



Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

NEW QUESTION 1

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 2

- (Exam Topic 3)

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

- A. Configure transparent traffic redirection using WCCP in the Cisco WSA and on the network device
- B. Configure active traffic redirection using WPAD in the Cisco WSA and on the network device
- C. Use the Layer 4 setting in the Cisco WSA to receive explicit forward requests from the network device
- D. Use PAC keys to allow only the required network devices to send the traffic to the Cisco WSA

Answer: A

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_Management_of_Endpoint_IoC.pdf

NEW QUESTION 5

- (Exam Topic 3)

Which two capabilities does an MDM provide? (Choose two.)

- A. delivery of network malware reports to an inbox in a schedule
- B. unified management of mobile devices, Macs, and PCs from a centralized dashboard
- C. enforcement of device security policies from a centralized dashboard
- D. manual identification and classification of client devices
- E. unified management of Android and Apple devices from a centralized dashboard

Answer: BC

NEW QUESTION 6

- (Exam Topic 3)

Which benefit does DMVPN provide over GETVPN?

- A. DMVPN supports QoS, multicast, and routing, and GETVPN supports only QoS.
- B. DMVPN is a tunnel-less VPN, and GETVPN is tunnel-based.
- C. DMVPN supports non-IP protocols, and GETVPN supports only IP protocols.
- D. DMVPN can be used over the public Internet, and GETVPN requires a private network.

Answer: D

NEW QUESTION 7

- (Exam Topic 3)

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

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

Answer: D

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 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 10

- (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 11

- (Exam Topic 3)

What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.) The eDirectory client must be installed on each client workstation.

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

Answer: AB

Explanation:

➤ Transparently identify users with authentication realms – This option is available when one or more authentication realms are configured to support transparent identification using one of the following authentication servers:

➤ Active Directory – Create an NTLM or Kerberos authentication realm and enable transparent user identification. In addition, you must deploy a separate Active Directory agent such as Cisco's Context Directory Agent. For more information, see Transparent User Identification with Active Directory.

➤ LDAP – Create an LDAP authentication realm configured as an eDirectory, and enable transparent user identification. For more information, see Transparent User Identification with LDAP.

Details:

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGui

NEW QUESTION 15

- (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 18

- (Exam Topic 3)

Which two parameters are used for device compliance checks? (Choose two.)

- A. endpoint protection software version
- B. Windows registry values
- C. DHCP snooping checks
- D. DNS integrity checks
- E. device operating system version

Answer: CE

NEW QUESTION 19

- (Exam Topic 3)

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

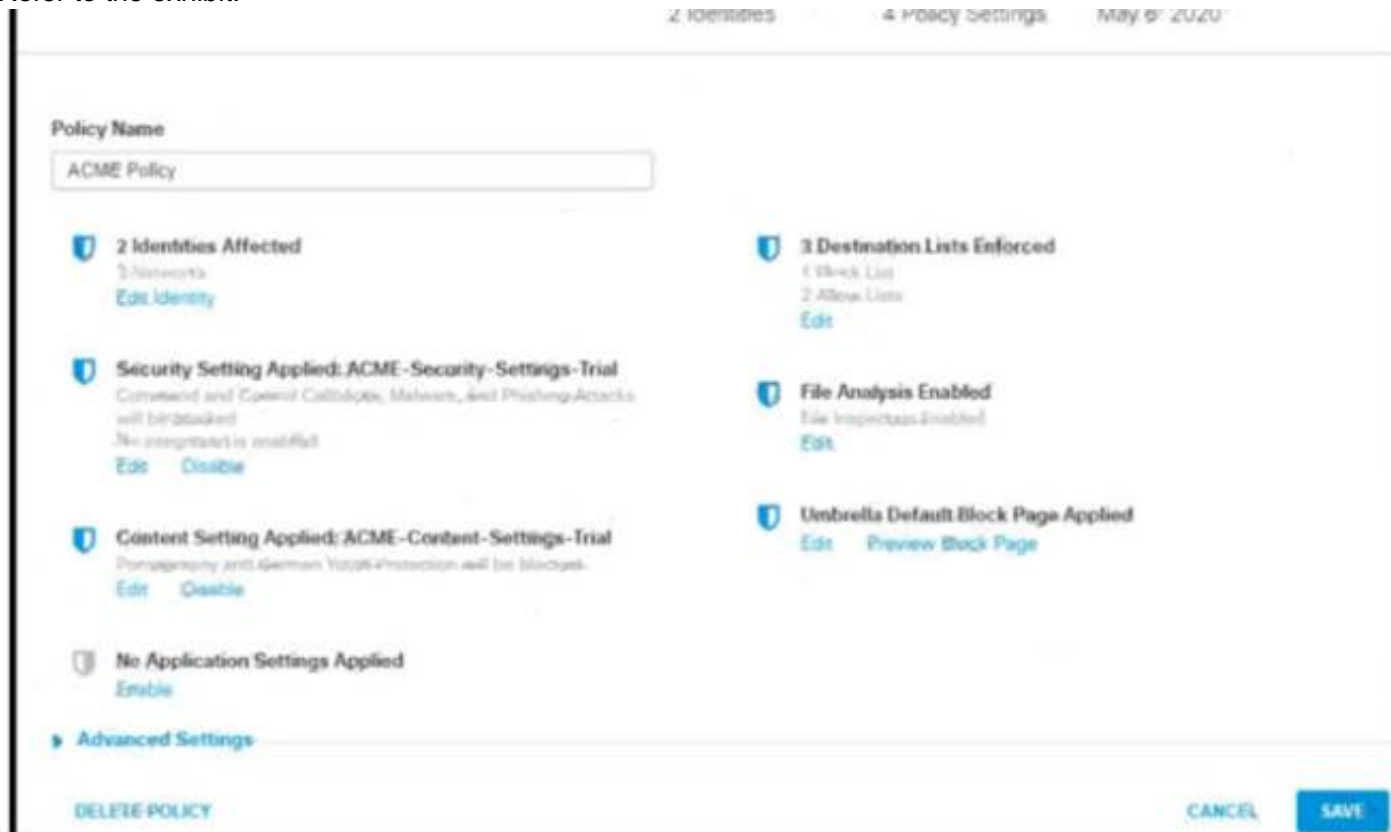
- A. flow-export event-type
- B. policy-map
- C. access-list
- D. flow-export template timeout-rate 15
- E. access-group

