



**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 attack is preventable by Cisco ESA but not by the Cisco WSA?

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

**Answer: D**

#### Explanation:

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user\\_guide/b\\_ESA\\_Admin\\_Guide\\_13-5/m\\_advance](https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advance)

### NEW QUESTION 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.

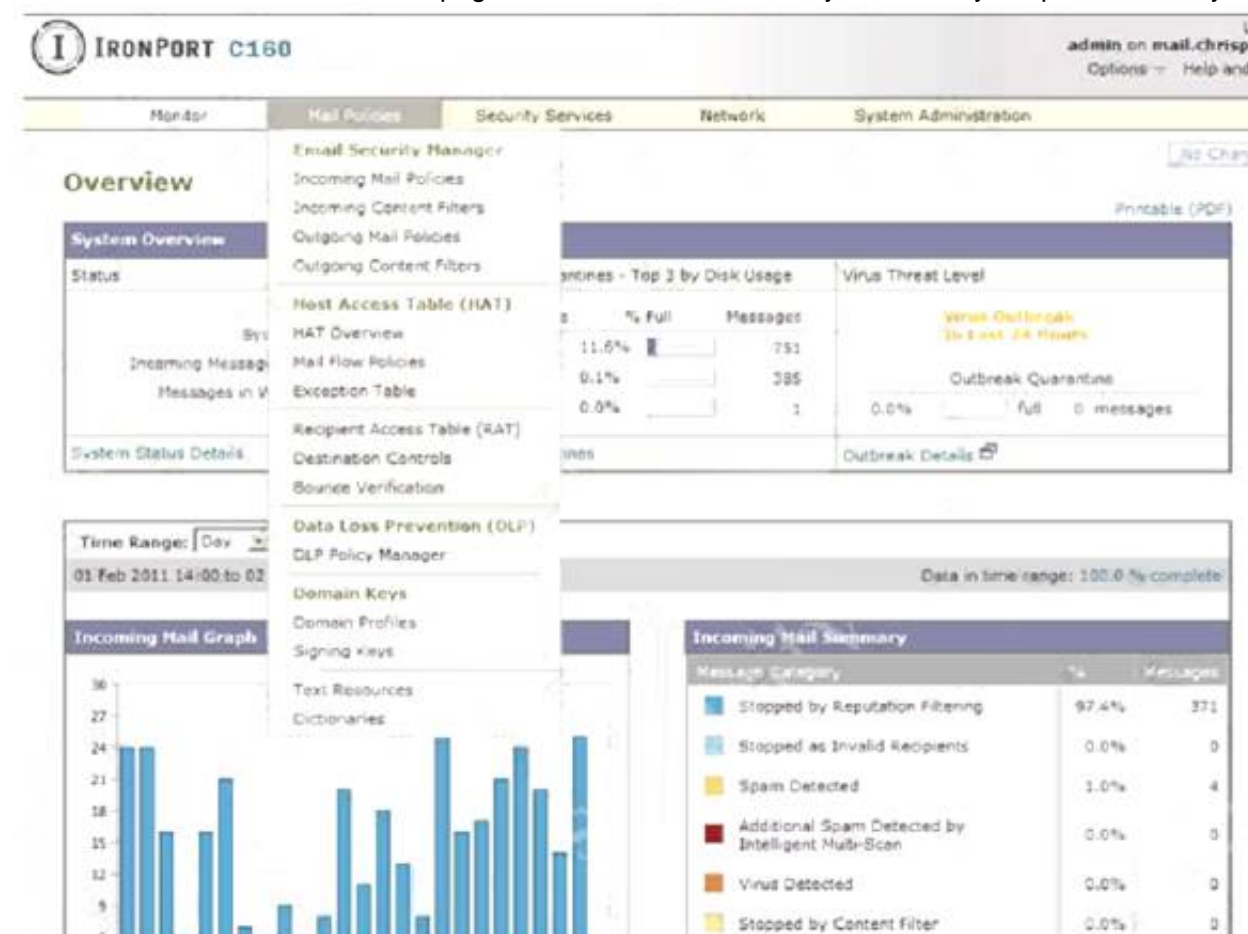
What must be configured to accomplish this?

- 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:

