

# Cisco

## Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies



**NEW QUESTION 1**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 2**

- (Exam Topic 2)

Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

A picture containing table Description automatically generated

**NEW QUESTION 3**

- (Exam Topic 2)

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

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

**Answer:** CE

**Explanation:**

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

**NEW QUESTION 4**

- (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 5**

- (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 6

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 7

- (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 move security activities to the start of the development life cycle and have built-in security practices in the continuous integration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer to 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 8

- (Exam Topic 2)

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

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

**Answer:** BE

**Explanation:**

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

#### NEW QUESTION 9

- (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 10**

- (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 10**

- (Exam Topic 1)

What is the primary role of the Cisco Email Security Appliance?

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

**Answer:** B

**Explanation:**

Reference: [https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/Cisco\\_SBA\\_BN\\_EmailSecurityUsing](https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/Cisco_SBA_BN_EmailSecurityUsing)

**NEW QUESTION 14**

- (Exam Topic 1)

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

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

**Answer:** AD

**Explanation:**

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

**NEW QUESTION 17**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 19**

- (Exam Topic 1)

Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?

- A. aaa server radius dynamic-author
- B. aaa new-model
- C. auth-type all
- D. ip device-tracking

**Answer:** D

**NEW QUESTION 22**

- (Exam Topic 1)

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

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

**Answer:** AD

**NEW QUESTION 26**

- (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 27**

- (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 30**

- (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 33**

- (Exam Topic 1)

Which technology must be used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

- A. DMVPN

- B. FlexVPN
- C. IPsec DVTI
- D. GET VPN

**Answer:** D

**Explanation:**

Reference:

[https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN\\_DIG\\_](https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_)

**NEW QUESTION 35**

- (Exam Topic 1)

A network engineer is configuring DMVPN and entered the crypto isakmp key cisc0380739941 address 1.1.1.1 command on hostA. The tunnel is not being established to hostB. What action is needed to authenticate the VPN?

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

**Answer:** C

**NEW QUESTION 39**

- (Exam Topic 1)

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

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

**Answer:** AB

**NEW QUESTION 42**

- (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 44**

- (Exam Topic 1)

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

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

**Answer:** CE

**NEW QUESTION 49**

- (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 51

- (Exam Topic 1)

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

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

**Answer:** BC

#### NEW QUESTION 55

- (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 57

- (Exam Topic 1)

Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 58

- (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 59

- (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 60

- (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 61**

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 63**

- (Exam Topic 1)

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

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

**Answer:** CE

**NEW QUESTION 65**

- (Exam Topic 1)

Which Cisco AMP file disposition valid?

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

**Answer:** B

**NEW QUESTION 67**

- (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 71**

- (Exam Topic 1)

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

- A. transparent
- B. redirection
- C. forward
- D. proxy gateway

**Answer:** A

**Explanation:**

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

**NEW QUESTION 75**

- (Exam Topic 1)

A malicious user gained network access by spoofing printer connections that were authorized using MAB on four different switch ports at the same time. What two catalyst switch security features will prevent further violations? (Choose two)

- A. DHCP Snooping
- B. 802.1AE MacSec
- C. Port security
- D. IP Device track
- E. Dynamic ARP inspection
- F. Private VLANs

**Answer:** AE

#### NEW QUESTION 77

- (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 79

- (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 82

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 83

- (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 88

- (Exam Topic 1)

Which API is used for Content Security?

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

**Answer:** D

#### NEW QUESTION 92

- (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 96

- (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 101

- (Exam Topic 1)

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

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

**Answer: AC**

#### NEW QUESTION 102

- (Exam Topic 1)

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

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

**Answer: DE**

#### Explanation:

Reference: [https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview\\_guide/Cisco\\_Cloud\\_Hybrid\\_Email\\_Security](https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security)

#### NEW QUESTION 105

- (Exam Topic 3)

What are two functionalities of northbound and southbound APIs within Cisco SDN architecture? (Choose two.)

- A. Southbound APIs are used to define how SDN controllers integrate with applications.
- B. Southbound interfaces utilize device configurations such as VLANs and IP addresses.
- C. Northbound APIs utilize RESTful API methods such as GET, POST, and DELETE.
- D. Southbound APIs utilize CLI, SNMP, and RESTCONF.
- E. Northbound interfaces utilize OpenFlow and OpFlex to integrate with network devices.

