

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

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



NEW QUESTION 1

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 2

- (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 3

- (Exam Topic 3)

What is a difference between GETVPN and IPsec?

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

Answer: C

NEW QUESTION 4

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 5

- (Exam Topic 3)

Based on the NIST 800-145 guide, which cloud architecture may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises?

- A. hybrid cloud
- B. private cloud
- C. public cloud
- D. community cloud

Answer: D

NEW QUESTION 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 the purpose of CA in a PKI?

- A. To issue and revoke digital certificates
- B. To validate the authenticity of a digital certificate
- C. To create the private key for a digital certificate
- D. To certify the ownership of a public key by the named subject

Answer: A

Explanation:

Reference: <https://cheapsslsecurity.com/blog/understanding-the-role-of-certificate-authorities-in-pki/>

NEW QUESTION 9

- (Exam Topic 3)

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 10

- (Exam Topic 3)

Which cloud service offering allows customers to access a web application that is being hosted, managed, and maintained by a cloud service provider?

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

Answer: B

NEW QUESTION 10

- (Exam Topic 3)

Which CoA response code is sent if an authorization state is changed successfully on a Cisco IOS device?

- A. CoA-NCL
- B. CoA-NAK
- C. ???-???
- D. CoA-ACK

Answer: D

NEW QUESTION 14

- (Exam Topic 3)

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

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

Answer: CD

NEW QUESTION 18

- (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 22

- (Exam Topic 3)

DoS attacks are categorized as what?

- A. phishing attacks
- B. flood attacks
- C. virus attacks
- D. trojan attacks

Answer: B

NEW QUESTION 24

- (Exam Topic 3)

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

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

Answer: AB

NEW QUESTION 26

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 27

- (Exam Topic 3)

Which solution should be leveraged for secure access of a CI/CD pipeline?

- A. Duo Network Gateway
- B. remote access client
- C. SSL WebVPN
- D. Cisco FTD network gateway

Answer: A

NEW QUESTION 32

- (Exam Topic 3)

Which Cisco ISE service checks the compliance of endpoints before allowing the endpoints to connect to the network?

- A. posture
- B. profiler
- C. Cisco TrustSec
- D. Threat Centric NAC

Answer: A

NEW QUESTION 33

- (Exam Topic 3)

An email administrator is setting up a new Cisco ESA. The administrator wants to enable the blocking of greymail for the end user. Which feature must the administrator enable first?

- A. File Analysis
- B. IP Reputation Filtering
- C. Intelligent Multi-Scan
- D. Anti-Virus Filtering

Answer: C

NEW QUESTION 36

- (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 38

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 42

- (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 46

- (Exam Topic 3)

Why is it important to patch endpoints consistently?

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

Answer: B

NEW QUESTION 47

- (Exam Topic 3)

A network engineer is configuring NetFlow top talkers on a Cisco router Drag and drop the steps in the process from the left into the sequence on the right

Configure the ip flow-top-talkers command.	step 1
Configure the ip flow command on an interface.	step 2
Configure IP routing and enable Cisco Express Forwarding.	step 3
Set the top-talkers sorting criterion.	step 4
Specify the maximum number of top talkers.	step 5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 52

- (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 57

- (Exam Topic 3)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 60

- (Exam Topic 3)

An engineer needs to configure an access control policy rule to always send traffic for inspection without using the default action. Which action should be configured for this rule?

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

Answer: B

Explanation:

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

<https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/acce>

NEW QUESTION 61

- (Exam Topic 3)

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

- A. Advanced Custom Detection
- B. Blocked Application

- C. Isolation
- D. Simple Custom Detection

Answer: B

NEW QUESTION 64

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 67

- (Exam Topic 3)

An engineer must modify a policy to block specific addresses using Cisco Umbrella. The policy is created already and is actively u: of the default policy elements. What else must be done to accomplish this task?

- A. Add the specified addresses to the identities list and create a block action.
- B. Create a destination list for addresses to be allowed or blocked.
- C. Use content categories to block or allow specific addresses.
- D. Modify the application settings to allow only applications to connect to required addresses.

Answer: B

NEW QUESTION 72

- (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 73

- (Exam Topic 3)

Which metric is used by the monitoring agent to collect and output packet loss and jitter information?

- A. WSAv performance
- B. AVC performance
- C. OTCP performance
- D. RTP performance

Answer: D

NEW QUESTION 76

- (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 81

- (Exam Topic 3)

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

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

Answer:

D

NEW QUESTION 84

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 87

- (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 92

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 96

- (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 100

- (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 101

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 106

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 108

- (Exam Topic 3)

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

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

Answer: AC

NEW QUESTION 110

- (Exam Topic 3)

Which Cisco Firewall solution requires zone definition?

- A. CBAC
- B. Cisco AMP
- C. ZBFW
- D. Cisco ASA

Answer: C

NEW QUESTION 113

- (Exam Topic 3)

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

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

Answer: AB

NEW QUESTION 115

- (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 120

- (Exam Topic 3)

What is a benefit of using Cisco Tetration?

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

Answer: C

NEW QUESTION 124

- (Exam Topic 3)

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

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

Answer: CE

NEW QUESTION 125

- (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 130

- (Exam Topic 3)

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

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

Answer: AC

NEW QUESTION 133

- (Exam Topic 3)

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

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

Answer: CE

NEW QUESTION 136

- (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 141

- (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 145

- (Exam Topic 3)

Which feature does the IaaS model provide?

