# Cisco

## Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

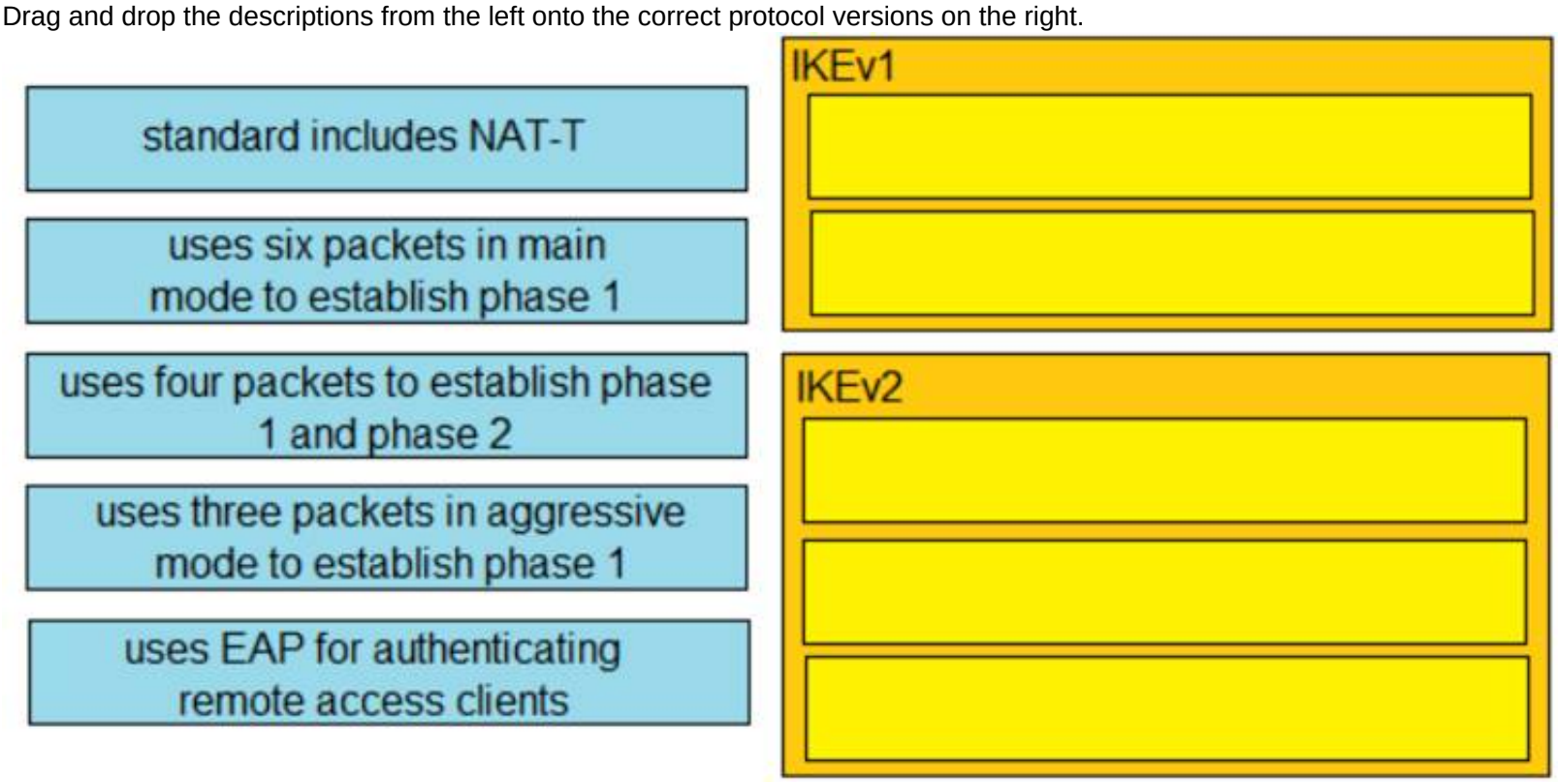
**NEW QUESTION 1**
- (Exam Topic 2)
Which attack is preventable by Cisco ESA but not by the Cisco WSA?