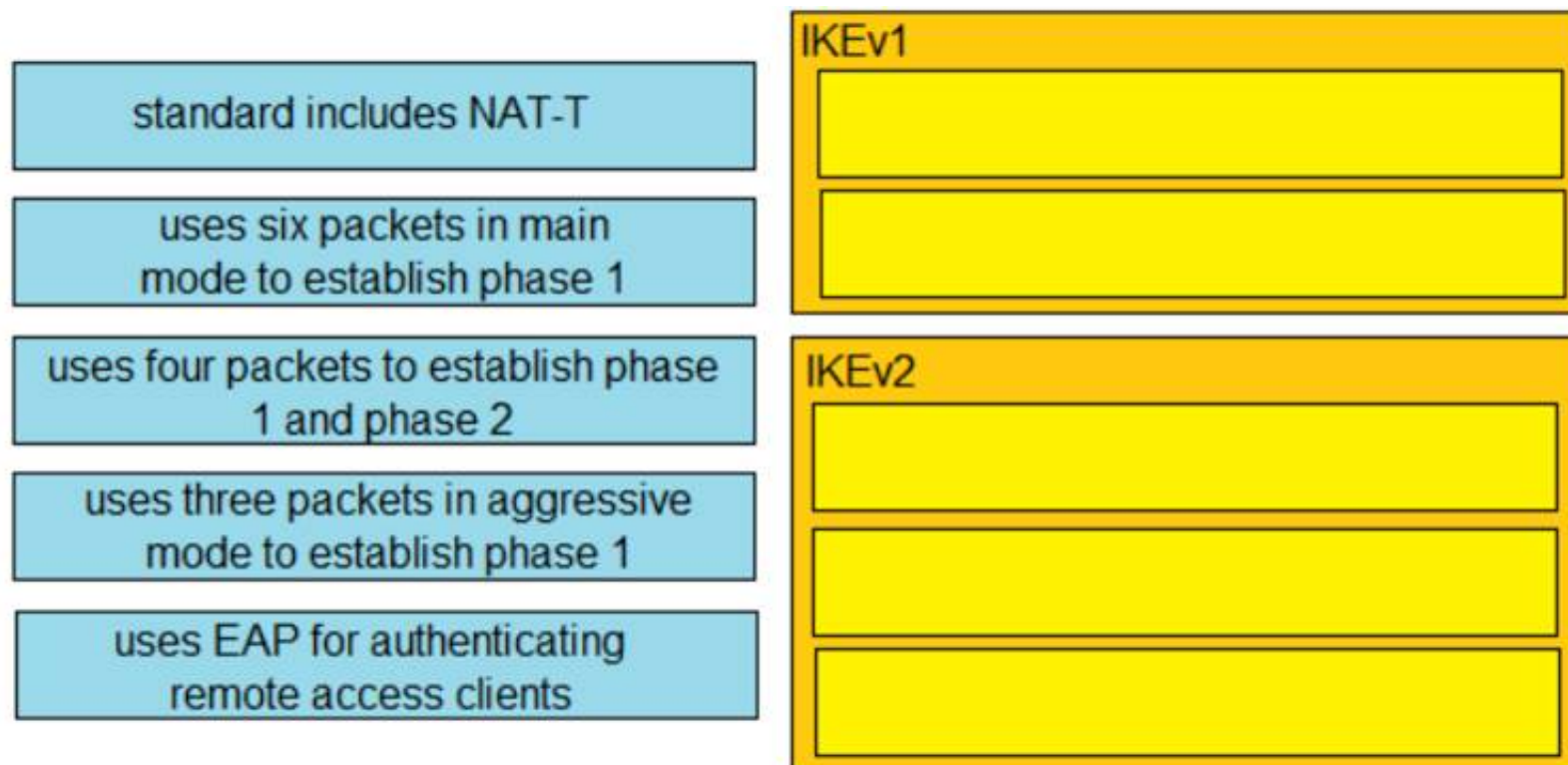
The Mail Policies menu is where almost all of the controls related to email filtering happens. All the security and content filtering policies are set here, so it's likely that, as an ESA administrator, the pages on this menu are where you are likely to spend most of your time.



### 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)

An attacker needs to perform reconnaissance on a target system to help gain access to it. The system has weak passwords, no encryption on the VPN links, and software bugs on the system's applications. Which vulnerability allows the attacker to see the passwords being transmitted in clear text?

- A. weak passwords for authentication  
B. unencrypted links for traffic  
C. software bugs on applications  
D. improper file security

**Answer:** B

**NEW QUESTION 6**

- (Exam Topic 2)

Which public cloud provider supports the Cisco Next Generation Firewall Virtual?

- A. Google Cloud Platform  
B. Red Hat Enterprise Visualization  
C. VMware ESXi  
D. Amazon Web Services

**Answer:** D

**Explanation:**

Reference:

<https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html>

**NEW QUESTION 7**

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 8**

- (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 9

- (Exam Topic 2)

An organization recently installed a Cisco WSA and would like to take advantage of the AVC engine to allow the organization to create a policy to control application specific activity. After enabling the AVC engine, what must be done to implement this?

- A. Use security services to configure the traffic monitor, .
- B. Use URL categorization to prevent the application traffic.
- C. Use an access policy group to configure application control settings.
- D. Use web security reporting to validate engine functionality

**Answer:** C

**Explanation:**

The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or allow applications individually or according to application type. You can also apply controls to particular application types.

