

# Cisco

## Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies



**NEW QUESTION 1**

- (Exam Topic 2)

A network administrator is configuring SNMPv3 on a new router. The users have already been created; however, an additional configuration is needed to facilitate access to the SNMP views. What must the administrator do to accomplish this?

- A. map SNMPv3 users to SNMP views
- B. set the password to be used for SNMPv3 authentication
- C. define the encryption algorithm to be used by SNMPv3
- D. specify the UDP port used by SNMP

**Answer: B**

**NEW QUESTION 2**

- (Exam Topic 2)

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

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

**Answer: A**

**Explanation:**

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin\\_guide/b\\_ISE\\_admin\\_guide\\_24/m\\_ise\\_devices\\_by](https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_by)

**NEW QUESTION 3**

- (Exam Topic 2)

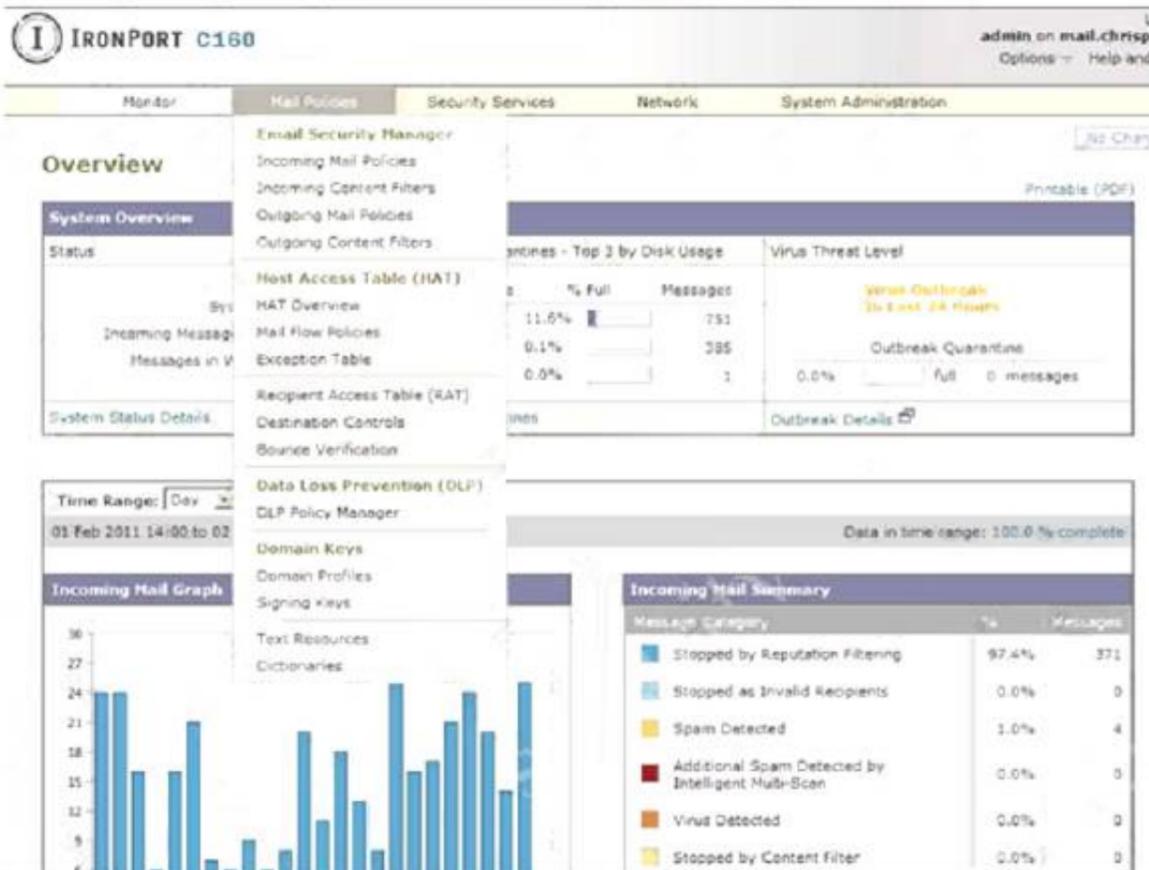
An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically. What must be configured to accomplish this?