Answer: AB

NEW QUESTION 21

- (Exam Topic 3)

Refer to the exhibit.



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

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

Answer: B

NEW QUESTION 23

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 28

- (Exam Topic 3)

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

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

- A. It uses the POST HTTP method to obtain a username and password to be used for authentication.
- B. It uses the POST HTTP method to obtain a token to be used for authentication.
- C. It uses the GET HTTP method to obtain a token to be used for authentication.
- D. It uses the GET HTTP method to obtain a username and password to be used for authentication

Answer: B

NEW QUESTION 31

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 32

- (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 35

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 37

- (Exam Topic 3)

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

- A. SQL injection is a hacking method used to attack SQL databases, whereas XSS attacks can exist in many different types of applications
- B. XSS is a hacking method used to attack SQL databases, whereas SQL injection attacks can exist in many different types of applications

- C. SQL injection attacks are used to steal information from databases whereas XSS attacks are used to redirect users to websites where attackers can steal data from them
- D. XSS attacks are used to steal information from databases whereas SQL injection attacks are used to redirect users to websites where attackers can steal data from them

Answer: C

Explanation:

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

NEW QUESTION 42

- (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 46

- (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 49

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 54

- (Exam Topic 3)

What is a description of microsegmentation?

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

Answer: B

NEW QUESTION 55

- (Exam Topic 3)

Which MDM configuration provides scalability?

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

Answer: C

NEW QUESTION 60

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 62

- (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 64

- (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 66

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 68

- (Exam Topic 3)

Why is it important for the organization to have an endpoint patching strategy?

- A. so the organization can identify endpoint vulnerabilities
- B. so the internal PSIRT organization is aware of the latest bugs
- C. so the network administrator is notified when an existing bug is encountered
- D. so the latest security fixes are installed on the endpoints

Answer: D

NEW QUESTION 69

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 74

- (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 77

- (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 80

- (Exam Topic 3)

Which two authentication protocols are supported by the Cisco WSA? (Choose two.)

- A. WCCP
- B. NTLM
- C. TLS
- D. SSL
- E. LDAP

Answer: BE

NEW QUESTION 82

- (Exam Topic 3)

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

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

Answer: B

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp3880782430>The command “crypto enrollment peer address” is not valid either. The command “crypto ca identity ...” is only used to declare a trusted CA for the router and puts you in the caidentity configuration mode. Also it should be followed by a name, not an IP address. For example: “crypto caidentity CA-Server” -> Answer A is not correct. Only answer B is the best choice left.

NEW QUESTION 83

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 85

- (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 88

- (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 90

- (Exam Topic 3)

Which encryption algorithm provides highly secure VPN communications?

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

Answer: B

NEW QUESTION 91

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 96

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 101

- (Exam Topic 3)

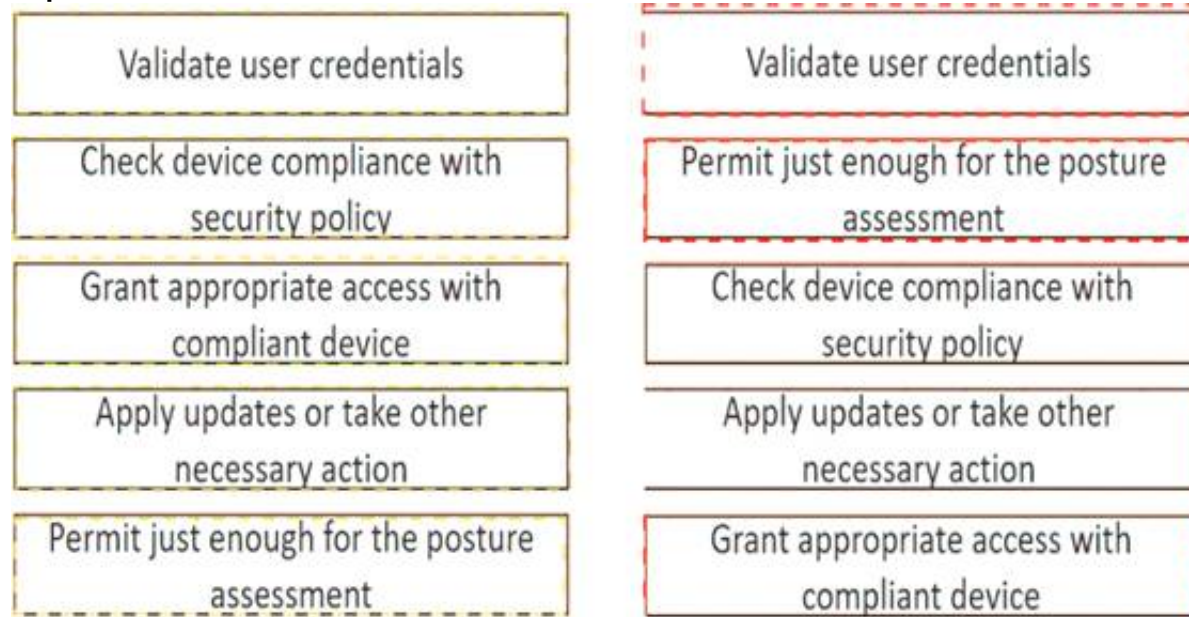
Drag and drop the posture assessment flow actions from the left into a sequence on the right.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 104