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

**Answer:** D

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

**NEW QUESTION 2**
- (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 3**
- (Exam Topic 2)
What is a benefit of conducting device compliance checks?

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

**Answer:** B

**NEW QUESTION 4**
- (Exam Topic 2)
What is a function of 3DES in reference to cryptography?

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

**Answer:** C

**NEW QUESTION 5**
- (Exam Topic 2)
Using Cisco Firepower's Security Intelligence policies, upon which two criteria is Firepower block based? (Choose two)

A. URLs
B. protocol IDs
C. IP addresses
D. MAC addresses
E. port numbers

**Answer:** AC

**Explanation:**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-configguide-v623/secu

**NEW QUESTION 6**
- (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.htmlIn this question, it stated “the network is congested” (not the file analysis server was overloaded) so theappliance will not try to upload the file again.

**NEW QUESTION 7**
- (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 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)
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 10**
- (Exam Topic 2)
An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?

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

**Answer:** D

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

**NEW QUESTION 15**
- (Exam Topic 2)
An engineer has enabled LDAP accept queries on a listener. Malicious actors must be prevented from quickly identifying all valid recipients. What must be done on the Cisco ESA to accomplish this goal?

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

**Answer:** C

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

**NEW QUESTION 20**
- (Exam Topic 2)
What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

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

**Answer:** B

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

**NEW QUESTION 22**
- (Exam Topic 2)
Why is it important to implement MFA inside of an organization?

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

**Answer:** C

**NEW QUESTION 24**
- (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 27**
- (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 34**
- (Exam Topic 2)
What is an attribute of the DevSecOps process?

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

**Answer:** C

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

**NEW QUESTION 37**
- (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 providedevice-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 42**
- (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 47**
- (Exam Topic 2)
A network engineer is deciding whether to use stateful or stateless failover when configuring two ASAs for high availability. What is the connection status in both cases?

A. need to be reestablished with stateful failover and preserved with stateless failover
B. preserved with stateful failover and need to be reestablished with stateless failover
C. preserved with both stateful and stateless failover
D. need to be reestablished with both stateful and stateless failover

**Answer:** B

**NEW QUESTION 51**
- (Exam Topic 2)
What is a benefit of using Cisco FMC over Cisco ASDM?

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

**Answer:** B

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

**NEW QUESTION 54**
- (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 58**
- (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)

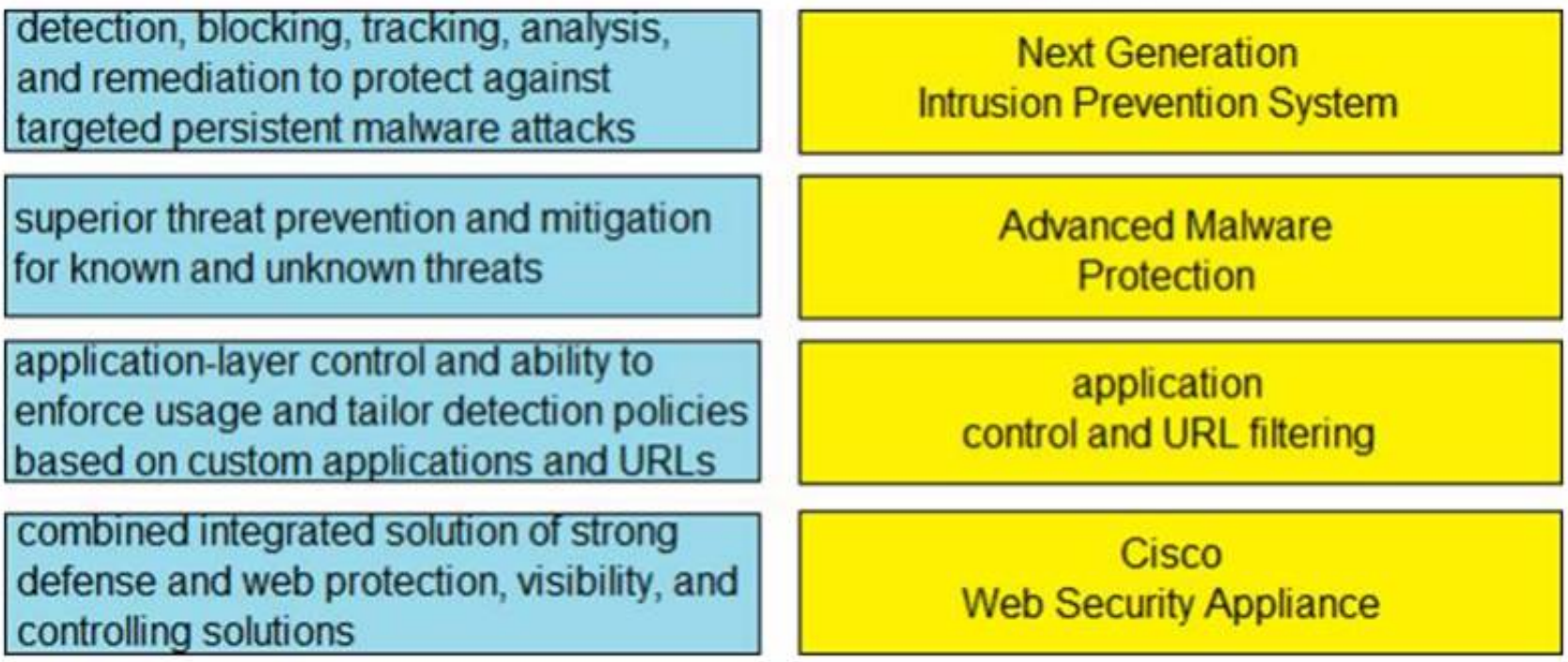
A. permit
B. trust
C. reset
D. allow
E. monitor