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

**Answer: D**

**Explanation:**

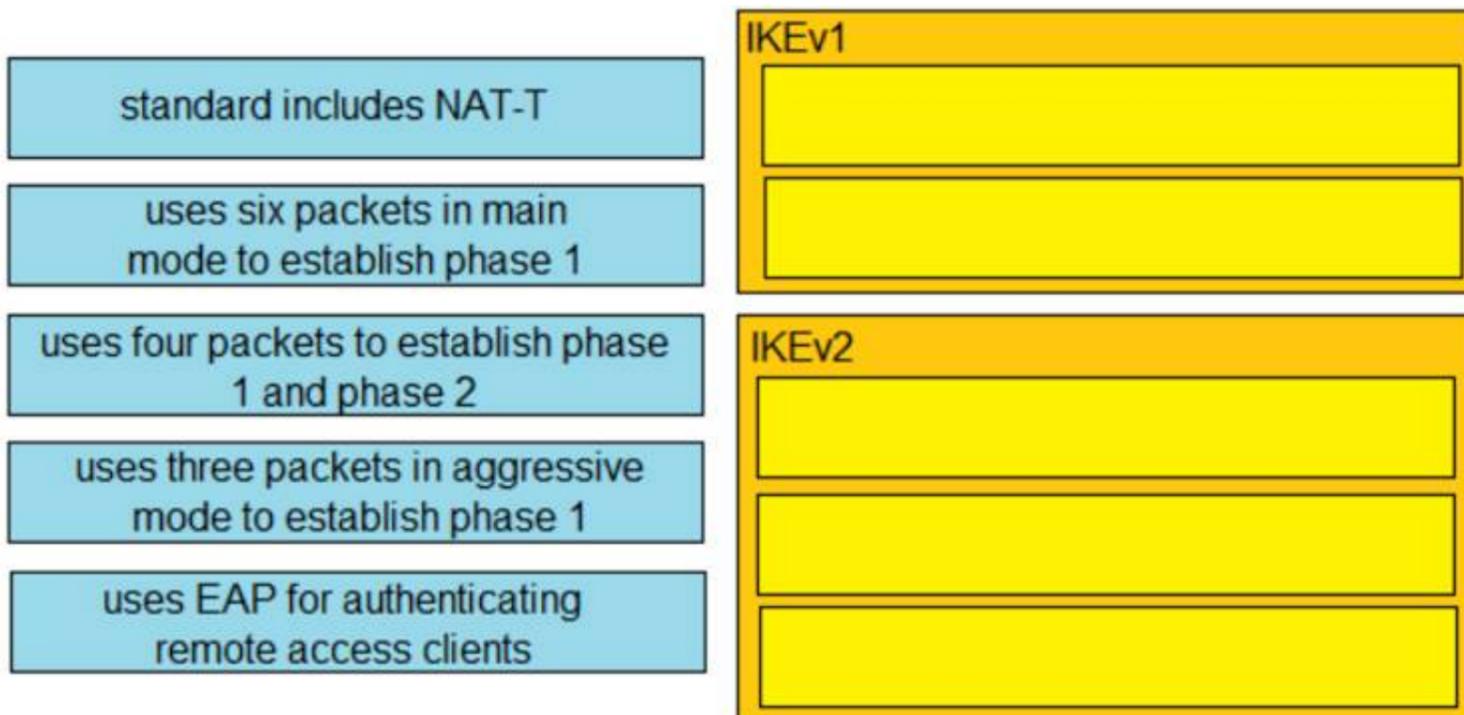
The Mail Policies menu is where almost all of the controls related to email filtering happens. All the security and content filtering policies are set here, so it's likely that, as an ESA administrator, the pages on this menu are where you are likely to spend most of your time.



**NEW QUESTION 4**

- (Exam Topic 2)

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface Description automatically generated with low confidence

**NEW QUESTION 5**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 6**

- (Exam Topic 2)

What is a benefit of conducting device compliance checks?

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

**Answer:** B

**NEW QUESTION 7**

- (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 8**

- (Exam Topic 2)

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

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

E. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).

**Answer:** CE

**Explanation:**

Reference:

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

#### **NEW QUESTION 9**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

Reference:

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

#### **NEW QUESTION 10**

- (Exam Topic 2)

How does Cisco Advanced Phishing Protection protect users?

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

**Answer:** D

**Explanation:**

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

#### **NEW QUESTION 10**

- (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 12**

- (Exam Topic 2)

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

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

**Answer:** D

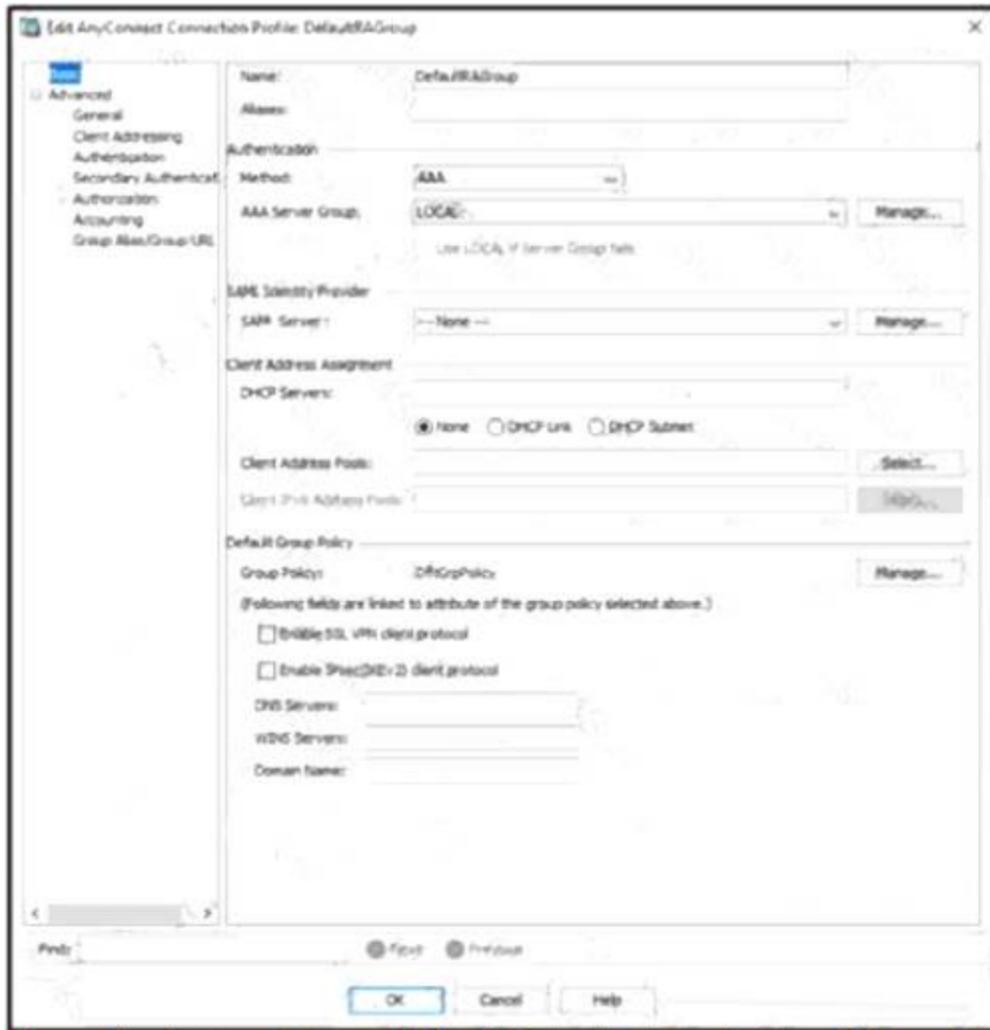
**Explanation:**

Reference: <https://docs.umbrella.com/cloudlock-documentation/docs/endpoints>Note:+ Security information and event management (SIEM) platforms collect log and event data from security systems, 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 a condition of an alerting policy has been met.