- (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 106

- (Exam Topic 3)

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

- A. NAT-T is supported in IKEv1 but not in IKEv2.
- B. With IKEv1, when using aggressive mode, the initiator and responder identities are passed cleartext
- C. With IKEv1, mode negotiates faster than main mode
- D. IKEv1 uses EAP authentication
- E. IKEv1 conversations are initiated by the IKE_SA_INIT message

Answer: CE

NEW QUESTION 109

- (Exam Topic 3)

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

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

Answer: CE

NEW QUESTION 113

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 116

- (Exam Topic 3)

Which Cisco ISE feature helps to detect missing patches and helps with remediation?

- A. posture assessment

- B. profiling policy
- C. authentication policy
- D. enabling probes

Answer: B

NEW QUESTION 119

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 123

- (Exam Topic 3)

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

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

Answer: C

Explanation:

"configure INTRUSION RULES for DNP3" -> Documentation states, that enabling INTRUSION RULES is mandatory for CIP to work + required preprocessors (in Network Access Policy - NAP) will be enabled automatically:

"If you want the CIP preprocessor rules listed in the following table to generate events, you MUST enable them. See Setting Intrusion Rule States for information on enabling rules."

"If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings, although the preprocessor remains disabled in the web interface for the corresponding network analysis policy."

[1]
<https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada>

NEW QUESTION 124

- (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](https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html#:~:text=Pow%20Cisco%20Advanced%20Malware%20Protection%20(AMP)%20for%20endpoints%20can%20be%20seen%20as%20a%20replacement%20for%20the%20traditional%20antivirus%20solution.%20It%20is%20a%20next%20generation%20cloud%20delivered%20endpoint%20protection%20platform%20(EPP)%2C%20and%20advanced%20endpoint%20detection%20and%20response%20(EDR).%20Providing%20Protection%20%E2%80%93%20Detection%20Response) 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 128

- (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 131

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 135

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 138

- (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 143

- (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 148

- (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 152

- (Exam Topic 3)

Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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

- A. imports requests
- B. HTTP authorization

- C. HTTP authentication
- D. plays dent ID

Answer: C

NEW QUESTION 153

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 157

- (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 158

- (Exam Topic 3)

An administrator is configuring N I P on Cisco ASA via ASDM and needs to ensure that rogue NTP servers cannot insert themselves as the authoritative time source Which two steps must be taken to accomplish this task? (Choose two)

- A. Specify the NTP version
- B. Configure the NTP stratum
- C. Set the authentication key
- D. Choose the interface for syncing to the NTP server
- E. Set the NTP DNS hostname

Answer: CD

NEW QUESTION 163

- (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 168

- (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 172

- (Exam Topic 3)

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

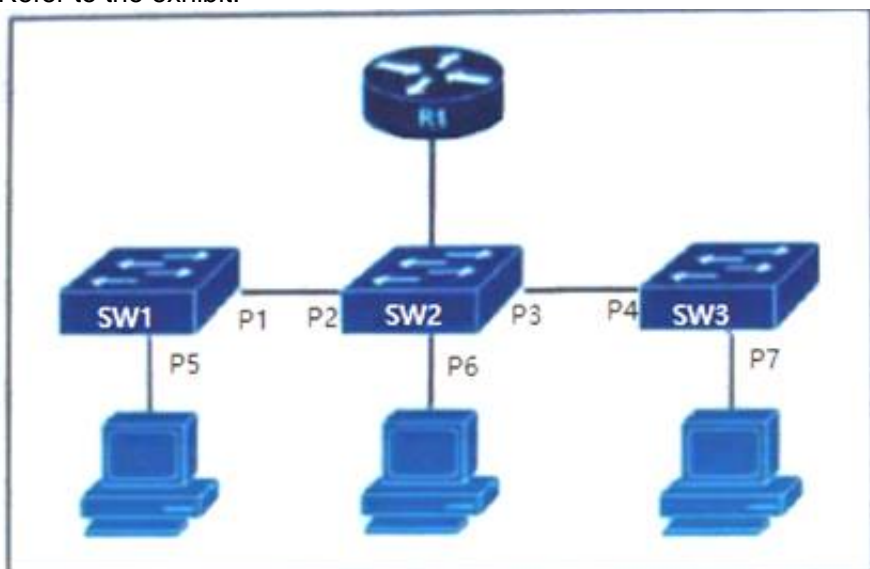
- A. by specifying blocked domains in the policy settings
- B. by specifying the websites in a custom blocked category
- C. by adding the websites to a blocked type destination list
- D. by adding the website IP addresses to the Cisco Umbrella blocklist

Answer: C

NEW QUESTION 175

- (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 177

- (Exam Topic 3)

Which endpoint solution protects a user from a phishing attack?