**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 60**
- (Exam Topic 2)
Drag and drop the capabilities from the left onto the correct technologies on the right.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Text, chat or text message Description automatically generated

**NEW QUESTION 63**
- (Exam Topic 1)
What is the primary role of the Cisco Email Security Appliance?

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

**Answer:** B

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

**NEW QUESTION 65**
- (Exam Topic 2)
An organization has two systems in their DMZ that have an unencrypted link between them for communication. The organization does not have a defined password policy and uses several default accounts on the systems. The application used on those systems also have not gone through stringent code reviews. Which vulnerability would help an attacker brute force their way into the systems?

A. weak passwords
B. lack of input validation
C. missing encryption
D. lack of file permission

**Answer:** C

**Explanation:**
Reference: https://tools.ietf.org/html/rfc3954

**NEW QUESTION 70**
- (Exam Topic 1)
Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two)

A. accounting
B. assurance
C. automation
D. authentication
E. encryption

**Answer:** BC

**Explanation:**

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

**NEW QUESTION 74**
- (Exam Topic 1)
Which option is the main function of Cisco Firepower impact flags?

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

**Answer:** C

**NEW QUESTION 76**
- (Exam Topic 1)
Which VPN technology can support a multivendor environment and secure traffic between sites?

A. SSL VPN
B. GET VPN
C. FlexVPN
D. DMVPN

**Answer:** C

**Explanation:**
FlexVPN is an IKEv2-based VPN technology that provides several benefits beyond traditional site-to-site VPN implementations. FlexVPN is a standards-based solution that can interoperate with non-Cisco IKEv2implementations. Therefore FlexVPN can support a multivendor environment. All of the three VPN technologies support traffic between sites (site-to-site or spoke-to-spoke).

**NEW QUESTION 80**
- (Exam Topic 1)
What is the primary benefit of deploying an ESA in hybrid mode?

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

**Answer:** D

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

**NEW QUESTION 82**
- (Exam Topic 1)
Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?

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

**Answer:** B

**NEW QUESTION 86**
- (Exam Topic 1)
Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two)

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

**Answer:** AC

**NEW QUESTION 90**
- (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 91**
- (Exam Topic 1)
Refer to the exhibit.

```
snmp-server group SNMP v3 auth access
15
```

What does the number 15 represent in this configuration?