#### **NEW QUESTION 14**

- (Exam Topic 2)

Refer to the exhibit.



When configuring a remote access VPN solution terminating on the Cisco ASA, an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication using machine certificates. Which configuration item must be modified to allow this?

- A. Group Policy
- B. Method
- C. SAML Server
- D. DHCP Servers

**Answer: B**

**Explanation:**

In order to use AAA along with an external token authentication mechanism, set the "Method" as "Both" in the Authentication.

**NEW QUESTION 17**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 21**

- (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 24**

- (Exam Topic 2)

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

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

D. when there is a need to have more advanced detection capabilities

**Answer:** D

**Explanation:**

Endpoint protection platforms (EPP) prevent endpoint security threats like known and unknown malware. Endpoint detection and response (EDR) solutions can detect and respond to threats that your EPP and other security tools did not catch. EDR and EPP have similar goals but are designed to fulfill different purposes. EPP is designed to provide device-level protection by identifying malicious files, detecting potentially malicious activity, and providing tools for incident investigation and response. The preventative nature of EPP complements proactive EDR. EPP acts as the first line of defense, filtering out attacks that can be detected by the organization's deployed security solutions. EDR acts as a second layer of protection, enabling security analysts to perform threat hunting and identify more subtle threats to the endpoint. Effective endpoint defense requires a solution that integrates the capabilities of both EDR and EPP to provide protection against cyber threats without overwhelming an organization's security team.

**NEW QUESTION 25**

- (Exam Topic 2)

Refer to the exhibit.



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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 29**

- (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 34**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 36**

- (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 37**

- (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 39**

- (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 42**

- (Exam Topic 1)

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

- A. Group Policy

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

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 44**

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 47**

- (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 49**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 54**

- (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 58**

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 61

- (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 64

- (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 66

- (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 67

- (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 70

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 73

- (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 78

- (Exam Topic 1)

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 80

- (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 85

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 89

- (Exam Topic 1)

What is the function of the Context Directory Agent?

- A. maintains users' group memberships

- B. relays user authentication requests from Web Security Appliance to Active Directory
- C. reads the Active Directory logs to map IP addresses to usernames
- D. accepts user authentication requests on behalf of Web Security Appliance for user identification

**Answer:** C

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/ibf/cda\\_10/Install\\_Config\\_guide/cda10/cda\\_oveviw.html](https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_oveviw.html)

**NEW QUESTION 94**

- (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 96**

- (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 101**

- (Exam Topic 1)

What are two rootkit types? (Choose two)

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

**Answer:** CD

**Explanation:**

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

**NEW QUESTION 103**

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

Reference:

[https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config\\_](https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_)

**NEW QUESTION 107**

- (Exam Topic 1)

Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

url = 'https://api.amp.cisco.com/v1/computers'

response = requests.get(url, auth=(client_id, api_key))

response_json = response.json()

