https://learn-umbrella.cisco.com/i/802005-umbrella-security-report/3?> <https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html#:~:text=Pow> Cisco Advanced Malware Protection (AMP) for endpoints can be seen as a replacement for the traditional antivirus solution. It is a next generation, cloud delivered endpoint protection platform (EPP), and advanced endpoint detection and response (EDR). Providing Protection – Detection Response

While Cisco Umbrella can enforce security at the DNS-, IP-, and HTTP/S-layer, this report does not require that blocking is enabled and only monitors your DNS activity. Any malicious domains requested and IPs resolved are indicators of compromise (IOC).

Any malicious domains requested and IPs resolved are indicators of compromise IO(C)

NEW QUESTION 160

- (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 163

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 165

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 170

- (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 171

- (Exam Topic 3)

An engineer is configuring Dropbox integration with Cisco Cloudlock. Which action must be taken before granting API access in the Dropbox admin console?

- A. Authorize Dropbox within the Platform settings in the Cisco Cloudlock portal.
- B. Add Dropbox to the Cisco Cloudlock Authentication and API section in the Cisco Cloudlock portal.
- C. Send an API request to Cisco Cloudlock from Dropbox admin portal.
- D. Add Cisco Cloudlock to the Dropbox admin portal.

Answer: A

NEW QUESTION 176

- (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 180

- (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 183

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 188

- (Exam Topic 3)

Which Cisco AMP feature allows an engineer to look back to trace past activities, such as file and process activity on an endpoint?

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

Answer: D

NEW QUESTION 193

- (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 194

- (Exam Topic 3)

What must be enabled to secure SaaS-based applications?

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

Answer: C

NEW QUESTION 198

- (Exam Topic 3)

Drag and drop the security solutions from the left onto the benefits they provide on the right.

Full contextual awareness	detection, blocking, tracking, analysis, and remediation to protect the enterprise against targeted and persistent malware attacks
NGIPS	policy enforcement based on complete visibility of users, mobile devices, client-side applications, communication between virtual machines, vulnerabilities, threats, and URLs
Cisco AMP for Endpoints	unmatched security and web reputation intelligence provides real-time threat intelligence and security protection
Collective Security Intelligence	superior threat prevention and mitigation for known and unknown threats

- A. Mastered
- B. Not Mastered

Answer: A

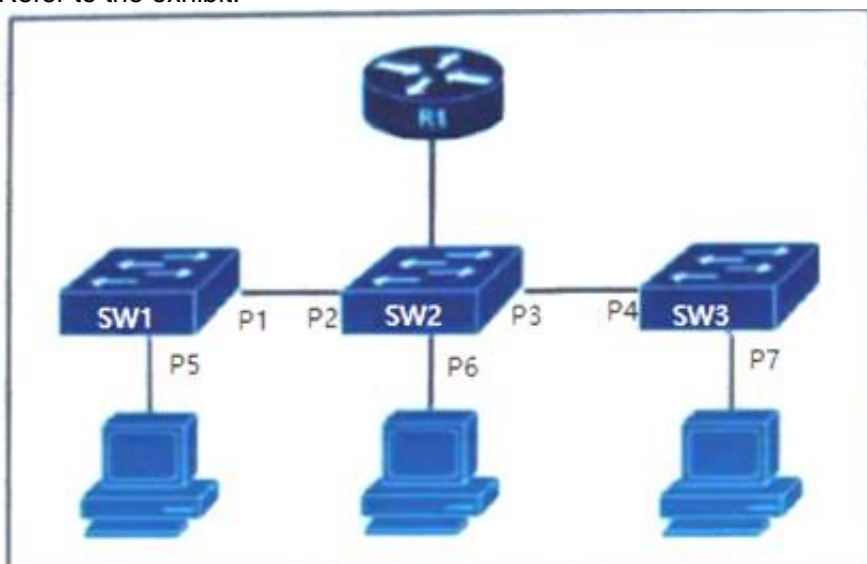
Explanation:

Diagram Description automatically generated

NEW QUESTION 200

- (Exam Topic 3)

Refer to the exhibit.



The DHCP snooping database resides on router R1, and dynamic ARP inspection is configured only on switch SW2. Which ports must be configured as untrusted so that dynamic ARP inspection operates normally?

- A. P2 and P3 only
- B. P5, P6, and P7 only

- C. P1, P2, P3, and P4 only
- D. P2, P3, and P6 only

Answer: D

NEW QUESTION 203

- (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 208

- (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 213

- (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 215

- (Exam Topic 3)

A network engineer entered the `snmp-server user asmith myv7 auth sha cisco priv aes 256 cisc0xxxxxxxxx` command and needs to send SNMP information to a host at 10.255.255.1. Which command achieves this goal?