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

Answer: C

NEW QUESTION 149

- (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 150

- (Exam Topic 3)

During a recent security audit a Cisco IOS router with a working IPSEC configuration using IKEv1 was flagged for using a wildcard mask with the crypto isakmp key command The VPN peer is a SOHO router with a dynamically assigned IP address Dynamic DNS has been configured on the SOHO router to map the dynamic IP address to the host name of vpn.sohoroutercompany.com In addition to the command crypto isakmp key Cisc425007536 hostname vpn.sohoroutercompany.com what other two commands are now required on the Cisco IOS router for the VPN to continue to function after the wildcard command is removed? (Choose two)

- A. ip host vpn.sohoroutercompany.eom <VPN Peer IP Address>
- B. crypto isakmp identity hostname
- C. Add the dynamic keyword to the existing crypto map command
- D. fqdn vpn.sohoroutercompany.com <VPN Peer IP Address>
- E. ip name-server <DNS Server IP Address>

Answer: BC

NEW QUESTION 155

- (Exam Topic 3)

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

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

Answer: D

Explanation:

<https://learn-umbrella.cisco.com/i/802005-umbrella-security-report/3?> <https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html#:~:text=Pow>e 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 156

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 158

- (Exam Topic 3)

Which Cisco security solution provides patch management in the cloud?

- A. Cisco Umbrella
- B. Cisco ISE
- C. Cisco CloudLock
- D. Cisco Tetration

Answer: C

NEW QUESTION 160

- (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 165

- (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 166

- (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 171

- (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 175

- (Exam Topic 3)

When a Cisco WSA checks a web request, what occurs if it is unable to match a user-defined policy?

- A. It blocks the request.
- B. It applies the global policy.
- C. It applies the next identification profile policy.
- D. It applies the advanced policy.

Answer: B

NEW QUESTION 176

- (Exam Topic 3)

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

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

D. Configure the integrations with Talos Intelligence to take advantage of the threat intelligence that it provides.

Answer: D

NEW QUESTION 180

- (Exam Topic 3)

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

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

A. Mastered

B. Not Mastered

Answer: A

Explanation:

user entity behavior assessment	cloud security strategy workshop
cloud data protection assessment	cloud security architecture assessment
cloud security strategy workshop	cloud data protection assessment
cloud security architecture assessment	user entity behavior assessment

NEW QUESTION 185

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 186

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 188

- (Exam Topic 3)

What is a feature of container orchestration?

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

Answer: C

NEW QUESTION 191

- (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 196

- (Exam Topic 3)

A company recently discovered an attack propagating throughout their Windows network via a file named abc428565580xyz.exe. The malicious file was uploaded to a Simple Custom Detection list in the AMP for Endpoints Portal and the currently applied policy for the Windows clients was updated to reference the detection list. Verification testing scans on known infected systems shows that AMP for Endpoints is not detecting the presence of this file as an indicator of compromise. What must be performed to ensure detection of the malicious file?

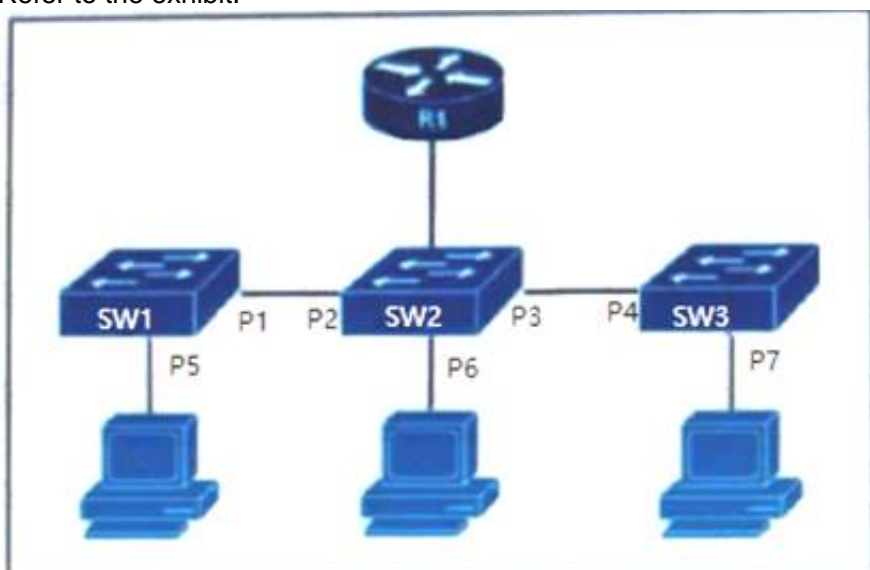
- A. Upload the malicious file to the Blocked Application Control List
- B. Use an Advanced Custom Detection List instead of a Simple Custom Detection List
- C. Check the box in the policy configuration to send the file to Cisco Threat Grid for dynamic analysis
- D. Upload the SHA-256 hash for the file to the Simple Custom Detection List

Answer: D

NEW QUESTION 200

- (Exam Topic 3)

Refer to the exhibit.



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

- A. P2 and P3 only
- B. P5, P6, and P7 only
- C. P1, P2, P3, and P4 only
- D. P2, P3, and P6 only

Answer: D

NEW QUESTION 204

- (Exam Topic 3)

A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to ensure that bandwidth is available for VPN users needing access to corporate resources on the 10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the network?

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

Answer: A

NEW QUESTION 207

- (Exam Topic 3)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 212

- (Exam Topic 3)

An engineer is adding a Cisco router to an existing environment. NTP authentication is configured on all devices in the environment with the command `ntp authentication-key 1 md5 Clsc427128380`. There are two routers on the network that are configured as NTP servers for redundancy, 192.168.1.110 and 192.168.1.111. 192.168.1.110 is configured as the authoritative time source. What command must be configured on the new router to use 192.168.1.110 as its primary time source without the new router attempting to offer time to existing devices?