- A. Cisco Identity Services Engine
- B. Cisco AnyConnect with ISE Posture module
- C. Cisco AnyConnect with Network Access Manager module
- D. Cisco AnyConnect with Umbrella Roaming Security module

Answer: D

NEW QUESTION 180

- (Exam Topic 3)

What is an advantage of network telemetry over SNMP pulls?

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

Answer: D

NEW QUESTION 182

- (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 183

- (Exam Topic 3)

Which standard is used to automate exchanging cyber threat information?

- A. TAXII
- B. MITRE
- C. IoC
- D. STIX

Answer: A

NEW QUESTION 184

- (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 188

- (Exam Topic 3)

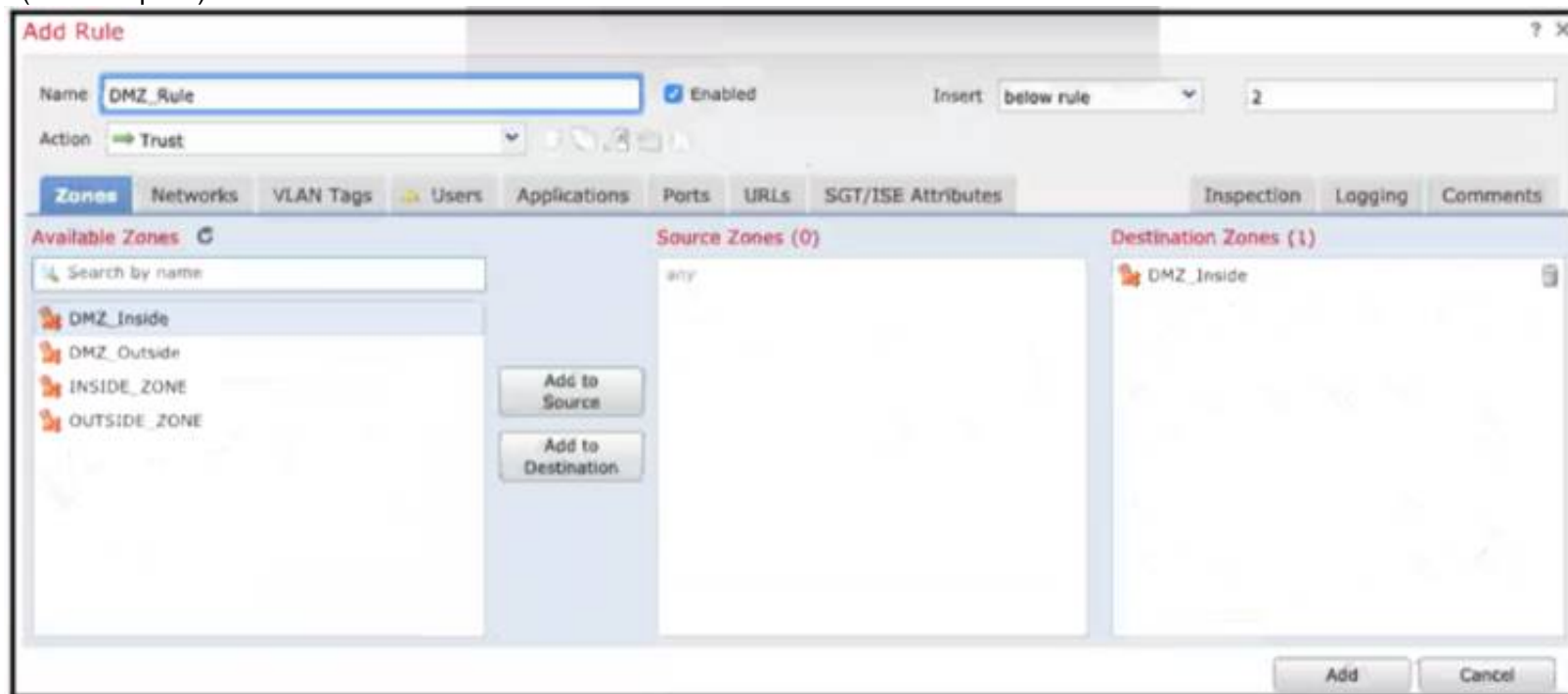
In which scenario is endpoint-based security the solution?

- 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 192

- (Exam Topic 3)



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

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

Answer: A

NEW QUESTION 197

- (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 202

- (Exam Topic 3)

Which type of data exfiltration technique encodes data in outbound DNS requests to specific servers and can be stopped by Cisco Umbrella?

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

Answer: A

NEW QUESTION 204

- (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 206

- (Exam Topic 3)

Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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

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

Answer: D

NEW QUESTION 209

- (Exam Topic 3)

What are two workloaded security models? (Choose two)

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

Answer: CD

NEW QUESTION 212

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Reference:

<https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45-738565.pdf>

NEW QUESTION 213

- (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 214

- (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 219

- (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 221

- (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 224

- (Exam Topic 2)

Refer to the exhibit.