- A. `snmp-server host inside 10.255.255.1 version 3 myv7`
- B. `snmp-server host inside 10.255.255.1 snmpv3 myv7`
- C. `snmp-server host inside 10.255.255.1 version 3 asmith`
- D. `snmp-server host inside 10.255.255.1 snmpv3 asmith`

Answer: C

NEW QUESTION 217

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 222

- (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 224

- (Exam Topic 3)

Which Cisco solution integrates Encrypted Traffic Analytics to perform enhanced visibility, promote compliance, shorten response times, and provide administrators with the information needed to provide educated and automated decisions to secure the environment?

- A. Cisco DNA Center
- B. Cisco SDN
- C. Cisco ISE
- D. Cisco Security Compliance Solution

Answer: D

NEW QUESTION 226

- (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 231

- (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 233

- (Exam Topic 3)

An engineer is configuring device-hardening on a router in order to prevent credentials from being seen if the router configuration was compromised. Which command should be used?

- A. service password-encryption
- B. username <username> privilege 15 password <password>
- C. service password-recovery
- D. username < username> password <password>

Answer: A

NEW QUESTION 236

- (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 237

- (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 241

- (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 245

- (Exam Topic 3)

Which ESA implementation method segregates inbound and outbound email?

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

Answer: D

NEW QUESTION 246

- (Exam Topic 3)

How does Cisco AMP for Endpoints provide next-generation protection?

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

Answer: B

NEW QUESTION 251

- (Exam Topic 3)

Which statement describes a serverless application?

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

Answer: B

NEW QUESTION 252

- (Exam Topic 3)

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

- A. DSCP value
- B. Source interface
- C. Exporter name
- D. Exporter description

Answer: C

Explanation:

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

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 257

- (Exam Topic 2)

An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 261

- (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 264

- (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 265

- (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 268

- (Exam Topic 2)

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

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

Answer: BE

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mtbook/sec-pk

NEW QUESTION 273

- (Exam Topic 2)

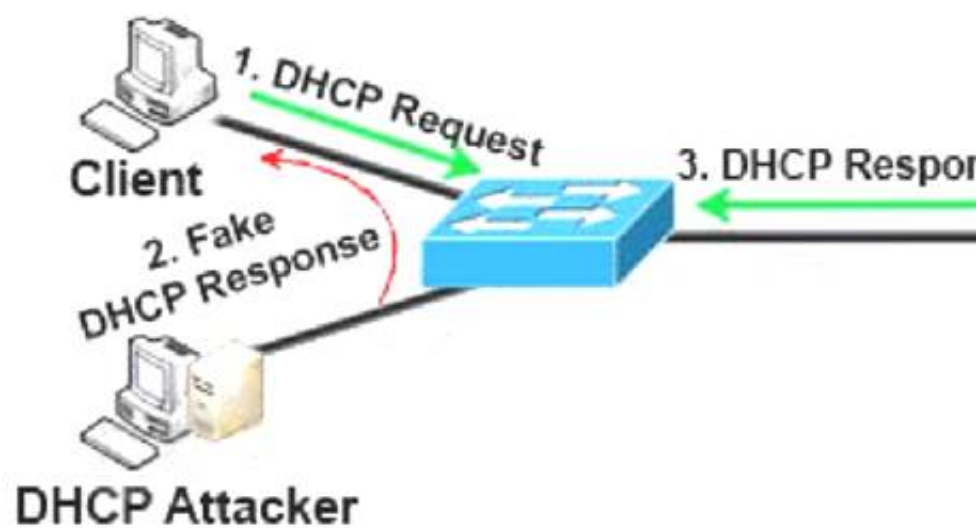
An administrator is configuring a DHCP server to better secure their environment. They need to be able to ratelimit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?

- A. Set a trusted interface for the DHCP server
- B. Set the DHCP snooping bit to 1
- C. Add entries in the DHCP snooping database
- D. Enable ARP inspection for the required VLAN

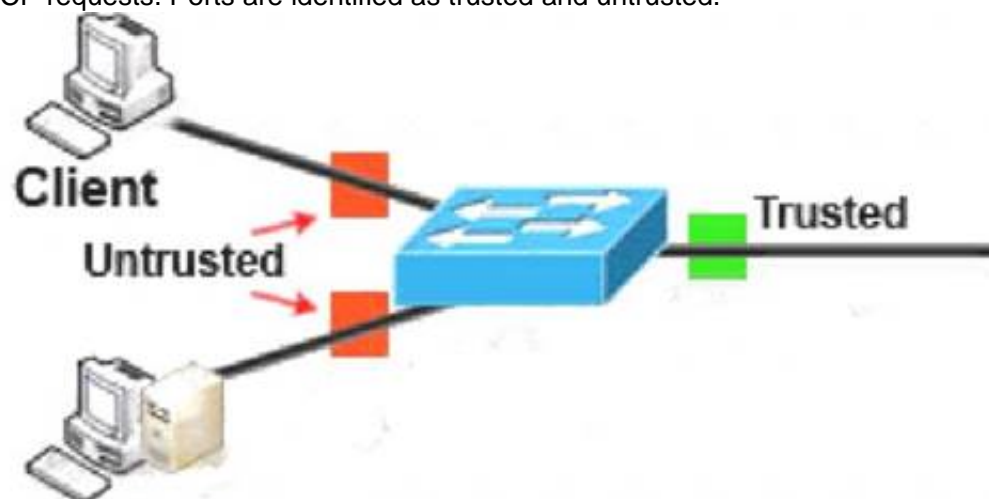
Answer: A

Explanation:

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



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



DHCP Attacker

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

NEW QUESTION 276

- (Exam Topic 2)

What is the function of SDN southbound API protocols?