#### NEW QUESTION 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)

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

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

**Answer:** D

#### NEW QUESTION 15

- (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 16

- (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**

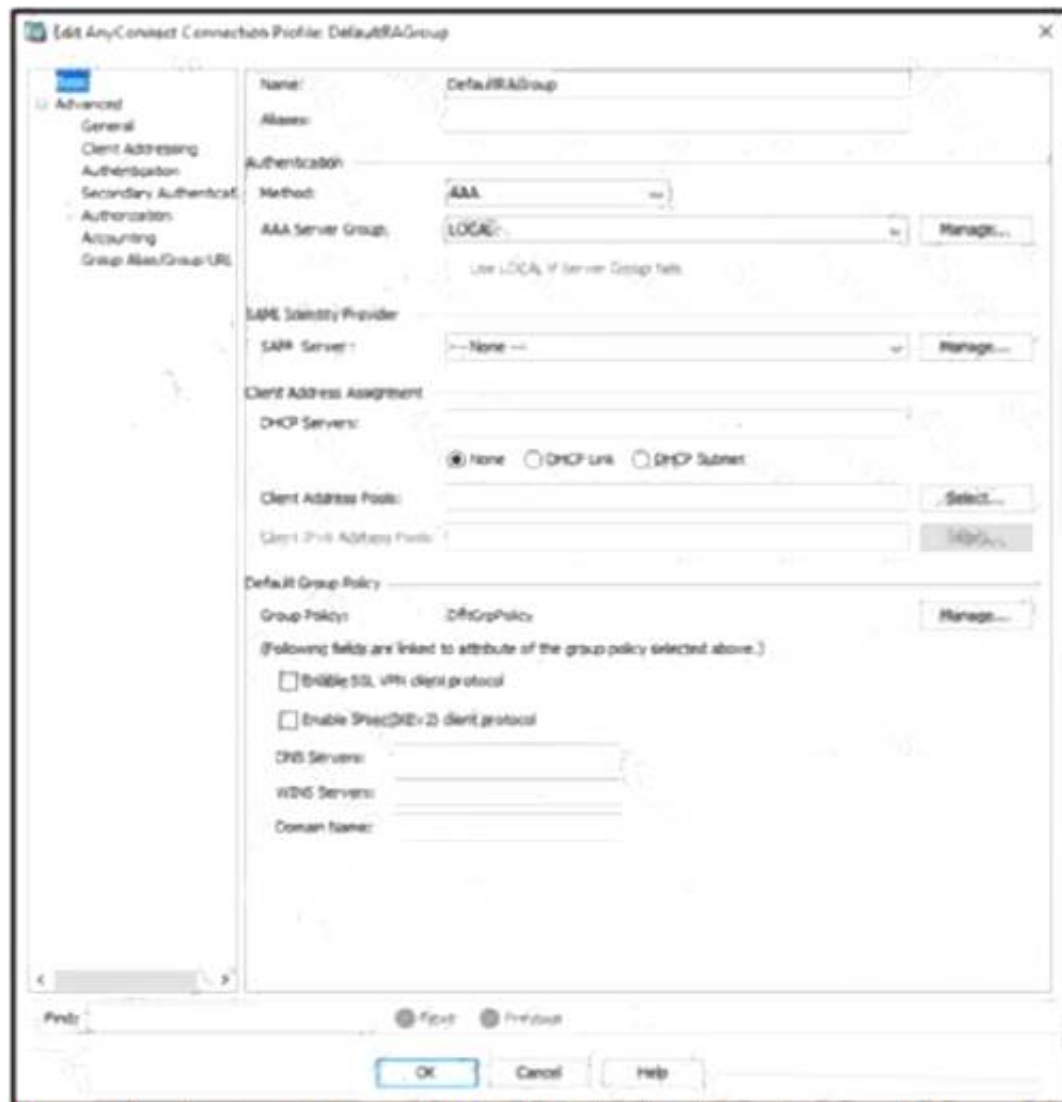
**Explanation:**

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 20**

- (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 25**

- (Exam Topic 2)

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

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

**Answer: C**

**Explanation:**

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



#### NEW QUESTION 28

- (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 29

- (Exam Topic 2)

What are two DDoS attack categories? (Choose two)

- A. sequential
- B. protocol
- C. database
- D. volume-based
- E. screen-based

**Answer:** BD

#### Explanation:

There are three basic categories of attack:+ volume-based attacks, which use high traffic to inundate the network bandwidth+ protocol attacks, which focus on exploiting server resources+ application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks

Reference: <https://www.esecurityplanet.com/networks/types-of-ddos-attacks/>

#### NEW QUESTION 31

- (Exam Topic 2)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 35

- (Exam Topic 2)

What is an attribute of the DevSecOps process?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 39

- (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 41**

- (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 44**

- (Exam Topic 2)

Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 49**

- (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 50**

- (Exam Topic 2)

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text, chat or text message Description automatically generated

**NEW QUESTION 51**

- (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 56**

- (Exam Topic 1)

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

- A. AES is less secure than 3DES.
- B. AES is more secure than 3DES.
- C. AES can use a 168-bit key for encryption.
- D. AES can use a 256-bit key for encryption.
- E. AES encrypts and decrypts a key three times in sequence.

**Answer:** BD

**NEW QUESTION 61**

- (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 63**

- (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 64**

- (Exam Topic 1)

Which ASA deployment mode can provide separation of management on a shared appliance?

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

**Answer:** C

**NEW QUESTION 65**

- (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 69**

- (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 74**

- (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 75**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 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 82**

- (Exam Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 84**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user\\_guide/b\\_ESA\\_Admin\\_Guide\\_12\\_0/b\\_ESA\\_A](https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_A)

**NEW QUESTION 87**

- (Exam Topic 1)

Which technology is used to improve web traffic performance by proxy caching?

- A. WSA
- B. Firepower
- C. FireSIGHT
- D. ASA

**Answer:** A

**NEW QUESTION 89**

- (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 91

- (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 94

- (Exam Topic 1)

Which deployment model is the most secure when considering risks to cloud adoption?

- A. Public Cloud
- B. Hybrid Cloud
- C. Community Cloud
- D. Private Cloud

**Answer:** D

#### NEW QUESTION 96

- (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 100

- (Exam Topic 1)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 101

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 102

- (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 103**

- (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 107**

- (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 111**

- (Exam Topic 1)

When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, which name is used?

- A. Common Security Exploits
- B. Common Vulnerabilities and Exposures
- C. Common Exploits and Vulnerabilities
- D. Common Vulnerabilities, Exploits and Threats

**Answer:** B

**Explanation:**

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

**NEW QUESTION 112**

- (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 Service. Note: A flow is a unidirectional series of packets between a given source and destination.

**NEW QUESTION 116**

- (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 117

- (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 118

- (Exam Topic 1)

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

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

**Answer:** A

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa\\_84\\_cli\\_config/monitor\\_nsel.h](https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_nsel.html)

#### NEW QUESTION 120

- (Exam Topic 1)

Which statement about the configuration of Cisco ASA NetFlow v9 Secure Event Logging is true?

- A. To view bandwidth usage for NetFlow records, the QoS feature must be enabled.
- B. A sysopt command can be used to enable NSEL on a specific interface.
- C. NSEL can be used without a collector configured.
- D. A flow-export event type must be defined under a policy

**Answer:** D

#### NEW QUESTION 121

- (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 125

- (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 130

- (Exam Topic 1)

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

- A. automated email encryption

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

**Answer:** C

#### NEW QUESTION 133

- (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 137

- (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 140

- (Exam Topic 1)

When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?

- A. Spero analysis
- B. dynamic analysis
- C. sandbox analysis
- D. malware analysis

**Answer:** B

#### Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide/v60/Refere> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload

thewhole file. Dynamic analysis sends files to AMP ThreatGrid.Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco ThreatGrid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file ismalicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threatscore, you can view a dynamic analysis summary report with the reasons for the assigned threat score. Youcan also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well asscrubbed reports with limited data for files that

your organization did not submit. Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources. -> Malware analysis does not upload files to anywhere, it only checks the files locally. There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in a virtual machine.

#### NEW QUESTION 141

- (Exam Topic 1)

A network engineer has entered the `snmp-server user andy myv3 auth sha cisco priv aes 256 cisc0380739941` command and needs to send SNMP information to a host at 10.255.254.1. Which command achieves this goal?