**Answer: CD**

#### NEW QUESTION 107

- (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 110**

- (Exam Topic 3)

Why is it important to patch endpoints consistently?

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

**Answer: B**

**NEW QUESTION 115**

- (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 116**

- (Exam Topic 3)

Which algorithm is an NGE hash function?

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

**Answer: D**

**NEW QUESTION 117**

- (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 121**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 123**

- (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 127**

- (Exam Topic 3)

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

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

**Answer: AE**

**NEW QUESTION 132**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 135**

- (Exam Topic 3)

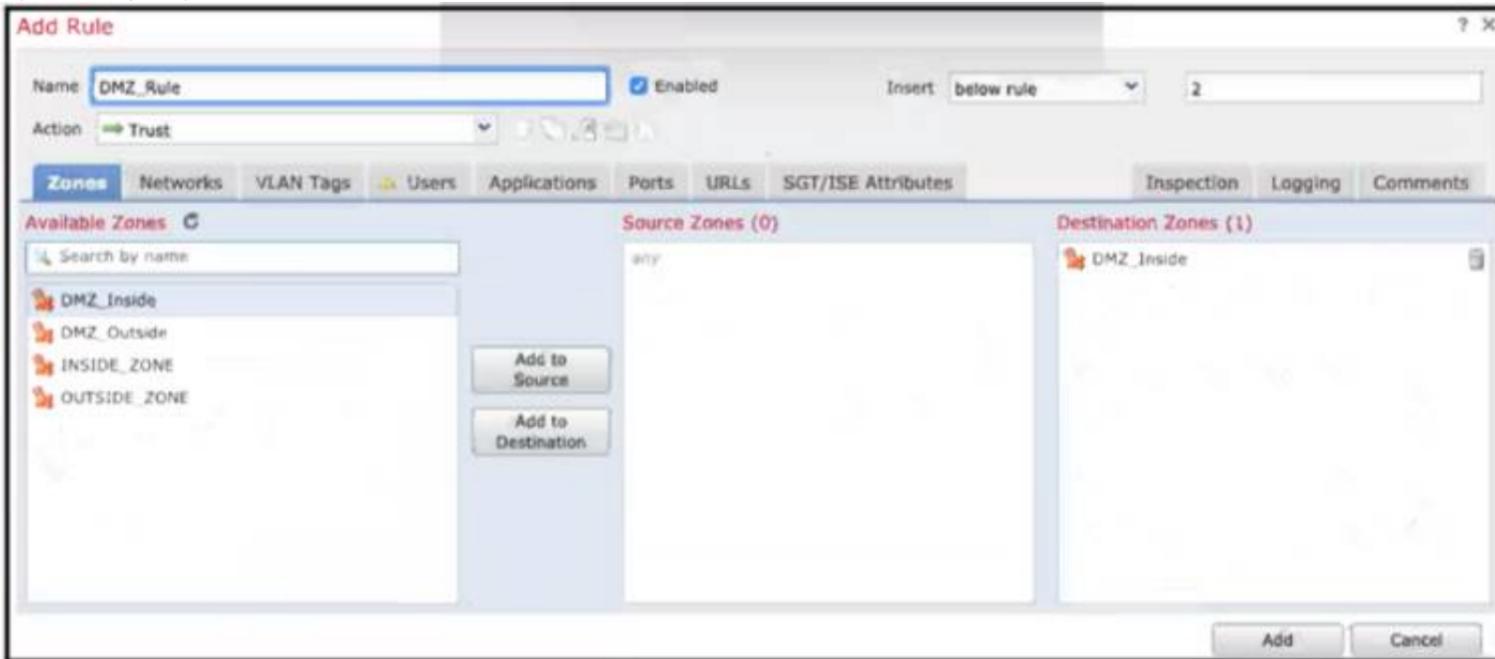
An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users.

- 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 140**

- (Exam Topic 3)



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

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

**Answer: A**

**NEW QUESTION 142**

- (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 144**

- (Exam Topic 3)  
 Refer to the exhibit.

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

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

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

**Answer:** A

**NEW QUESTION 147**

- (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 150**

- (Exam Topic 3)

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

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

Answer: A

**NEW QUESTION 153**

- (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 158**

- (Exam Topic 3)

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

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

Answer: D

**NEW QUESTION 159**

- (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 163**

- (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 164**

- (Exam Topic 3)

An engineer is adding a Cisco DUO solution to the current TACACS+ deployment using Cisco ISE. The engineer wants to authenticate users using their account when they log into network devices. Which action accomplishes this task?