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

Answer: B

Explanation:

Reference: <https://www.ciscopress.com/articles/article.asp?p=3004581&seqNum=2>

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

NEW QUESTION 280

- (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 281

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 283

- (Exam Topic 2)

Which algorithm provides asymmetric encryption?

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

Answer: C

NEW QUESTION 287

- (Exam Topic 2)

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

- A. LDAP injection
- B. man-in-the-middle
- C. cross-site scripting
- D. insecure API

Answer: B

NEW QUESTION 292

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 294

- (Exam Topic 2)

What is a benefit of conducting device compliance checks?

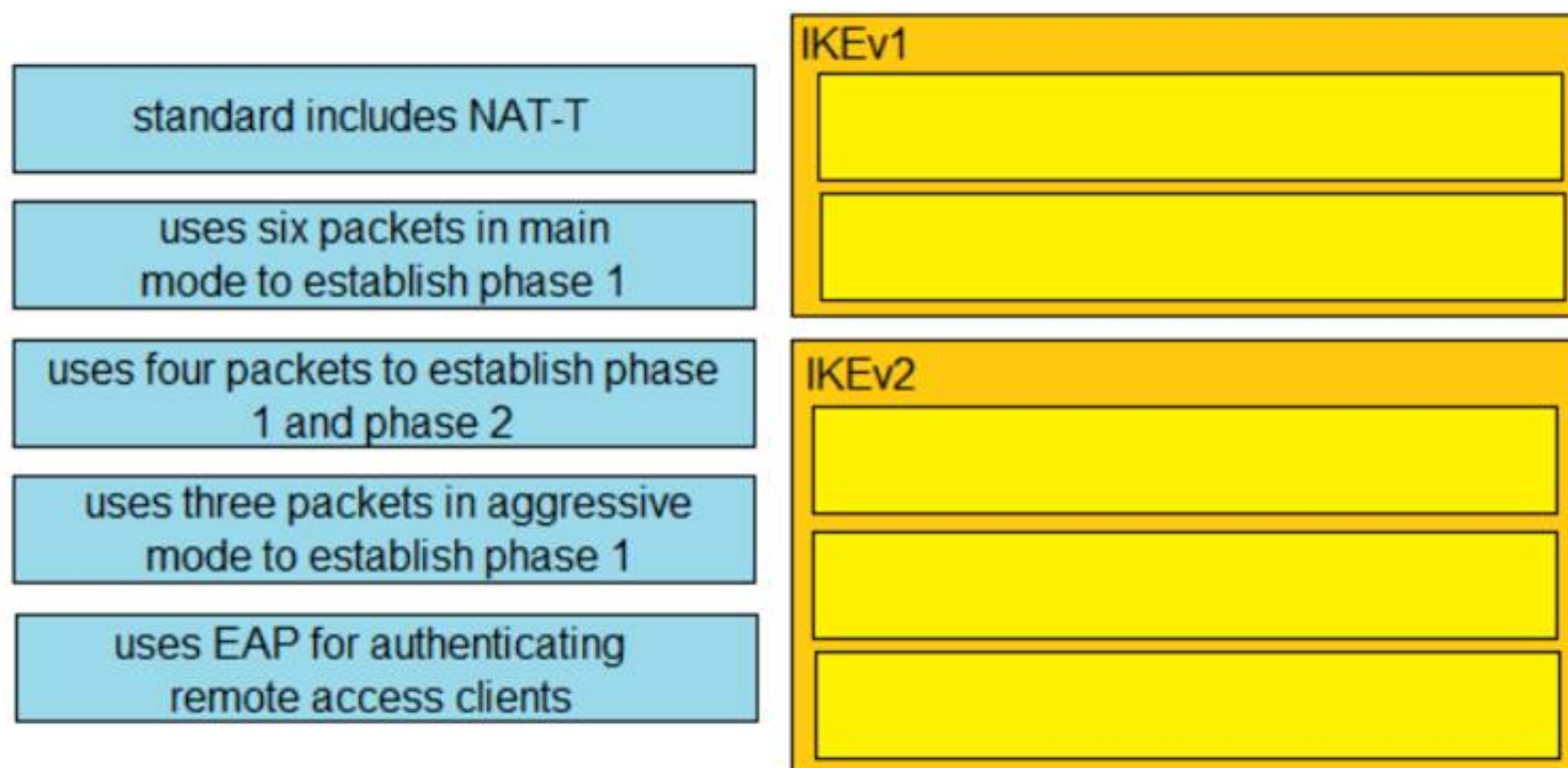
- A. It indicates what type of operating system is connecting to the network.
- B. It validates if anti-virus software is installed.
- C. It scans endpoints to determine if malicious activity is taking place.
- D. It detects email phishing attacks.