for computer in response_json['data']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
        mac = network_interface.get('mac')
        ip = network_interface.get('ip')
        ipv6 = network_interface.get('ipv6')
        print(mac, ip, ipv6)
```

What does the API do when connected to a Cisco security appliance?

- A. get the process and PID information from the computers in the network
- B. create an SNMP pull mechanism for managing AMP
- C. gather network telemetry information from AMP for endpoints
- D. gather the network interface information about the computers AMP sees

**Answer:** D

**Explanation:**

Reference:

[https://api-docs.amp.cisco.com/api\\_actions/details?api\\_action=GET+%2Fv1%2Fcomputers&api\\_host=api.apjc](https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc).

#### NEW QUESTION 108

- (Exam Topic 1)

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

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

**Answer:** AB

#### NEW QUESTION 113

- (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 118

- (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 120

- (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 124

- (Exam Topic 1)

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

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

**Answer:** CE

#### NEW QUESTION 129

- (Exam Topic 1)

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

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

**Answer:** AD

#### Explanation:

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

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

#### NEW QUESTION 132

- (Exam Topic 1)

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

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

**Answer:** BC

#### NEW QUESTION 136

- (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 139

- (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 143**

- (Exam Topic 1)

What is a feature of the open platform capabilities of Cisco DNA Center?

- A. intent-based APIs
- B. automation adapters
- C. domain integration
- D. application adapters

**Answer: A**

**NEW QUESTION 147**

- (Exam Topic 1)

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

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

**Answer: AD**

**Explanation:**

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

**NEW QUESTION 150**

- (Exam Topic 1)

What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services? (Choose two)

- A. multiple factor auth
- B. local web auth
- C. single sign-on
- D. central web auth
- E. TACACS+

**Answer: BD**

**NEW QUESTION 152**

- (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 157**

- (Exam Topic 1)

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

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

**Answer: DE**

**Explanation:**

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

**NEW QUESTION 158**

- (Exam Topic 1)

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

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

**Answer: B**

**NEW QUESTION 162**

- (Exam Topic 1)

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

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

**Answer: A**

**NEW QUESTION 165**

- (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 168**

- (Exam Topic 1)

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

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

**Answer: BE**

**NEW QUESTION 173**

- (Exam Topic 1)

Refer to the exhibit.

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

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

- A. show authentication registrations
- B. show authentication method

- C. show dot1x all
- D. show authentication sessions

**Answer: D**

**Explanation:**

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-c> Displaying the Summary of All Auth Manager Sessions on the Switch

Enter the following:

Switch# show authentication sessions

Interface MAC Address Method Domain Status Session ID

Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success

0A3462B10000000D24F80B58

Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

**NEW QUESTION 178**

- (Exam Topic 1)

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

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

**Answer: AC**

**Explanation:**

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

[File Conditions List > pc\\_W10\\_64\\_KB4012606\\_Ms17-010\\_1507\\_W](#)

**File Condition**

\* Name **pc\_W10\_64\_KB4012606\_Ms1**

Description **Cisco Predefined Check: Micro**

\* Operating System **Windows 10 (All)**

Compliance Module **Any version**

\* File Type **FileVersion**

\* File Path **SYSTEM\_32**

\* Operator **LaterThan**

\* File Version **10.0.10240.17318**

Cancel

**NEW QUESTION 182**

- (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 187**

- (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 190**

- (Exam Topic 1)

The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the ASA be added on the Cisco UC Manager platform?

- A. Certificate Trust List
- B. Endpoint Trust List
- C. Enterprise Proxy Service
- D. Secured Collaboration Proxy

**Answer:** A

**NEW QUESTION 194**

- (Exam Topic 1)

What is a characteristic of Firepower NGIPS inline deployment mode?

- A. ASA with Firepower module cannot be deployed.
- B. It cannot take actions such as blocking traffic.
- C. It is out-of-band from traffic.
- D. It must have inline interface pairs configured.

**Answer:** D

**NEW QUESTION 196**

- (Exam Topic 1)

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

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

**Answer:** CD

**Explanation:**

Reference:

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

**NEW QUESTION 201**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 204**

- (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 208**

- (Exam Topic 1)

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

