Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

NEW QUESTION 1
- (Exam Topic 3)
An organization wants to use Cisco FTD or Cisco ASA devices. Specific URLs must be blocked from being accessed via the firewall which requires that the administrator input the bad URL categories that the organization wants blocked into the access policy. Which solution should be used to meet this requirement?

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

Answer: C

NEW QUESTION 2
- (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 3
- (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 4
- (Exam Topic 3)
Which function is performed by certificate authorities but is a limitation of registration authorities?

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

Answer: C

NEW QUESTION 5
- (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 m 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 6
- (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 7
- (Exam Topic 3)

How does a cloud access security broker function?

A. It is an authentication broker to enable single sign-on and multi-factor authentication for a cloud solution
B. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution
C. It acts as a security information and event management solution and receives syslog from other cloud solutions.
D. It scans other cloud solutions being used within the network and identifies vulnerabilities

Answer: B

NEW QUESTION 8
- (Exam Topic 3)
What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.) The eDirectory client must be installed on each client workstation.

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

Answer: AB

Explanation:
> Transparently identify users with authentication realms – This option is available when one or more authentication realms are configured to support transparent identification using one of the following authentication servers:
> Active Directory – Create an NTLM or Kerberos authentication realm and enable transparent user identification. In addition, you must deploy a separate Active Directory agent such as Cisco's Context Directory Agent. For more information, see Transparent User Identification with Active Directory.
> LDAP – Create an LDAP authentication realm configured as an eDirectory, andenable transparent user identification. For more information, see Transparent User Identification with LDAP.
Details:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGui

NEW QUESTION 9
- (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 10
- (Exam Topic 3)
Using Cisco Cognitive Threat Analytics, which platform automatically blocks risky sites, and test unknown sites for hidden advanced threats before allowing users to click them?

A. Cisco Identity Services Engine (ISE)
B. Cisco Enterprise Security Appliance (ESA)
C. Cisco Web Security Appliance (WSA)
D. Cisco Advanced Stealthwatch Appliance (ASA)

Answer: C

NEW QUESTION 10
- (Exam Topic 3)
Which two parameters are used for device compliance checks? (Choose two.)

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

Answer: CE

NEW QUESTION 14
- (Exam Topic 3)
Which solution supports high availability in routed or transparent mode as well as in northbound and southbound deployments?

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

Answer: B

NEW QUESTION 18
- (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 19
- (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

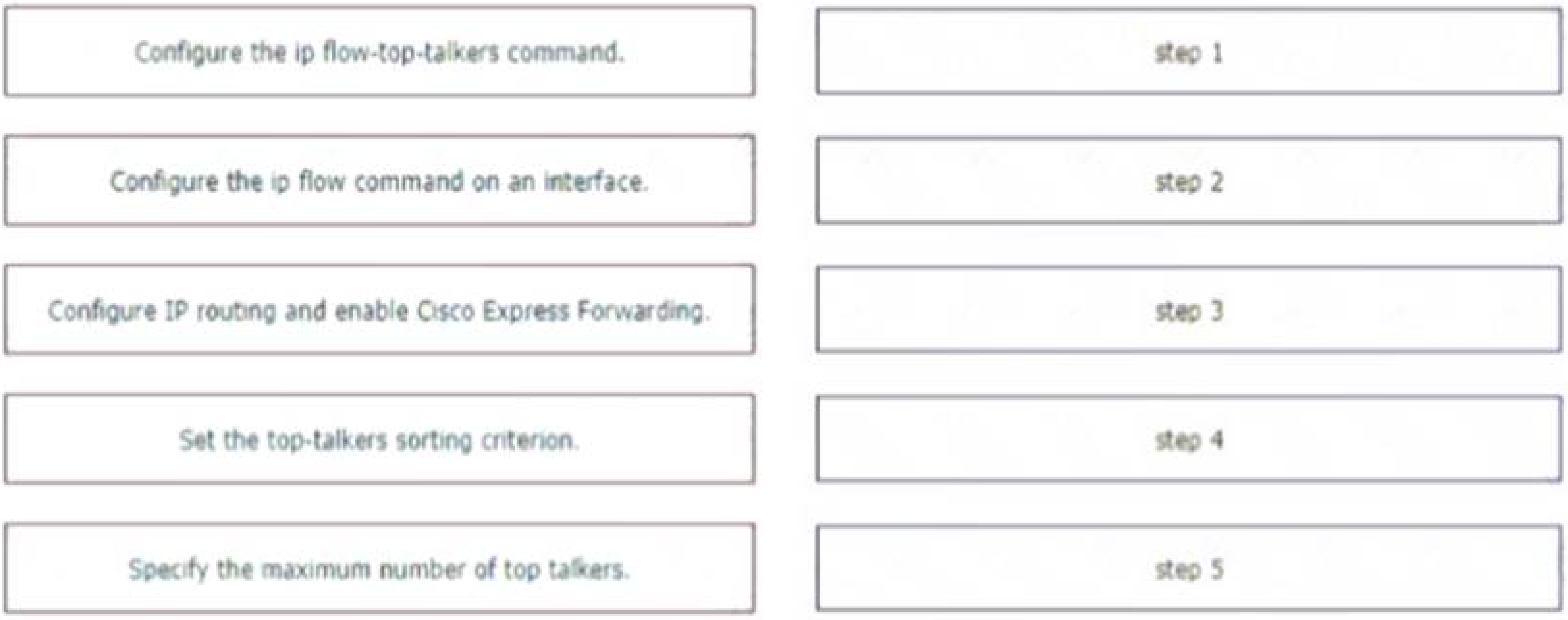
Answer: B

NEW QUESTION 23
- (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 28
- (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.

Configure the ip flow command on an interface.

Configure IP routing and enable Cisco Express Forwarding.

Set the top-talkers sorting criterion.

Specify the maximum number of top talkers.

step 1

step 2

step 3

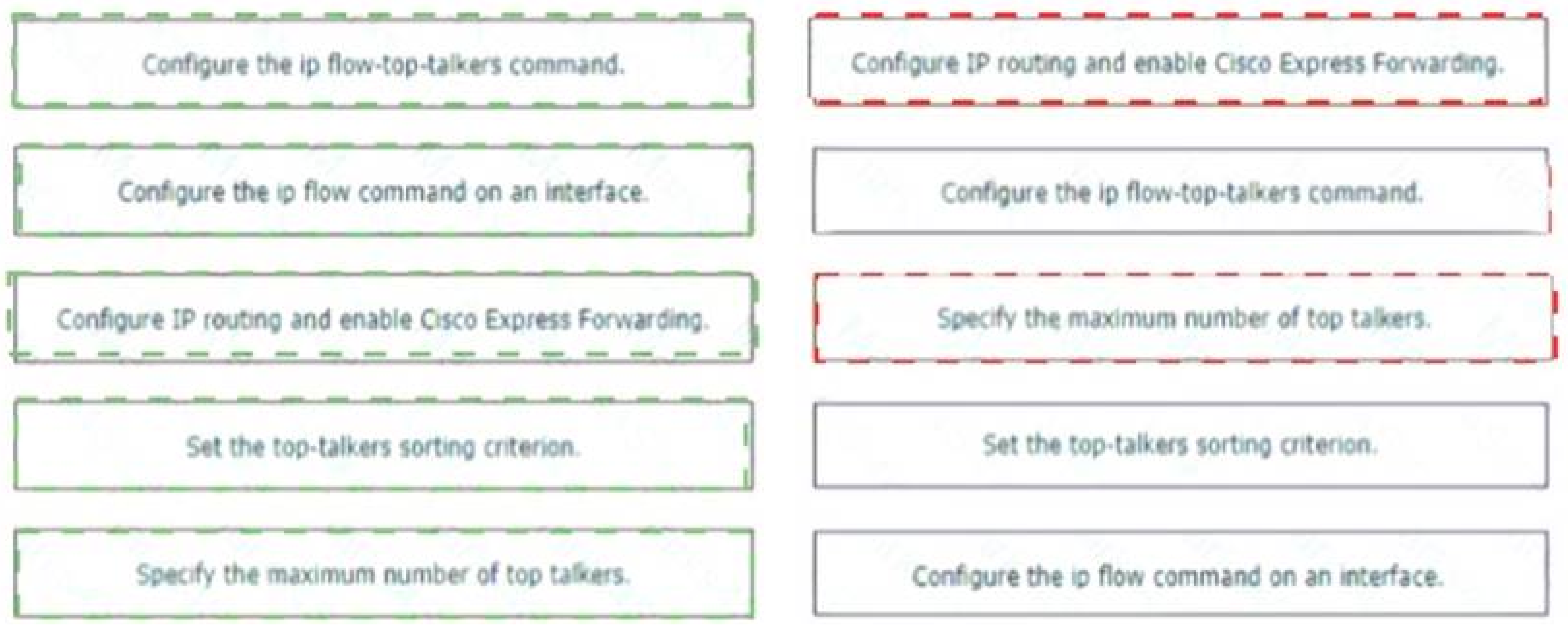
step 4

step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Configure the ip flow-top-talkers command.

Configure the ip flow command on an interface.

Configure IP routing and enable Cisco Express Forwarding.

Set the top-talkers sorting criterion.

Specify the maximum number of top talkers.

Configure IP routing and enable Cisco Express Forwarding.

Configure the ip flow-top-talkers command.

Specify the maximum number of top talkers.

Set the top-talkers sorting criterion.

Configure the ip flow command on an interface.

NEW QUESTION 29
- (Exam Topic 3)
An engineer is configuring Cisco WSA and needs to enable a separated email transfer flow from the Internet and from the LAN. Which deployment mode must be used to accomplish this goal?

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

Answer: D

NEW QUESTION 33
- (Exam Topic 3)
What is a difference between an XSS attack and an SQL injection attack?

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

Answer: C

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

NEW QUESTION 38
- (Exam Topic 3)
An administrator configures new authorization policies within Cisco ISE and has difficulty profiling the devices. Attributes for the new Cisco IP phones that are profiled based on the RADIUS authentication are seen however the attributes for CDP or DHCP are not. What should the administrator do to address this issue?

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

Answer: D

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

NEW QUESTION 42
- (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 45
- (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 48
- (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>/capure/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 51
- (Exam Topic 3)
What is a function of the Layer 4 Traffic Monitor on a Cisco WSA?

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

Answer: C

NEW QUESTION 54
- (Exam Topic 3)
An organization is implementing AAA for their users. They need to ensure that authorization is verified for every command that is being entered by the network administrator. Which protocol must be configured in order to provide this capability?

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

Answer: D

NEW QUESTION 58
- (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 62
- (Exam Topic 3)
Which solution for remote workers enables protection, detection, and response on the endpoint against known and unknown threats?

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

Answer: A

NEW QUESTION 64
- (Exam Topic 3)
What are two ways that Cisco Container Platform provides value to customers who utilize cloud service providers? (Choose two.)

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

Answer: AE

NEW QUESTION 66
- (Exam Topic 3)
Which MDM configuration provides scalability?

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

Answer: C

NEW QUESTION 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 71
- (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 75
- (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 76
- (Exam Topic 3)
Which two methods must be used to add switches into the fabric so that administrators can control how switches are added into DCNM for private cloud management? (Choose two.)

A. Cisco Cloud Director
B. Cisco Prime Infrastructure
C. PowerOn Auto Provisioning
D. Seed IP
E. CDP AutoDiscovery

Answer: CD

NEW QUESTION 77

- (Exam Topic 3)
Which characteristic is unique to a Cisco WSAv as compared to a physical appliance?

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

Answer: A

NEW QUESTION 81
- (Exam Topic 3)
An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation. What must be un solution?

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

Answer: D

NEW QUESTION 84
- (Exam Topic 3)
Which two authentication protocols are supported by the Cisco WSA? (Choose two.)

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

Answer: BE

NEW QUESTION 88
- (Exam Topic 3)
What is the function of the crypto is a kmp key cisc406397954 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel?

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

Answer: B

NEW QUESTION 92
- (Exam Topic 3)
Which Cisco WSA feature supports access control using URL categories?

A. transparent user identification
B. SOCKS proxy services
C. web usage controls
D. user session restrictions

Answer: A

NEW QUESTION 94
- (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 96
- (Exam Topic 3)
A university policy must allow open access to resources on the Internet for research, but internal workstations are exposed to malware. Which Cisco AMP feature allows the engineering team to determine whether a file is installed on a selected few workstations?

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

Answer: A

NEW QUESTION 100
- (Exam Topic 3)
What is the recommendation in a zero-trust model before granting access to corporate applications and resources?