Answer: B

NEW QUESTION 295

- (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 296

- (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 304

- (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 306

- (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 307

- (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 311

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 316

- (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 319

- (Exam Topic 2)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 324

- (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 327

- (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 330

- (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

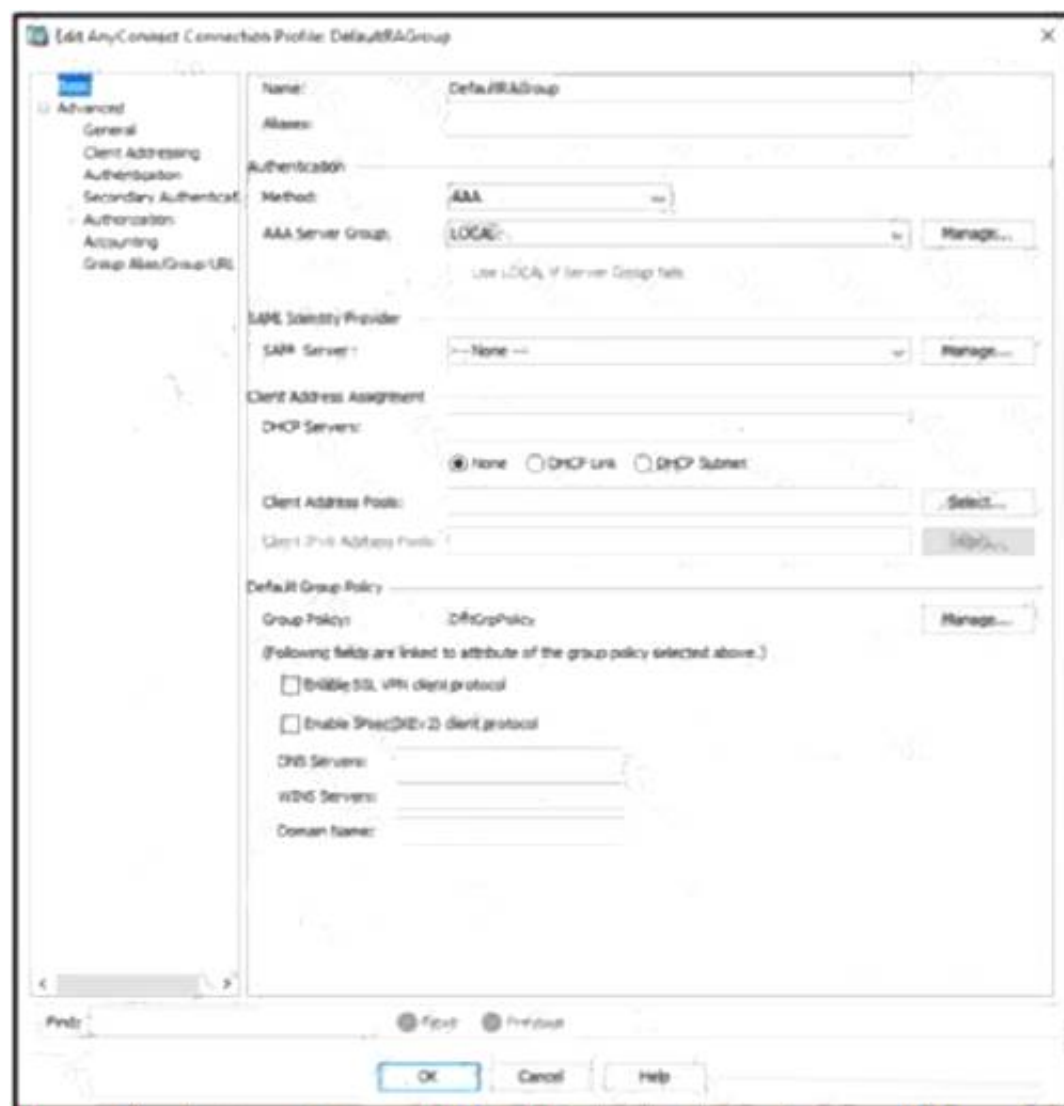
Explanation:

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 331

- (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 332

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 334

- (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 338

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 340

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 341

- (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 346

- (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 347

- (Exam Topic 2)

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

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

Answer: BE

Explanation:

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

NEW QUESTION 348

- (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 349

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Configure a Crypto ISAKMP Key

In order to configure a preshared

configuration mode:

authentication key, enter thcrypto isakmp key

command in global

crypto isakmp key cisco123 address 172.16.1.1

<https://community.cisco.com/t5/vpn/isakmp-with-0-0-0-0-dmvpn/td-p/4312380>

It is a bad practice but it is valid. 172.16.0.0/16 the full range will be accepted as possible PEER

[https://www.examtopycs.com/discussions/cisco/view/46191-exam-350-701-topic-1-question-71-discussion/#:~:t=Testing without a netmask shows that command interpretation has a preference for /16 and /24.](https://www.examtopycs.com/discussions/cisco/view/46191-exam-350-701-topic-1-question-71-discussion/#:~:t=Testing%20without%20a%20netmask%20shows%20that%20command%20interpretation%20has%20a%20preference%20for%20%2F16%20and%20%2F24.)