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

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

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

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 226

- (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 helps us communicate with data plane (not control plane) applications

NEW QUESTION 229

- (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 232

- (Exam Topic 2)

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

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

Answer: BC

Explanation:

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

NEW QUESTION 235

- (Exam Topic 2)

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

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

Answer: CE

Explanation:

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

NEW QUESTION 240

- (Exam Topic 2)

Which algorithm provides asymmetric encryption?

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

Answer: C

NEW QUESTION 245

- (Exam Topic 2)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 249

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 254

- (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 256

- (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 257

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 261

- (Exam Topic 2)

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

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

IKEv2

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated with low confidence

NEW QUESTION 265

- (Exam Topic 2)

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

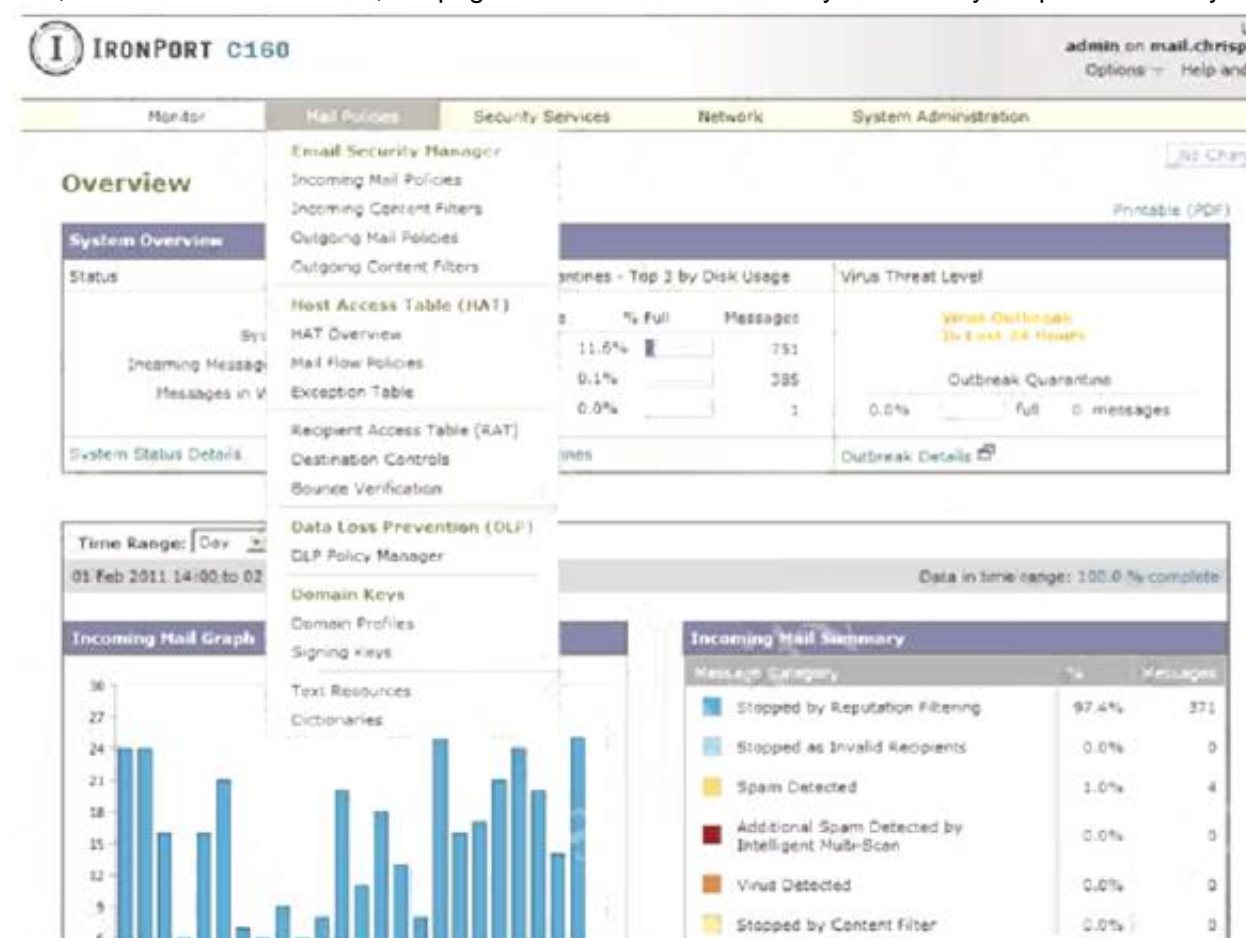
What must be configured to accomplish this?

- A. Configure the Cisco WSA to modify policies based on the traffic seen
- B. Configure the Cisco ESA to receive real-time updates from Talos
- C. Configure the Cisco WSA to receive real-time updates from Talos
- D. Configure the Cisco ESA to modify policies based on the traffic seen

Answer: D

Explanation:

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



NEW QUESTION 267

- (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 268

- (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 273

- (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 274

- (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 279

- (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 284

- (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 285

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access>

NEW QUESTION 286

- (Exam Topic 2)

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

- A. It allows multiple security products to share information and work together to enhance security posture in the network.
- B. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.
- C. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.
- D. It integrates with third-party products to provide better visibility throughout the network.
- E. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).

Answer: CE

Explanation:

Reference:

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-witheasy-connect-c>

NEW QUESTION 290

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Reference: <https://docs.umbrella.com/cloudlock-documentation/docs/endpoints>Note:+ Security information and event management (SIEM) platforms collect log and event data from securitysystems, networks and computers, and turn it into actionable security insights.+ An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when acondition of an alerting policy has been met.