- A. `ntp server 192.168.1.110 primary key 1`
- B. `ntp peer 192.168.1.110 prefer key 1`
- C. `ntp server 192.168.1.110 key 1 prefer`
- D. `ntp peer 192.168.1.110 key 1 primary`

Answer: A

NEW QUESTION 214

- (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 216

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 220

- (Exam Topic 3)

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

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

Answer: AE

Explanation:

Reference:

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

NEW QUESTION 224

- (Exam Topic 3)

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

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

Answer: BD

NEW QUESTION 229

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 234

- (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 237

- (Exam Topic 3)

Which feature must be configured before implementing NetFlow on a router?

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

Answer: D

NEW QUESTION 241

- (Exam Topic 3)

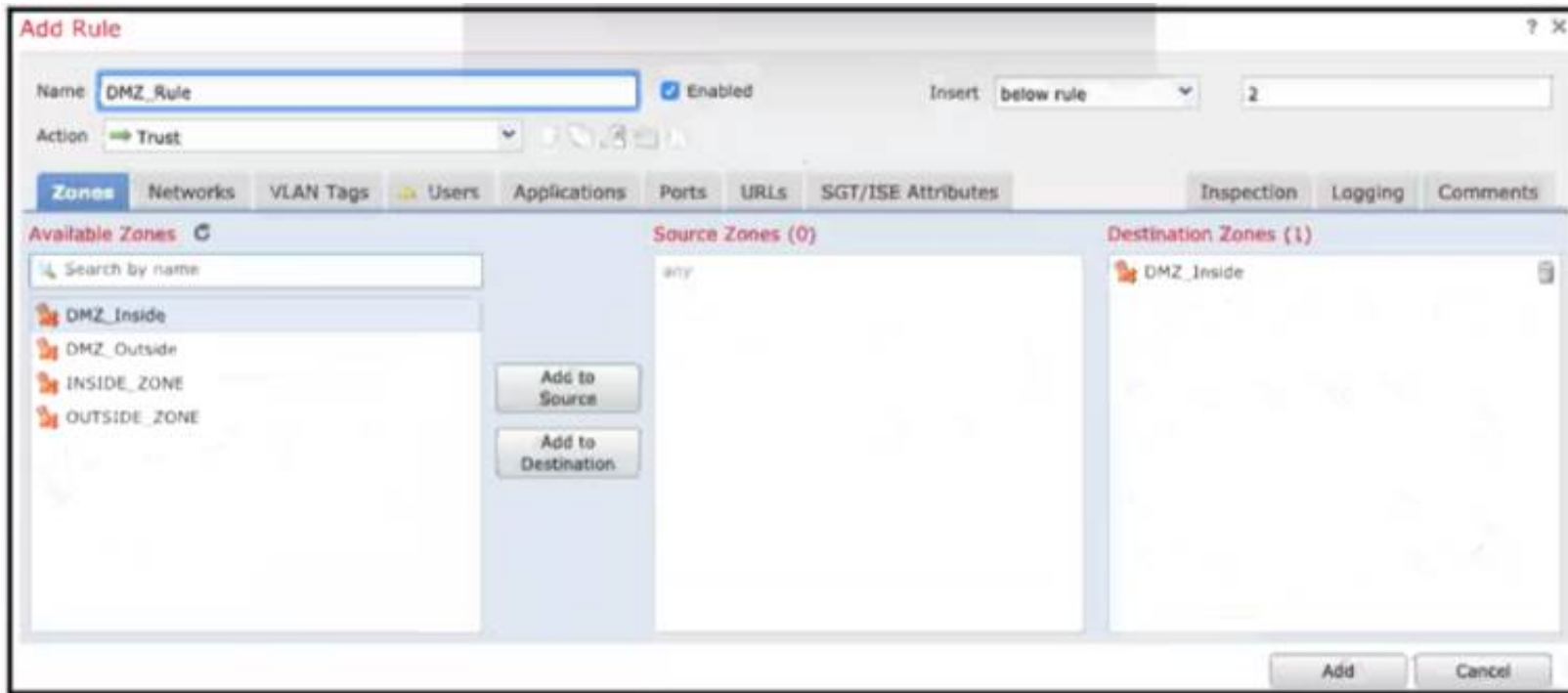
Which capability is provided by application visibility and control?

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

Answer: D

NEW QUESTION 246

- (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 250

- (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 254

- (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 256

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 261

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 265

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 268

- (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 269

- (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 270

- (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 272

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 275

- (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 277

- (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 279

- (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 283

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 288

- (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.