CSR-1(config)#crypto isakmp key cisco123 address 172.16.0.0

CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.0.0 [255.255.0.0] cisco123

CSR-1(config)#no crypto isakmp key cisco123 address 172.16.0.0 CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.0 CSR-1(config)#do show crypto isakmp key | i cisco

default 172.16.1.0 [255.255.255.0] cisco123

CSR-1(config)#no crypto isakmp key cisco123 address 172.16.1.0 CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.128

CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.1.128 cisco123 CSR-1(config)#

NEW QUESTION 354

- (Exam Topic 1)

Refer to the exhibit.

```
Sysauthcontrol          Enabled
Dot1x Protocol Version      3

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

Which command was used to display this output?

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

Answer: A

NEW QUESTION 359

- (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 362

- (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 367

- (Exam Topic 1)

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

- A. They alert administrators when critical events occur.
- B. They highlight known and suspected malicious IP addresses in reports.
- C. They correlate data about intrusions and vulnerability.
- D. They identify data that the ASA sends to the Firepower module.

Answer: C

NEW QUESTION 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 376

- (Exam Topic 1)

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

- A. Enable IP Layer enforcement.
- B. Activate the Advanced Malware Protection license
- C. Activate SSL decryption.
- D. Enable Intelligent Proxy.

Answer: D

NEW QUESTION 380

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 382

- (Exam Topic 1)

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

- A. Windows service
- B. computer identity
- C. user identity
- D. Windows firewall
- E. default browser

Answer: AD

NEW QUESTION 384

- (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 389

- (Exam Topic 1)

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

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

Answer: CD

Explanation:

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

NEW QUESTION 390

- (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 395

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 398

- (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 401

- (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 405

- (Exam Topic 1)

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

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

Answer: A

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_A

NEW QUESTION 409

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 411

- (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 414

- (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 419

- (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 423

- (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 427

- (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 428

- (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 430

- (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 435

- (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 439

- (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 441

- (Exam Topic 1)

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

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

Answer: CE

NEW QUESTION 445

- (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 448

- (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 449

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 450

- (Exam Topic 1)

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

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

Answer: AD

Explanation:

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

NEW QUESTION 455

- (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 457

- (Exam Topic 1)

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

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

Answer: BE

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide/v60/Apply.html> uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

NEW QUESTION 460

- (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 465

- (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 469

- (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 473

- (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 476

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 478

- (Exam Topic 1)

An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA. Which Cisco ASA command must be used?

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

Answer: A

Explanation:

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

NEW QUESTION 480

- (Exam Topic 1)

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

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

Answer: AE

NEW QUESTION 481

- (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 ransomware 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

Cancel

NEW QUESTION 484

- (Exam Topic 1)

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

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

Answer: BD

Explanation:

Reference:

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