A. privilege level for an authorized user to this router
B. access list that identifies the SNMP devices that can access the router
C. interval in seconds between SNMPv3 authentication attempts
D. number of possible failed attempts until the SNMPv3 user is locked out

**Answer:** B

**Explanation:**
The syntax of this command is shown below:snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]}] [read read-view] [write write-view] [notify notify-view] [access access-list]The command above restricts which IP source addresses are allowed to access SNMP functions on the router. You could restrict SNMP access by simply applying an interface ACL to block incoming SNMP packets that don't come from trusted servers. However, this would not be as effective as using the global SNMP commands shown in this recipe. Because you can apply this method once for the whole router, it is much simpler than applying ACLs to block SNMP on all interfaces separately. Also, using interface ACLs would block not only SNMP packets intended for this router, but also may stop SNMP packets that just happened to be passing through on their way to some other destination device.

**NEW QUESTION 92**
- (Exam Topic 1)
Refer to the exhibit.

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

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

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

**Answer:** C

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

**NEW QUESTION 96**
- (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 101**
- (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 104**

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

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

**Answer:** D

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

**NEW QUESTION 106**
- (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

**NEW QUESTION 107**
- (Exam Topic 1)
An engineer configured a new network identity in Cisco Umbrella but must verify that traffic is being routed through the Cisco Umbrella network. Which action tests the routing?

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

**Answer:** B

**NEW QUESTION 111**
- (Exam Topic 1)
What is the function of the Context Directory Agent?

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

**Answer:** C

**Explanation:**
Reference: https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_oveviw.html

**NEW QUESTION 116**
- (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 118**
- (Exam Topic 1)
An engineer is configuring AMP for endpoints and wants to block certain files from executing. Which outbreak control method is used to accomplish this task?

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

**Answer:**

C

**NEW QUESTION 123**
- (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 127**
- (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 thehighest possible level of access privileges, similar to an ‘Administrator’ in Windows. The word ‘kit’ refers to thesoftware that grants root-level access to the machine. Put the two together and you get ‘rootkit’, a program thatgives 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 129**
- (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 130**
- (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 134**
- (Exam Topic 1)
Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?

A. IP Blacklist Center
B. File Reputation Center
C. AMP Reputation Center
D. IP and Domain Reputation Center

**Answer:** D

**NEW QUESTION 136**
- (Exam Topic 1)
Which network monitoring solution uses streams and pushes operational data to provide a near real-time view of activity?

A. SNMP
B. SMTP
C. syslog
D. model-driven telemetry

**Answer:** D

**Explanation:**

Reference: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide

**NEW QUESTION 139**
- (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 DNSqueries and responses. DNS tunneling often includes data payloads that can be added to an attacked DNSserver and used to control a remote server and applications.

**NEW QUESTION 143**
- (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 144**
- (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 146**
- (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 149**
- (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 150**
- (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 154**
- (Exam Topic 1)
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)

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

**Answer:** DE

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

**NEW QUESTION 156**
- (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 158**
- (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 163**
- (Exam Topic 1)
Which two mechanisms are used to control phishing attacks? (Choose two)

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

**Answer:** AE

**NEW QUESTION 165**
- (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 166**
- (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 169**
- (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-guidev60/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, andother types of files for the most common types of malware, using a detection rule set provided by the CiscoTalos 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 doesnot 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 avirtual machine.

**NEW QUESTION 173**
- (Exam Topic 1)
What are two list types within AMP for Endpoints Outbreak Control? (Choose two)

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

**Answer:** BD

**Explanation:**
Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists.A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect andquarantine.Allowed applications lists are for files you never want to

convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf

**NEW QUESTION 175**
- (Exam Topic 1)
Which two features of Cisco Email Security can protect your organization against email threats? (Choose two)

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

**Answer:** BD

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

**NEW QUESTION 179**
- (Exam Topic 1)
Which statement describes a traffic profile on a Cisco Next Generation Intrusion Prevention System?

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

**Answer:** B

**NEW QUESTION 184**
- (Exam Topic 1)
Which Cisco AMP file disposition valid?

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

**Answer:** B

**NEW QUESTION 188**
- (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 189**
- (Exam Topic 1)
What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?