- A. Configure Cisco DUO with the external Active Directory connector and tie it to the policy set within Cisco ISE.
- B. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE
- C. Create an identity policy within Cisco ISE to send all authentication requests to Cisco DUO.
- D. Modify the current policy with the condition MFASourceSequence DUO=true in the authorization conditions within Cisco ISE

Answer: B

**NEW QUESTION 165**

- (Exam Topic 3)

Which Cisco security solution stops exfiltration using HTTPS?

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

Answer: C

**Explanation:**

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

**NEW QUESTION 166**

- (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 167**

- (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 170**

- (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 171**

- (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 176**

- (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 180**

- (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 184**

- (Exam Topic 3)

Which Cisco security solution provides patch management in the cloud?

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

**Answer: C**

**NEW QUESTION 186**

- (Exam Topic 3)

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

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

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

**Answer: D**

**NEW QUESTION 188**

- (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 191**

- (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 192**

- (Exam Topic 3)

What is the target in a phishing attack?

- A. perimeter firewall
- B. IPS
- C. web server
- D. endpoint

**Answer: D**

**NEW QUESTION 196**

- (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 198**

- (Exam Topic 3)

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

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

Answer: A

**NEW QUESTION 203**

- (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 205**

- (Exam Topic 3)

Which function is included when Cisco AMP is added to web security?

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

Answer: B

**NEW QUESTION 209**

- (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:



**NEW QUESTION 212**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 216**

- (Exam Topic 3)

Which IETF attribute is supported for the RADIUS CoA feature?

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

**Answer: A**

**NEW QUESTION 220**

- (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 222**

- (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 223**

- (Exam Topic 3)

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

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

Answer: B

**NEW QUESTION 226**

- (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 230**

- (Exam Topic 3)

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

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

Answer: BE

**NEW QUESTION 232**

- (Exam Topic 3)

An engineer is implementing DHCP security mechanisms and needs the ability to add additional attributes to profiles that are created within Cisco ISE Which action accomplishes this task?

- A. Define MAC-to-IP address mappings in the switch to ensure that rogue devices cannot get an IP address
- B. Use DHCP option 82 to ensure that the request is from a legitimate endpoint and send the information to Cisco ISE
- C. Modify the DHCP relay and point the IP address to Cisco ISE.
- D. Configure DHCP snooping on the switch VLANs and trust the necessary interfaces

Answer: D

**NEW QUESTION 233**

- (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 235**

- (Exam Topic 3)

Using Cisco Cognitive Threat Analytics, which platform automatically blocks risky sites, and test unknown sites for hidden advanced threats before allowing users to click them?

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

Answer: C

**NEW QUESTION 236**

- (Exam Topic 3)

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

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

Answer: B

**NEW QUESTION 239**

- (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 241**

- (Exam Topic 3)

Which posture assessment requirement provides options to the client for remediation and requires the remediation within a certain timeframe?

- A. Audit
- B. Mandatory
- C. Optional
- D. Visibility

**Answer:** B

**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin\\_guide/b\\_ISE\\_admin\\_guide\\_24/m\\_client\\_posture\\_Mandatory\\_Requirements\\_During\\_policy\\_evaluation,](https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_client_posture_Mandatory_Requirements_During_policy_evaluation.html) the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings

**NEW QUESTION 243**

- (Exam Topic 3)

An engineer must set up 200 new laptops on a network and wants to prevent the users from moving their laptops around to simplify administration. Which switch port MAC address security setting must be used?

- A. sticky
- B. static
- C. aging
- D. maximum

**Answer:** A

**NEW QUESTION 247**

- (Exam Topic 3)

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Diagram Description automatically generated

**NEW QUESTION 249**

- (Exam Topic 3)

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

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

Answer: D

**NEW QUESTION 251**

- (Exam Topic 3)

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

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

Answer: C

**NEW QUESTION 253**

- (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 255**

- (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 259**

- (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 263

- (Exam Topic 3)

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 268

- (Exam Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 272

- (Exam Topic 3)

An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation. What must be un solution?