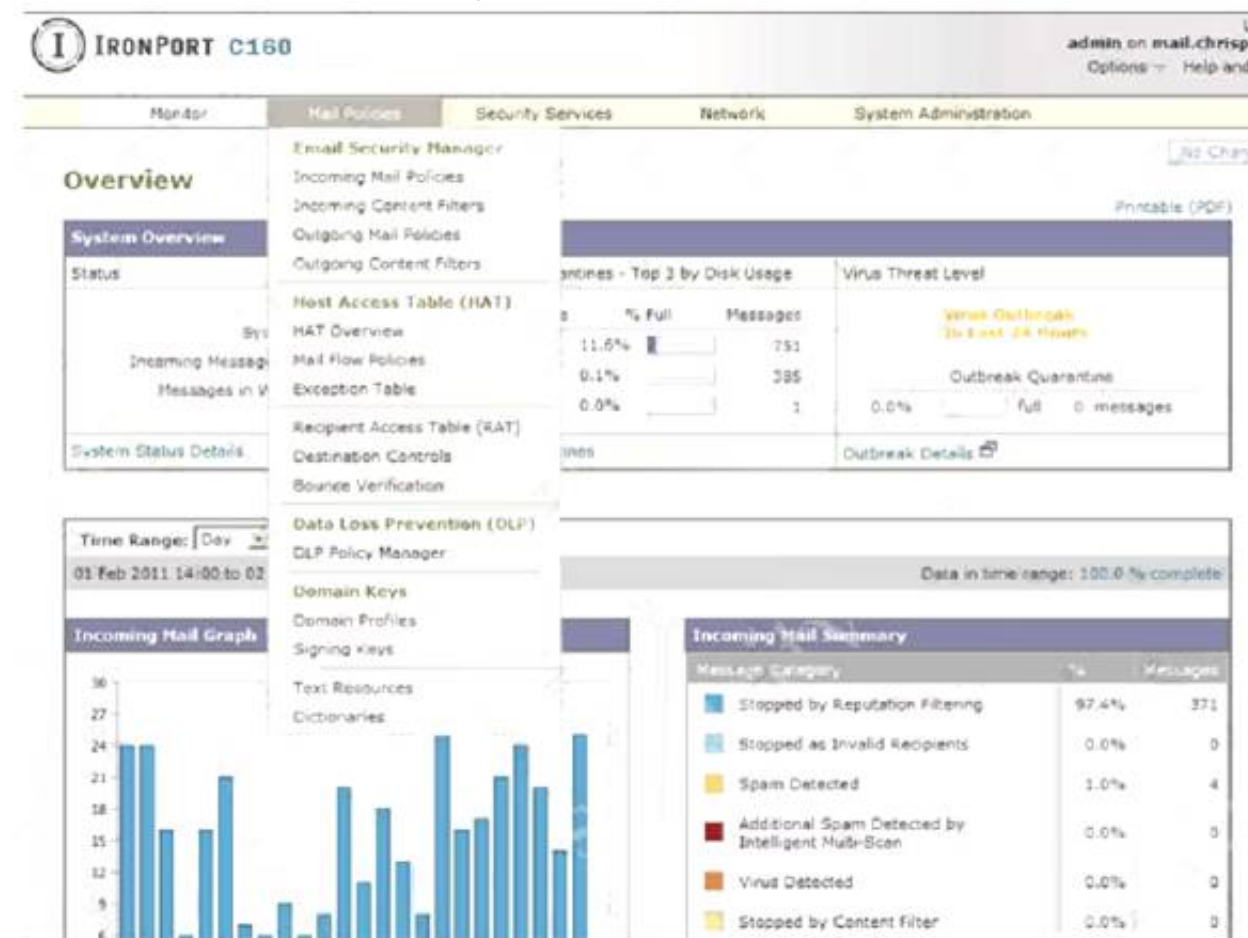
What must be configured to accomplish this?

- 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 290

- (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 291

- (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 295

- (Exam Topic 2)

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

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

Answer: C

Explanation:

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technoteesa-00.html>In this question, it stated “the network is congested” (not the file analysis server was overloaded) so the appliance will not try to upload the file again.

NEW QUESTION 296

- (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 298

- (Exam Topic 2)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 301

- (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 304

- (Exam Topic 2)

Why is it important to have logical security controls on endpoints even though the users are trained to spot security threats and the network devices already help prevent them?

- A. to prevent theft of the endpoints

- B. because defense-in-depth stops at the network
- C. to expose the endpoint to more threats
- D. because human error or insider threats will still exist

Answer: D

NEW QUESTION 309

- (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 313

- (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 317

- (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 320

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Endpoint protection platforms (EPP) prevent endpoint security threats like known and unknown malware. Endpoint detection and response (EDR) solutions can detect and respond to threats that your EPP and other security tools did not catch. EDR and EPP have similar goals but are designed to fulfill different purposes. EPP is designed to provide device-level protection by identifying malicious files, detecting potentially malicious activity, and providing tools for incident investigation and response. The preventative nature of EPP complements proactive EDR. EPP acts as the first line of defense, filtering out attacks that can be detected by the organization's deployed security solutions. EDR acts as a second layer of protection, enabling security analysts to perform threat hunting and identify more subtle threats to the endpoint. Effective endpoint defense requires a solution that integrates the capabilities of both EDR and EPP to provide protection against cyber

threats without overwhelming an organization's security team.

NEW QUESTION 322

- (Exam Topic 2)

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

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

Answer: BE

Explanation:

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

NEW QUESTION 326

- (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.examttopics.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.examttopics.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 328

- (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 329

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 332

- (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 336

- (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 341

- (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 344

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 348

- (Exam Topic 1)

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 353

- (Exam Topic 1)

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

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

Answer: AD

NEW QUESTION 358

- (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 361

- (Exam Topic 1)

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

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

Answer: CD

Explanation:

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

NEW QUESTION 363

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 367

- (Exam Topic 1)

Refer to the exhibit.

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

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

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

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

Answer: C

NEW QUESTION 372

- (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 375

- (Exam Topic 1)

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

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

Answer: AD

Explanation:

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

NEW QUESTION 379

- (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 380

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 384

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 389

- (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 391

- (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 394

- (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 399

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 400

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 402

- (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 404

- (Exam Topic 1)

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

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

Answer: AB

NEW QUESTION 407

- (Exam Topic 1)

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

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

Answer: AD

Explanation:

Malware means “malicious software”, is any software intentionally designed to cause damage to a computer, server, client, or computer network. The most popular types of malware includes viruses, ransomware and spyware. Virus Possibly the most common type of malware, viruses attach their malicious code to clean code and wait to be run.

Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again. Spyware is spying software that can secretly record everything you enter, upload, download, and store on your computers or mobile devices. Spyware always tries to keep itself hidden. An exploit is a code that takes advantage of a software vulnerability or security flaw. Exploits and malware are two risks for endpoints that are not up to date. ARP spoofing and eavesdropping are attacks against the network while denial-of-service attack is based on the flooding of IP packets.

NEW QUESTION 410

- (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 411

- (Exam Topic 1)

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

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

Answer: BC

NEW QUESTION 412

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 413

- (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 414

- (Exam Topic 1)

Which function is the primary function of Cisco AMP threat Grid?

- A. automated email encryption
- B. applying a real-time URI blacklist
- C. automated malware analysis
- D. monitoring network traffic

Answer: C

NEW QUESTION 417

- (Exam Topic 1)

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

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

Answer: BE

NEW QUESTION 420

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 424

- (Exam Topic 1)

Refer to the exhibit.

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

Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

- A. show authentication registrations
- B. show authentication method
- C. show dot1x all
- D. show authentication sessions

Answer: D

Explanation:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-c/Displaying the Summary of All Auth Manager Sessions on the Switch](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-c/Displaying%20the%20Summary%20of%20All%20Auth%20Manager%20Sessions%20on%20the%20Switch.html)

Enter the following:

```
Switch# show authentication sessions
Interface MAC Address Method Domain Status Session ID
Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success
0A3462B10000000D24F80B58
Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94
```

NEW QUESTION 427

- (Exam Topic 1)

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

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

Answer: AC

Explanation:

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

File Conditions List > **pc_W10_64_KB4012606_Ms17-010_1507_W**

File Condition

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

NEW QUESTION 430

- (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 432

- (Exam Topic 1)

Which Cisco AMP file disposition valid?

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

Answer: B

NEW QUESTION 437

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 439

- (Exam Topic 1)

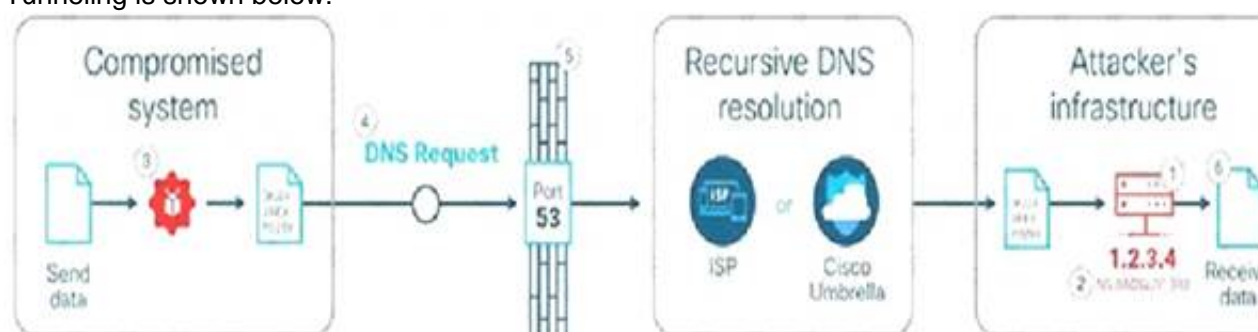
How is DNS tunneling used to exfiltrate data out of a corporate network?

- A. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.
- B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.
- C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network.
- D. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.

Answer: B

Explanation:

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



➤ The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNSnameserver (NS) and malicious payload.2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. attackerdomain.com) is registered or reused. The registrar informs the top-level domain (.com) nameservers to refer requests for attackerdomain.com to ns.attackerdomain.com, which has a DNS record mapped to 1.2.3.43. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, P028X977W,...).4. The payload initiates thousands of unique DNS record requests to the attacker's domain with each string as

Reference: <https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0>

NEW QUESTION 441

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 444

- (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 446

- (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 450

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 451

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 455

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 458

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 460

- (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 462

- (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 463

- (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 465

- (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 469

- (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 474

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 479

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 480

- (Exam Topic 1)

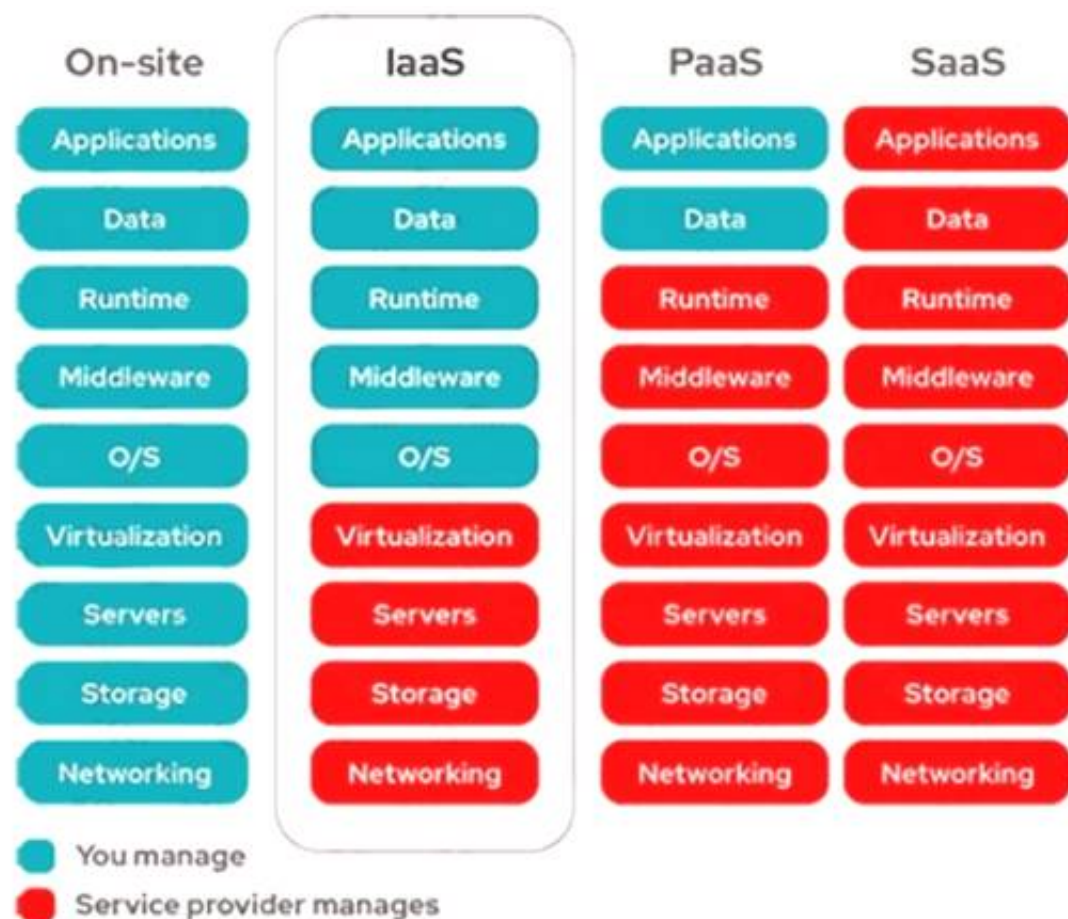
In which cloud services model is the tenant responsible for virtual machine OS patching?