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

**Answer:** D

**NEW QUESTION 191**
- (Exam Topic 1)
Which two deployment modes does the Cisco ASA FirePower module support? (Choose two)

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

**Answer:** CD

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

**NEW QUESTION 195**
- (Exam Topic 1)
What Cisco command shows you the status of an 802.1X connection on interface gi0/1?

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

**Answer:** B

**NEW QUESTION 200**
- (Exam Topic 1)
Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?

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

**Answer:** A

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

**NEW QUESTION 202**
- (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 ciscXXXXXXXX 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 ciscXXXXXXXX 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 ciscXXXXXXXX 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 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

**Answer:** D

**NEW QUESTION 203**
- (Exam Topic 1)
An engineer needs a solution for TACACS+ authentication and authorization for device administration. The engineer also wants to enhance wired and wireless network security by requiring users and endpoints to use 802.1X, MAB, or WebAuth. Which product meets all of these requirements?

A. Cisco Prime Infrastructure
B. Cisco Identity Services Engine
C. Cisco Stealthwatch
D. Cisco AMP for Endpoints

**Answer:** B

**NEW QUESTION 205**
- (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 209**
- (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 212**
- (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 213**
- (Exam Topic 1)
Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

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

**Answer:** D

**NEW QUESTION 218**
- (Exam Topic 1)
Which IPS engine detects ARP spoofing?

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

**Answer:** A

**NEW QUESTION 223**
- (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. dotlx reauthentication
C. cisp enable
D. dot1x pae authenticator

**Answer:** D

**NEW QUESTION 225**
- (Exam Topic 1)
Under which two circumstances is a CoA issued? (Choose two)

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

**Answer:** BD

**Explanation:**
The profiling service issues the change of authorization in the following cases:– Endpoint deleted—When an endpoint is deleted from the Endpoints page and the endpoint is disconnectedor removed from the network.An exception action is configured—If you have an exception action configured per profile that leads to anunusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to thecorresponding static profile by issuing a CoA.– An endpoint is profiled for the first time—When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.+ An endpoint identity group has changed—When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide

**NEW QUESTION 229**
- (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

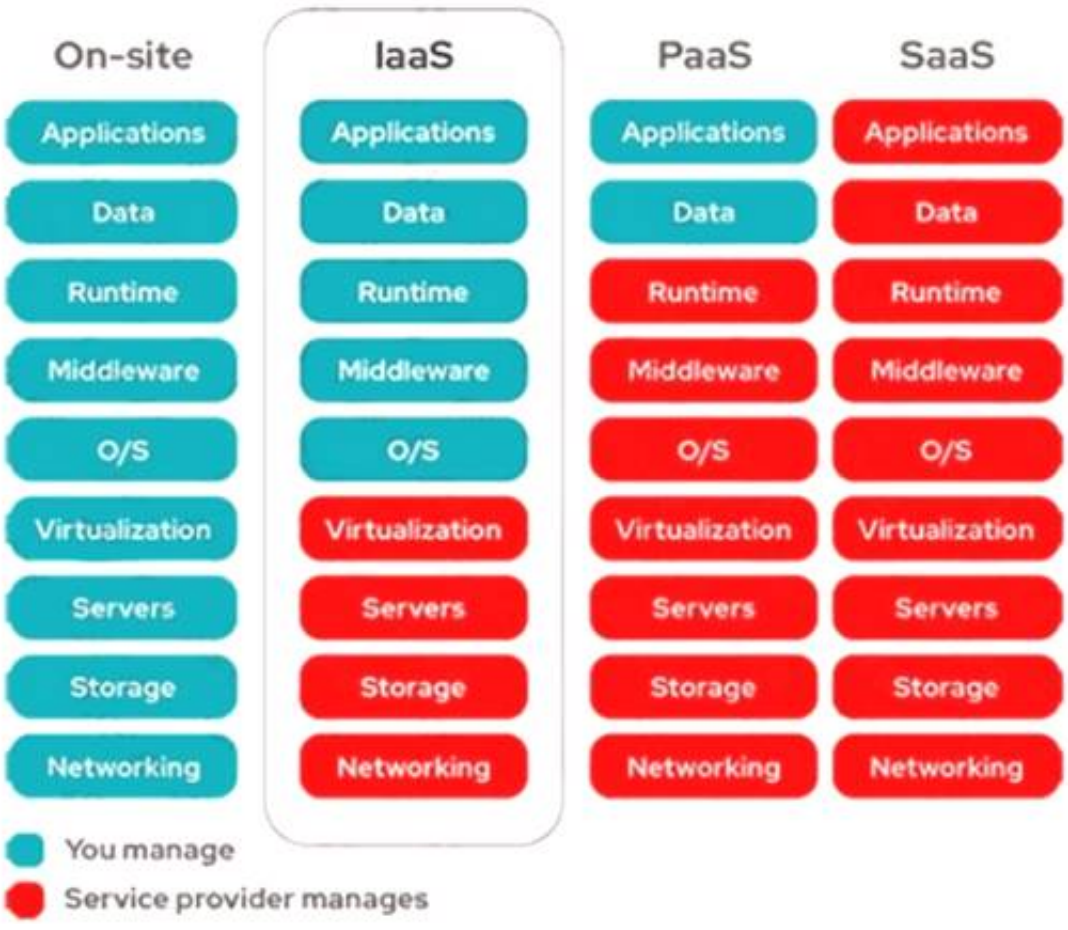
**Explanation:**
Reference: https://docs.umbrella.com/deployment-umbrella/docs/manage-logs