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

**Answer: D**

#### NEW QUESTION 274

- (Exam Topic 3)

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

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

**Answer: B**

#### Explanation:

Reference:

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

#### NEW QUESTION 276

- (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 281

- (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 282

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 286

- (Exam Topic 3)

Which encryption algorithm provides highly secure VPN communications?

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

**Answer:** B

#### NEW QUESTION 288

- (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 289

- (Exam Topic 3)

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

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

**Answer:** CE

#### NEW QUESTION 294

- (Exam Topic 3)

An engineer is configuring Cisco WSA and needs to enable a separated email transfer flow from the Internet and from the LAN. Which deployment mode must be used to accomplish this goal?

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

**Answer:** D

#### NEW QUESTION 298

- (Exam Topic 3)

With Cisco AMP for Endpoints, which option shows a list of all files that have been executed in your environment?

- A. Prevalence
- B. File analysis
- C. Detections
- D. Vulnerable software
- E. Threat root cause

**Answer:** A

#### Explanation:

Reference: <https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf>

**NEW QUESTION 300**

- (Exam Topic 3)

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 302**

- (Exam Topic 3)

An organization is implementing AAA for their users. They need to ensure that authorization is verified for every command that is being entered by the network administrator. Which protocol must be configured in order to provide this capability?

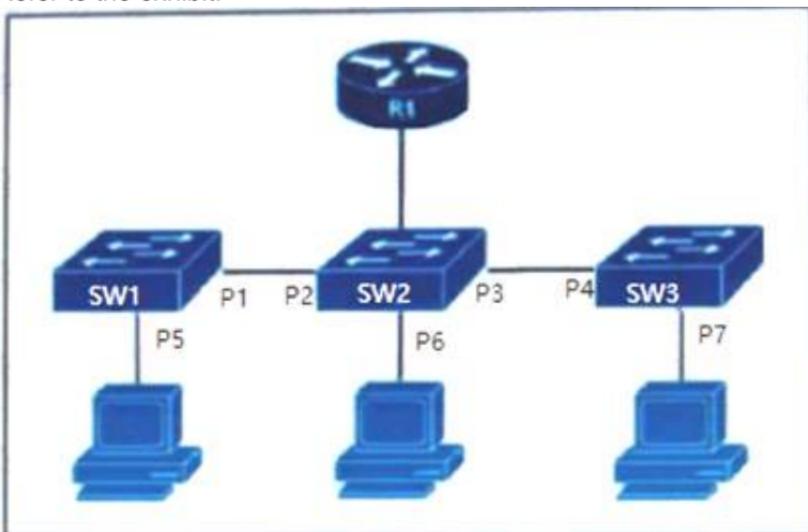
- A. EAPOL
- B. SSH
- C. RADIUS
- D. TACACS+

**Answer: D**

**NEW QUESTION 306**

- (Exam Topic 3)

Refer to the exhibit.



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

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

**Answer: D**

**NEW QUESTION 308**

- (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 312**

- (Exam Topic 3)