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

Answer: A

Explanation:

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



NEW QUESTION 483

- (Exam Topic 1)

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

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

Answer: BC

NEW QUESTION 485

- (Exam Topic 1)

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

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

Answer: BD

Explanation:

Ping of Death (PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command. A correctly-formed ping packet is typically 56 bytes in size, or 64 bytes when the ICMP header is considered, and 84 including Internet Protocol version 4 header. However, any IPv4 packet (including pings) may be as large as 65,535 bytes. Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented. Like other large but well-formed packets, a ping of death is fragmented into groups of 8 octets before transmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code.

NEW QUESTION 489

- (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 490

- (Exam Topic 1)

Refer to the exhibit.

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

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

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

Answer: B

Explanation:

The user "admin5" was configured with privilege level 5. In order to allow configuration (enter globalconfiguration mode), we must type this command:(config)#privilege exec level 5 configure terminalWithout this command, this user cannot do any configuration.Note: Cisco IOS supports privilege levels from 0 to 15, but the privilege levels which are used by default are privilege level 1 (user EXEC) and level privilege 15 (privilege EXEC)

NEW QUESTION 491

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 493

- (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 497

- (Exam Topic 1)

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

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

Answer: AC

NEW QUESTION 501

- (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 506

- (Exam Topic 1)

Which two capabilities does TAXII support? (Choose two)

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

Answer: AB

Explanation:

The Trusted Automated eXchange of Indicator Information (TAXII) specifies mechanisms for exchanging structured cyber threat information between parties over the network. TAXII exists to provide specific capabilities to those interested in sharing structured cyber threat information. TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilities that this version of TAXII supports: push messaging, pull messaging, and discovery. Although there is no “binding” capability in the list but it is the best answer here.

NEW QUESTION 509

- (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 513

- (Exam Topic 1)

How is Cisco Umbrella configured to log only security events?

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

Answer: A

Explanation:

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

NEW QUESTION 516

- (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 521

- (Exam Topic 1)

Which API is used for Content Security?

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

Answer: D

NEW QUESTION 523

- (Exam Topic 1)

Which algorithm provides encryption and authentication for data plane communication?

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

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html>

NEW QUESTION 527

- (Exam Topic 1)

Which type of attack is social engineering?

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

Answer: B

Explanation:

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

NEW QUESTION 528

- (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 531

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 533

- (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_vpnav/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 537

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 538

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 541

- (Exam Topic 1)

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

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

Answer: DE

Explanation:

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

NEW QUESTION 546

- (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 547

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 550

- (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 551

- (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 556

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 559

- (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 561

- (Exam Topic 3)

An engineer is configuring web filtering for a network using Cisco Umbrella Secure Internet Gateway.