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

Answer: D

**NEW QUESTION 213**

- (Exam Topic 1)

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

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

Answer: B

**Explanation:**

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

**NEW QUESTION 217**

- (Exam Topic 1)

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

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

Answer: D

**NEW QUESTION 220**

- (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 224**

- (Exam Topic 1)

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

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

Answer: BD

**Explanation:**

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

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin\\_guide/b\\_ise\\_admin\\_guide\\_21/b\\_ise\\_admin\\_guide](https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide)

**NEW QUESTION 229**

- (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 231**

- (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 233**

- (Exam Topic 1)

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

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

**Answer: B**

**NEW QUESTION 237**

- (Exam Topic 1)

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

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

**Answer: BE**

**Explanation:**

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

**NEW QUESTION 238**

- (Exam Topic 1)

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 241**

- (Exam Topic 1)

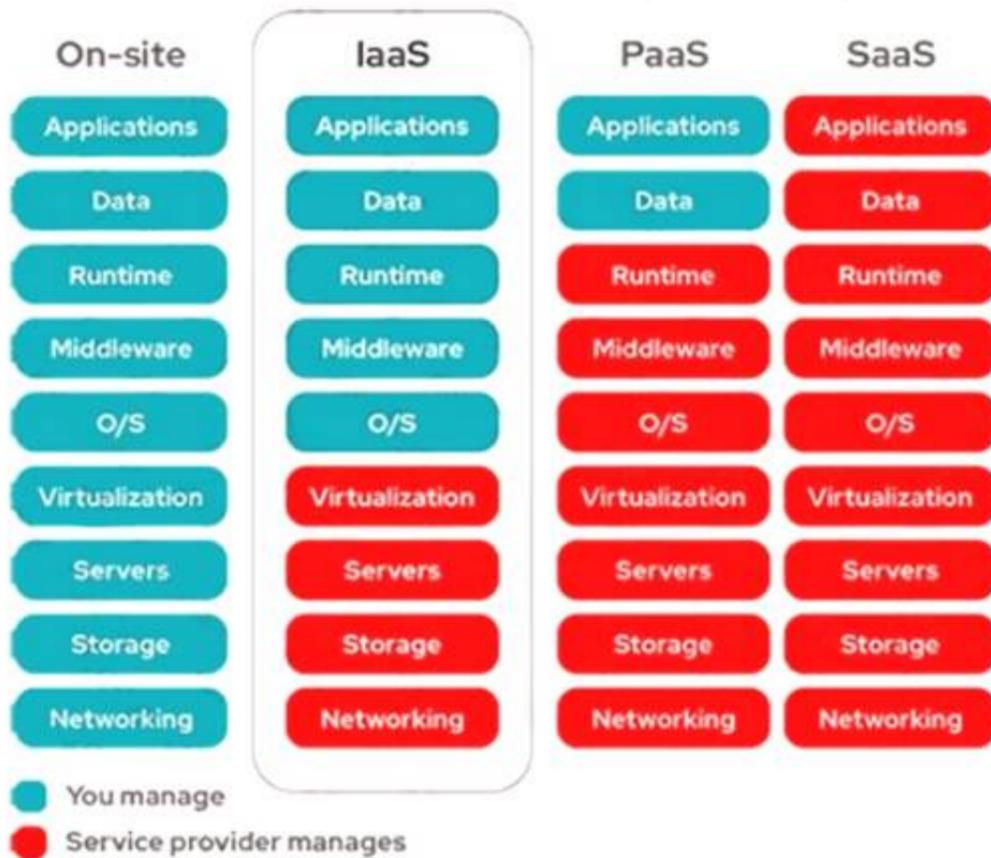
In which cloud services model is the tenant responsible for virtual machine OS patching?

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

**Answer: A**

**Explanation:**

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



**NEW QUESTION 244**

- (Exam Topic 1)

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

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

**Answer: AD**

**NEW QUESTION 248**

- (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 249**

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 252**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 257**

- (Exam Topic 1)

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

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

**Answer:** BD

**Explanation:**

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

**NEW QUESTION 258**

- (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 263**

- (Exam Topic 1)

What is a characteristic of Dynamic ARP Inspection?

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

**Answer:** A

**NEW QUESTION 265**

- (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 269**

- (Exam Topic 1)

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

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

**Answer:** AB

**NEW QUESTION 272**

- (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 273**

- (Exam Topic 1)

How is ICMP used as an exfiltration technique?

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

**Answer:** C

**NEW QUESTION 277**

- (Exam Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 279**

- (Exam Topic 1)

How is Cisco Umbrella configured to log only security events?

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

**Answer:** A

**Explanation:**

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

#### **NEW QUESTION 283**

- (Exam Topic 1)

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

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

**Answer:** D

#### **NEW QUESTION 286**

- (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 291**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

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

#### **NEW QUESTION 296**

- (Exam Topic 1)

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

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

**Answer:** D

#### **NEW QUESTION 298**

- (Exam Topic 1)

How does Cisco Stealthwatch Cloud provide security for cloud environments?

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 299

- (Exam Topic 1)

Which type of attack is social engineering?

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 302

- (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 304

- (Exam Topic 1)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 307

- (Exam Topic 1)

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 311

- (Exam Topic 1)

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

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

**Answer: AC**

#### NEW QUESTION 314

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 317**

- (Exam Topic 3)

Drag and drop the deployment models from the left onto the explanations on the right.

routed	A GRE tunnel is utilized in this solution.
passive	This solution allows inspection between hosts on the same subnet.
passive with ERSPAN	Attacks are not prevented with this solution.
transparent	This solution does not provide filtering between hosts on the same subnet.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

routed	passive
passive	routed
passive with ERSPAN	passive with ERSPAN
transparent	transparent

**NEW QUESTION 321**

- (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 322**

- (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 325**

- (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 326**

- (Exam Topic 3)

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

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

**Answer: AE**

**NEW QUESTION 328**

- (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 331**

- (Exam Topic 3)

Which algorithm is an NGE hash function?

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

**Answer: D**

**NEW QUESTION 334**

- (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 336**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 340**

- (Exam Topic 3)  
 Refer to the exhibit,