Refer to the exhibit.

```

"remarks" [],
"destinationService" {
  "kind" serviceKind,
  "value" destinationService { Enter your search term
},
"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 316**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 319**

- (Exam Topic 3)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 323**

- (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 327**

- (Exam Topic 3)

What is a description of microsegmentation?

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

Answer: B

**NEW QUESTION 332**

- (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 337**

- (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 338**

- (Exam Topic 3)

Refer to the exhibit.



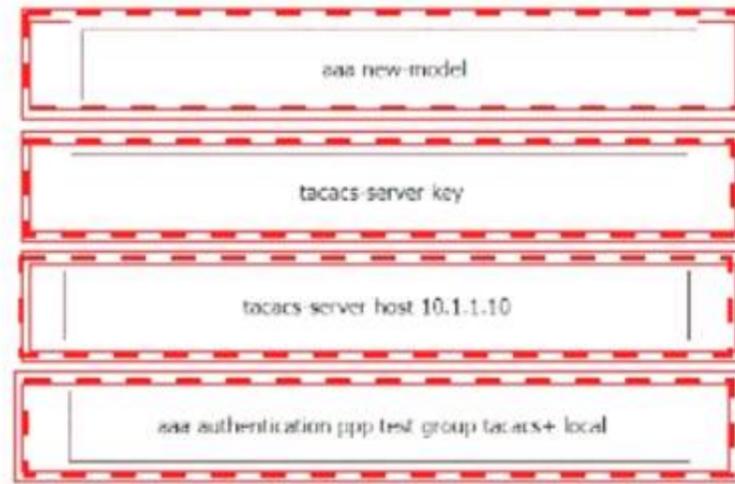
An engineer must configure a Cisco switch to perform PPP authentication via a TACACS server located at IP address 10.1.1.10. Authentication must fall back to the local database using the username LocalUser and password C1Sc0451069341I if the TACACS server is unreachable. Drag and drop the commands from the left onto the corresponding configuration steps on the right.

- aaa new-model
- tacacs-server key
- tacacs server host 10.1.1.10
- aaa authentication ppp test group tacacs+ local

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



**NEW QUESTION 342**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 345**

- (Exam Topic 3)

Which method of attack is used by a hacker to send malicious code through a web application to an unsuspecting user to request that the victim's web browser executes the code?

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

**Answer: D**

**NEW QUESTION 350**

- (Exam Topic 3)

What is a benefit of using a multifactor authentication strategy?

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

**Answer: D**

**NEW QUESTION 353**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 356**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 359**

- (Exam Topic 3)

Which category includes DoS Attacks?

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

**Answer: C**

**NEW QUESTION 364**

- (Exam Topic 3)

What is a feature of NetFlow Secure Event Logging?

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

**Answer: A**

**NEW QUESTION 369**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 373**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 375**

- (Exam Topic 2)

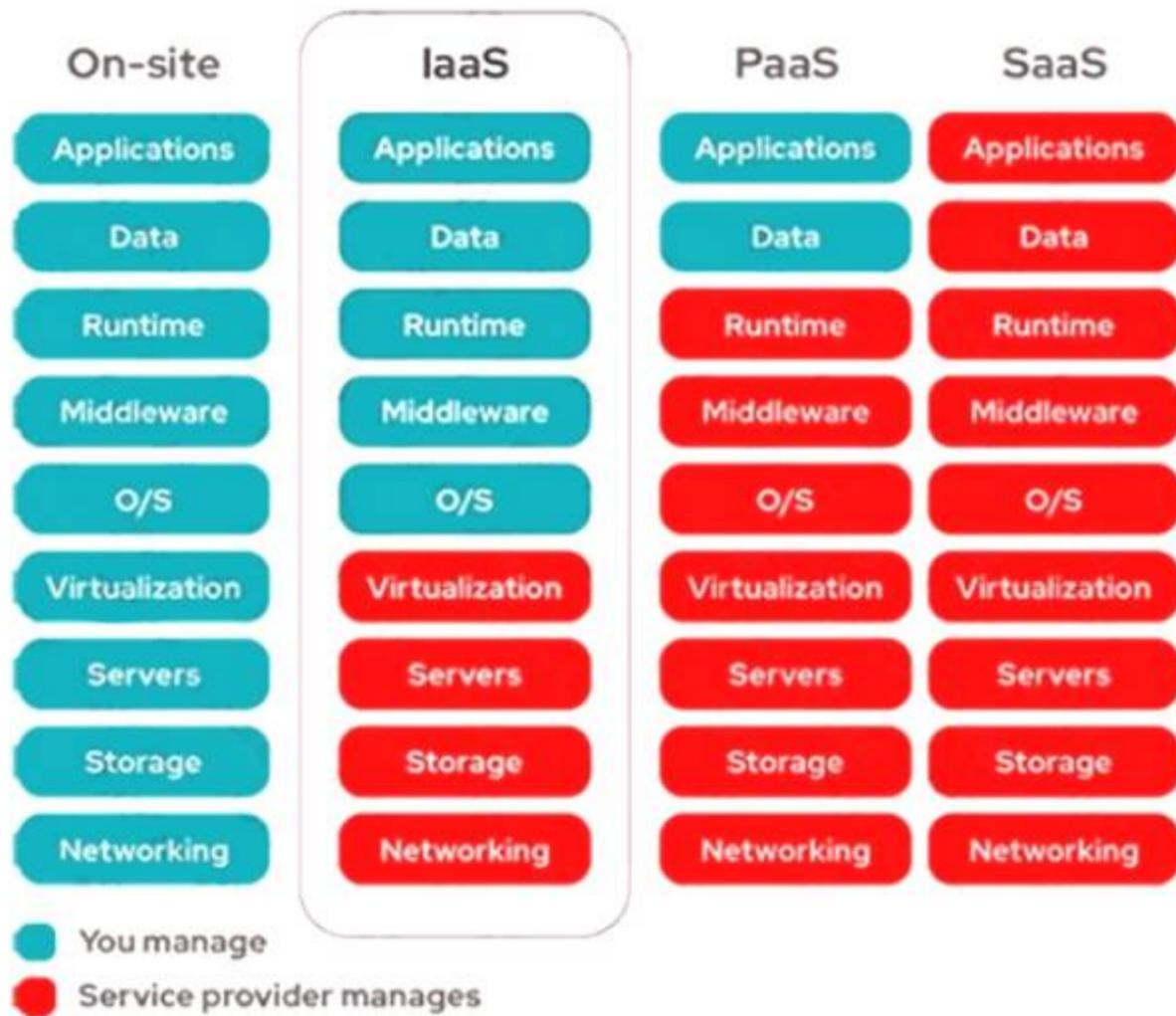
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two)

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

**Answer: DE**

**Explanation:**

Customers must manage applications and data in PaaS.



**NEW QUESTION 377**

- (Exam Topic 3)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 381**

- (Exam Topic 2)

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

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

**Answer:** AD

**Explanation:**

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

**NEW QUESTION 385**

- (Exam Topic 2)

A network administrator is configuring a rule in an access control policy to block certain URLs and selects the "Chat and Instant Messaging" category. Which reputation score should be selected to accomplish this goal?

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

**Answer:** D

**Explanation:**

We choose "Chat and Instant Messaging" category in "URL Category":

**Edit Action**

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

**URL Category** Help

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

Available Categories: Add > < Remove

- Advertisements
- Alcohol
- Arts
- Astrology
- Auctions
- Business and Industry
- Chat and Instant Messagir
- Cheating and Plagiarism
- Computer Security
- Computers and Internet

Selected Categories:

- Adult
- Child Abuse Content
- Illegal Activities
- Illegal Downloads
- Illegal Drugs

Use a URL whitelist: None : ?

Action on URL:

- Defang URL ?
- Redirect to Cisco Security Proxy ?
- Replace URL with text message

Perform Action for:

- All messages
- Unsigned messages

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

**Edit Condition**

Message Body or Attachment  
 Message Body  
 URL Category  
**URL Reputation**  
 Message Size  
 Attachment Content  
 Attachment File Info  
 Attachment Protection  