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

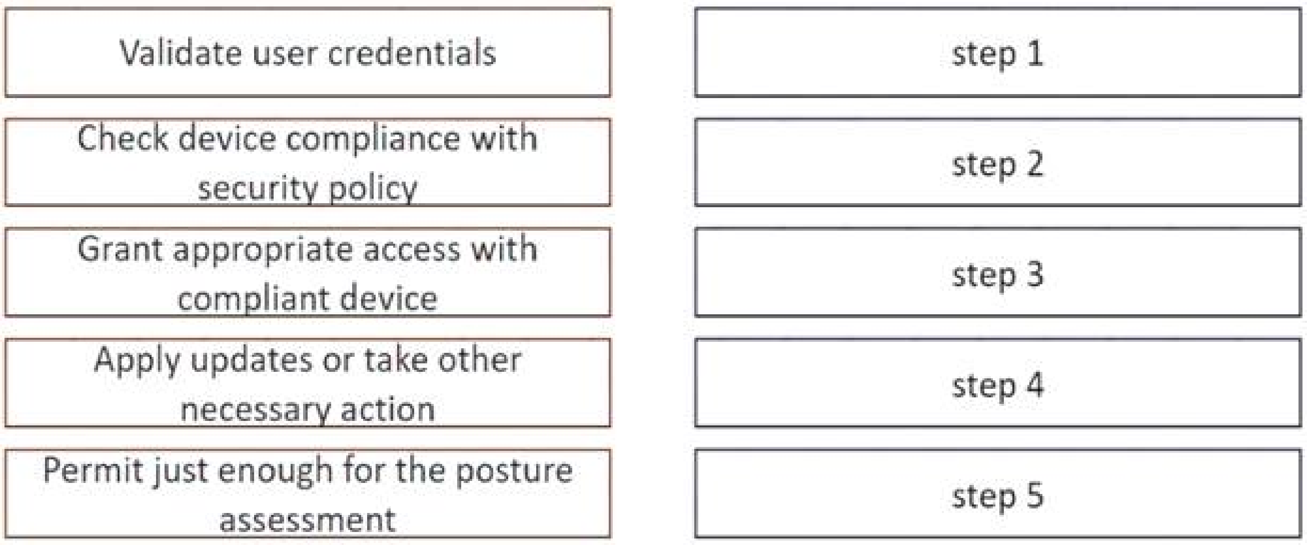
Answer: A

NEW QUESTION 102
- (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 105
- (Exam Topic 3)
Drag and drop the posture assessment flow actions from the left into a sequence on the right.

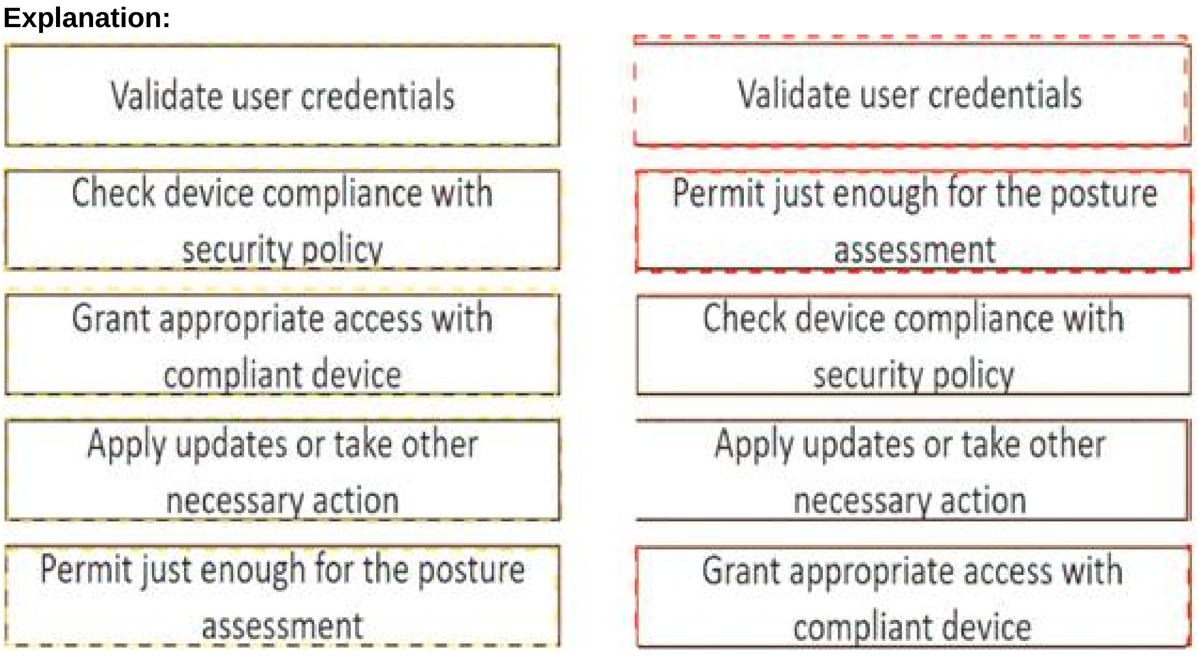


Validate user credentials	step 1
Check device compliance with security policy	step 2
Grant appropriate access with compliant device	step 3
Apply updates or take other necessary action	step 4
Permit just enough for the posture assessment	step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

NEW QUESTION 108
- (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 111
- (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 114
- (Exam Topic 3)
Which feature does the laaS model provide?

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

Answer: C

NEW QUESTION 115
- (Exam Topic 3)
An organization configures Cisco Umbrella to be used for its DNS services. The organization must be able to block traffic based on the subnet that the endpoint is on but it sees only the requests from its public IP address instead of each internal IP address. What must be done to resolve this issue?

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

Answer: A

NEW QUESTION 118
- (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 119
- (Exam Topic 3)
A network engineer must configure a Cisco ESA to prompt users to enter two forms of information before gaining access The Cisco ESA must also join a cluster machine using preshared keys What must be configured to meet these requirements?

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

Answer: A

NEW QUESTION 120
- (Exam Topic 3)
Refer to the exhibit. When creating an access rule for URL filtering, a network engineer adds certain categories and individual URLs to block. What is the result of the configuration?

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

Answer: A

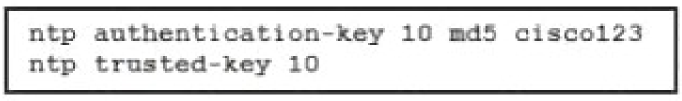
NEW QUESTION 125

- (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 129
- (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.

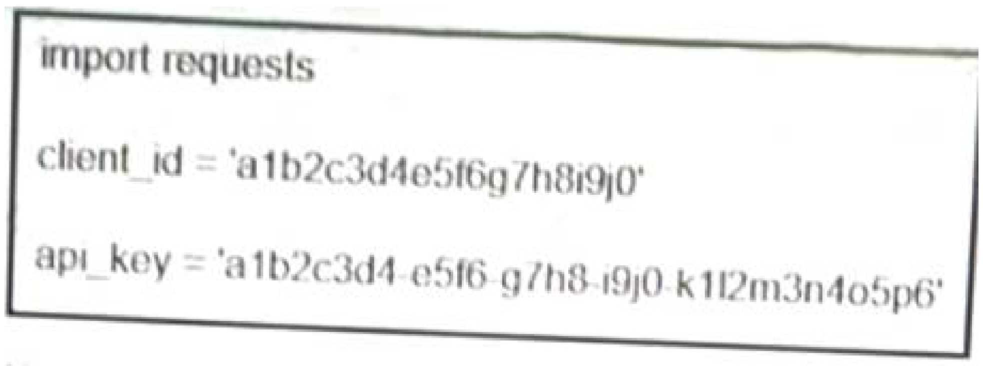
Answer: B

NEW QUESTION 133
- (Exam Topic 3)
Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)

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

Answer: AE

NEW QUESTION 138
- (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 141
- (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 146
- (Exam Topic 3)
An administrator is configuring N I P on Cisco ASA via ASDM and needs to ensure that rogue NTP servers cannot insert themselves as the authoritative time source Which two steps must be taken to accomplish this task? (Choose two)

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

Answer: CD

NEW QUESTION 147
- (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 150
- (Exam Topic 3)
A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to
ensure that bandwidth is available for VPN users needing access to corporate resources on the10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the
network?

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

Answer: A

NEW QUESTION 155
- (Exam Topic 3)
Which endpoint solution protects a user from a phishing attack?

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

Answer: D

NEW QUESTION 156
- (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 161
- (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 163
- (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 166
- (Exam Topic 3)
A network engineer entered the snmp-server user asmith myv7 auth sha cisco priv aes 256 cisc0xxxxxxxxx command and needs to send SNMP information to a host at 10.255.255.1. Which command achieves this goal?

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

Answer: C

NEW QUESTION 168
- (Exam Topic 3)
Which algorithm is an NGE hash function?

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

Answer: D

NEW QUESTION 169
- (Exam Topic 3)
Which method of attack is used by a hacker to send malicious code through a web application to an unsuspecting user to request that the victim's web browser executes the code?

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

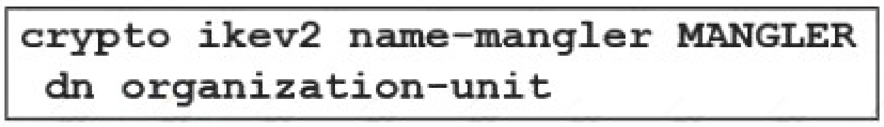
Answer: D

NEW QUESTION 173
- (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 175
- (Exam Topic 3)
Refer to the exhibit.



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

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

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

Answer: A

NEW QUESTION 177

- (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 178
- (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 181
- (Exam Topic 3)
An engineer is configuring device-hardening on a router in order to prevent credentials from being seen if the router configuration was compromised. Which command should be used?

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

Answer: A

NEW QUESTION 184
- (Exam Topic 3)
Which feature must be configured before implementing NetFlow on a router?

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

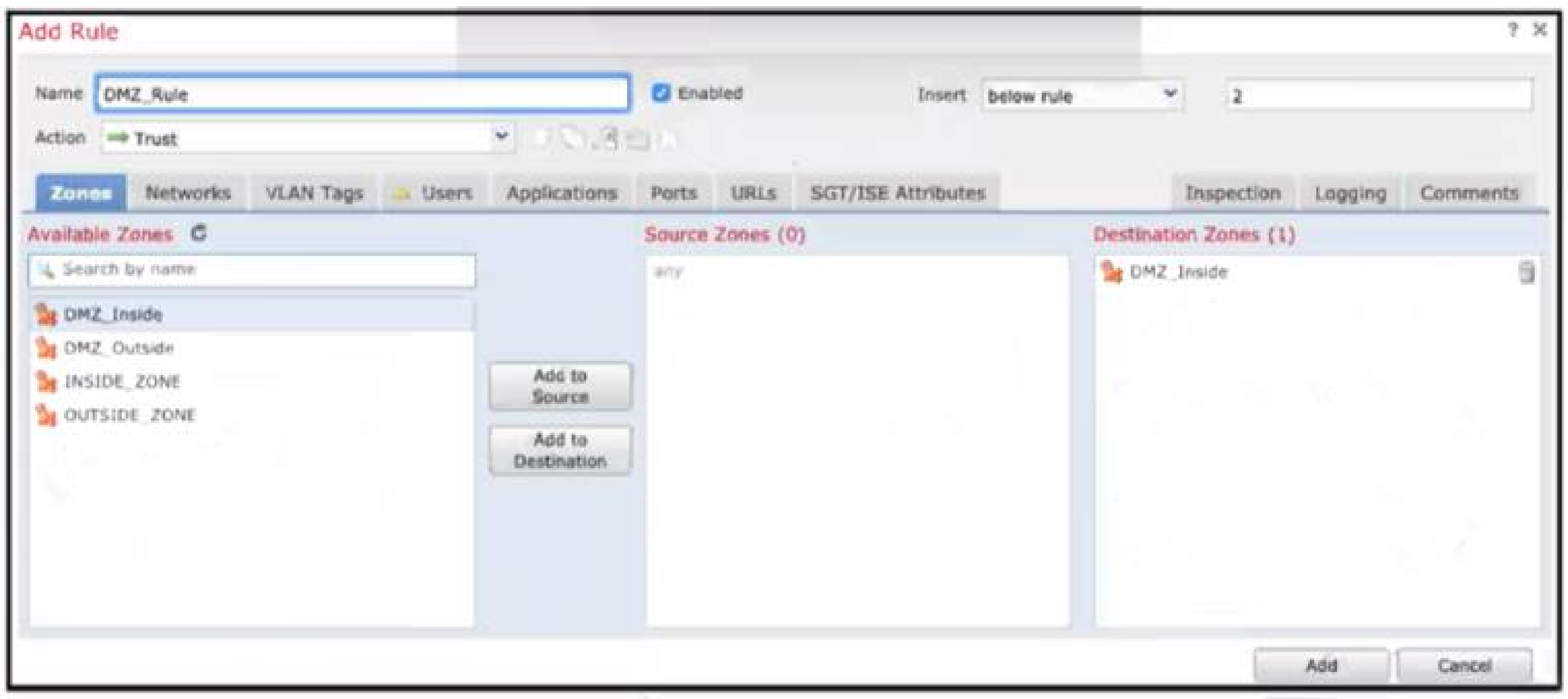
Answer: D

NEW QUESTION 187
- (Exam Topic 3)
In which scenario is endpoint-based security the solution?