- A. `snmp-server host inside 10.255.254.1 version 3 andy`
- B. `snmp-server host inside 10.255.254.1 version 3 myv3`
- C. `snmp-server host inside 10.255.254.1 snmpv3 andy`
- D. `snmp-server host inside 10.255.254.1 snmpv3 myv3`

**Answer: A**

#### Explanation:

The command `"snmp-server user user-name group-name [remote ip-address [udp-port port]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]"` adds a new user (in this case "andy") to an SNMPv3 group (in this case group name "myv3") and configures a password for the user. In the `"snmp-server host"` command, we need to: + Specify the SNMP version with key word "version {1 | 2 | 3}" + Specify the username ("andy"), not group name ("myv3"). Note: In `"snmp-server host inside ..."` command, "inside" is the interface name of the ASA interface through which the NMS (located at 10.255.254.1) can be reached.

#### NEW QUESTION 143

- (Exam Topic 1)

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

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

**Answer: BD**

#### Explanation:

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user\\_guide\\_fs/b\\_ESA\\_Admin\\_Guide\\_11\\_0/b\\_ESA](https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA)

#### NEW QUESTION 148

- (Exam Topic 1)

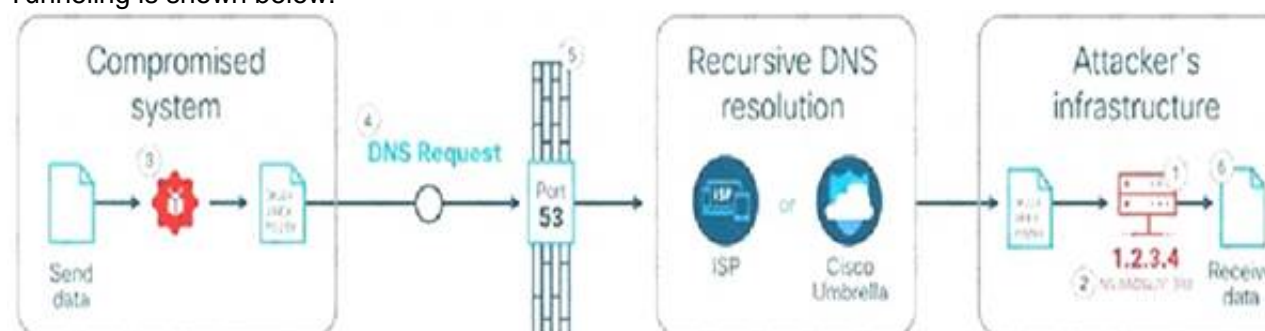
How is DNS tunneling used to exfiltrate data out of a corporate network?

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

**Answer: B**

#### Explanation:

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



> The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNS nameserver (NS) and malicious payload. 2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. attackerdomain.com) is registered or reused. The registrar informs the top-level domain (.com) nameservers to refer requests for attackerdomain.com to ns.attackerdomain.com, which has a DNS record mapped to 1.2.3.43. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, P028X977W,...). 4. The payload initiates thousands of unique DNS record requests to the attacker's domain with each string as Reference: <https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0>

#### NEW QUESTION 152

- (Exam Topic 1)

Which Cisco AMP file disposition valid?

- A. pristine



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

**Answer:** B

#### NEW QUESTION 156

- (Exam Topic 1)

Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?

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

**Answer:** C

#### Explanation:

Reference:

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

#### NEW QUESTION 161

- (Exam Topic 1)

Which benefit does endpoint security provide the overall security posture of an organization?

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

**Answer:** D

#### NEW QUESTION 163

- (Exam Topic 1)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 165

- (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 authn sess int gi0/1
- C. show connection status gi0/1
- D. show ver gi0/1

**Answer:** B

#### NEW QUESTION 168

- (Exam Topic 1)

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

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

**Answer:** A

#### Explanation:

Reference: [https://www.cisco.com/c/dam/global/en\\_uk/products/switches/cisco\\_nexus\\_9300\\_ex\\_platform\\_switches\\_white\\_](https://www.cisco.com/c/dam/global/en_uk/products/switches/cisco_nexus_9300_ex_platform_switches_white_)

#### NEW QUESTION 171

- (Exam Topic 1)

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



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

**Answer:** D

#### NEW QUESTION 176

- (Exam Topic 1)

Which feature of Cisco ASA allows VPN users to be postured against Cisco ISE without requiring an inline posture node?

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

**Answer:** A

#### NEW QUESTION 181

- (Exam Topic 1)

On which part of the IT environment does DevSecOps focus?

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

**Answer:** A

#### NEW QUESTION 186

- (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 189

- (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 192

- (Exam Topic 1)

Refer to the exhibit.

```
SwitchA(config)#interface gigabitethernet1/0/1
SwitchA(config-if)#dot1x host-mode multi-host
SwitchA(config-if)#dot1x timeout quiet-period 3
SwitchA(config-if)#dot1x timeout tx-period 15
SwitchA(config-if)#authentication port-control
auto
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 12
```

An engineer configured wired 802.1x on the network and is unable to get a laptop to authenticate. Which port configuration is missing?

- A. authentication open
- B. dot1x reauthentication
- C. cisp enable
- D. dot1x pae authenticator

**Answer:** D

#### NEW QUESTION 196

- (Exam Topic 1)

Which compliance status is shown when a configured posture policy requirement is not met?

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

**Answer:** D

#### Explanation:

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin\\_guide/b\\_ise\\_admin\\_guide\\_13/b\\_ise\\_admin\\_guide](https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide)

#### NEW QUESTION 197

- (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 202

- (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 207**

- (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 211**

- (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 214**

- (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 215**

- (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 220**

- (Exam Topic 1)

Which threat involves software being used to gain unauthorized access to a computer system?

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

**Answer:** A

**NEW QUESTION 223**

- (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 226**

- (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 230**

- (Exam Topic 1)

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

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

**Answer:** AC

**NEW QUESTION 231**

- (Exam Topic 1)

How is ICMP used as an exfiltration technique?