NEW QUESTION 488

- (Exam Topic 1)

Which Cisco AMP file disposition valid?

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

Answer: B

NEW QUESTION 493

- (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 495

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 499

- (Exam Topic 1)

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

- A. interpacket variation
- B. software package variation
- C. flow insight variation
- D. process details variation

Answer: A

Explanation:

Reference: https://www.cisco.com/c/dam/global/en_uk/products/switches/cisco_nexus_9300_ex_platform_switches_white_

NEW QUESTION 501

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 505

- (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 509

- (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 513

- (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 518

- (Exam Topic 1)

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

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

Answer: A

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.h> BVI interface is not used for management purpose. But we can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA.

NEW QUESTION 521

- (Exam Topic 1)

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

- A. show authorization status
- B. show authen sess int gi0/1
- C. show connection status gi0/1
- D. show ver gi0/1

Answer: B

NEW QUESTION 524

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 529

- (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 532

- (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 533

- (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 535

- (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 538

- (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 541

- (Exam Topic 1)
What is a difference between FlexVPN and DMVPN?

- A. DMVPN uses IKEv1 or IKEv2, FlexVPN only uses IKEv1
- B. DMVPN uses only IKEv1 FlexVPN uses only IKEv2
- C. FlexVPN uses IKEv2, DMVPN uses IKEv1 or IKEv2
- D. FlexVPN uses IKEv1 or IKEv2, DMVPN uses only IKEv2

Answer: C

NEW QUESTION 544

- (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 548

- (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 551

- (Exam Topic 1)

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

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

Answer: AD

NEW QUESTION 553

- (Exam Topic 1)

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

- A. RBAC
- B. ETHOS detection engine
- C. SPERO detection engine
- D. TETRA detection engine

Answer: B

NEW QUESTION 554

- (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 556

- (Exam Topic 1)

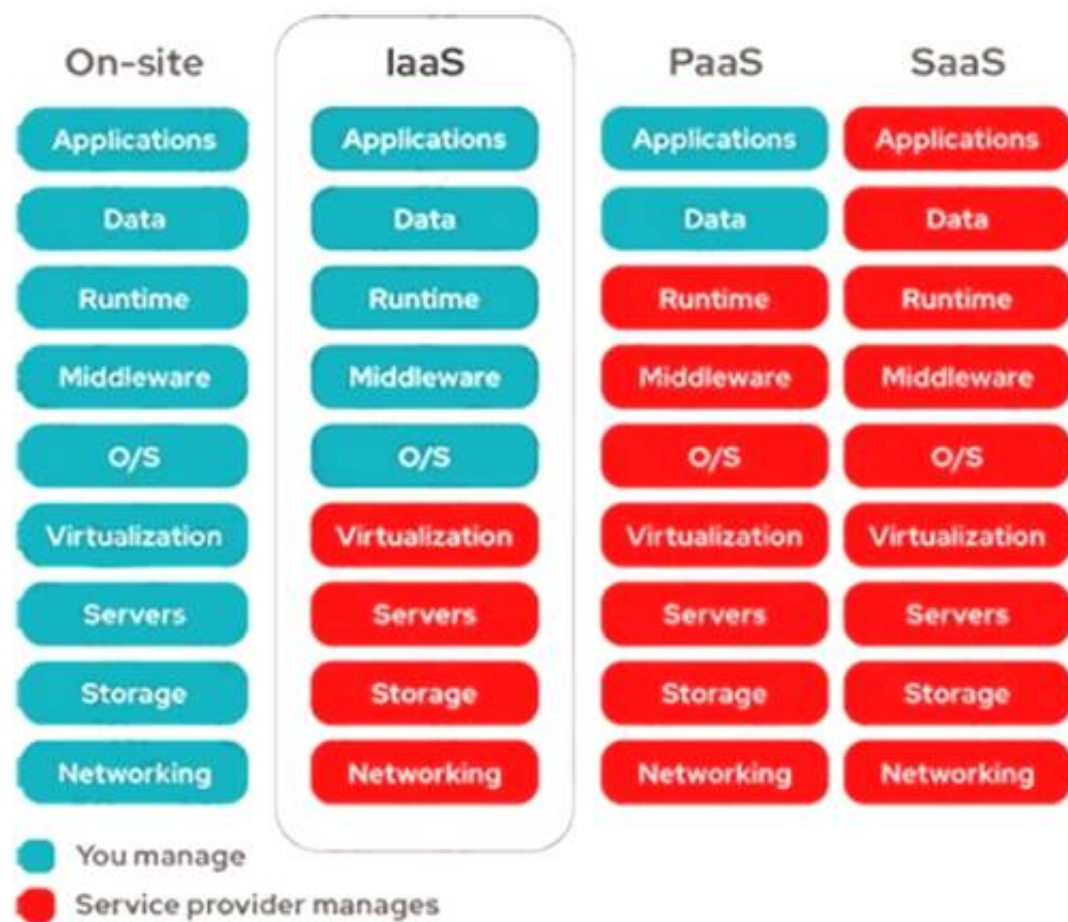
In which cloud services model is the tenant responsible for virtual machine OS patching?

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

Answer: A

Explanation:

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



NEW QUESTION 560

- (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 564

- (Exam Topic 1)

What is a characteristic of Dynamic ARP Inspection?

- A. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCP snooping binding database.
- B. In a typical network, make all ports as trusted except for the ports connecting to switches, which are untrusted
- C. DAI associates a trust state with each switch.
- D. DAI intercepts all ARP requests and responses on trusted ports only.

Answer: A

NEW QUESTION 565

- (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 570

- (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 572

- (Exam Topic 1)

How is ICMP used as an exfiltration technique?

- A. by flooding the destination host with unreachable packets
- B. by sending large numbers of ICMP packets with a targeted host's source IP address using an IP broadcast address
- C. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host
- D. by overwhelming a targeted host with ICMP echo-request packets

Answer: C

NEW QUESTION 574

- (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 577

- (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 578

- (Exam Topic 1)

What is the function of Cisco Cloudlock for data security?

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

Answer: A

NEW QUESTION 583

- (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 586

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 590

- (Exam Topic 1)

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

- A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS
- B. Cisco FTDv with one management interface and two traffic interfaces configured
- C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises
- D. Cisco FTDv with two management interfaces and one traffic interface configured
- E. Cisco FTDv configured in routed mode and IPv6 configured

Answer: AC

NEW QUESTION 593

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 596

- (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 599

- (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 600

- (Exam Topic 3)

Which feature enables a Cisco ISR to use the default bypass list automatically for web filtering?

- A. filters
- B. group key
- C. company key
- D. connector

Answer: D

NEW QUESTION 602

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 603

- (Exam Topic 3)