```
*Jul 1 15:33:50.027: ISAKMP: (0):Enqueued KEY_MGR_SESSION_CLOSED for Tunnel0 deletion
*Jul 1 15:33:50.027: ISAKMP: (0):Deleting peer node by peer_reap for 2.2.2.2: D1250B0
*Jul 1 15:33:50.029: ISAKMP: (1001):peer does not do paranoid keepalives.
*Jul 1 15:33:54.781: ISAKMP-PAK: (0):received packet from 2.2.2.2 dport 500 sport 500 Global (N) NEW SA
*Jul 1 15:33:54.781: ISAKMP: (0):Created a peer struct for 2.2.2.2, peer port 500
*Jul 1 15:33:54.781: ISAKMP: (0):New peer created peer = 0x11026528 peer_handle = 0x80000004
*Jul 1 15:33:54.781: ISAKMP: (0):Locking peer struct 0x11026528, refcount 1 for crypto_isakmp_process_block
*Jul 1 15:33:54.782: ISAKMP: (0):local port 500, remote port 500
*Jul 1 15:33:54.782: ISAKMP: (0):Find a dup sa in the avl tree during calling isadb_insert sa = 104E3C68
*Jul 1 15:33:54.782: ISAKMP: (0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Jul 1 15:33:54.782: ISAKMP: (0):Old State = IKE_READY New State = IKE_R_MM1
```

which command results in these messages when attempting to troubleshoot an IPsec VPN connection?

- A. debug crypto isakmp
- B. debug crypto ipsec endpoint
- C. debug crypto ipsec
- D. debug crypto isakmp connection

**Answer: A**

**NEW QUESTION 345**

- (Exam Topic 3)

An engineer is configuring their router to send NetFlow data to Stealthwatch which has an IP address of 1.1.11 using the flow record Stealthwatch406397954 command. Which additional command is required to complete the flow record?

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

**Answer: B**

**NEW QUESTION 346**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 348**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 350**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 355**

- (Exam Topic 3)

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

- A. Cisco AMP for Endpoints is a cloud-based service, and Cisco Umbrella is not.

- B. Cisco AMP for Endpoints prevents connections to malicious destinations, and C malware.
- C. Cisco AMP for Endpoints automatically researches indicators of compromise ..
- D. Cisco AMP for Endpoints prevents, detects, and responds to attacks before and against Internet threats.

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 359**

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 362**

- (Exam Topic 3)

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

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

**Answer:** BC

**NEW QUESTION 367**

- (Exam Topic 3)

Which solution is more secure than the traditional use of a username and password and encompasses at least two of the methods of authentication?

- A. single-sign on
- B. RADIUS/LDAP authentication
- C. Kerberos security solution

D. multifactor authentication

**Answer:** D

**NEW QUESTION 372**

- (Exam Topic 3)

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

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

**Answer:** A

**Explanation:**

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

Reference:

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

**NEW QUESTION 374**

- (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 378**

- (Exam Topic 3)

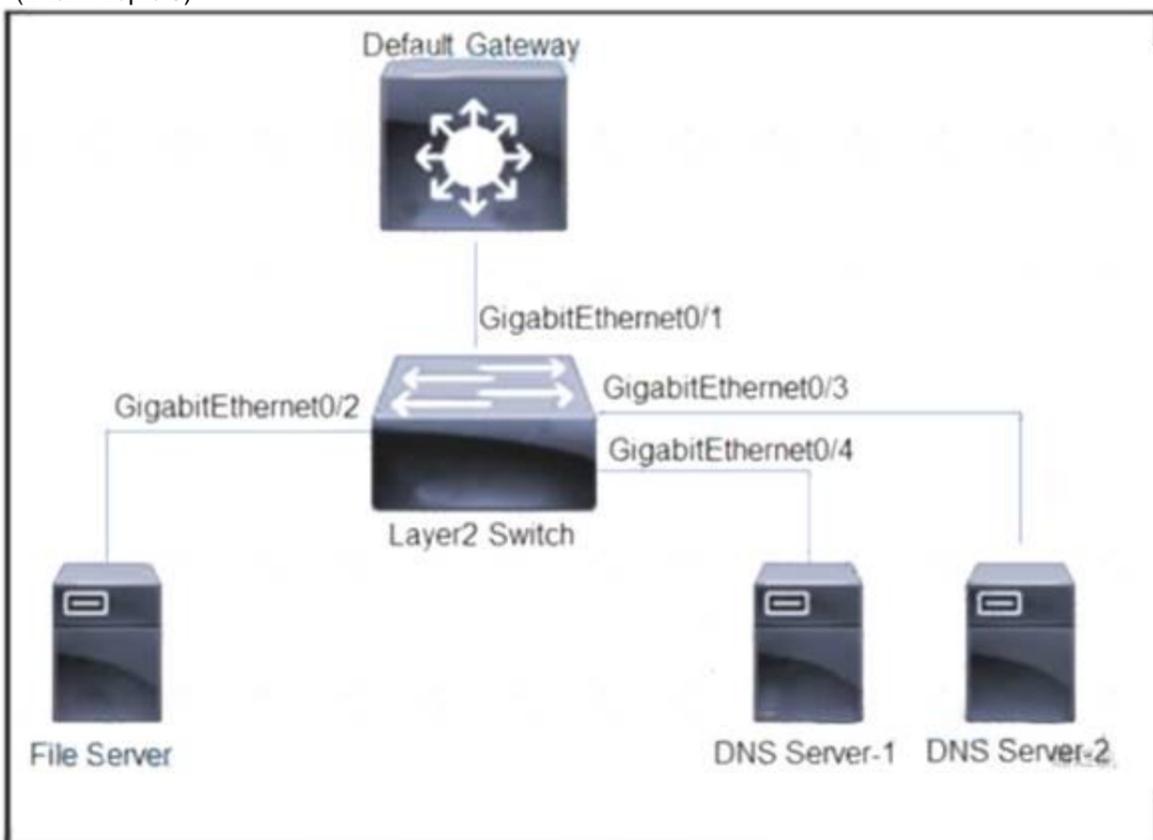
Which security solution uses NetFlow to provide visibility across the network, data center, branch offices, and cloud?

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

**Answer:** B

**NEW QUESTION 381**

- (Exam Topic 3)



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

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

**Answer: C**

**NEW QUESTION 383**

- (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 386**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 388**

- (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 389**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 392**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 394**

- (Exam Topic 3)

What is a benefit of using Cisco Umbrella?

- A. DNS queries are resolved faster.

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

**Answer: B**

**NEW QUESTION 395**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 400**

- (Exam Topic 3)

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

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

**Answer: AC**

**NEW QUESTION 405**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 409**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 410**

- (Exam Topic 3)

Which Cisco security solution stops exfiltration using HTTPS?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 415**

- (Exam Topic 3)

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

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

Answer: AD

**NEW QUESTION 419**

- (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 420**

- (Exam Topic 3)

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

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

Answer: D

**Explanation:**

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

**NEW QUESTION 422**

- (Exam Topic 3)

An engineer is configuring web filtering for a network using Cisco Umbrella Secure Internet Gateway. The requirement is that all traffic needs to be filtered. Using the SSL decryption feature, which type of certificate should be presented to the end-user to accomplish this goal?

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

Answer: C

**NEW QUESTION 426**

- (Exam Topic 3)

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

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

Answer: D

**NEW QUESTION 427**

- (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 432**

- (Exam Topic 3)

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

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

Answer: CD

**NEW QUESTION 437**

- (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 441**

- (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 446**

- (Exam Topic 3)

What do tools like Jenkins, Octopus Deploy, and Azure DevOps provide in terms of application and infrastructure automation?

- A. continuous integration and continuous deployment
- B. cloud application security broker
- C. compile-time instrumentation
- D. container orchestration

**Answer: A**

**NEW QUESTION 447**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 450**

- (Exam Topic 3)

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

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

**Answer: B**

**Explanation:**

Reference:

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

**NEW QUESTION 453**

- (Exam Topic 3)

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

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

Answer: B

**NEW QUESTION 456**

- (Exam Topic 3)

An engineer needs to detect and quarantine a file named abc424400664 zip based on the MD5 signature of the file using the Outbreak Control list feature within Cisco Advanced Malware Protection (AMP) for Endpoints The configured detection method must work on files of unknown disposition Which Outbreak Control list must be configured to provide this?

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

Answer: C

**NEW QUESTION 459**

- (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 463**

- (Exam Topic 3)

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

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

Answer: A

**NEW QUESTION 464**

- (Exam Topic 3)

Which standard is used to automate exchanging cyber threat information?

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

Answer: A

**NEW QUESTION 467**

- (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 470**

- (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 472**

- (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 476**

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Full Context Awareness - policy enforcement NGIPS - threat prevention

AMP - real-time

Collective Sec Intel - Detection, blocking an remediation

**NEW QUESTION 480**

- (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 483**

- (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 486**

- (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 490**

- (Exam Topic 3)

Refer to the exhibit.