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

**Answer:** C

**NEW QUESTION 234**

- (Exam Topic 1)

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

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

**Answer:** B

**Explanation:**

Reference:

[https://www.cisco.com/c/en/us/td/docs/ios/solutions\\_docs/avc/guide/avc-user-guide/avc\\_tech\\_overview.html](https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/guide/avc-user-guide/avc_tech_overview.html)

**NEW QUESTION 236**

- (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 241

- (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 244

- (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 247

- (Exam Topic 1)

What is the difference between deceptive phishing and spear phishing?

- A. Deceptive phishing is an attack aimed at a specific user in the organization who holds a C-level role.
- B. A spear phishing campaign is aimed at a specific person versus a group of people.
- C. Spear phishing is when the attack is aimed at the C-level executives of an organization.
- D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

**Answer:** B

#### Explanation:

In deceptive phishing, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.

Spear phishing is carefully designed to get a single recipient to respond. Criminals select an individual target within an organization, using social media and other public information – and craft a fake email tailored for that person.

#### NEW QUESTION 251

- (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 253

- (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 258

- (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 260**

- (Exam Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 261**

- (Exam Topic 1)

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

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

**Answer:** CE

**Explanation:**

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

Reference:

[\*\*NEW QUESTION 262\*\*](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpn/configuration/15-mt/sec-vpnavailability-15- the prerequisites only stated that “Both routers should be the same type of device” but in the “Restrictions for Stateful Failover for IPsec” section of the link above, it requires “Both the active and standby devices must run the identical version of the Cisco IOS software” so answer E is better than answer B.</a></p></div><div data-bbox=)

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 266**

- (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 268

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 273

- (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 277

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 280

- (Exam Topic 3)

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

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

Answer: D

#### NEW QUESTION 285

- (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 287

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 290

- (Exam Topic 3)

What is the term for the concept of limiting communication between applications or containers on the same node?

- A. container orchestration
- B. software-defined access
- C. microservicing
- D. microsegmentation

**Answer: D**

#### NEW QUESTION 292

- (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 296

- (Exam Topic 3)

A company has 5000 Windows users on its campus. Which two precautions should IT take to prevent WannaCry ransomware from spreading to all clients? (Choose two.)

- A. Segment different departments to different IP blocks and enable Dynamic ARP inspection on all VLANs
- B. Ensure that noncompliant endpoints are segmented off to contain any potential damage.
- C. Ensure that a user cannot enter the network of another department.
- D. Perform a posture check to allow only network access to those Windows devices that are already patched.
- E. Put all company users in the trusted segment of NGFW and put all servers to the DMZ segment of the Cisco NGF
- F. ni

**Answer: BD**

#### NEW QUESTION 299

- (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 302

- (Exam Topic 3)

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

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

**Answer:** BD

#### NEW QUESTION 305

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 306

- (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.

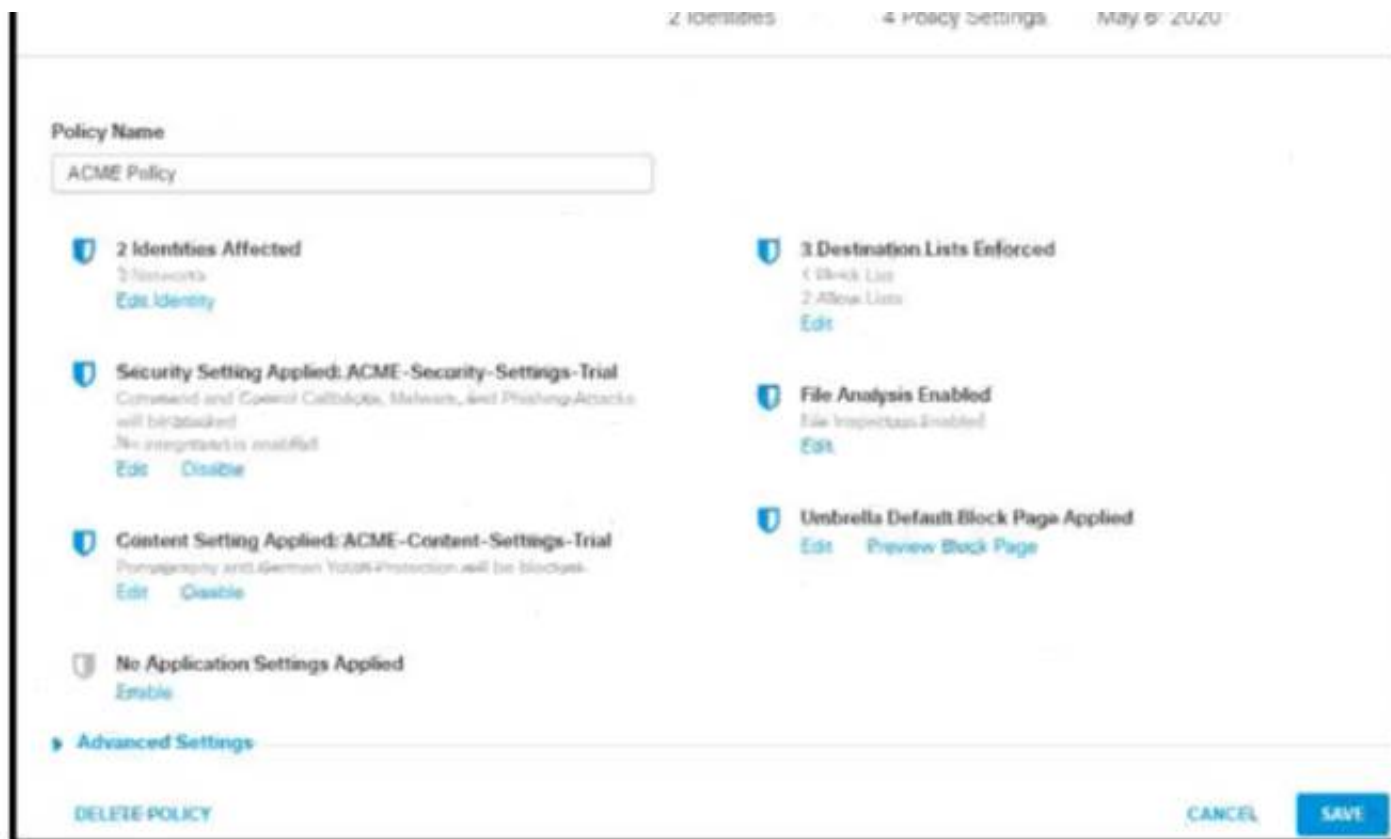
- A. Upload the organization root CA to the Umbrella admin portal
- B. Modify the user's browser settings to suppress errors from Umbrella.
- C. Restrict access to only websites with trusted third-party signed certificates.
- D. Import the Umbrella root CA into the trusted root store on the user's device.