Which security solution uses NetFlow to provide visibility across the network, data center, branch offices, and cloud?

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

Answer: B

NEW QUESTION 608

- (Exam Topic 3)

An engineer is trying to decide whether to use Cisco Umbrella, Cisco CloudLock, Cisco Stealthwatch, or Cisco AppDynamics Cloud Monitoring for visibility into data transfers as well as protection against data exfiltration Which solution best meets these requirements?

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

Answer: D

NEW QUESTION 609

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 611

- (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 614

- (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 619

- (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 620

- (Exam Topic 3)

Which Cisco platform onboards the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing the endpoint to gain network access?

- A. Cisco ISE

- B. Cisco NAC
- C. Cisco TACACS+
- D. Cisco WSA

Answer: A

NEW QUESTION 622

- (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 624

- (Exam Topic 3)

Which system performs compliance checks and remote wiping?

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

Answer: A

NEW QUESTION 626

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 627

- (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 632

- (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 636

- (Exam Topic 3)

Which technology provides a combination of endpoint protection endpoint detection, and response?

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

Answer: A

NEW QUESTION 639

- (Exam Topic 3)

What is a feature of NetFlow Secure Event Logging?

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

Answer: A

NEW QUESTION 644

- (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 647

- (Exam Topic 3)

Refer to the exhibit.



Consider that any feature of DNS requests, such as the length off the domain name and the number of subdomains, can be used to construct models of expected behavior to which observed values can be compared. Which type of malicious attack are these values associated with?

- A. Spectre Worm
- B. Eternal Blue Windows
- C. Heartbleed SSL Bug
- D. W32/AutoRun worm

Answer: D

NEW QUESTION 650

- (Exam Topic 3)

What is the target in a phishing attack?

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

Answer: D

NEW QUESTION 651

- (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 652

- (Exam Topic 3)

When NetFlow is applied to an interface, which component creates the flow monitor cache that is used to collect traffic based on the key and nonkey fields in the

configured record?

- A. records
- B. flow exporter
- C. flow sampler
- D. flow monitor

Answer: D

NEW QUESTION 656

- (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 657

- (Exam Topic 3)

Which type of data does the Cisco Stealthwatch system collect and analyze from routers, switches, and firewalls?

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

Answer: D

NEW QUESTION 658

- (Exam Topic 3)

Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)

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

Answer: AB

NEW QUESTION 659

- (Exam Topic 3)

Drag and drop the cryptographic algorithms for IPsec from the left onto the cryptographic processes on the right.

esp-3des	Authentication
esp-aes-256	
esp-md5-hmac	Encryption
esp-sha-hmac	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Diagram Description automatically generated

NEW QUESTION 661

- (Exam Topic 3)

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

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

Answer: A

Explanation:

Reference: <https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf>

NEW QUESTION 666

- (Exam Topic 3)

Which open source tool does Cisco use to create graphical visualizations of network telemetry on Cisco IOS XE devices?

- A. InfluxDB
- B. Splunk
- C. SNMP
- D. Grafana

Answer: D

NEW QUESTION 667

- (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 670

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 672

- (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 676

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 679

- (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 683

- (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 688

- (Exam Topic 3)

Which feature requires that network telemetry be enabled?

- A. per-interface stats
- B. SNMP trap notification
- C. Layer 2 device discovery
- D. central syslog system

Answer: D

NEW QUESTION 693

- (Exam Topic 3)

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

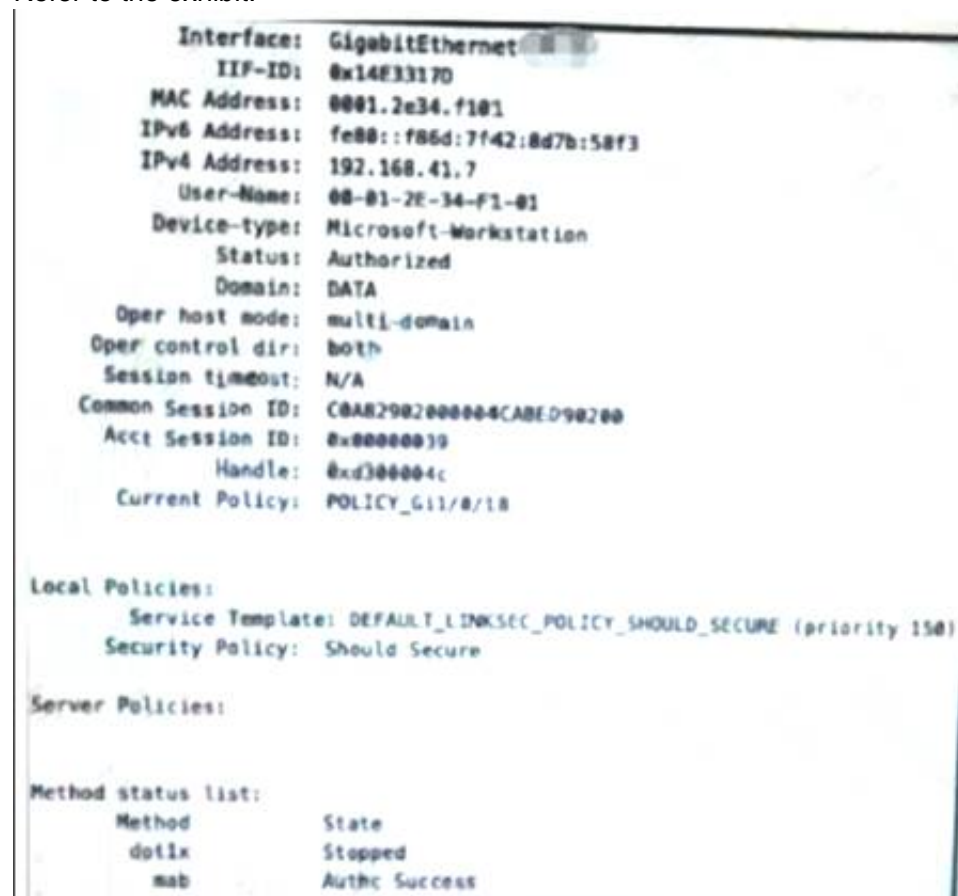
- A. Northbound APIs provide a programmable interface for applications to dynamically configure the network.
- B. Northbound APIs form the interface between the SDN controller and business applications.
- C. OpenFlow is a standardized northbound API protocol.
- D. Northbound APIs use the NETCONF protocol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

Answer: AB

NEW QUESTION 694

- (Exam Topic 3)

Refer to the exhibit.



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

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

Answer: C

NEW QUESTION 696

- (Exam Topic 3)