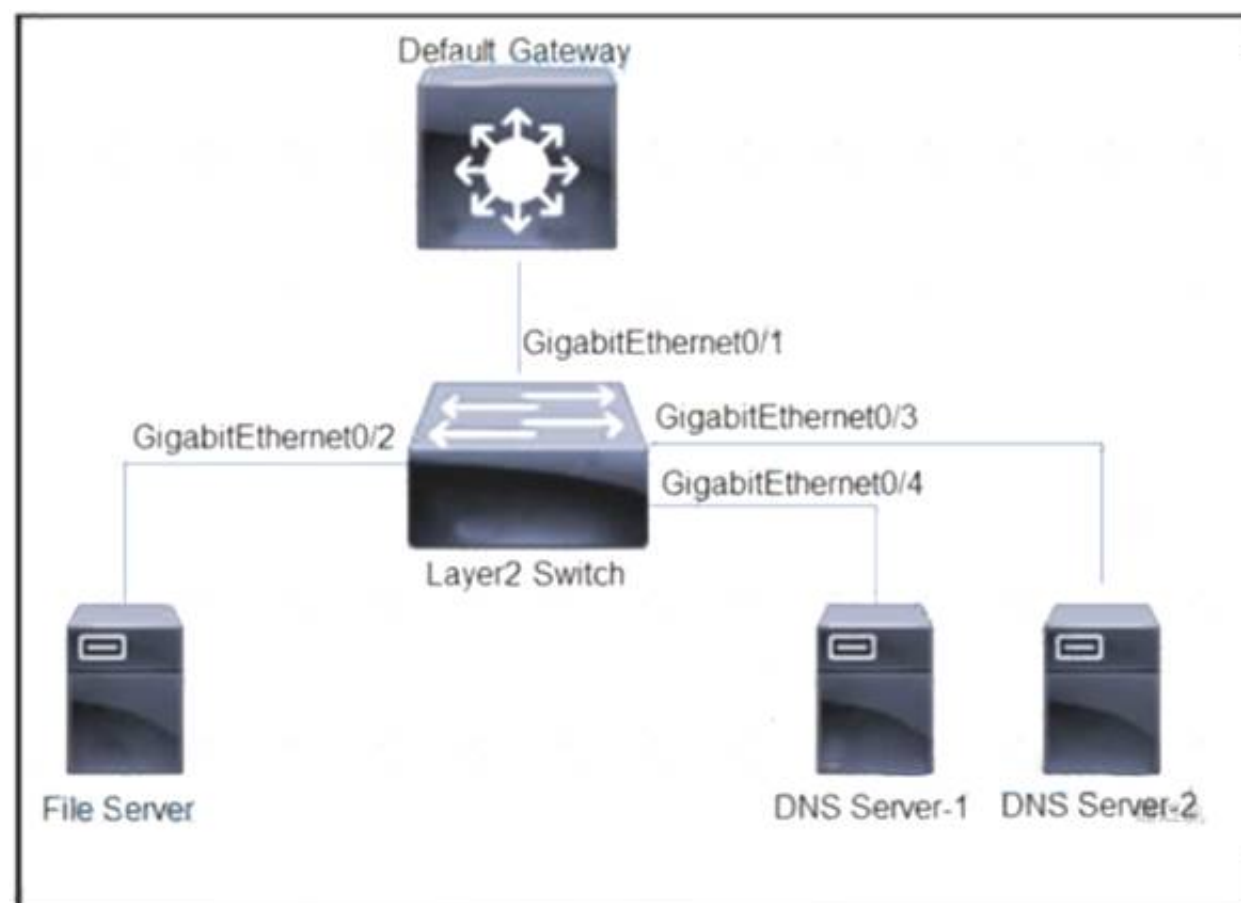
The requirement is that all traffic needs to be filtered. Using the SSL decryption feature, which type of certificate should be presented to the end-user to accomplish this goal?

- A. third-party
- B. self-signed
- C. organization owned root
- D. SubCA

Answer: C

NEW QUESTION 566

- (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 571

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 573

- (Exam Topic 3)

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

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

Answer: B

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec

NEW QUESTION 578

- (Exam Topic 3)

Which system performs compliance checks and remote wiping?

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

Answer: A

NEW QUESTION 582

- (Exam Topic 3)

Which Cisco security solution stops exfiltration using HTTPS?

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

Answer: C

Explanation:

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

NEW QUESTION 587

- (Exam Topic 3)

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

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

Answer: A

Explanation:

The FMC and managed devices communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305. Cisco strongly recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate with each other.

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmtnw.html>

NEW QUESTION 592

- (Exam Topic 3)

An engineer needs to configure a Cisco Secure Email Gateway (SEG) to prompt users to enter multiple forms of identification before gaining access to the SEG. The SEG must also join a cluster using the preshared key of cisc421555367. What steps must be taken to support this?

- A. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG GUI.
- B. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG CLI.
- C. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG CLI
- D. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG GUI.

Answer: C

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 595

- (Exam Topic 3)

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

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

Answer: AE

NEW QUESTION 597

- (Exam Topic 3)

What is a feature of NetFlow Secure Event Logging?

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

Answer: A

NEW QUESTION 602

- (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 603

- (Exam Topic 3)

Which direction do attackers encode data in DNS requests during exfiltration using DNS tunneling?

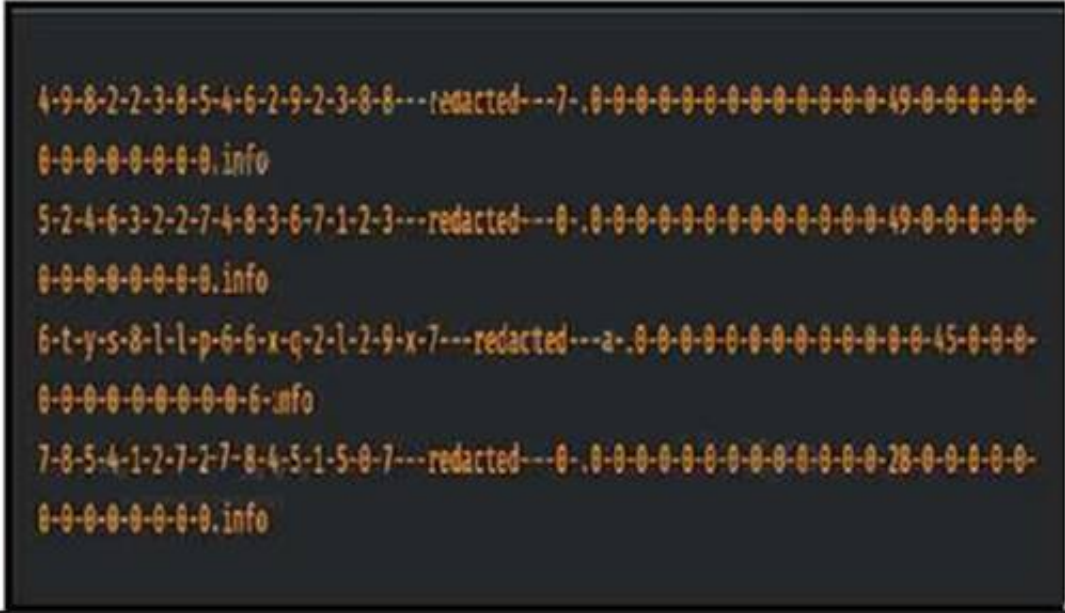
- A. inbound
- B. north-south
- C. east-west
- D. outbound

Answer: D

NEW QUESTION 604

- (Exam Topic 3)

Refer to the exhibit.