**Answer:** A

#### NEW QUESTION 311

- (Exam Topic 3)

Refer to the exhibit.



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

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

**Answer:** B

#### NEW QUESTION 315

- (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 318

- (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:



#### NEW QUESTION 323

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 325

- (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 328

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 333

- (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 336

- (Exam Topic 3)

Which ESA implementation method segregates inbound and outbound email?

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

**Answer:** D

#### NEW QUESTION 339

- (Exam Topic 3)

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

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

**Answer:** A

#### Explanation:

Reference:

[https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/2-6/admin\\_guide](https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/2-6/admin_guide)

#### NEW QUESTION 343

- (Exam Topic 3)

Which feature requires that network telemetry be enabled?

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

**Answer:** D

#### NEW QUESTION 345

- (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 350

- (Exam Topic 3)

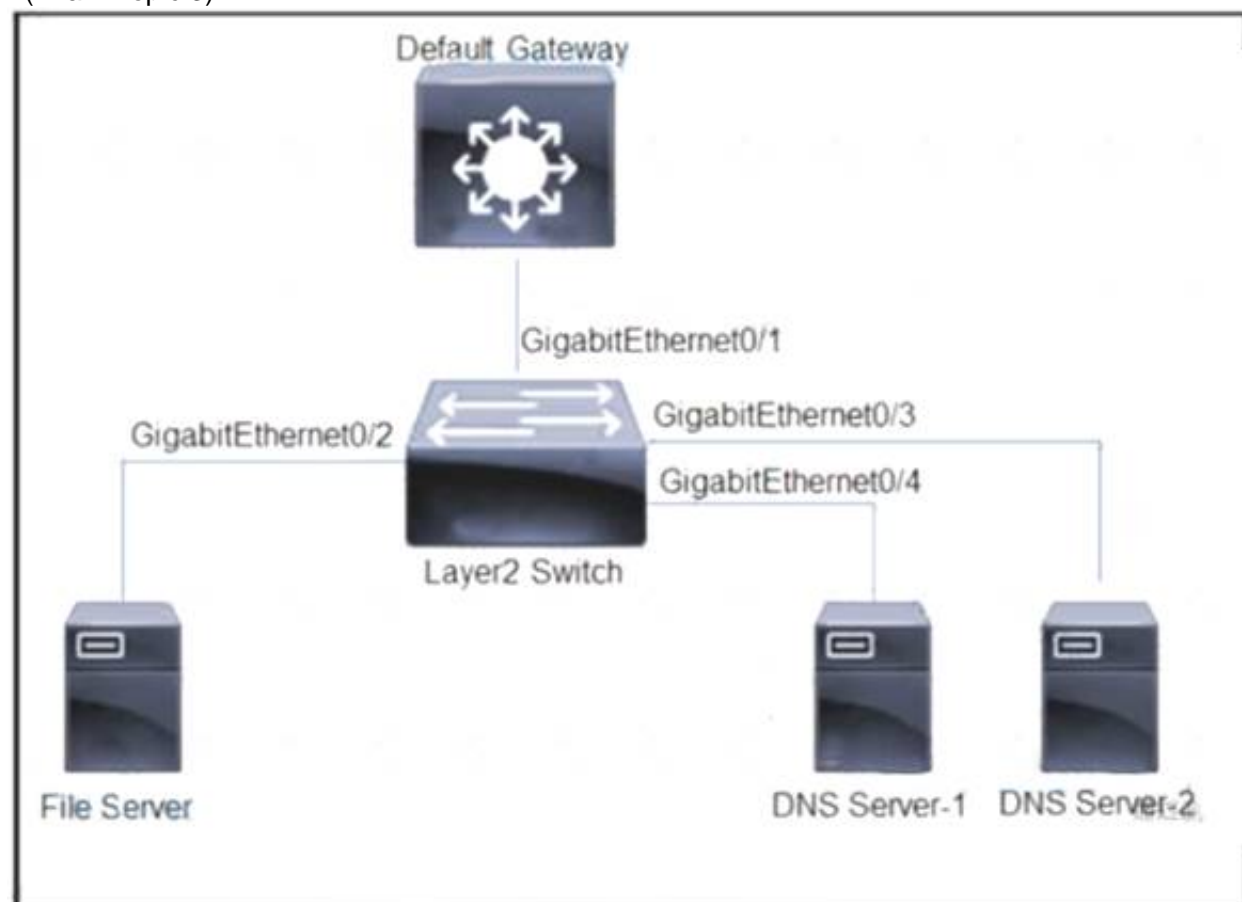
Which two components do southbound APIs use to communicate with downstream devices? (Choose two.)

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

**Answer:** BE

#### NEW QUESTION 352

- (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 355

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 357

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 359

- (Exam Topic 3)

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

- A. Malware installation
- B. Command-and-control communication

- C. Network footprinting
- D. Data exfiltration

**Answer:** D

**Explanation:**

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

**NEW QUESTION 360**

- (Exam Topic 3)

Which two protocols must be configured to authenticate end users to the Web Security Appliance? (Choose two.)

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

**Answer:** AB

**NEW QUESTION 363**

- (Exam Topic 3)

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

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

**Answer:** AB

**NEW QUESTION 366**

- (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 369**

- (Exam Topic 3)

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

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

**Answer:** AC

**NEW QUESTION 370**

- (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 375**

- (Exam Topic 3)

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

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

**Answer:**

AE

#### NEW QUESTION 377

- (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 381

- (Exam Topic 3)

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 385

- (Exam Topic 3)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 387

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 390

- (Exam Topic 3)

What is the term for when an endpoint is associated to a provisioning WLAN that is shared with guest access, and the same guest portal is used as the BYOD portal?