```

Interface: GigabitEthernet0/1
 IIF-ID: 0x14E3317D
 MAC Address: 0001.2e34.f101
 IPv6 Address: fe80::f86d:7f42:8d7b:58f3
 IPv4 Address: 192.168.41.7
 User-Name: 00-01-2E-34-F1-01
 Device-type: Microsoft-Workstation
 Status: Authorized
 Domain: DATA
 Oper host mode: multi-domain
 Oper control dir: both
 Session timeout: N/A
 Common Session ID: C0A82982000004CABED90200
 Acct Session ID: 0x00000010
 Handle: 0xd300004c
 Current Policy: POLICY_G11/8/18

Local Policies:
 Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
 Security Policy: Should Secure

Server Policies:

Method status list:
 Method      State
 dot1x      Stopped
 mab        Authc Success
    
```

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

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

**Answer: C**

**NEW QUESTION 492**

- (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 495**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 500**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 504**

- (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 507**

- (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 508**

- (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 509**

- (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 514**

- (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 516**

- (Exam Topic 3)

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

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

**Answer:** BE

**NEW QUESTION 518**

- (Exam Topic 3)

With regard to RFC 5176 compliance, how many IETF attributes are supported by the RADIUS CoA feature?

- A. 3
- B. 5
- C. 10
- D. 12

**Answer:**

D

**NEW QUESTION 519**

- (Exam Topic 3)

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

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

Answer: D

**NEW QUESTION 524**

- (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 527**

- (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 528**

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Reference:

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

**NEW QUESTION 533**

- (Exam Topic 3)

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

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

Answer: C

**NEW QUESTION 534**

- (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 538**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 539**

- (Exam Topic 3)

Based on the NIST 800-145 guide, which cloud architecture is provisioned for exclusive use by a specific group of consumers from different organizations and may be owned, managed, and operated by one or more of those organizations?

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

**Answer: C**

**NEW QUESTION 542**

- (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 547**

- (Exam Topic 3)

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

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

**Answer: AD**

**NEW QUESTION 550**

- (Exam Topic 3)

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

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

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

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

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

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

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

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

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

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

**Answer:** C

#### NEW QUESTION 553

- (Exam Topic 3)

What is the purpose of the Cisco Endpoint IoC feature?

- A. It is an incident response tool.
- B. It provides stealth threat prevention.
- C. It is a signature-based engine.
- D. It provides precompromise detection.

**Answer:** A

#### Explanation:

Reference: <https://docs.amp.cisco.com/Cisco%20Endpoint%20IOC%20Attributes.pdf>

The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

#### NEW QUESTION 557

- (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 562

- (Exam Topic 3)

Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using higher-level protocols without readdressing the network?

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

**Answer:** B

**NEW QUESTION 563**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 568**

- (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](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 573**

- (Exam Topic 3)

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

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

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 575**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 576**

- (Exam Topic 3)

Which Cisco network security device supports contextual awareness?

- A. Firepower
- B. CISCO ASA
- C. Cisco IOS
- D. ISE

**Answer:** D

**NEW QUESTION 577**

- (Exam Topic 3)

Which threat intelligence standard contains malware hashes?

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

**Answer:** A

**NEW QUESTION 582**

- (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 587**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 590**

- (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 591**

- (Exam Topic 3)

Which Cisco Umbrella package supports selective proxy for inspection of traffic from risky domains?

- A. SIG Advantage
- B. DNS Security Essentials
- C. SIG Essentials
- D. DNS Security Advantage

**Answer: C**

**NEW QUESTION 592**

- (Exam Topic 3)

Which Cisco Firewall solution requires zone definition?

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

**Answer: C**

**NEW QUESTION 597**

- (Exam Topic 3)

Which encryption algorithm provides highly secure VPN communications?

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

**Answer: B**

**NEW QUESTION 600**

- (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 602**

- (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 603**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 605**

- (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 610**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 612**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 616**

- (Exam Topic 3)

Email security has become a high priority task for a security engineer at a large multi-national organization due to ongoing phishing campaigns. To help control this, the engineer has deployed an Incoming Content Filter with a URL reputation of (-10 00 to -6 00) on the Cisco ESA Which action will the system perform to disable any links in messages that match the filter?

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 617

- (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 618

- (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 621

- (Exam Topic 3)

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

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

**Answer:** CD

#### NEW QUESTION 622

- (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 623

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 627

- (Exam Topic 3)

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

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

**Answer:** AB

**Explanation:**

- Transparently identify users with authentication realms – This option is available when one or more authentication realms are configured to support transparent identification using one of the following authentication servers:
- Active Directory – Create an NTLM or Kerberos authentication realm and enable transparent user identification. In addition, you must deploy a separate Active Directory agent such as Cisco's Context Directory Agent. For more information, see Transparent User Identification with Active Directory.
- LDAP – Create an LDAP authentication realm configured as an eDirectory, and enable transparent user identification. For more information, see Transparent User Identification with LDAP.

Details:

[https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user\\_guide/b\\_WSA\\_UserGuide/b\\_WSA\\_UserGui](https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGui)

**NEW QUESTION 629**

- (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 632**

- (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 634**

- (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 639**

- (Exam Topic 3)

Refer to the exhibit.

```

"remarks" [],
"destinationService" {
  "kind" serviceKind,
  "value" destinationService,
},
"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 642

- (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 647

- (Exam Topic 3)

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

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

Answer: A

#### NEW QUESTION 652

- (Exam Topic 3)

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

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

Answer: D

#### NEW QUESTION 656

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 659**

- (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 660**

- (Exam Topic 3)

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

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

**Answer: DE**

**NEW QUESTION 664**

- (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 666**

- (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 667**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 669**

- (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 671**

- (Exam Topic 3)

What provides total management for mobile and PC including managing inventory and device tracking, remote view, and live troubleshooting using the included native remote desktop support?

- A. mobile device management
- B. mobile content management
- C. mobile application management
- D. mobile access management

**Answer: A**

**NEW QUESTION 675**

- (Exam Topic 3)

What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?

- A. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not
- B. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA.
- C. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA
- D. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA

**Answer: A**

**NEW QUESTION 680**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 682**

- (Exam Topic 3)

Which technology limits communication between nodes on the same network segment to individual applications?

- A. serverless infrastructure
- B. microsegmentation
- C. SaaS deployment
- D. machine-to-machine firewalling

**Answer: B**

**NEW QUESTION 686**

- (Exam Topic 3)

Refer to the exhibit.

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

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

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

**Answer: B**

**NEW QUESTION 690**

- (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 695**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 697**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 698**

- (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 700**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 704**

- (Exam Topic 3)

Which category includes DoS Attacks?