 Subject Header  
 Other Header  
 Envelope Sender  
 Envelope Recipient  
 Receiving Listener  
 Remote IP/Hostname  
 Reputation Score

**URL Reputation**

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

URL Reputation is:

- Malicious (-10.0 to -6.0)
- Suspect (-5.9 to 5.9)
- Clean (6.0 to 10.0)
- Custom Range (min to max)
- No Score

Use a URL whitelist: None : ?

**NEW QUESTION 390**

- (Exam Topic 2)

Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats?

- A. PSIRT
- B. Talos
- C. CSIRT
- D. DEVNET

**Answer: B**

**Explanation:**

Reference: <https://talosintelligence.com/newsletters>

**NEW QUESTION 395**

- (Exam Topic 2)

Which attack type attempts to shut down a machine or network so that users are not able to access it?

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

**Answer: A**

**Explanation:**

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

IPbroadcast address.

**NEW QUESTION 398**

- (Exam Topic 2)

What features does Cisco FTDv provide over ASAv?

- A. Cisco FTDv runs on VMWare while ASAv does not
- B. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not
- C. Cisco FTDv runs on AWS while ASAv does not
- D. Cisco FTDv supports URL filtering while ASAv does not

**Answer:** D

**NEW QUESTION 403**

- (Exam Topic 2)

Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.

Install monitoring extension for AWS EC2.	step 1
Restart the Machine Agent.	step 2
Update config.yaml.	step 3
Configure a Machine Agent or SIM Agent.	step 4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

**NEW QUESTION 407**

- (Exam Topic 2)

What is a benefit of performing device compliance?

- A. Verification of the latest OS patches
- B. Device classification and authorization
- C. Providing multi-factor authentication
- D. Providing attribute-driven policies

**Answer:** A

**NEW QUESTION 412**

- (Exam Topic 2)

In an IaaS cloud services model, which security function is the provider responsible for managing?

- A. Internet proxy
- B. firewalling virtual machines
- C. CASB
- D. hypervisor OS hardening

**Answer:** B

**Explanation:**

In this IaaS model, cloud providers offer resources to users/machines that include computers as virtual machines, raw (block) storage, firewalls, load balancers, and network devices. Note: Cloud access security broker (CASB) provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware such as ransomware.

**NEW QUESTION 414**

- (Exam Topic 2)

Drag and drop the threats from the left onto examples of that threat on the right

DoS/DDoS	A stolen customer database that contained social security numbers and was published online.
Insecure APIs	A phishing site appearing to be a legitimate login page captures user login information.
data breach	An application attack using botnets from multiple remote locations that flood a web application causing a degraded performance or a complete outage.
compromised credentials	A malicious user gained access to an organization's database from a cloud-based application programming interface that lacked strong authentication controls.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. When your credentials have been compromised, it means someone other than you may be in possession of your account information, such as your username and/or password.

**NEW QUESTION 419**

- (Exam Topic 2)

What is the benefit of installing Cisco AMP for Endpoints on a network?

- A. It provides operating system patches on the endpoints for security.
- B. It provides flow-based visibility for the endpoints network connections.
- C. It enables behavioral analysis to be used for the endpoints.
- D. It protects endpoint systems through application control and real-time scanning

**Answer:** D

**NEW QUESTION 420**

- (Exam Topic 2)

Which risk is created when using an Internet browser to access cloud-based service?

- A. misconfiguration of infrastructure, which allows unauthorized access
- B. intermittent connection to the cloud connectors
- C. vulnerabilities within protocol
- D. insecure implementation of API

**Answer:** D

**NEW QUESTION 423**

- (Exam Topic 2)

What is the purpose of the certificate signing request when adding a new certificate for a server?

- A. It is the password for the certificate that is needed to install it with.