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

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

Answer: D

NEW QUESTION 605

- (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 609

- (Exam Topic 3)

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

esp-3des

esp-aes-256

esp-md5-hmac

esp-sha-hmac

Authentication

Encryption

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Diagram Description automatically generated

NEW QUESTION 610

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 615

- (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 617

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 618

- (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 620

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 623

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 628

- (Exam Topic 3)

Which feature requires that network telemetry be enabled?

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

Answer: D

NEW QUESTION 630

- (Exam Topic 3)

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

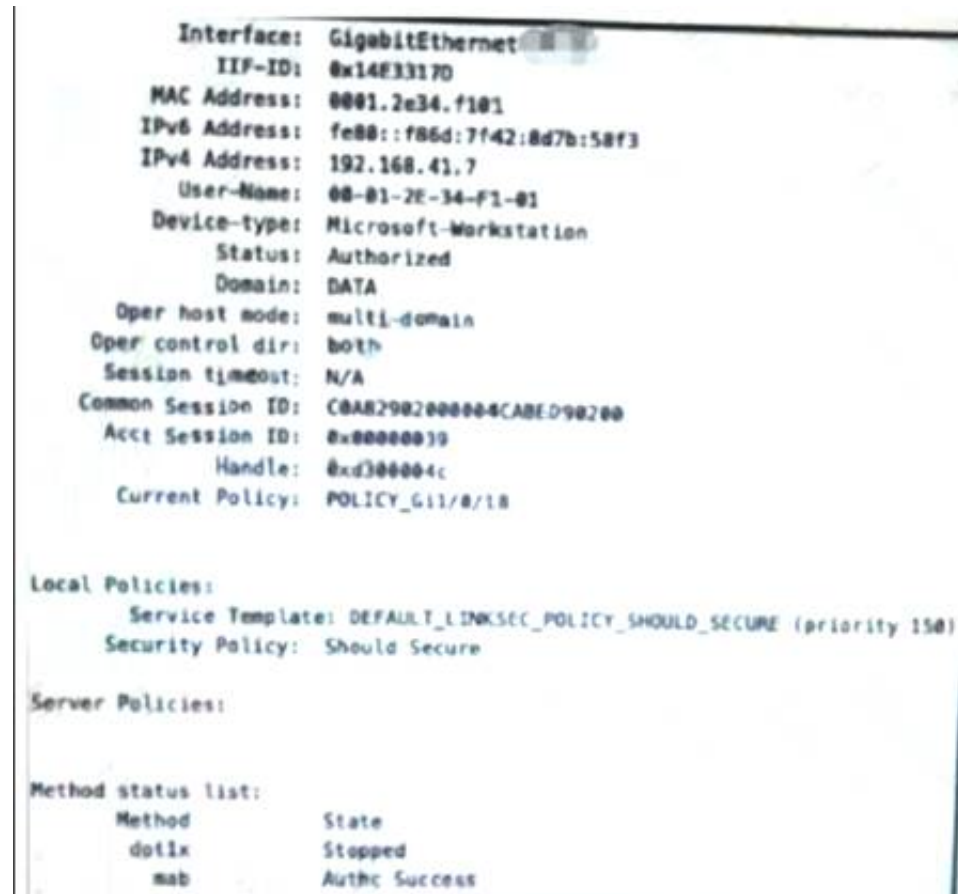
- A. AES-192
- B. IKEv1
- C. AES-256
- D. ESP

Answer: D

NEW QUESTION 632

- (Exam Topic 3)

Refer to the exhibit.



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

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

Answer: C

NEW QUESTION 635

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 637

- (Exam Topic 3)

Which DoS attack uses fragmented packets in an attempt to crash a target machine?

- A. teardrop
- B. smurf
- C. LAND
- D. SYN flood

Answer: A

Explanation:

Reference: <https://www.radware.com/security/ddos-knowledge-center/ddospedia/teardrop-attack/>

NEW QUESTION 642

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 647

- (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 649

- (Exam Topic 3)

Which IETF attribute is supported for the RADIUS CoA feature?

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

Answer: A

NEW QUESTION 654

- (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 657

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 660

- (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 662

- (Exam Topic 3)

Which role is a default guest type in Cisco ISE?

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

Answer: C

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/1-4-1/admin_guide/b_ise_admin_guide_141/b_ise_admin_g

NEW QUESTION 666

- (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 668

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 672

- (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 675

- (Exam Topic 3)

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

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

Answer: CD

NEW QUESTION 679

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 684

- (Exam Topic 3)

Which Cisco security solution integrates with cloud applications like Dropbox and Office 365 while protecting data from being exfiltrated?

- A. Cisco Tajos
- B. Cisco Steaithwatch Cloud
- C. Cisco Cloudlock
- D. Cisco Umbrella Investigate

Answer: C

NEW QUESTION 688

- (Exam Topic 3)

Which category includes DoS Attacks?

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

Answer: C

NEW QUESTION 691

- (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 693

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

350-701 Practice Exam Features:

- * 350-701 Questions and Answers Updated Frequently
- * 350-701 Practice Questions Verified by Expert Senior Certified Staff
- * 350-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 350-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year