Which Cisco ASA Platform mode disables the threat detection features except for Advanced Threat Statistics?

- A. cluster
- B. transparent
- C. routed
- D. multiple context

Answer: B

NEW QUESTION 697

- (Exam Topic 3)

Drag and drop the features of Cisco ASA with Firepower from the left onto the benefits on the right.

Full Context Awareness	detection, blocking and remediation to protect the enterprise against targeted malware attacks
NGIPS	policy enforcement based on complete visibility of users and communication between virtual machines
AMP	real-time threat intelligence and security protection
Collective Security Intelligence	threat prevention and mitigation for known and unknown threats

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Full Context Awareness - policy enforcement NGIPS - threat prevention

AMP - real-time

Collective Sec Intel - Detection, blocking an remediation

NEW QUESTION 698

- (Exam Topic 3)

What is the process of performing automated static and dynamic analysis of files against preloaded behavioral indicators for threat analysis?

- A. deep visibility scan
- B. point-in-time checks
- C. advanced sandboxing
- D. advanced scanning

Answer: C

NEW QUESTION 699

- (Exam Topic 3)

Which service allows a user export application usage and performance statistics with Cisco Application Visibility and control?

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

Answer: B

Explanation:

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

NEW QUESTION 701

- (Exam Topic 3)

Which two parameters are used to prevent a data breach in the cloud? (Choose two.)

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

E. antispoofing programs

Answer: AB

NEW QUESTION 702

- (Exam Topic 3)

Which security solution is used for posture assessment of the endpoints in a BYOD solution?

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

Answer: D

NEW QUESTION 703

- (Exam Topic 3)

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

- A. Link Aggregation
- B. Reverse ARP
- C. private VLANs
- D. Dynamic ARP Inspection

Answer: D

NEW QUESTION 704

- (Exam Topic 3)

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

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

Answer: BC

Explanation:

Reference:

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

NEW QUESTION 708

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 713

- (Exam Topic 3)

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


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

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

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

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

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

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

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

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

- A. It allows authentication with TLSv1 SSL protocol
- B. It authenticates to a Cisco ISE with an SSH connection.
- C. It authenticates to a Cisco ISE server using the username of ersad
- D. It lists the LDAP users from the external identity store configured on Cisco ISE

Answer: C

NEW QUESTION 717

- (Exam Topic 3)

What is a benefit of flexible NetFlow records?

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

Answer: D

Explanation:

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

NEW QUESTION 718

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 721

- (Exam Topic 3)

Why should organizations migrate to an MFA strategy for authentication?

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

Answer: A

NEW QUESTION 724

- (Exam Topic 3)

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

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

Answer: D

Explanation:

SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts. The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data. Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc. Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics.

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

NEW QUESTION 725

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 730

- (Exam Topic 3)

A large organization wants to deploy a security appliance in the public cloud to form a site-to-site VPN and link the public cloud environment to the private cloud in the headquarters data center. Which Cisco security appliance meets these requirements?

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

Answer: B

NEW QUESTION 735

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 738

- (Exam Topic 3)

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

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

Answer: CD

NEW QUESTION 743

- (Exam Topic 3)

Which endpoint protection and detection feature performs correlation of telemetry, files, and intrusion events that are flagged as possible active breaches?

- A. retrospective detection
- B. indication of compromise
- C. file trajectory
- D. elastic search

Answer: B

NEW QUESTION 748

- (Exam Topic 3)

Which solution detects threats across a private network, public clouds, and encrypted traffic?

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

Answer: A

NEW QUESTION 753

.....

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