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

Answer: C

NEW QUESTION 192
- (Exam Topic 3)



Name DMZ_Rule ☑ Enabled Insert below rule 2

Action ➡ Trust

Available Zones: DMZ_Inside, DMZ_Outside, INSIDE_ZONE, OUTSIDE_ZONE

Source Zones (0): any

Destination Zones (1): DMZ_Inside

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

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

Answer: A

NEW QUESTION 193
- (Exam Topic 3)
What is the most commonly used protocol for network telemetry?

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

Answer: D

NEW QUESTION 195
- (Exam Topic 3)
Which ESA implementation method segregates inbound and outbound email?

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

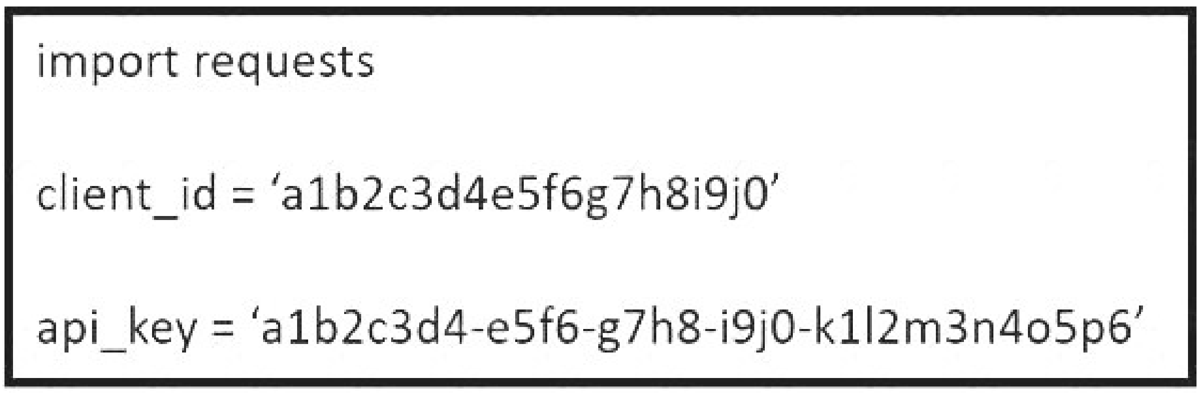
Answer: D

NEW QUESTION 197
- (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 201
- (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 205
- (Exam Topic 3)
Which parameter is required when configuring a Netflow exporter on a Cisco Router?

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

Answer: C

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

NEW QUESTION 209
- (Exam Topic 3)
What are two workloaded security models? (Choose two)

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

Answer: CD

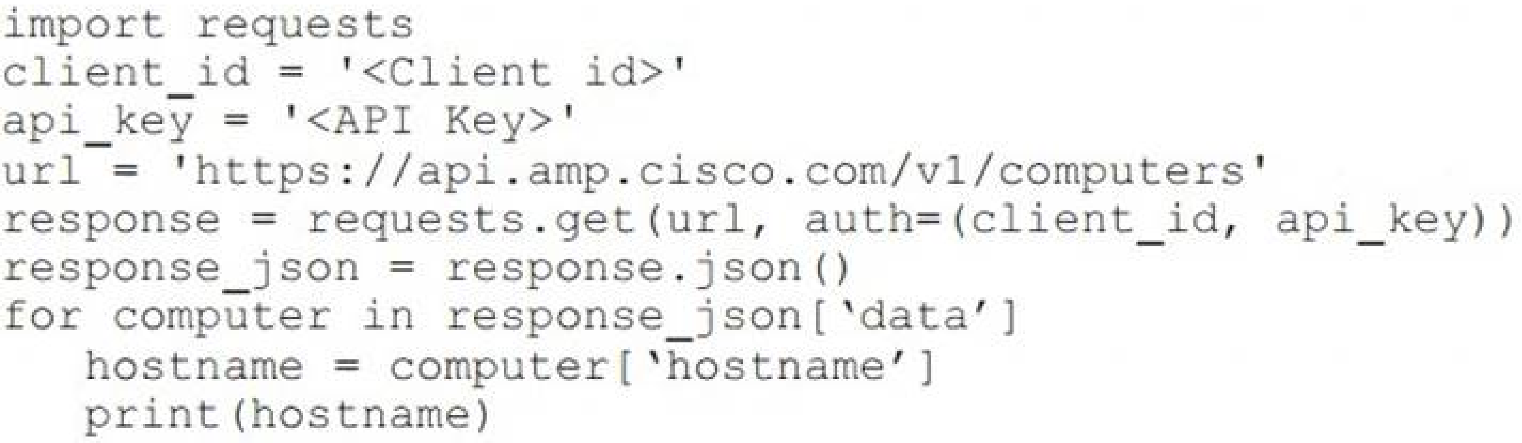
NEW QUESTION 212
- (Exam Topic 2)
An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?

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

Answer: D

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

NEW QUESTION 215
- (Exam Topic 2)
Refer to the exhibit.



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

What will happen when the Python script is executed?

A. The hostname will be translated to an IP address and printed.
B. The hostname will be printed for the client in the client ID field.
C. The script will pull all computer hostnames and print them.
D. The script will translate the IP address to FODN and print it

Answer: C

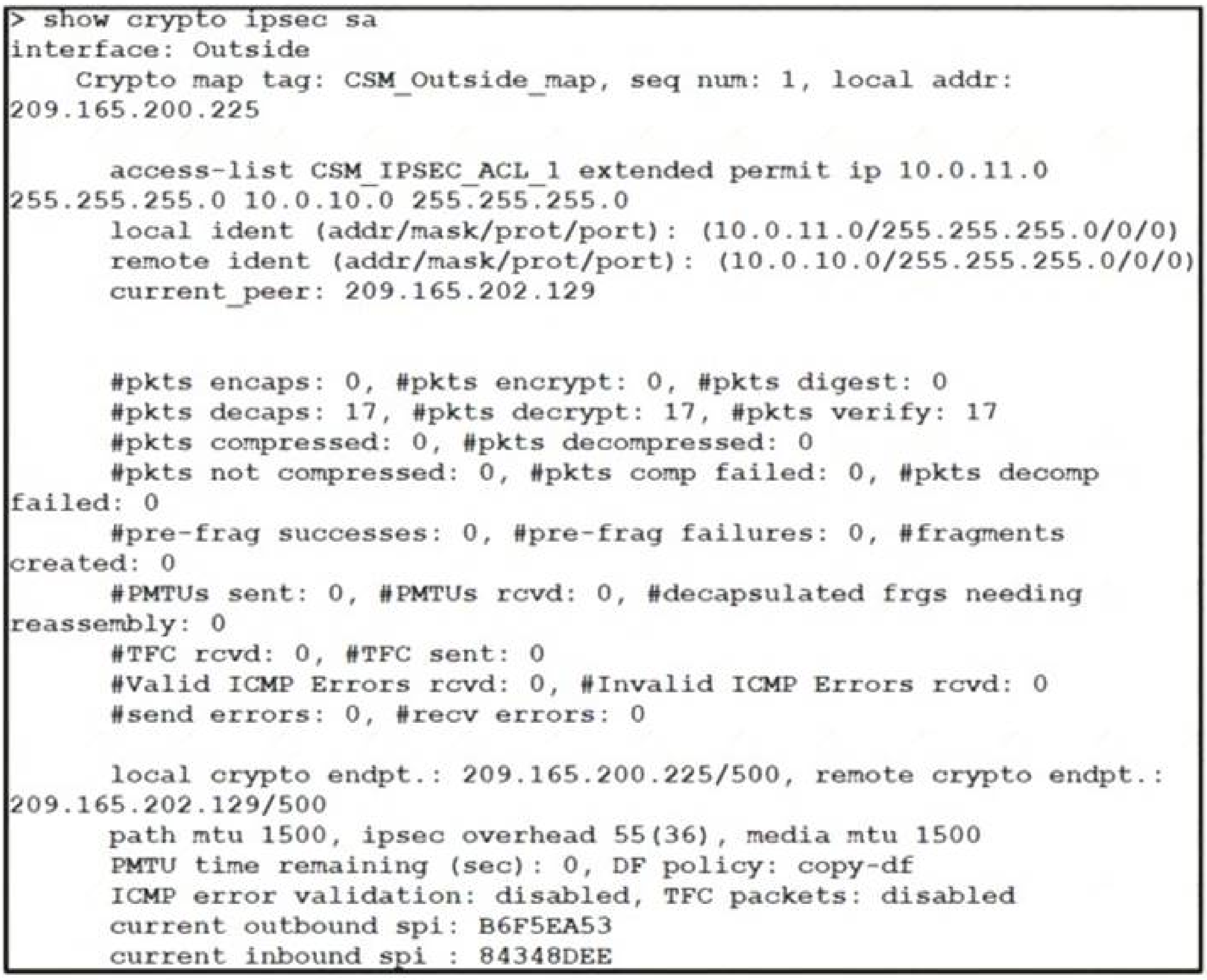
NEW QUESTION 220
- (Exam Topic 2)
An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?

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 224
- (Exam Topic 2)
Refer to the exhibit.



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

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


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

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

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

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

Answer: A

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

NEW QUESTION 228
- (Exam Topic 2)
A switch with Dynamic ARP Inspection enabled has received a spoofed ARP response on a trusted interface. How does the switch behave in this situation?

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

Answer: B

NEW QUESTION 229
- (Exam Topic 2)
What is the function of SDN southbound API protocols?

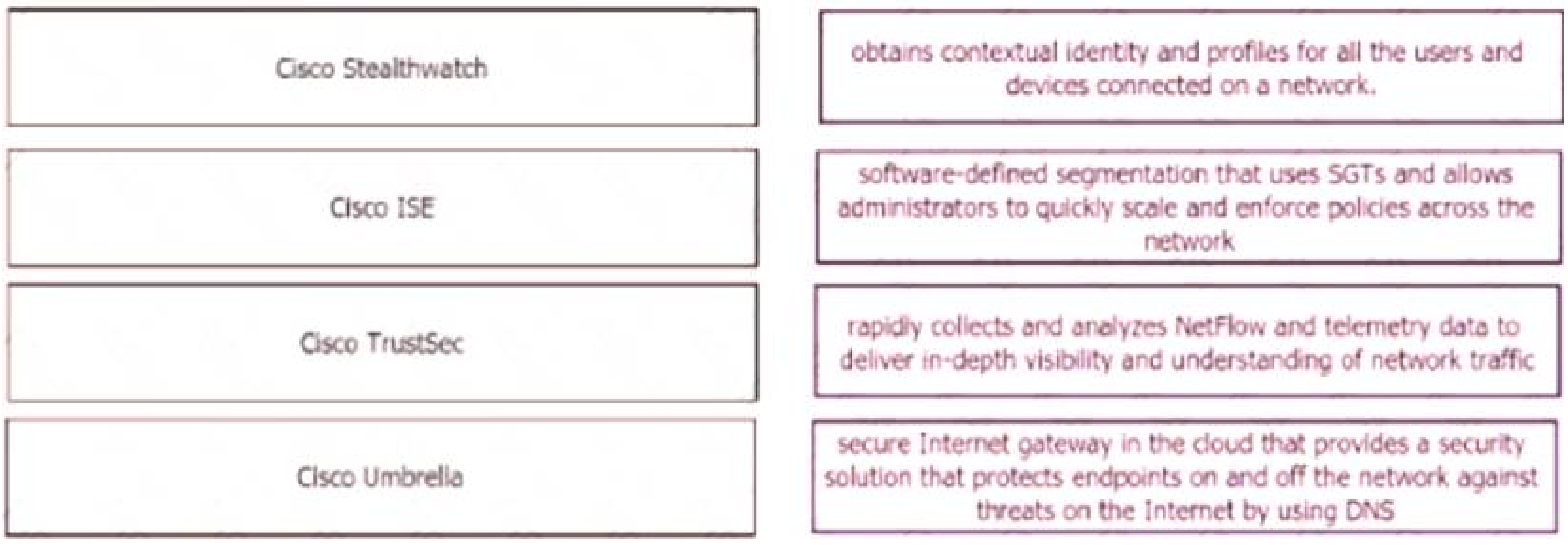
A. to allow for the dynamic configuration of control plane applications
B. to enable the controller to make changes
C. to enable the controller to use REST

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 230
- (Exam Topic 2)
Drag and drop the solutions from the left onto the solution's benefits on the right.