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

**Answer: C**

**NEW QUESTION 706**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 709**

- (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 711**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 715**

- (Exam Topic 2)

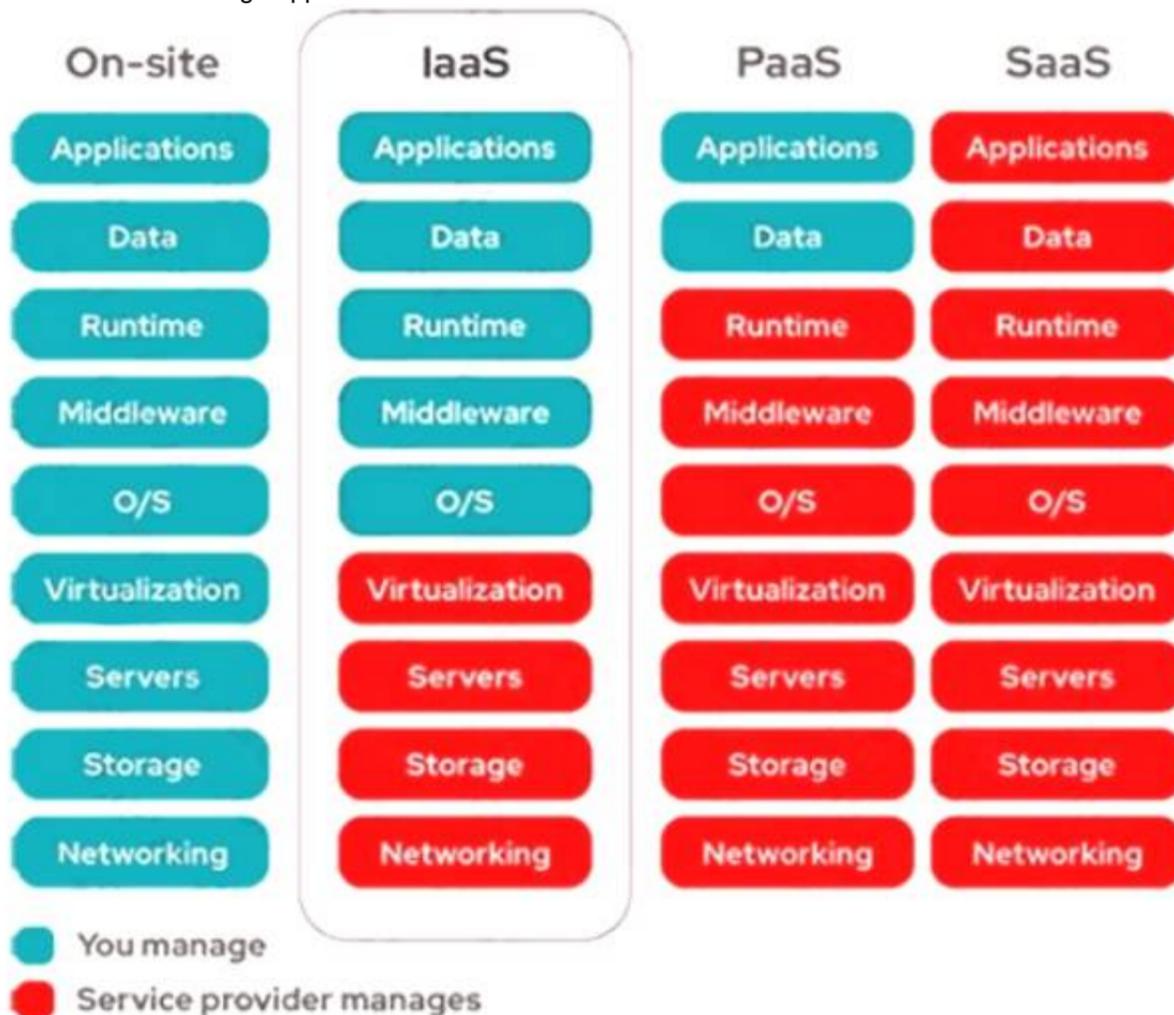
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two)

- A. virtualization
- B. middleware
- C. operating systems
- D. applications
- E. data

**Answer: DE**

**Explanation:**

Customers must manage applications and data in PaaS.



**NEW QUESTION 718**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 722**

- (Exam Topic 3)

What is a description of microsegmentation?

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

**Answer:** A

**NEW QUESTION 725**

- (Exam Topic 2)

What are two differences between a Cisco WSA that is running in transparent mode and one running in explicit mode? (Choose two)

- A. The Cisco WSA responds with its own IP address only if it is running in explicit mode.
- B. The Cisco WSA is configured in a web browser only if it is running in transparent mode.
- C. The Cisco WSA responds with its own IP address only if it is running in transparent mode.
- D. The Cisco WSA uses a Layer 3 device to redirect traffic only if it is running in transparent mode.
- E. When the Cisco WSA is running in transparent mode, it uses the WSA's own IP address as the HTTP request destination.

**Answer:** AD

**Explanation:**

In explicit proxy mode, users are configured to use a web proxy and the web traffic is sent directly to the Cisco WSA. In contrast, in transparent proxy mode the Cisco WSA intercepts user's web traffic redirected from other network devices, such as switches, routers, or firewalls.

**NEW QUESTION 728**

- (Exam Topic 2)

An engineer needs behavioral analysis to detect malicious activity on the hosts, and is configuring the organization's public cloud to send telemetry using the cloud provider's mechanisms to a security device.

Which mechanism should the engineer configure to accomplish this goal?

- A. mirror port
- B. Flow
- C. NetFlow
- D. VPC flow logs

**Answer:** C

**NEW QUESTION 733**

- (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 736**

- (Exam Topic 2)

Which type of dashboard does Cisco DNA Center provide for complete control of the network?

- A. service management
- B. centralized management
- C. application management
- D. distributed management

**Answer:** B

**Explanation:**

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

**NEW QUESTION 740**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

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

2nd - Questions and Answers in PDF Format

### **350-701 Practice Exam Features:**

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

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