NEW QUESTION 294

- (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 298

- (Exam Topic 2)

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

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

Answer: B

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nse1.pdf>

NEW QUESTION 301

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 302

- (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 304

- (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 306

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 310

- (Exam Topic 2)

Refer to the exhibit.

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

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

Answer: D

Explanation:

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

NEW QUESTION 311

- (Exam Topic 2)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, chat or text message Description automatically generated

NEW QUESTION 315

- (Exam Topic 1)

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

- A. AES is less secure than 3DES.
- B. AES is more secure than 3DES.
- C. AES can use a 168-bit key for encryption.
- D. AES can use a 256-bit key for encryption.

E. AES encrypts and decrypts a key three times in sequence.

Answer: BD

NEW QUESTION 319

- (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 the crypto 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.examtips.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.examtips.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 320

- (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 321

- (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 323

- (Exam Topic 1)

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

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

Answer: AD

Explanation:

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

NEW QUESTION 324

- (Exam Topic 1)

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

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

Answer: BC

Explanation:

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

NEW QUESTION 327

- (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 330

- (Exam Topic 1)

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

- A. RADIUS
- B. TACACS+
- C. DHCP
- D. sFlow
- E. SMTP

Answer: AC

NEW QUESTION 333

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Reference:

<https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector>

NEW QUESTION 335

- (Exam Topic 1)

Refer to the exhibit.

snmp-server group SNMP v3 auth access 15

What does the number 15 represent in this configuration?

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

Answer: B

Explanation:

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

NEW QUESTION 338

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 342

- (Exam Topic 1)

Refer to the exhibit.