Cisco Stealthwatch

Cisco ISE

Cisco TrustSec

Cisco Umbrella

obtains contextual identity and profiles for all the users and devices connected on a network.

software-defined segmentation that uses SGTs and allows administrators to quickly scale and enforce policies across the network

rapidly collects and analyzes NetFlow and telemetry data to deliver in-depth visibility and understanding of network traffic

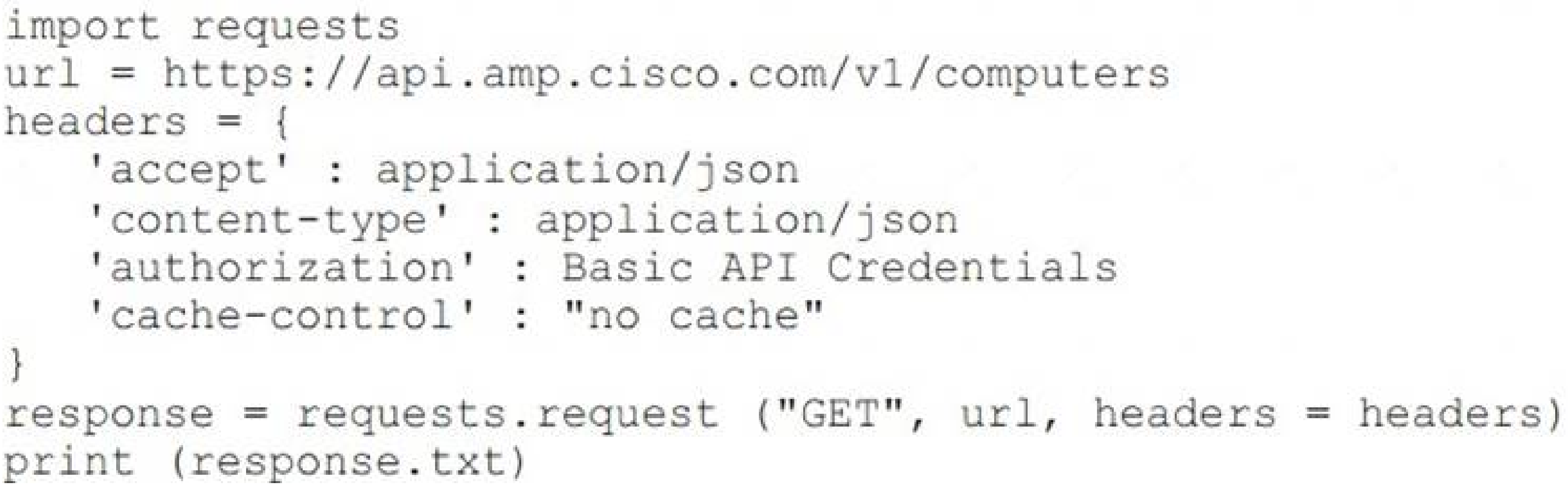
secure Internet gateway in the cloud that provides a security solution that protects endpoints on and off the network against threats on the Internet by using DNS

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Cisco Stealthwatch - rapidly collects and analyzes netflow and telementy data to deliver in-depth visibility and understanding of network traffic
Cisco ISE – obtains contextual identity and profiles for all users and device
Cisco TrustSec – software defined segmentation that uses SGTs
Cisco Umbrella – secure internet gateway ion the cloud that provides a security solution

NEW QUESTION 235
- (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 236
- (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 241
- (Exam Topic 2)
When configuring ISAKMP for IKEv1 Phase1 on a Cisco IOS router, an administrator needs to input the command crypto isakmp key cisco address 0.0.0.0. The administrator is not sure what the IP addressing in this command issued for. What would be the effect of changing the IP address from 0.0.0.0 to 1.2.3.4?

A. The key server that is managing the keys for the connection will be at 1.2.3.4
B. The remote connection will only be allowed from 1.2.3.4
C. The address that will be used as the crypto validation authority
D. All IP addresses other than 1.2.3.4 will be allowed

Answer: B

Explanation:
The command crypto isakmp key cisco address 1.2.3.4 authenticates the IP address of the 1.2.3.4 peer by using the key cisco. The address of “0.0.0.0” will authenticate any address with this key

NEW QUESTION 243
- (Exam Topic 2)
Which algorithm provides asymmetric encryption?

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

Answer: C

NEW QUESTION 245
- (Exam Topic 2)
What is a key difference between Cisco Firepower and Cisco ASA?

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

Answer: C

NEW QUESTION 246
- (Exam Topic 2)
Which attack is preventable by Cisco ESA but not by the Cisco WSA?

A. buffer overflow
B. DoS
C. SQL injection
D. phishing

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advance

NEW QUESTION 249
- (Exam Topic 2)
What does Cisco AMP for Endpoints use to help an organization detect different families of malware?

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

Answer: A

Explanation:
Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdfETHOS = Fuzzy Fingerprinting using static/passive heuristics
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/BRKSEC-2139.pdf

NEW QUESTION 252

- (Exam Topic 2)
What is a function of 3DES in reference to cryptography?

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

Answer: C

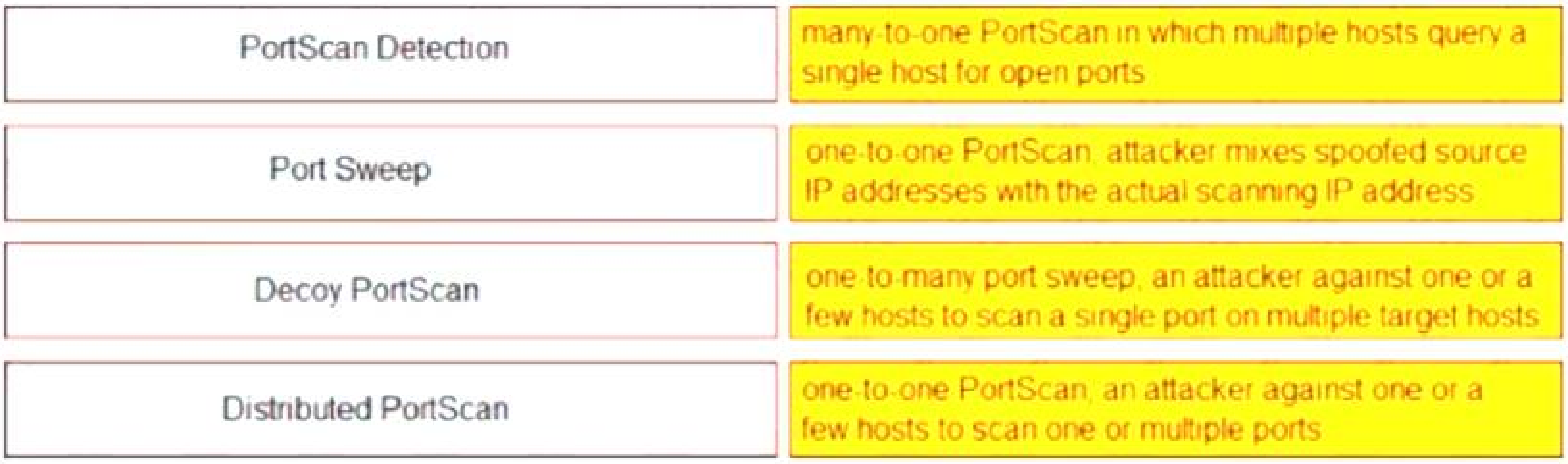
NEW QUESTION 256
- (Exam Topic 2)
Which public cloud provider supports the Cisco Next Generation Firewall Virtual?

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 257
- (Exam Topic 2)
Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.



PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A picture containing table Description automatically generated

NEW QUESTION 262
- (Exam Topic 2)
An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco Firepower. Which feature should be used to accomplish this?

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

Answer: A

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

NEW QUESTION 267
- (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 268
- (Exam Topic 2)
An organization has a Cisco ESA set up with policies and would like to customize the action assigned for violations. The organization wants a copy of the message to be delivered with a message added to flag it as a DLP violation. Which actions must be performed in order to provide this capability?

A. deliver and send copies to other recipients
B. quarantine and send a DLP violation notification
C. quarantine and alter the subject header with a DLP violation
D. deliver and add disclaimer text

Answer: D

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

NEW QUESTION 273
- (Exam Topic 2)
An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?

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

Answer: D

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

NEW QUESTION 276
- (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 281
- (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 285
- (Exam Topic 2)
What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

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

Answer: B

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

NEW QUESTION 290
- (Exam Topic 2)
An engineer has enabled LDAP accept queries on a listener. Malicious actors must be prevented from quickly identifying all valid recipients. What must be done on the Cisco ESA to accomplish this goal?

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

Answer: C

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

NEW QUESTION 295
- (Exam Topic 2)
What is an attribute of the DevSecOps process?

A. mandated security controls and check lists
B. security scanning and theoretical vulnerabilities
C. development security
D. isolated security team

Answer: C

Explanation:
DevSecOps (development, security, and operations) is a concept used in recent years to describe how to movesecurity activities to the start of the development life cycle and have built-in security practices in the continuousintegration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closerto IT and business objectives.Three key things make a real DevSecOps environment:+ Security testing is done by the development team.+ Issues found during that testing is managed by the development team.+ Fixing those issues stays within the development team.

NEW QUESTION 299
- (Exam Topic 2)
An organization is trying to implement micro-segmentation on the network and wants to be able to gain visibility on the applications within the network. The solution must be able to maintain and force compliance. Which product should be used to meet these requirements?

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

Answer: D

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

NEW QUESTION 300
- (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 305
- (Exam Topic 2)
A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?

A. Use MAB with profiling
B. Use MAB with posture assessment.

C. Use 802.1X with posture assessment.
D. Use 802.1X with profiling.

Answer: A

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

NEW QUESTION 306
- (Exam Topic 1)
What is the primary role of the Cisco Email Security Appliance?

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

Answer: B

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

NEW QUESTION 308
- (Exam Topic 2)
Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?

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

Answer: C

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

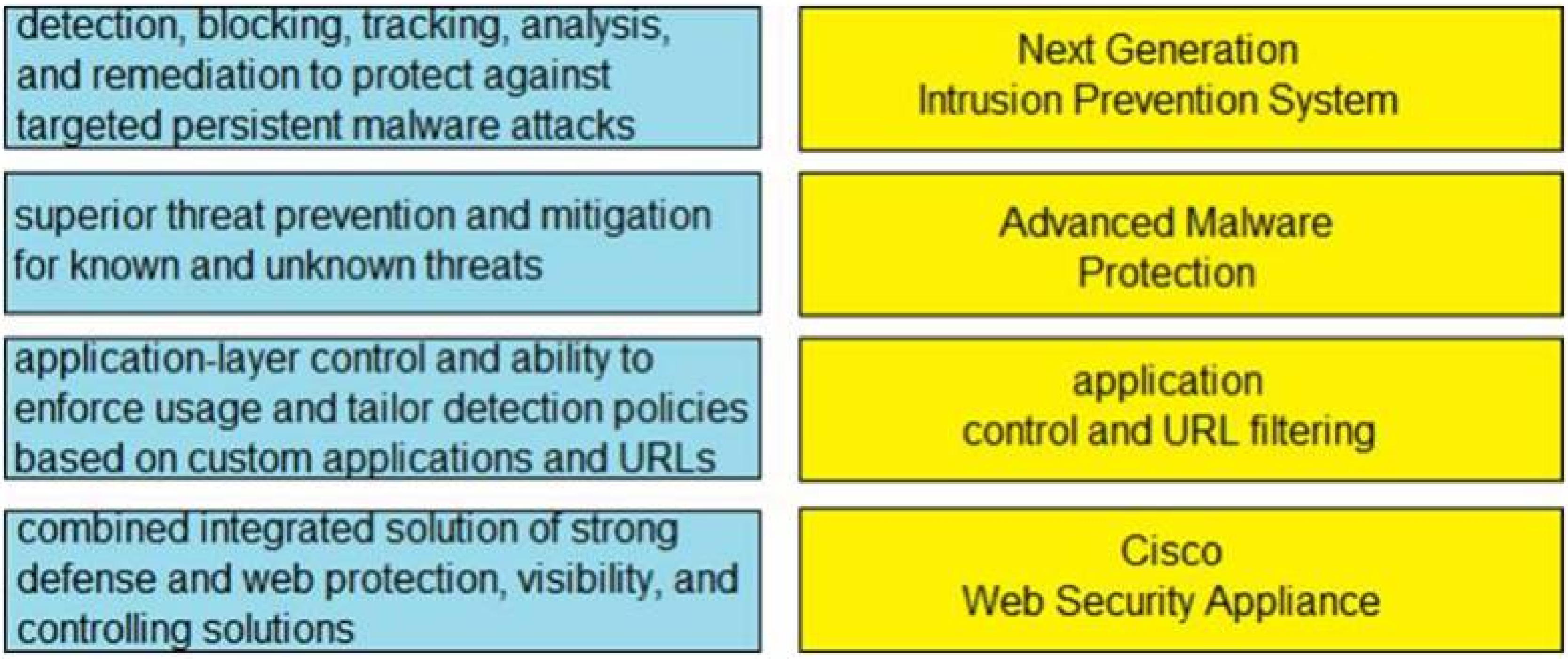
NEW QUESTION 311
- (Exam Topic 2)
A Cisco Firepower administrator needs to configure a rule to allow a new application that has never been seen on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose
two)

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 312
- (Exam Topic 2)
Drag and drop the capabilities from the left onto the correct technologies on the right.