- B. It provides the server information so a certificate can be created and signed
- C. It provides the certificate client information so the server can authenticate against it when installing
- D. It is the certificate that will be loaded onto the server

**Answer:** B

**Explanation:**

A certificate signing request (CSR) is one of the first steps towards getting your own SSL Certificate. Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) that the Certificate Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key

**NEW QUESTION 424**

- (Exam Topic 2)

An organization has noticed an increase in malicious content downloads and wants to use Cisco Umbrella to prevent this activity for suspicious domains while allowing normal web traffic. Which action will accomplish this task?

- A. Set content settings to High
- B. Configure the intelligent proxy.
- C. Use destination block lists.
- D. Configure application block lists.

**Answer:** B

**Explanation:**

Reference: <https://docs.umbrella.com/deployment-umbrella/docs/what-is-the-intelligent-proxy>

**NEW QUESTION 426**

- (Exam Topic 2)

What is the purpose of the My Devices Portal in a Cisco ISE environment?

- A. to register new laptops and mobile devices
- B. to request a newly provisioned mobile device
- C. to provision userless and agentless systems
- D. to manage and deploy antivirus definitions and patches on systems owned by the end user

**Answer:** A

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b\\_mydevices\\_2x.html](https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html)

**NEW QUESTION 428**

- (Exam Topic 2)

What is provided by the Secure Hash Algorithm in a VPN?

- A. integrity
- B. key exchange
- C. encryption
- D. authentication

**Answer:** A

**Explanation:**

Reference: <https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=4>

**NEW QUESTION 431**

- (Exam Topic 2)

Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks	<b>Cisco Firepower</b>  <div style="border: 1px solid black; height: 20px; width: 100%; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 20px; width: 100%; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 20px; width: 100%;"></div>
provides superior threat prevention and mitigation for known and unknown threats	
provides outbreak control through custom detections	
provides the root cause of a threat based on the indicators of compromise seen	<b>Cisco AMP</b>  <div style="border: 1px solid black; height: 20px; width: 100%; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 20px; width: 100%; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 20px; width: 100%;"></div>
provides the ability to perform network discovery	
provides intrusion prevention before malware compromises the host	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Application Description automatically generated with low confidence explanation The Firepower System uses network discovery and identity policies to collect host, application, and user data for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible. The Cisco Advanced Malware Protection (AMP) solution enables you to detect and block malware, continuously analyze for malware, and get retrospective alerts. AMP for Networks delivers network-based advanced malware protection that goes beyond point-in-time detection to protect your organization across the entire attack continuum – before, during, and after an attack. Designed for Cisco Firepower® network threat appliances, AMP for Networks detects, blocks, tracks, and contains malware threats across multiple threat vectors within a single system. It also provides the visibility and control necessary to protect your organization against highly sophisticated, targeted, zero-day, and persistent advanced malware threats.

**NEW QUESTION 435**

- (Exam Topic 2)

A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an undetermined verdict. What is causing this issue?

- A. The policy was created to send a message to quarantine instead of drop
- B. The file has a reputation score that is above the threshold
- C. The file has a reputation score that is below the threshold
- D. The policy was created to disable file analysis