- A. single-SSID BYOD
- B. multichannel GUI
- C. dual-SSID BYOD
- D. streamlined access

**Answer:** C

#### NEW QUESTION 394

- (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 396

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 401

- (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 404

- (Exam Topic 3)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 407

- (Exam Topic 3)

What is a benefit of using Cisco Tetration?

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

**Answer:** C

#### NEW QUESTION 410

- (Exam Topic 3)

What is an advantage of the Cisco Umbrella roaming client?

- A. the ability to see all traffic without requiring TLS decryption
- B. visibility into IP-based threats by tunneling suspicious IP connections
- C. the ability to dynamically categorize traffic to previously uncategorized sites
- D. visibility into traffic that is destined to sites within the office environment

**Answer:** C

#### NEW QUESTION 411

- (Exam Topic 3)

What is the purpose of joining Cisco WSAs to an appliance group?

- A. All WSAs in the group can view file analysis results.
- B. The group supports improved redundancy
- C. It supports cluster operations to expedite the malware analysis process.
- D. It simplifies the task of patching multiple appliances.

**Answer:** A

#### NEW QUESTION 416



- (Exam Topic 3)

An organization must add new firewalls to its infrastructure and wants to use Cisco ASA or Cisco FTD.

The chosen firewalls must provide methods of blocking traffic that include offering the user the option to bypass the block for certain sites after displaying a warning page and to reset the connection. Which solution should the organization choose?

- A. Cisco FTD because it supports system rate level traffic blocking, whereas Cisco ASA does not
- B. Cisco ASA because it allows for interactive blocking and blocking with reset to be configured via the GUI, whereas Cisco FTD does not.
- C. Cisco FTD because it enables interactive blocking and blocking with reset natively, whereas Cisco ASA does not
- D. Cisco ASA because it has an additional module that can be installed to provide multiple blocking capabilities, whereas Cisco FTD does not.

**Answer: C**

#### NEW QUESTION 420

- (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 423

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 428

- (Exam Topic 3)

Refer to the exhibit.

```
ASA# show service-policy sfr

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

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

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

**Answer: AE**

#### Explanation:

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

#### NEW QUESTION 432

- (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 436**

- (Exam Topic 3)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 441**

- (Exam Topic 3)

How does a WCCP-configured router identify if the Cisco WSA is functional?

- A. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the router.
- B. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the WSA.
- C. The WSA sends a Here-I-Am message every 10 seconds, and the router acknowledges with an ISee-You message.
- D. The router sends a Here-I-Am message every 10 seconds, and the WSA acknowledges with an ISee-You message.

**Answer: C**

**NEW QUESTION 442**

- (Exam Topic 3)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 445**

- (Exam Topic 3)

Drag and drop the concepts from the left onto the correct descriptions on the right

guest services	requires probes to collect attributes of connected endpoints
profiling	sponsor portal that is used to gain access to network resources
posture assessment	My Devices portal that allows users to register their device
BYOD	Results can have a status of compliant or noncompliant.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



#### NEW QUESTION 448

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 451

- (Exam Topic 3)

Which role is a default guest type in Cisco ISE?

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

**Answer:** C

#### Explanation:

[https://www.cisco.com/c/en/us/td/docs/security/ise/1-4-1/admin\\_guide/b\\_ise\\_admin\\_guide\\_141/b\\_ise\\_admin\\_g](https://www.cisco.com/c/en/us/td/docs/security/ise/1-4-1/admin_guide/b_ise_admin_guide_141/b_ise_admin_g)

#### NEW QUESTION 455

- (Exam Topic 3)

Which benefit does DMVPN provide over GETVPN?

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

**Answer:** D

#### NEW QUESTION 456

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 461

- (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 464

- (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 467

- (Exam Topic 3)  
Which RADIUS feature provides a mechanism to change the AAA attributes of a session after it is authenticated?

- A. Authorization
- B. Accounting
- C. Authentication
- D. CoA

Answer: D

NEW QUESTION 470

- (Exam Topic 3)  
Drag and drop the exploits from the left onto the type of security vulnerability on the right.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

causes memory access errors	gives unauthorized access to web server files
makes the client the target of attack	makes the client the target of attack
gives unauthorized access to web server files	accesses or modifies application data
accesses or modifies application data	causes memory access errors

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 477

- (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 481

- (Exam Topic 3)

Which Cisco DNA Center RESTful PNP API adds and claims a device into a workflow?

A. api/v1/fie/config

B. api/v1/onboarding/pnp-device/import

C. api/v1/onboarding/pnp-device

D. api/v1/onboarding/workflow

**Answer:** B

#### NEW QUESTION 483

- (Exam Topic 3)

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

A. Cisco FTD

B. Cisco ASA

C. Cisco Umbrella

D. Cisco ISE

**Answer:** D

#### NEW QUESTION 484

- (Exam Topic 3)

What is a difference between a DoS attack and a DDoS attack?

A. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where multiple systems target a single system with a DoS attack

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

C. A DoS attack is where a computer is used to flood a server with UDP packets whereas a DDoS attack is where a computer is used to flood a server with TCP packets

D. A DoS attack is where a computer is used to flood a server with TCP packets whereas a DDoS attack is where a computer is used to flood a server with UDP packets

**Answer:** A

#### NEW QUESTION 486

- (Exam Topic 3)

An engineer needs to add protection for data in transit and have headers in the email message. Which configuration is needed to accomplish this goal?

- A. Provision the email appliance
- B. Deploy an encryption appliance.
- C. Map sender IP addresses to a host interface.
- D. Enable flagged message handling

**Answer:** D

#### NEW QUESTION 487

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 492

- (Exam Topic 3)

Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?

- A. RADIUS-based REAP
- B. fingerprinting
- C. Dynamic ARP Inspection
- D. multifactor authentication

**Answer:** D

#### NEW QUESTION 493

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 495

- (Exam Topic 3)

In which scenario is endpoint-based security the solution?

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

**Answer:** C

#### NEW QUESTION 496

- (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 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. userSudiSerlalNos and deviceInfo
- C. POST and name
- D. lastSyncTime and pid

**Answer:** A

**NEW QUESTION 503**

- (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 504**

- (Exam Topic 3)

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

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

**Answer:** BC

**NEW QUESTION 508**

- (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 511**

- (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 513**

- (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 517**

- (Exam Topic 3)

What is the most common type of data exfiltration that organizations currently experience?

- A. HTTPS file upload site
- B. Microsoft Windows network shares
- C. SQL database injections
- D. encrypted SMTP

**Answer:** B

**Explanation:**

Reference: <https://blogs.cisco.com/security/sensitive-data-exfiltration-and-the-insider>

#### NEW QUESTION 522

- (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 525

- (Exam Topic 3)

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

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

**Answer:** BE

#### NEW QUESTION 530

- (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 532

- (Exam Topic 3)

Refer to the exhibit.