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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, chat or text message Description automatically generated

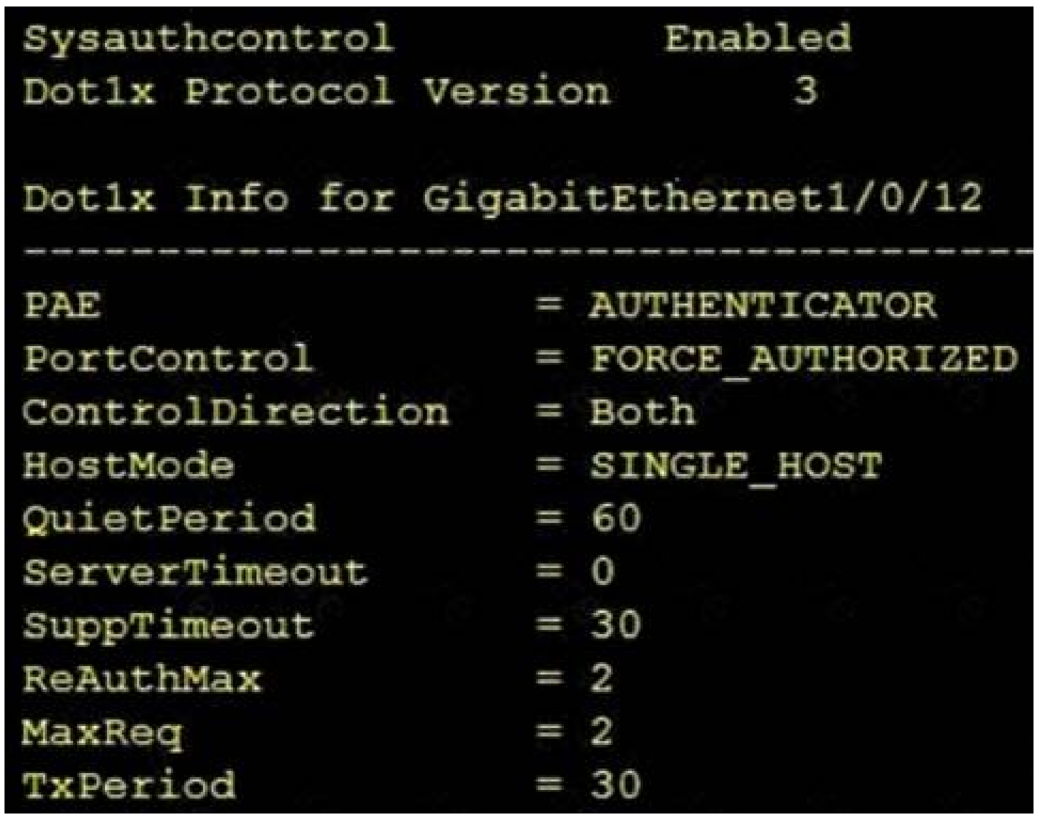
NEW QUESTION 313
- (Exam Topic 2)
What is a benefit of using Cisco FMC over Cisco ASDM?