**NEW QUESTION 231**
- (Exam Topic 1)
In which cloud services model is the tenant responsible for virtual machine OS patching?

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

**Answer:** A

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




**NEW QUESTION 235**
- (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 236**
- (Exam Topic 1)
How is ICMP used an exfiltration technique?

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

**Answer:** C

**NEW QUESTION 239**
- (Exam Topic 1)
Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and
prioritize application traffic?

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

**Answer:** B

**Explanation:**

Reference:
https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/guide/avc-user-guide/avc_tech_overview.html

**NEW QUESTION 240**
- (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 244**
- (Exam Topic 1)
What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?

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

**Answer:** A

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

**NEW QUESTION 245**
- (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 250**
- (Exam Topic 1)
Which type of attack is social engineering?

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

**Answer:** B

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

**NEW QUESTION 252**
- (Exam Topic 1)
What is the function of Cisco Cloudlock for data security?

A. data loss prevention
B. controls malicious cloud apps
C. detects anomalies
D. user and entity behavior analytics

**Answer:** A

**NEW QUESTION 256**
- (Exam Topic 1)
Which two capabilities does TAXII support? (Choose two)

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

**Answer:** AB

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

**NEW QUESTION 261**
- (Exam Topic 1)
An engineer is trying to securely connect to a router and wants to prevent insecure algorithms from being used. However, the connection is failing. Which action should be taken to accomplish this goal?

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

**Answer:** D

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

**NEW QUESTION 266**
- (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 packetsafter a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automaticallytakes over the tasks of the active (primary) router if the active router loses connectivity for any reason. Thisfailover 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 eitherthe primary or secondary device. Both routers should be the same type of device, have the same CPU andmemory, and have either no encryption accelerator or identical encryption accelerators.Prerequisites for Stateful Failover for IPsec
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpnavailability-15- the prerequisites only stated that “Both routers should be the same type of device” but in the“Restrictions for Stateful Failover for IPsec” section of the link above, it requires “Both the active and standby devices must run the identical version of the Cisco IOS software” so answer E is better than answer B.

**NEW QUESTION 267**
- (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 270**
- (Exam Topic 1)
Which feature requires a network discovery policy on the Cisco Firepower Next Generation Intrusion Prevention System?

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

**Answer:** B

**NEW QUESTION 273**
- (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 277**
- (Exam Topic 1)
Which form of attack is launched using botnets?

A. EIDDOS
B. virus
C. DDOS
D. TCP flood

**Answer:** C

**Explanation:**
A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them.Cyber criminals use botnets to instigate botnet attacks, which include malicious activities such as credentialsleaks, unauthorized access, data theft and DDoS attacks.