```
ntp authentication-key 10 md5 cisco123
ntp trusted-key 10
```

A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced What is the cause of this issue?

- A. The key was configured in plain text.
- B. NTP authentication is not enabled.
- C. The hashing algorithm that was used was MD5. which is unsupported.
- D. The router was not rebooted after the NTP configuration updated.

**Answer:** B

#### NEW QUESTION 537

- (Exam Topic 3)

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

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

**Answer:** AC

#### NEW QUESTION 541

- (Exam Topic 3)

What is the most commonly used protocol for network telemetry?

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

**Answer:** D

#### NEW QUESTION 543

- (Exam Topic 3)



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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 544**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 547**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 549**

- (Exam Topic 3)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 553**

- (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 554**

- (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 559

- (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 564

- (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 568

- (Exam Topic 3)

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

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

D. Cisco Stealthwatch

**Answer:** D

#### NEW QUESTION 572

- (Exam Topic 3)

Which technology provides the benefit of Layer 3 through Layer 7 innovative deep packet inspection, enabling the platform to identify and output various applications within the network traffic flows?

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

**Answer:** A

#### NEW QUESTION 573

- (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 574

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 578

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 582

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 587

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 589

- (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 593

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 595

- (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 599

- (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 603

- (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 606

- (Exam Topic 3)

Which system performs compliance checks and remote wiping?

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

**Answer:** A

#### NEW QUESTION 607

- (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 611

- (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 614

- (Exam Topic 3)

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

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

**Answer:** B

#### Explanation:

Reference:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_usr\\_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec)

#### NEW QUESTION 619

- (Exam Topic 3)

Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?

- A. SDLC
- B. Docker
- C. Lambda
- D. Contiv

**Answer:** B

#### NEW QUESTION 624

- (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 629

- (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 634

- (Exam Topic 3)

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

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

**Answer:** BE

#### NEW QUESTION 635

- (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 636

- (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 637

- (Exam Topic 3)

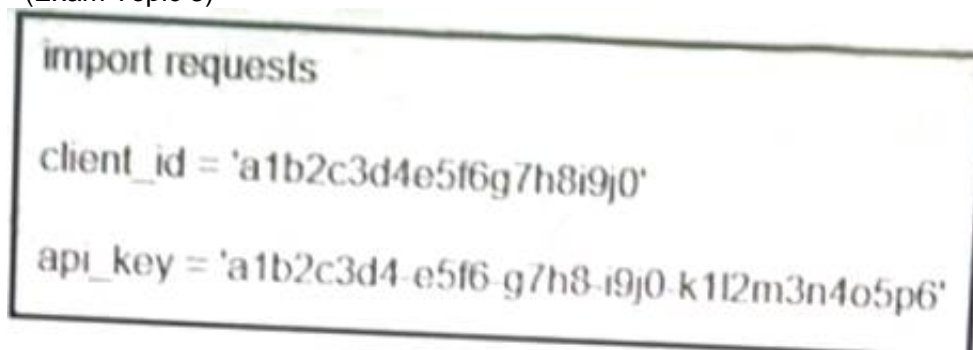
How does Cisco Workload Optimization portion of the network do EPP solutions solely performance issues?

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

**Answer:** B

#### NEW QUESTION 640

- (Exam Topic 3)



```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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

- A. imports requests
- B. HTTP authorization
- C. HTTP authentication
- D. plays dent ID

**Answer:** C

#### NEW QUESTION 641

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 644

- (Exam Topic 3)

Which VPN provides scalability for organizations with many remote sites?

- A. DMVPN
- B. site-to-site IPsec
- C. SSL VPN
- D. GRE over IPsec

**Answer:** A

#### NEW QUESTION 646

- (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 649

- (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 650

- (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 651

- (Exam Topic 3)

Which feature within Cisco ISE verifies the compliance of an endpoint before providing access to the network?

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

**Answer:** A

#### NEW QUESTION 656

- (Exam Topic 3)

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

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

**Answer:** BC

#### Explanation:

Reference:

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

#### NEW QUESTION 658

- (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 659

- (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 664

- (Exam Topic 3)

What must be enabled to secure SaaS-based applications?

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

Answer: C

#### NEW QUESTION 665

- (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 669

- (Exam Topic 3)

Which CLI command is used to enable URL filtering support for shortened URLs on the Cisco ESA?

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



**Answer:** B

**NEW QUESTION 671**

- (Exam Topic 3)

What is the intent of a basic SYN flood attack?

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

**Answer:** B

**NEW QUESTION 675**

- (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 676**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 680**

- (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 685**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 686**

- (Exam Topic 3)

A security engineer must add destinations into a destination list in Cisco Umbrella. What describes the application of these changes?

- A. The changes are applied immediately if the destination list is part of a policy.
- B. The destination list must be removed from the policy before changes are made to it.
- C. The changes are applied only after the configuration is saved in Cisco Umbrella.
- D. The user role of Block Page Bypass or higher is needed to perform these changes.

**Answer:** A

**NEW QUESTION 687**

- (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 689

.....

## 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](#)**