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

Answer: B

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

NEW QUESTION 316
- (Exam Topic 1)
Refer to the exhibit.



```
Sysauthcontrol              Enabled
Dot1x Protocol Version            3

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

Which command was used to display this output?

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

Answer: A

NEW QUESTION 321
- (Exam Topic 1)
What is a commonality between DMVPN and FlexVPN technologies?

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

Answer: D

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

NEW QUESTION 325
- (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 327
- (Exam Topic 1)
Which feature is supported when deploying Cisco ASAv within AWS public cloud?

A. multiple context mode
B. user deployment of Layer 3 networks
C. IPv6
D. clustering

Answer: B

Explanation:
The ASAv on AWS supports the following features:+ Support for Amazon EC2 C5 instances, the next generation of the Amazon EC2 Compute Optimized instancefamily.+ Deployment in the Virtual Private Cloud (VPC)+ Enhanced networking (SR-IOV) where available+ Deployment from Amazon Marketplace+ Maximum of four vCPUs per instance+ User deployment of L3 networks+ Routed mode (default)Note: The Cisco Adaptive Security Virtual Appliance (ASAv) runs the same software as physical Cisco ASAs to deliver proven security functionality in a virtual form factor. The ASAv can be deployed in the public AWS cloud.It can then be configured to protect virtual and physical data center workloads that expand, contract, or shift their location over time. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96 qsg/asavaws.html

NEW QUESTION 329
- (Exam Topic 1)
Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two)

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

Answer: AC

NEW QUESTION 333
- (Exam Topic 1)
Why would a user choose an on-premises ESA versus the CES solution?

A. Sensitive data must remain onsite.
B. Demand is unpredictable.
C. The server team wants to outsource this service.
D. ESA is deployed inline.

Answer: A

NEW QUESTION 336
- (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 securityinfrastructure both on premises and in the cloud. You can change the number of on-premises versus cloudusers 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 338
- (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

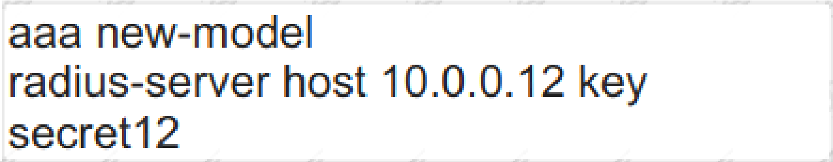
NEW QUESTION 341

- (Exam Topic 1)
Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?

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

Answer: B

NEW QUESTION 344
- (Exam Topic 1)
Refer to the exhibit.



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

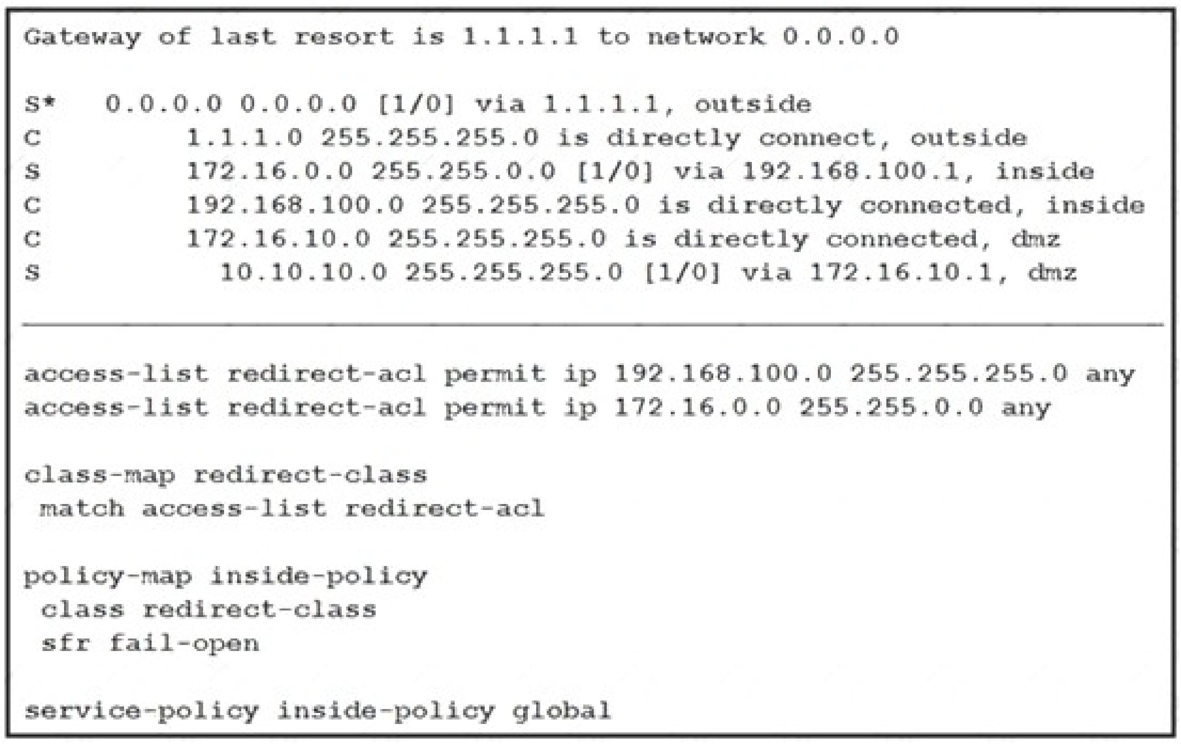
Which statement about the authentication protocol used in the configuration is true?

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

Answer: C

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

NEW QUESTION 347
- (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 351
- (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

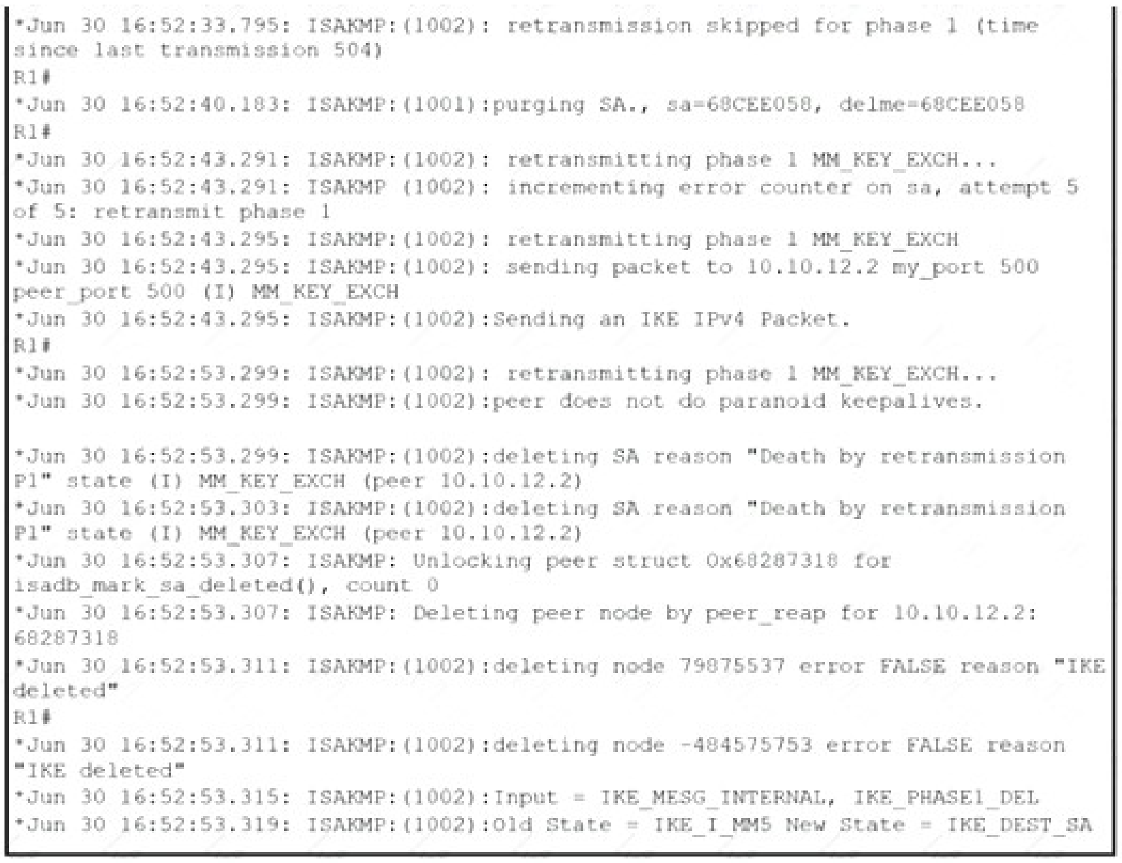
Explanation:
The AES encryption algorithm encrypts and decrypts data in blocks of 128 bits (block size). It can do this using 128-bit, 192-bit, or 256-bit keys

NEW QUESTION 356
- (Exam Topic 1)
Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?

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

Answer: C

NEW QUESTION 361
- (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_MESG_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 363
- (Exam Topic 1)
What are two reasons for implementing a multifactor authentication solution such as Duo Security provide to an organization? (Choose two)

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

Answer: AD

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

NEW QUESTION 365
- (Exam Topic 1)
Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

A. AMP
B. AnyConnect
C. DynDNS
D. Talos

Answer: D

Explanation:
When Umbrella receives a DNS request, it uses intelligence to determine if the request is safe, malicious or risky — meaning the domain contains both malicious and legitimate content. Safe and malicious requests are routed as usual or blocked, respectively. Risky requests are routed to our cloud-based proxy for deeper inspection. The Umbrella proxy uses Cisco Talos web reputation and other third-party feeds to determine if a URL is malicious.

NEW QUESTION 366
- (Exam Topic 1)
A company is experiencing exfiltration of credit card numbers that are not being stored on-premise. The company needs to be able to protect sensitive data throughout the full environment. Which tool should be used to accomplish this goal?

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

Answer: B

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

NEW QUESTION 368
- (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 372
- (Exam Topic 1)
An engineer is configuring AMP for endpoints and wants to block certain files from executing. Which outbreak control method is used to accomplish this task?

A. device flow correlation
B. simple detections
C. application blocking list
D. advanced custom detections

Answer: C

NEW QUESTION 375
- (Exam Topic 1)
What is a characteristic of traffic storm control behavior?

A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
B. Traffic storm control cannot determine if the packet is unicast or broadcast.
C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

Answer: A

NEW QUESTION 376
- (Exam Topic 1)
A network engineer is configuring DMVPN and entered the crypto isakmp key cisc0380739941 address 1.1.1.1 command on hostA. The tunnel is not being established to hostB. What action is needed to authenticate the VPN?

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

Answer: C

NEW QUESTION 379
- (Exam Topic 1)
What provides visibility and awareness into what is currently occurring on the network?

A. CMX
B. WMI
C. Prime Infrastructure

D. Telemetry

Answer: D

Explanation:
Reference: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/activethreat-analytics

NEW QUESTION 384
- (Exam Topic 1)
Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?

A. RSA SecureID
B. Internal Database
C. Active Directory
D. LDAP

Answer: C

NEW QUESTION 388
- (Exam Topic 1)
Which information is required when adding a device to Firepower Management Center?

A. username and password
B. encryption method
C. device serial number
D. registration key

Answer: D

NEW QUESTION 393
- (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 395
- (Exam Topic 1)
Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

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

Answer: D

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

NEW QUESTION 397
- (Exam Topic 1)
Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

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

Answer: A

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

NEW QUESTION 400
- (Exam Topic 1)
Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two)

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

Answer: BE

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Applic uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

NEW QUESTION 403
- (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 reputablesource. 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 405
- (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 408
- (Exam Topic 1)
Which two mechanisms are used to control phishing attacks? (Choose two)

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

Answer: AE

NEW QUESTION 412
- (Exam Topic 1)
What are two list types within AMP for Endpoints Outbreak Control? (Choose two)

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

Answer: BD

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

NEW QUESTION 417
- (Exam Topic 1)

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

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

Answer: BD

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

NEW QUESTION 421
- (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 423
- (Exam Topic 1)
Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?

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

Answer: C

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

NEW QUESTION 426
- (Exam Topic 1)
Which statement describes a traffic profile on a Cisco Next Generation Intrusion Prevention System?

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

Answer: B

NEW QUESTION 429
- (Exam Topic 1)
Which two statements about a Cisco WSA configured in Transparent mode are true? (Choose two)

A. It can handle explicit HTTP requests.
B. It requires a PAC file for the client web browser.
C. It requires a proxy for the client web browser.
D. WCCP v2-enabled devices can automatically redirect traffic destined to port 80.
E. Layer 4 switches can automatically redirect traffic destined to port 80.

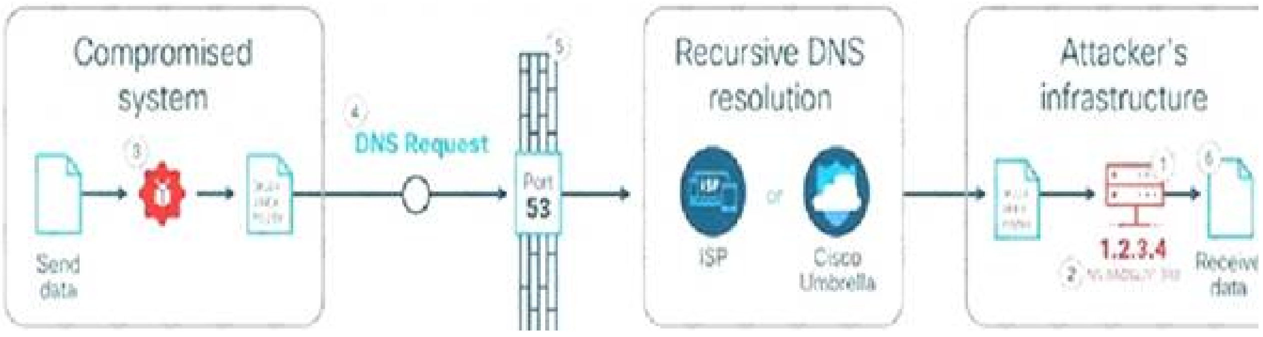
Answer: DE

NEW QUESTION 430
- (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 damageand 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 434
- (Exam Topic 1)
Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?

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

Answer: A

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

NEW QUESTION 437
- (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 438
- (Exam Topic 1)
Which benefit does endpoint security provide the overall security posture of an organization?

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

Answer: D

NEW QUESTION 442
- (Exam Topic 1)
Which feature of Cisco ASA allows VPN users to be postured against Cisco ISE without requiring an inline posture node?

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

Answer: A

NEW QUESTION 445
- (Exam Topic 1)
What is a characteristic of a bridge group in ASA Firewall transparent mode?

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

Answer: A

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

NEW QUESTION 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

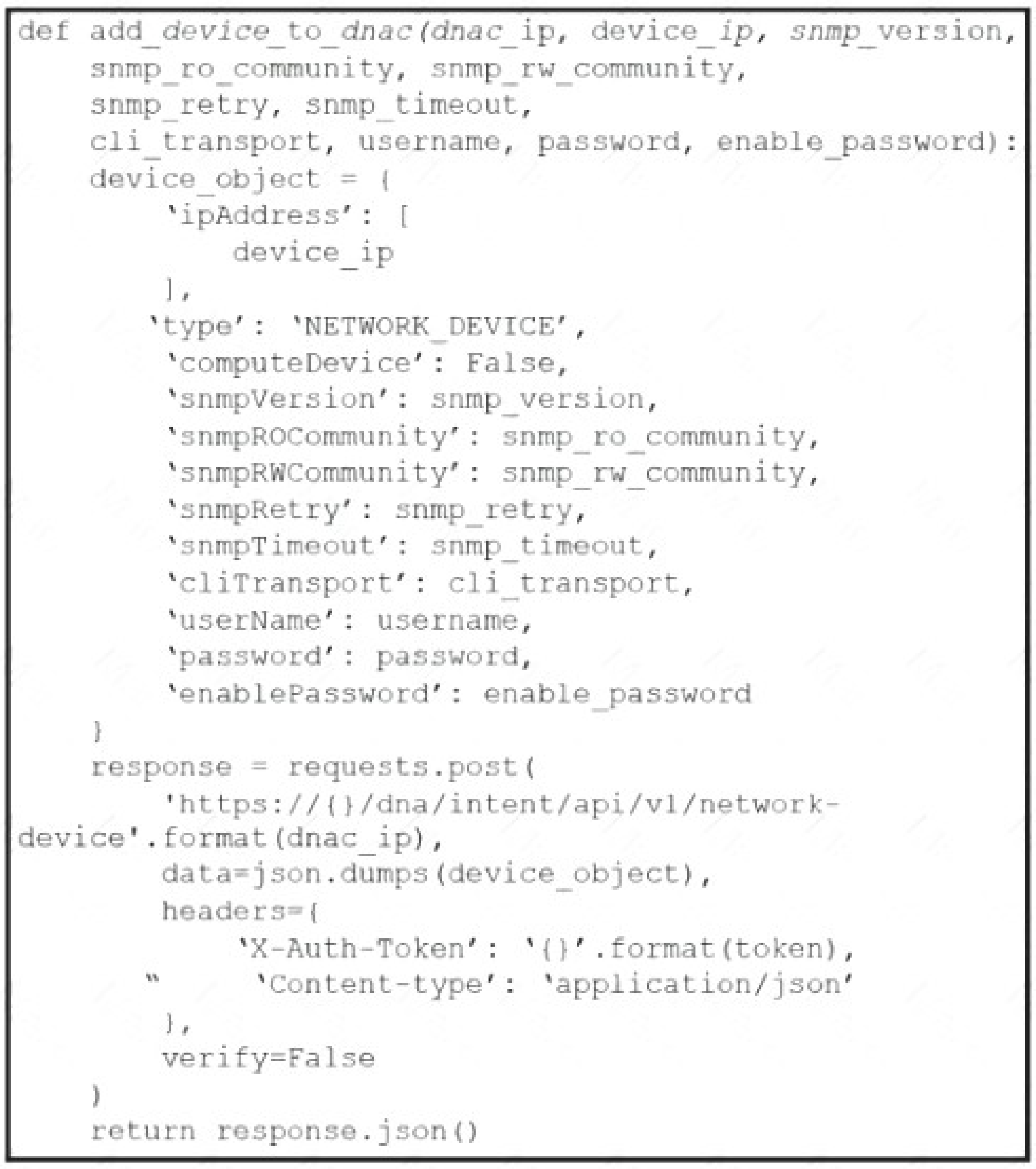
Explanation:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesign

NEW QUESTION 448
- (Exam Topic 1)
Which IPS engine detects ARP spoofing?

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

Answer: A

NEW QUESTION 450
- (Exam Topic 1)
Refer to the exhibit.



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

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

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

Answer: B

NEW QUESTION 451
- (Exam Topic 1)
What is a difference between FlexVPN and DMVPN?

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

Answer: C

NEW QUESTION 456
- (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 460
- (Exam Topic 1)
Which compliance status is shown when a configured posture policy requirement is not met?

A. compliant
B. unknown
C. authorized
D. noncompliant

Answer: D

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 462
- (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 466
- (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 469
- (Exam Topic 1)
Which threat involves software being used to gain unauthorized access to a computer system?

A. virus
B. NTP amplification
C. ping of death
D. HTTP flood

Answer: A

NEW QUESTION 470
- (Exam Topic 1)
Which two behavioral patterns characterize a ping of death attack? (Choose two)

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

Answer: BD

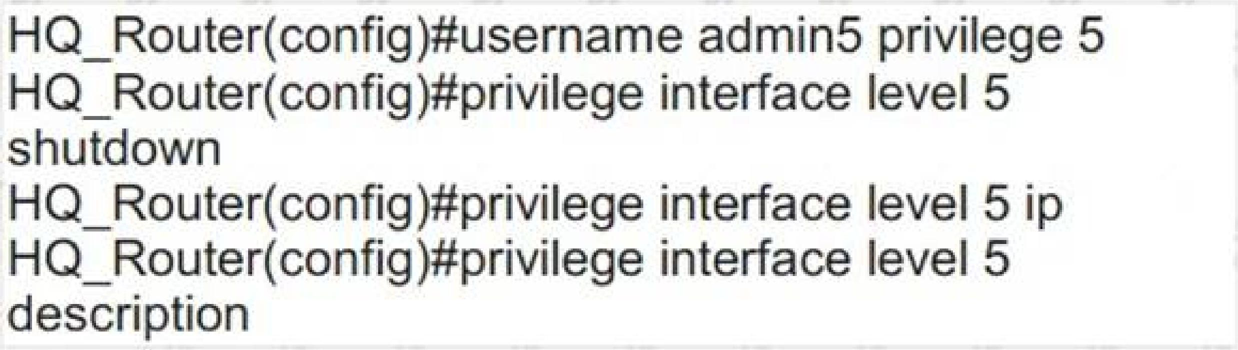