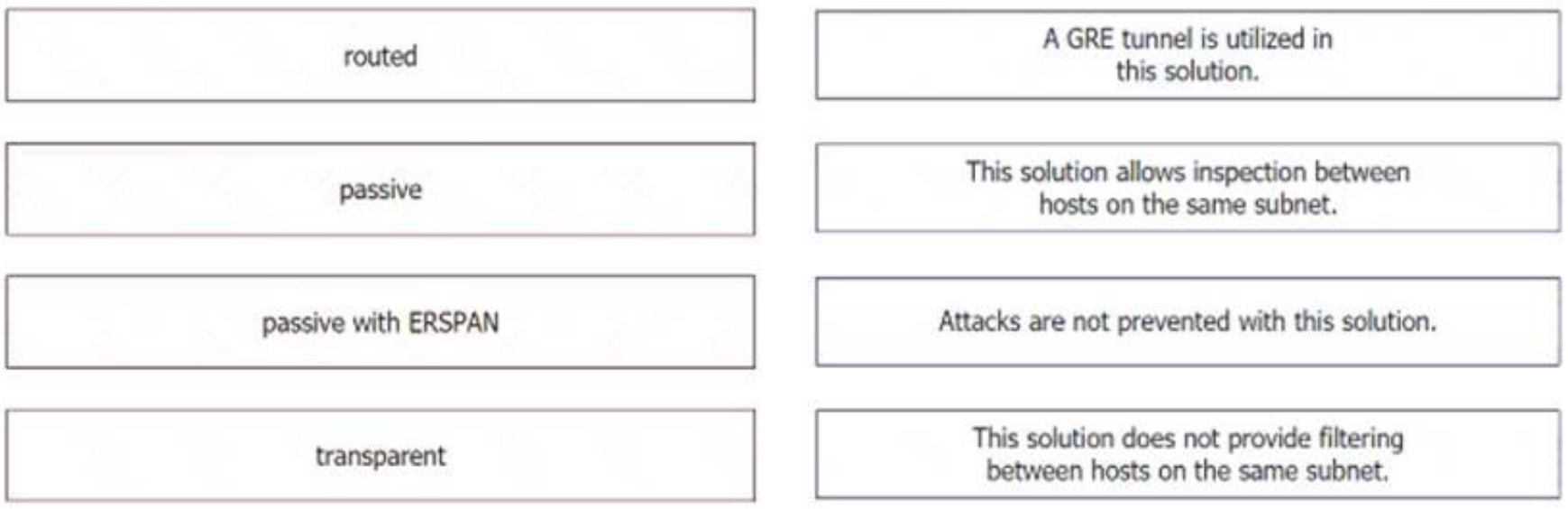
**NEW QUESTION 279**
- (Exam Topic 1)
Where are individual sites specified to be blacklisted in Cisco Umbrella?