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

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

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

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

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

service-policy inside-policy global
```

What is a result of the configuration?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 344

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 346

- (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 347

- (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 349

- (Exam Topic 1)

What are two rootkit types? (Choose two)

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

Answer: CD

Explanation:

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

NEW QUESTION 352

- (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 354

- (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 356

- (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 357

- (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 362

- (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 366

- (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 367

- (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 371

- (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 375

- (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 377

- (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-guidev60/Applic> uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

NEW QUESTION 379

- (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 380

- (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 385

- (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 388

- (Exam Topic 1)

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

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

Answer: BD

Explanation:

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

NEW QUESTION 392

- (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 394

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 397

- (Exam Topic 1)

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

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

Answer: CE

NEW QUESTION 401

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 403

- (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 404

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 406

- (Exam Topic 1)

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

- A. transparent
- B. redirection

- C. forward
- D. proxy gateway

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesign>

NEW QUESTION 410

- (Exam Topic 1)

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

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

Answer: CD

Explanation:

Reference:

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

NEW QUESTION 414

- (Exam Topic 1)

On which part of the IT environment does DevSecOps focus?

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

Answer: A

NEW QUESTION 419

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 421

- (Exam Topic 1)

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

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

Answer: D

Explanation:

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's allotted memory space. This happens quite frequently in the case of arrays.

NEW QUESTION 425

- (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 426

- (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 427

- (Exam Topic 1)

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

- A. by using the Application Programming Interface to fetch the logs
- B. by sending logs via syslog to an on-premises or cloud-based syslog server
- C. by the system administrator downloading the logs from the Cisco Umbrella web portal
- D. by being configured to send logs to a self-managed AWS S3 bucket

Answer: D

Explanation:

Reference: <https://docs.umbrella.com/deployment-umbrella/docs/manage-logs>

NEW QUESTION 432

- (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 434

- (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 435

- (Exam Topic 1)

Which command enables 802.1X globally on a Cisco switch?

- A. dot1x system-auth-control
- B. dot1x pae authenticator
- C. authentication port-control aut

D. aaa new-model

Answer: A

NEW QUESTION 437

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 442

- (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 445

- (Exam Topic 1)

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

What must the administrator implement to ensure that all devices are compliant before they are allowed on the network?

- A. Cisco Identity Services Engine and AnyConnect Posture module
- B. Cisco Stealthwatch and Cisco Identity Services Engine integration
- C. Cisco ASA firewall with Dynamic Access Policies configured
- D. Cisco Identity Services Engine with PxGrid services enabled

Answer: A

NEW QUESTION 449

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 450

- (Exam Topic 1)

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

- A. Enable client-side scripts on a per-domain basis.
- B. Incorporate contextual output encoding/escaping.
- C. Disable cookie inspection in the HTML inspection engine.
- D. Run untrusted HTML input through an HTML sanitization engine.
- E. Same Site cookie attribute should not be used.

Answer: AB

NEW QUESTION 452

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 454

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 459

- (Exam Topic 1)

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

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

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nse1.html>

NEW QUESTION 464

- (Exam Topic 1)

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

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

Answer: AB

Explanation:

Reference:

<https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-aglance-c45-73655>

NEW QUESTION 465

- (Exam Topic 1)

How does Cisco Stealthwatch Cloud provide security for cloud environments?

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

Answer: A

Explanation:

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

NEW QUESTION 467

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 470

- (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 473

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 477

- (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) upto 8 bridge groups are supported with 2-4 interface in each group. Prior to this only one bridge group was supported and only 2 interfaces. Up to 4 interfaces are permitted per bridge-group (inside, outside, DMZ1, DMZ2)

NEW QUESTION 479

- (Exam Topic 1)

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

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

Answer: CE

Explanation:

Stateful failover for IP Security (IPsec) enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This failover process is transparent to users and does not require adjustment or reconfiguration of any remote peer. Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators. Prerequisites for Stateful Failover for IPsec

Reference:

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

NEW QUESTION 480

- (Exam Topic 1)

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

- A. SDN controller and the cloud

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

Answer: D

NEW QUESTION 482

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 483

- (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 487

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 491

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 493

- (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 497

- (Exam Topic 3)

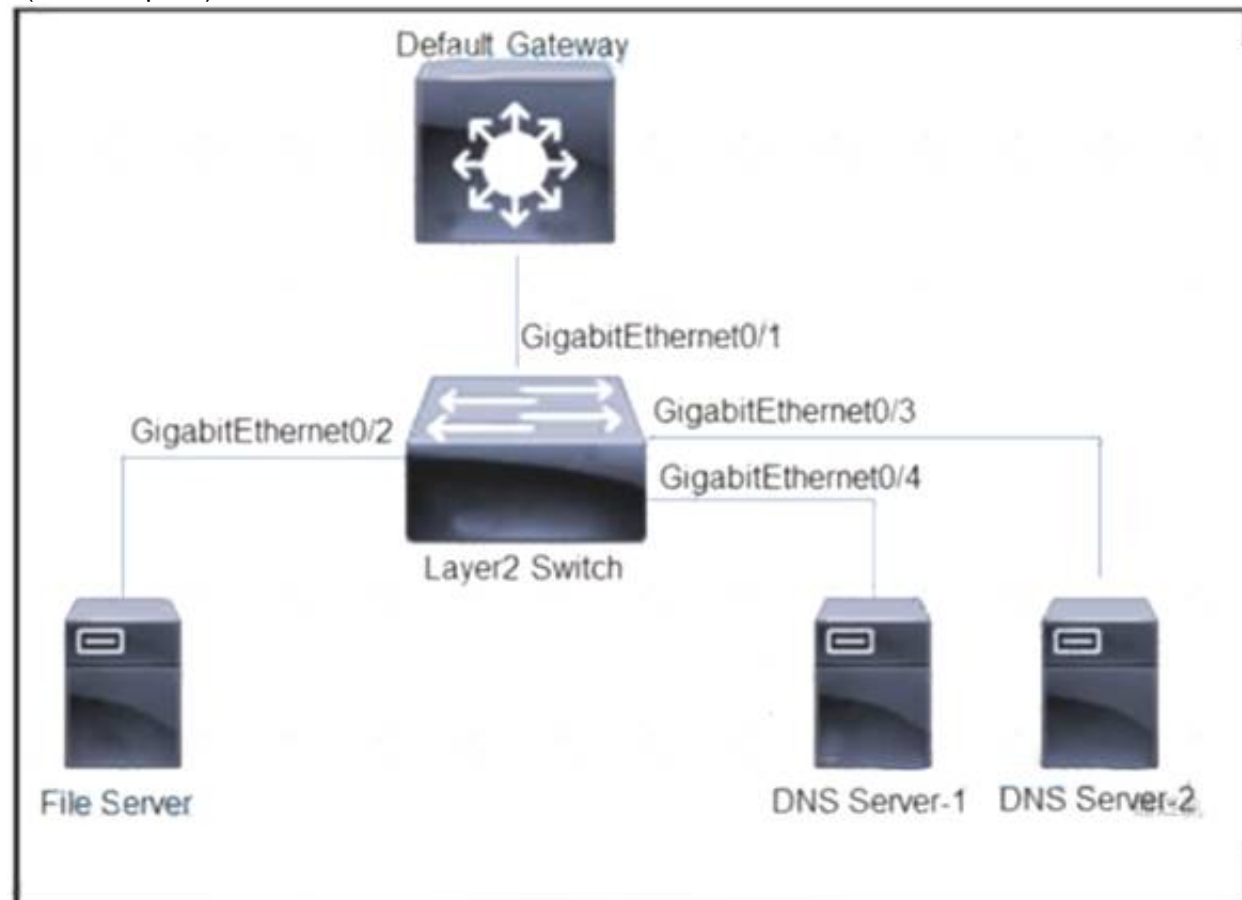
What is a characteristic of an EDR solution and not of an EPP solution?

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

Answer: B

NEW QUESTION 500

- (Exam Topic 3)



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

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

Answer: C

NEW QUESTION 503

- (Exam Topic 3)

When network telemetry is implemented, what is important to be enabled across all network infrastructure devices to correlate different sources?

- A. CDP
- B. NTP
- C. syslog
- D. DNS

Answer: B

NEW QUESTION 507

- (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 511

- (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 514

- (Exam Topic 3)

What are two benefits of using Cisco Duo as an MFA solution? (Choose two.)

- A. grants administrators a way to remotely wipe a lost or stolen device

- B. provides simple and streamlined login experience for multiple applications and users
- C. native integration that helps secure applications across multiple cloud platforms or on-premises environments
- D. encrypts data that is stored on endpoints
- E. allows for centralized management of endpoint device applications and configurations

Answer: BC

NEW QUESTION 517

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 521

- (Exam Topic 3)

What is the difference between EPP and EDR?

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

Answer: B

NEW QUESTION 524

- (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 525

- (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 528

- (Exam Topic 3)

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

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

Answer: BE

NEW QUESTION 533

- (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 538

- (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 541

- (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 542

- (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 547

- (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 552

- (Exam Topic 3)

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

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

Answer: BE

NEW QUESTION 553

- (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 556

- (Exam Topic 3)

What is a benefit of using a multifactor authentication strategy?

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

Answer: D

NEW QUESTION 559

- (Exam Topic 3)

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

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

Answer: BC

NEW QUESTION 563

- (Exam Topic 3)

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

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

Answer: BE

NEW QUESTION 566

- (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 567

- (Exam Topic 3)

Which API method and required attribute are used to add a device into Cisco DNA Center with the native API?

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

Answer: A

NEW QUESTION 571

- (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 576

- (Exam Topic 3)

How does Cisco Workload Optimization portion of the network do EPP solutions solely performance issues?

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

Answer: B

NEW QUESTION 579

- (Exam Topic 3)

Which action must be taken in the AMP for Endpoints console to detect specific MD5 signatures on endpoints and then quarantine the files?

- A. Configure an advanced custom detection list.
- B. Configure an IP Block & Allow custom detection list
- C. Configure an application custom detection list
- D. Configure a simple custom detection list

Answer: A

NEW QUESTION 580

- (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 584

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 589

- (Exam Topic 3)

What is a description of microsegmentation?

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

Answer: A

NEW QUESTION 592

- (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 593

- (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 596

- (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 597

- (Exam Topic 3)

Which industry standard is used to integrate Cisco ISE and pxGrid to each other and with other interoperable security platforms?

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

Answer: B

NEW QUESTION 599

- (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 600

- (Exam Topic 3)

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

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

Answer: CE

NEW QUESTION 601

- (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 605

- (Exam Topic 3)

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

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

Answer: AD

NEW QUESTION 607

- (Exam Topic 3)

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

- A. RSA is an asymmetric key establishment algorithm intended to output symmetric keys
- B. RSA is a symmetric key establishment algorithm intended to output asymmetric keys
- C. DH is a symmetric key establishment algorithm intended to output asymmetric keys
- D. DH is an asymmetric key establishment algorithm intended to output symmetric keys

Answer: D

Explanation:

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

NEW QUESTION 609

- (Exam Topic 3)

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

- A. AAA attributes
- B. CoA request
- C. AV pair
- D. carrier-grade NAT

Answer: C

NEW QUESTION 612

- (Exam Topic 3)

What are two benefits of using an MDM solution? (Choose two.)

- A. grants administrators a way to remotely wipe a lost or stolen device
- B. provides simple and streamlined login experience for multiple applications and users
- C. native integration that helps secure applications across multiple cloud platforms or on-premises environments
- D. encrypts data that is stored on endpoints
- E. allows for centralized management of endpoint device applications and configurations

Answer: AE

NEW QUESTION 617

- (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 622

- (Exam Topic 3)

Refer to the exhibit.