Explanation:
Ping of Death (PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash,destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.A correctly-formed ping packet is typically 56 bytes in size,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

NEW QUESTION 474
- (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 478
- (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 481
- (Exam Topic 1)
An organization has two machines hosting web applications. Machine 1 is vulnerable to SQL injection while machine 2 is vulnerable to buffer overflows. What action would allow the attacker to gain access to machine 1 but not machine 2?

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

Answer: D

NEW QUESTION 485
- (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 486

- (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 488

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

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

Answer: B

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

NEW QUESTION 492

- (Exam Topic 1)
Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?

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

Answer: A

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

NEW QUESTION 497

- (Exam Topic 1)
How many interfaces per bridge group does an ASA bridge group deployment support?

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

Answer: B

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

NEW QUESTION 500

- (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 502
- (Exam Topic 1)
Which feature requires a network discovery policy on the Cisco Firepower Next Generation Intrusion Prevention System?

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

Answer: B

NEW QUESTION 506
- (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 511
- (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 512
- (Exam Topic 3)
Which security solution uses NetFlow to provide visibility across the network, data center, branch offices, and cloud?

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

Answer: B

NEW QUESTION 517
- (Exam Topic 3)
An engineer is trying to decide whether to use Cisco Umbrella, Cisco CloudLock, Cisco Stealthwatch, or Cisco AppDynamics Cloud Monitoring for visibility into data transfers as well as protection against data exfiltration Which solution best meets these requirements?

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

Answer: D

NEW QUESTION 518
- (Exam Topic 3)
An engineer integrates Cisco FMC and Cisco ISE using pxGrid Which role is assigned for Cisco FMC?

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

Answer: D

NEW QUESTION 522
- (Exam Topic 3)
A customer has various external HTTP resources available including Intranet. Extranet, and Internet, with a proxy configuration running in explicit mode Which method allows the client desktop browsers to be configured to select when to connect direct or when to use the proxy?

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

Answer: C

NEW QUESTION 527
- (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 532
- (Exam Topic 3)
What is a characteristic of an EDR solution and not of an EPP solution?

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

Answer: B

NEW QUESTION 533
- (Exam Topic 3)
Which Cisco platform onboards the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing the endpoint to gain network access?

A. Cisco ISE
B. Cisco NAC
C. Cisco TACACS+
D. Cisco WSA

Answer: A

NEW QUESTION 535
- (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 537
- (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 539

- (Exam Topic 3)
An engineer adds a custom detection policy to a Cisco AMP deployment and encounters issues with the configuration. The simple detection mechanism is configured, but the dashboard indicates that the hash is not 64 characters and is non-zero. What is the issue?

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

Answer: A

NEW QUESTION 540
- (Exam Topic 3)
Which CLI command is used to enable URL filtering support for shortened URLs on the Cisco ESA?

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

Answer: B

NEW QUESTION 543
- (Exam Topic 3)
An engineer configures new features within the Cisco Umbrella dashboard and wants to identify and proxy traffic that is categorized as risky domains and may contain safe and malicious content. Which action accomplishes these objectives?

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

Answer: B

NEW QUESTION 548
- (Exam Topic 3)
What is the difference between EPP and EDR?

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

Answer: B

NEW QUESTION 551
- (Exam Topic 3)
An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices. The default management port conflicts with other communications on the network and must be changed. What must be done to ensure that all devices can communicate together?

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

Answer: A

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

NEW QUESTION 553
- (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 554
- (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 557
- (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 559
- (Exam Topic 3)
Which Cisco security solution determines if an endpoint has the latest OS updates and patches installed on the system?

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

Answer: A

NEW QUESTION 561
- (Exam Topic 3)
Which solution stops unauthorized access to the system if a user's password is compromised?

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

Answer: B

NEW QUESTION 562
- (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 564
- (Exam Topic 3)
A network engineer is tasked with configuring a Cisco ISE server to implement external authentication against Active Directory. What must be considered about the authentication requirements? (Choose two.)

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

Answer: BC

NEW QUESTION 566
- (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 571
- (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 576
- (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 579
- (Exam Topic 3)
Which type of attack is MFA an effective deterrent for?

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

Answer: B

NEW QUESTION 581
- (Exam Topic 3)
A network administrator is configuring a role in an access control policy to block certain URLs and selects the "Chat and instant Messaging" category. which reputation score should be selected to accomplish
this goal?

A. 3
B. 5
C. 10
D. 1

Answer: C

NEW QUESTION 582
- (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 587
- (Exam Topic 3)
What are two functionalities of SDN Northbound APIs? (Choose two.)

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

Answer: AB

NEW QUESTION 592
- (Exam Topic 3)
Which action must be taken in the AMP for Endpoints console to detect specific MD5 signatures on endpoints and then quarantine the files?

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

Answer: A

NEW QUESTION 594
- (Exam Topic 3)
What is the process of performing automated static and dynamic analysis of files against preloaded behavioral indicators for threat analysis?

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

Answer: C

NEW QUESTION 597
- (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 performancestatistics. This data can be used for analytics, billing, and security policies.

NEW QUESTION 601
- (Exam Topic 3)
Which two parameters are used to prevent a data breach in the cloud? (Choose two.)

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

Answer: AB

NEW QUESTION 604
- (Exam Topic 3)
What are two things to consider when using PAC files with the Cisco WSA? (Choose two.)

A. If the WSA host port is changed, the default port redirects web traffic to the correct port automatically.
B. PAC files use if-else statements to determine whether to use a proxy or a direct connection for traffic between the PC and the host.
C. The WSA hosts PAC files on port 9001 by default.
D. The WSA hosts PAC files on port 6001 by default.
E. By default, they direct traffic through a proxy when the PC and the host are on the same subnet.

Answer: AD

NEW QUESTION 605
- (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 608
- (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 609
- (Exam Topic 3)
Which function is included when Cisco AMP is added to web security?

A. multifactor, authentication-based user identity
B. detailed analytics of the unknown file's behavior
C. phishing detection on emails
D. threat prevention on an infected endpoint

Answer: B

NEW QUESTION 611
- (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 612
- (Exam Topic 3)
Which industry standard is used to integrate Cisco ISE and pxGrid to each other and with other interoperable security platforms?

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

Answer: B

NEW QUESTION 613
- (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 618
- (Exam Topic 3)
Why should organizations migrate to an MFA strategy for authentication?

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

Answer: A

NEW QUESTION 622
- (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 627
- (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 628
- (Exam Topic 3)
When choosing an algorithm to us, what should be considered about Diffie Hellman and RSA for key establishment?

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

Answer: D

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

NEW QUESTION 630
- (Exam Topic 3)
Which feature is used in a push model to allow for session identification, host reauthentication, and session termination?

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

Answer: C

NEW QUESTION 634
- (Exam Topic 3)
An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1 1 11 using the flow record Stea!thwatch406397954 command Which additional command is required to complete the flow record?

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

Answer: B

NEW QUESTION 635
- (Exam Topic 3)
Which security solution protects users leveraging DNS-layer security?

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

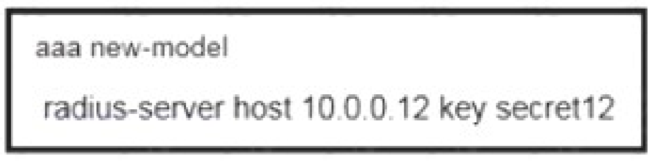
Answer: C

NEW QUESTION 639
- (Exam Topic 3)
Which VMware platform does Cisco ACI integrate with to provide enhanced visibility, provide policy integration and deployment, and implement security policies with access lists?

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

Answer: B

NEW QUESTION 641
- (Exam Topic 3)



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

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

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

Answer: D

NEW QUESTION 646
- (Exam Topic 3)
Which technology provides the benefit of Layer 3 through Layer 7 innovative deep packet inspection, enabling the platform to identify and output various applications within the network traffic flows?

A. Cisco NBAR2
B. Cisco ASAV
C. Account on Resolution
D. Cisco Prime Infrastructure

Answer: A

NEW QUESTION 649
- (Exam Topic 3)
What is the benefit of integrating Cisco ISE with a MDM solution?

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

Answer: A

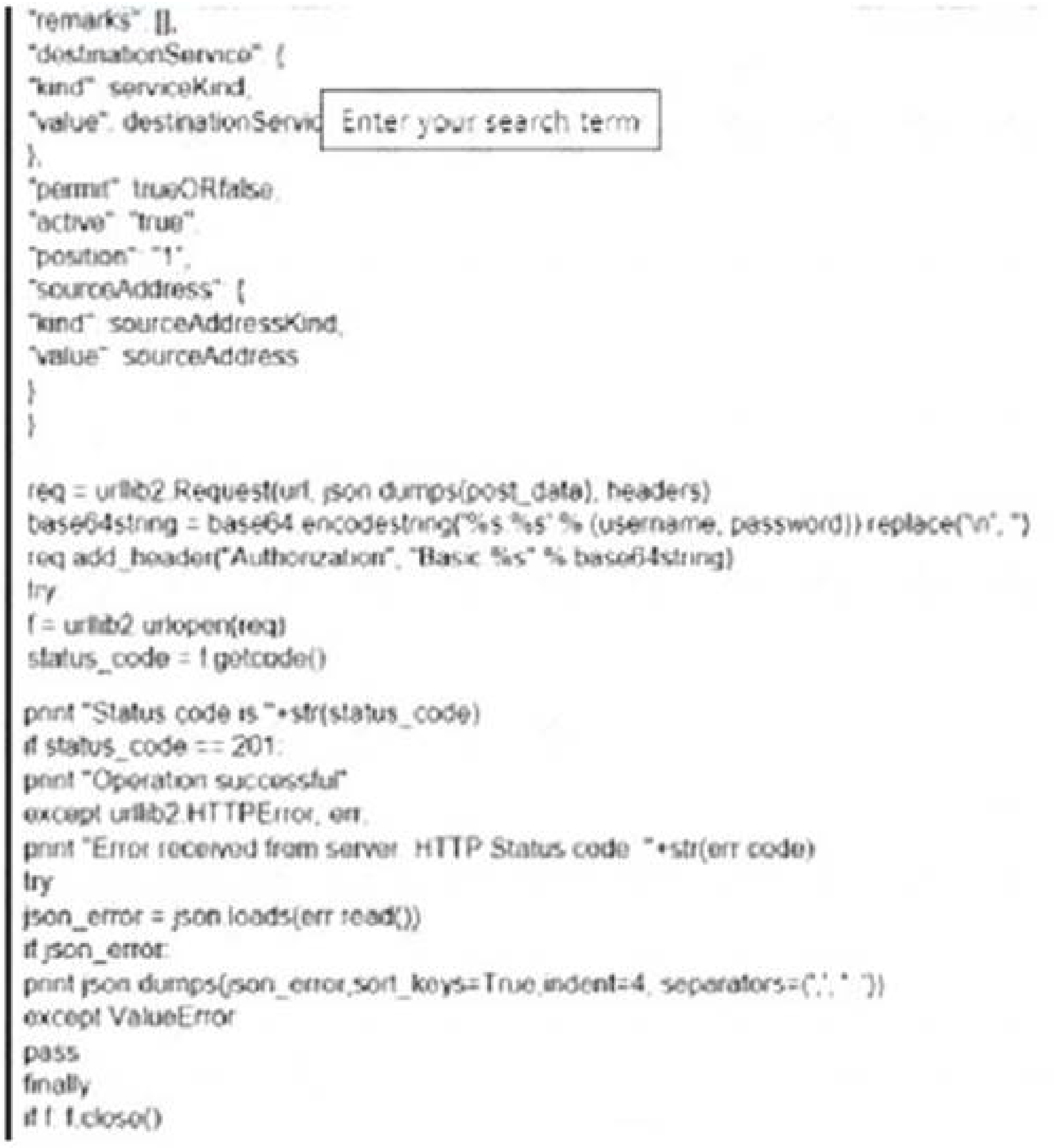
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperab

NEW QUESTION 652
- (Exam Topic 3)
Which Cisco solution extends network visibility, threat detection, and analytics to public cloud environments?

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

Answer: B

NEW QUESTION 655
- (Exam Topic 3)
Refer to the exhibit.