**Answer: D**

**Explanation:**

Maybe the "newly installed service" in this Q mentions about Advanced Malware Protection (AMP) which can be used along with ESA. AMP allows superior protection across the attack continuum.+ File Reputation – captures a fingerprint of each file as it traverses the ESA and sends it to AMP's cloudbased intelligence network for a reputation verdict. Given these results, you can automatically block malicious files and apply administrator-defined policy.+ File Analysis – provides the ability to analyze unknown files that are traversing the ESA. A highly secure sandbox environment enables AMP to glean precise details about the file's behavior and to combine that data with detailed human and machine analysis to determine the file's threat level. This disposition is then fed into AMP cloud-based intelligence network and used to dynamically update and expand the AMP cloud data set for enhanced protection

**NEW QUESTION 437**

- (Exam Topic 2)

Which component of Cisco umbrella architecture increases reliability of the service?

- A. Anycast IP
- B. AMP Threat grid
- C. Cisco Talos
- D. BGP route reflector

**Answer: C**

**NEW QUESTION 442**

- (Exam Topic 2)

Refer to the exhibit.

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

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

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

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

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 444**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 445**

- (Exam Topic 2)

An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?

- A. TCP 6514
- B. UDP 1700
- C. TCP 49
- D. UDP 1812

**Answer:** B

**Explanation:**

CoA Messages are sent on two different udp ports depending on the platform. Cisco standardizes on UDP port 1700, while the actual RFC calls out using UDP port 3799.

**NEW QUESTION 446**

- (Exam Topic 2)

What is the function of SDN southbound API protocols?

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

**Answer:** B

**Explanation:**

Reference: <https://www.ciscopress.com/articles/article.asp?p=3004581&seqNum=2>

Note: Southbound APIs helps us communicate with data plane (not control plane) applications

**NEW QUESTION 447**

- (Exam Topic 2)

Drag and drop the solutions from the left onto the solution's benefits on the right.

Cisco Stealthwatch	obtains contextual identity and profiles for all the users and devices connected on a network.
Cisco ISE	software-defined segmentation that uses SGTs and allows administrators to quickly scale and enforce policies across the network
Cisco TrustSec	rapidly collects and analyzes NetFlow and telemetry data to deliver in-depth visibility and understanding of network traffic
Cisco Umbrella	secure Internet gateway in the cloud that provides a security solution that protects endpoints on and off the network against threats on the Internet by using DNS

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

Cisco ISE – obtains contextual identity and profiles for all users and device

Cisco TrustSec – software defined segmentation that uses SGTs  
Cisco Umbrella – secure internet gateway on the cloud that provides a security solution

**NEW QUESTION 448**

- (Exam Topic 2)

When configuring ISAKMP for IKEv1 Phase1 on a Cisco IOS router, an administrator needs to input the command `crypto isakmp key cisco address 0.0.0.0`. The administrator is not sure what the IP addressing in this command issued for. What would be the effect of changing the IP address from 0.0.0.0 to 1.2.3.4?

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

**Answer: B**

**Explanation:**

The command `crypto isakmp key cisco address 1.2.3.4` authenticates the IP address of the 1.2.3.4 peer by using the key cisco. The address of "0.0.0.0" will authenticate any address with this key

**NEW QUESTION 453**

- (Exam Topic 2)

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

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

**Answer: CE**

**Explanation:**

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

**NEW QUESTION 454**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 455**

- (Exam Topic 2)

Which algorithm provides asymmetric encryption?

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

**Answer: C**

**NEW QUESTION 458**

.....

## **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](#)**