```
ASA# show service-policy sfr

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

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

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

Answer: AE

Explanation:

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

NEW QUESTION 625

- (Exam Topic 3)

An engineer is configuring their router to send NetFlow data to Stealthwatch which has an IP address of 1.1.1.11 using the flow record Stealthwatch406397954 command. Which additional command is required to complete the flow record?

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

Answer: B

NEW QUESTION 627

- (Exam Topic 3)

Which VMware platform does Cisco ACI integrate with to provide enhanced visibility, provide policy integration and deployment, and implement security policies with access lists?

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

Answer: B

NEW QUESTION 631

- (Exam Topic 3)

What is the intent of a basic SYN flood attack?

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

Answer: B

NEW QUESTION 632

- (Exam Topic 3)

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

Refer to the exhibit. What is the result of using this authentication protocol in the configuration?

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

Answer: D

NEW QUESTION 633

- (Exam Topic 3)

Which category includes DoS Attacks?

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

Answer: C

NEW QUESTION 638

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 639

- (Exam Topic 3)

Which Cisco solution extends network visibility, threat detection, and analytics to public cloud environments?

- A. Cisco Umbrella
- B. Cisco Stealthwatch Cloud
- C. Cisco Appdynamics
- D. Cisco CloudLock

Answer: B

NEW QUESTION 642

- (Exam Topic 3)

What does Cisco ISE use to collect endpoint attributes that are used in profiling?

- A. probes
- B. posture assessment
- C. Cisco AnyConnect Secure Mobility Client
- D. Cisco pxGrid

Answer: A

Explanation:

Reference:

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/2-6/admin_guide

NEW QUESTION 646

- (Exam Topic 3)

An administrator needs to configure the Cisco ASA via ASDM such that the network management system can actively monitor the host using SNMPv3. Which two tasks must be performed for this configuration? (Choose two.)

- A. Specify the SNMP manager and UDP port.
- B. Specify an SNMP user group
- C. Specify a community string.
- D. Add an SNMP USM entry
- E. Add an SNMP host access entry

Answer: BE

NEW QUESTION 651

- (Exam Topic 3)

What is the difference between a vulnerability and an exploit?

- A. A vulnerability is a hypothetical event for an attacker to exploit
- B. A vulnerability is a weakness that can be exploited by an attacker
- C. An exploit is a weakness that can cause a vulnerability in the network
- D. An exploit is a hypothetical event that causes a vulnerability in the network

Answer: B

NEW QUESTION 656

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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 First Try
- * 350-701 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 350-701 Practice Test Here](#)