```
"remarks": [],
"destinationService": {
"kind": serviceKind,
"value": destinationServic
},
"permit": trueORfalse,
"active": "true",
"position": "1",
"sourceAddress": {
"kind": sourceAddressKind,
"value": sourceAddress
}
}

req = urllib2.Request(url, json.dumps(post_data), headers)
base64string = base64.encodestring('%s:%s' % (username, password)).replace('\n', '')
req.add_header("Authorization", "Basic %s" % base64string)
try:
f = urllib2.urlopen(req)
status_code = f.getcode()

print "Status code is "+str(status_code)
if status_code == 201:
print "Operation successful"
except urllib2.HTTPError, err:
print "Error received from server. HTTP Status code: "+str(err.code)
try:
json_error = json.loads(err.read())
if json_error:
print json.dumps(json_error,sort_keys=True,indent=4, separators=(',', ': '))
except ValueError:
pass
finally:
if f: f.close()
```

What is the function of the Python script code snippet for the Cisco ASA REST API?

A. adds a global rule into policies
B. changes the hostname of the Cisco ASA
C. deletes a global rule from policies
D. obtains the saved configuration of the Cisco ASA firewall

Answer: A

NEW QUESTION 658
- (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 661
- (Exam Topic 3)
Which feature within Cisco ISE verifies the compliance of an endpoint before providing access to the network?

A. Posture
B. Profiling
C. pxGrid
D. MAB

Answer: A

NEW QUESTION 666
- (Exam Topic 3)
What is a difference between a DoS attack and a DDoS attack?

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

packets

Answer: A

NEW QUESTION 667
- (Exam Topic 3)
What is the difference between a vulnerability and an exploit?

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

Answer: B

NEW QUESTION 672
- (Exam Topic 3)
Which threat intelligence standard contains malware hashes?

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

Answer: C

NEW QUESTION 675
- (Exam Topic 2)
When planning a VPN deployment, for which reason does an engineer opt for an active/active FlexVPN configuration as opposed to DMVPN?

A. Multiple routers or VRFs are required.
B. Traffic is distributed statically by default.
C. Floating static routes are required.
D. HSRP is used for faliover.

Answer: B

NEW QUESTION 676
- (Exam Topic 2)
What are two Trojan malware attacks? (Choose two)

A. Frontdoor
B. Rootkit
C. Smurf
D. Backdoor
E. Sync

Answer: BD

NEW QUESTION 678
- (Exam Topic 2)
How does DNS Tunneling exfiltrate data?

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

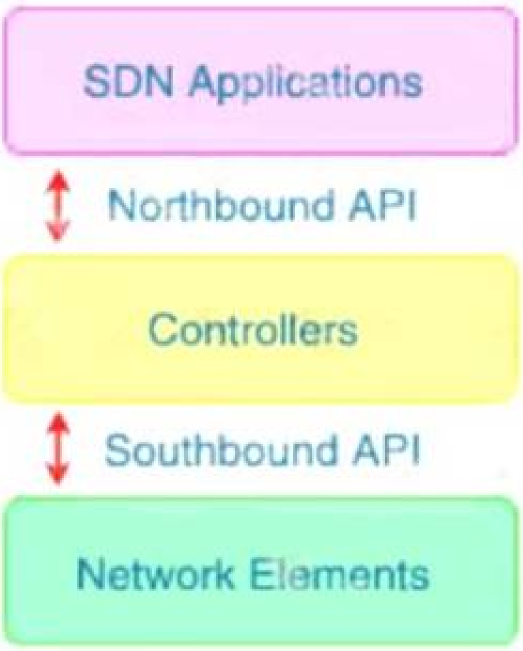
Answer: A

NEW QUESTION 682
- (Exam Topic 2)
Which type of API is being used when a controller within a software-defined network architecture dynamically makes configuration changes on switches within the network?

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

Answer: B

Explanation:
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands andscalability needs.

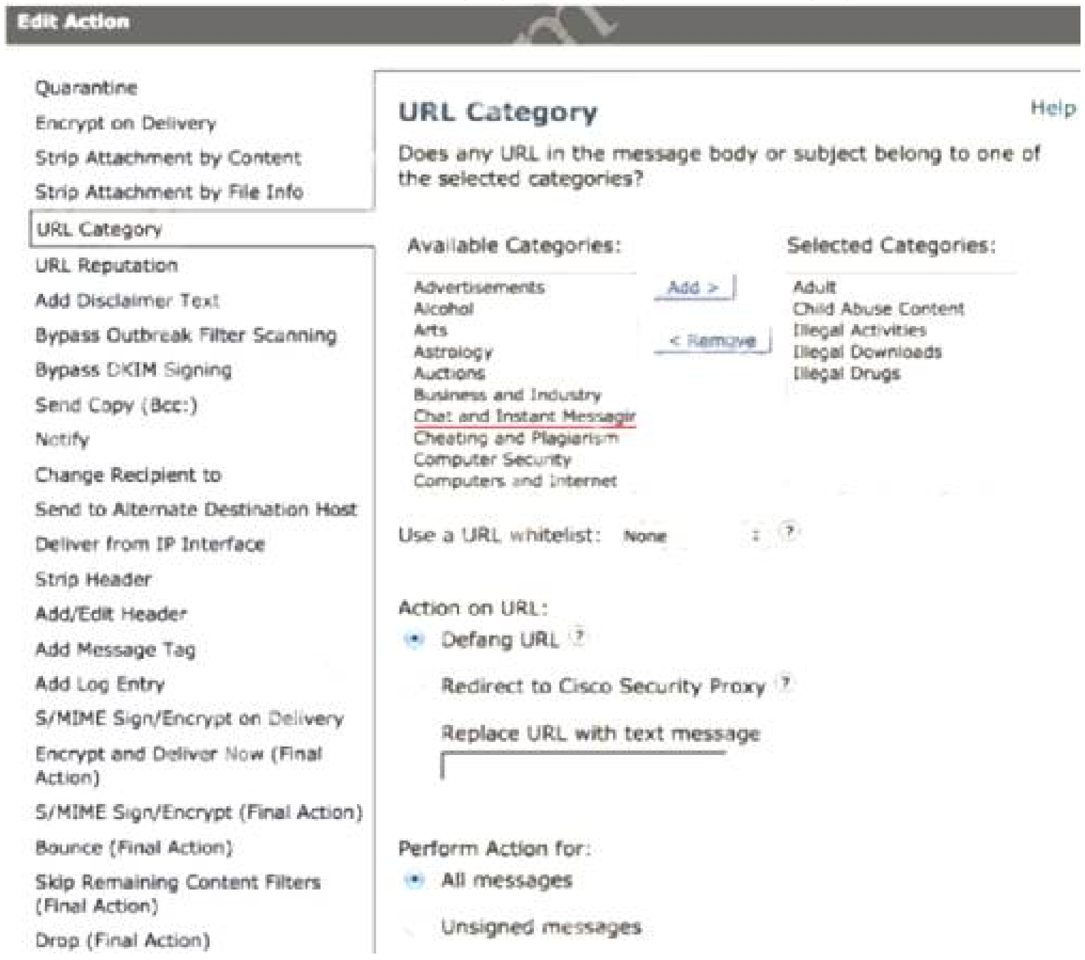


NEW QUESTION 687
- (Exam Topic 2)
A network administrator is configuring a rule in an access control policy to block certain URLs and selects the “Chat and Instant Messaging” category. Which reputation score should be selected to accomplish this goal?

A. 1
B. 3
C. 5
D. 10

Answer: D

Explanation:
We choose “Chat and Instant Messaging” category in “URL Category”:


Edit Action
Quarantine
Encrypt on Delivery
Strip Attachment by Content
Strip Attachment by File Info
URL Category
URL Reputation
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Bypass DKIM Signing
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add/Edit Header
Add Message Tag
Add Log Entry
S/MIME Sign/Encrypt on Delivery
Encrypt and Deliver Now (Final Action)
S/MIME Sign/Encrypt (Final Action)
Bounce (Final Action)
Skip Remaining Content Filters (Final Action)
Drop (Final Action)
Help
Add >
< Remove

URL Category

Does any URL in the message body or subject belong to one of the selected categories?

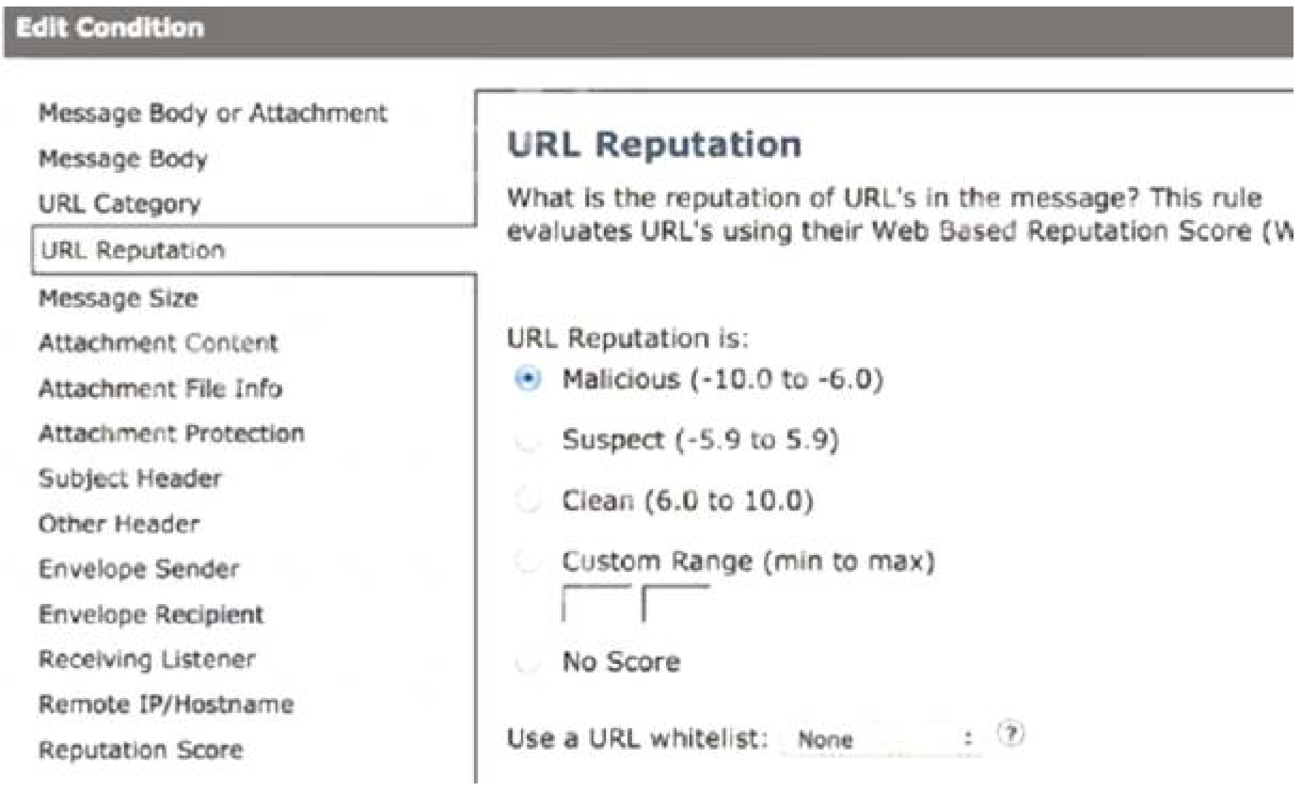
Available Categories:	Selected Categories:
Advertisements Alcohol Arts Astrology Auctions Business and Industry Chat and Instant Messagir Cheating and Plagiarism Computer Security Computers and Internet	Adult Child Abuse Content Illegal Activities Illegal Downloads Illegal Drugs

Use a URL whitelist: None

Action on URL:
● Defang URL
○ Redirect to Cisco Security Proxy
○ Replace URL with text message

Perform Action for:
● All messages
○ Unsigned messages

To block certain URLs we need to choose URL Reputation from 6 to 10.



URL Reputation

What is the reputation of URL's in the message? This rule evaluates URL's using their Web Based Reputation Score (W

URL Reputation is:

● Malicious (-10.0 to -6.0)

○ Suspect (-5.9 to 5.9)

○ Clean (6.0 to 10.0)

○ Custom Range (min to max)

○ No Score

Use a URL whitelist: None

NEW QUESTION 692
- (Exam Topic 2)
Which attack type attempts to shut down a machine or network so that users are not able to access it?

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

Answer: A

Explanation:
Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to itsintended users.The Smurf attack is a DDoS attack in which large numbers of Internet Control Message Protocol (ICMP)packets with the intended victim’s spoofed source IP are broadcast to a computer network using an IPbroadcast address.

NEW QUESTION 696
- (Exam Topic 2)
Which type of API is being used when a security application notifies a controller within a software-defined network architecture about a specific security threat?

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

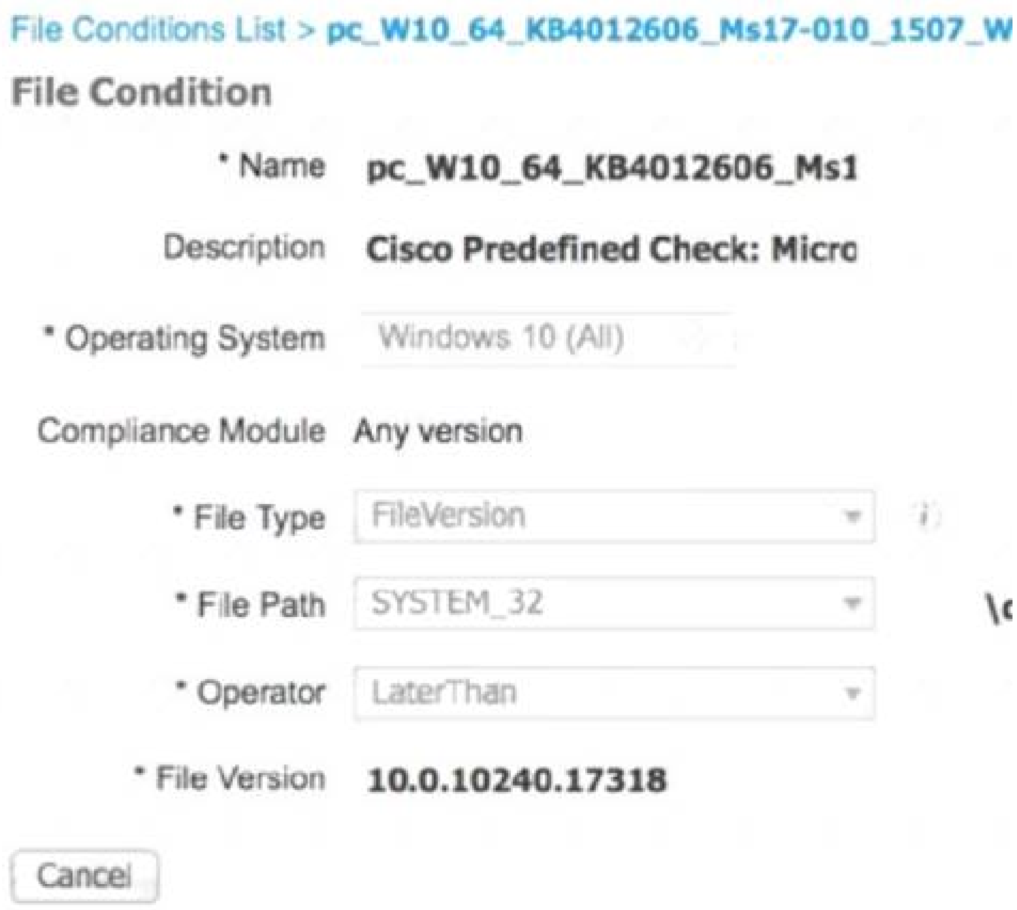
Answer: C

NEW QUESTION 697
- (Exam Topic 2)
Which Cisco platform ensures that machines that connect to organizational networks have the recommended antivirus definitions and patches to help prevent an organizational malware outbreak?

A. Cisco WiSM
B. Cisco ESA
C. Cisco ISE
D. Cisco Prime Infrastructure

Answer: C

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; and we can also configure ISE to update the client with this patch.



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

NEW QUESTION 698

……