A. application settings
B. content categories
C. security settings
D. destination lists

**Answer:** D

**Explanation:**
Reference: https://docs.umbrella.com/deployment-umbrella/docs/working-with-destination-lists

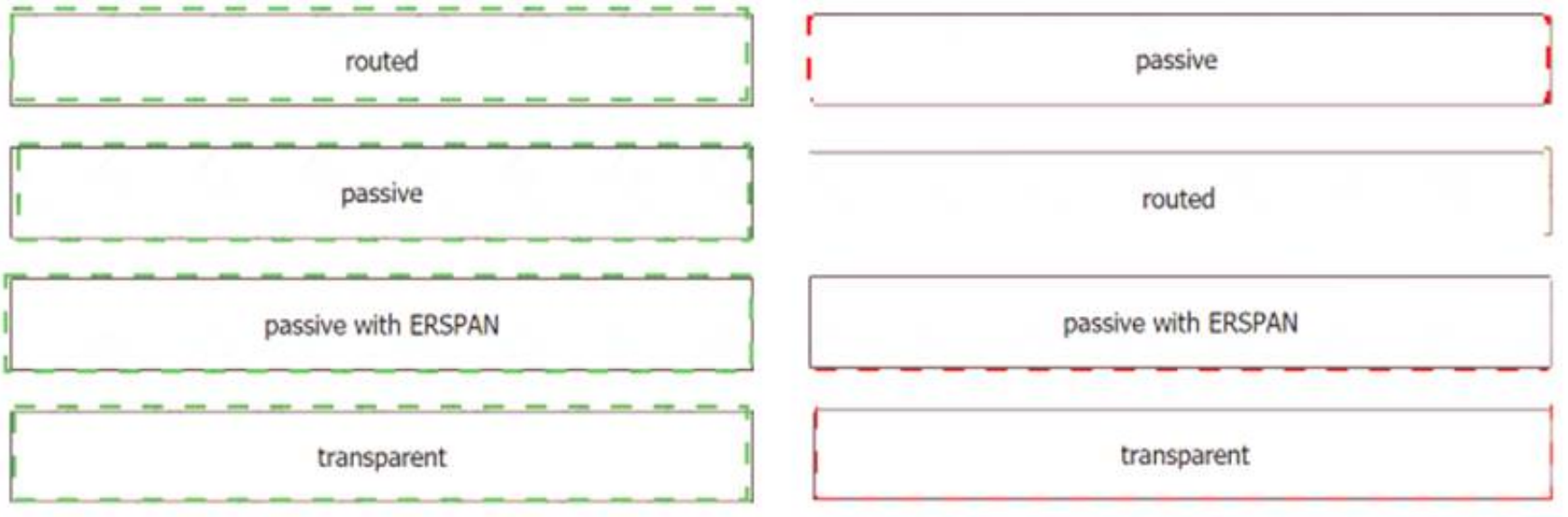
**NEW QUESTION 283**
- (Exam Topic 3)
Drag and drop the deployment models from the left onto the explanations on the right.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 286**
- (Exam Topic 3)
An engineer recently completed the system setup on a Cisco WSA Which URL information does the system send to SensorBase Network servers?

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

**Answer:** B

**NEW QUESTION 289**
- (Exam Topic 3)
Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)

A. It must include the current date.
B. It must reside in the trusted store of the WSA.
C. It must reside in the trusted store of the endpoint.
D. It must have been signed by an internal CA.
E. it must contain a SAN.

**Answer:** AB

**NEW QUESTION 290**
- (Exam Topic 3)
Which characteristic is unique to a Cisco WSAv as compared to a physical appliance?

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

**Answer:** A

**NEW QUESTION 291**
- (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 294**
- (Exam Topic 3)
What are two benefits of using an MDM solution? (Choose two.)

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

**Answer:** AE

**NEW QUESTION 297**
- (Exam Topic 3)
How does Cisco Workload Optimization Manager help mitigate application performance issues?

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

**Answer:** B

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

**NEW QUESTION 299**
- (Exam Topic 3)
Which algorithm is an NGE hash function?

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

**Answer:** D

**NEW QUESTION 303**
- (Exam Topic 3)
An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users. Which action accomplishes this goal?

A. Restrict access to only websites with trusted third-party signed certificates.
B. Modify the user's browser settings to suppress errors from Cisco Umbrella.
C. Upload the organization root CA to Cisco Umbrella.
D. Install the Cisco Umbrella root CA onto the user's device.

**Answer:** D

**NEW QUESTION 304**
- (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_MESG_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 306**
- (Exam Topic 3)
An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1 1 11 using the flow record Stea!thwatch406397954 command Which additional command is required to complete the flow record?

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

**Answer:** B

**NEW QUESTION 307**
- (Exam Topic 3)
Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

What does the API key do while working with https://api.amp.cisco.com/v1/computers?

A. displays client ID
B. HTTP authorization
C. Imports requests
D. HTTP authentication

**Answer:** D

**NEW QUESTION 311**
- (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 314**
- (Exam Topic 3)
An engineer is configuring Cisco Umbrella and has an identity that references two different policies. Which action ensures that the policy that the identity must use takes precedence over the second one?

A. Configure the default policy to redirect the requests to the correct policy
B. Place the policy with the most-specific configuration last in the policy order
C. Configure only the policy with the most recently changed timestamp
D. Make the correct policy first in the policy order

**Answer:** D

**NEW QUESTION 316**
- (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 317**
- (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

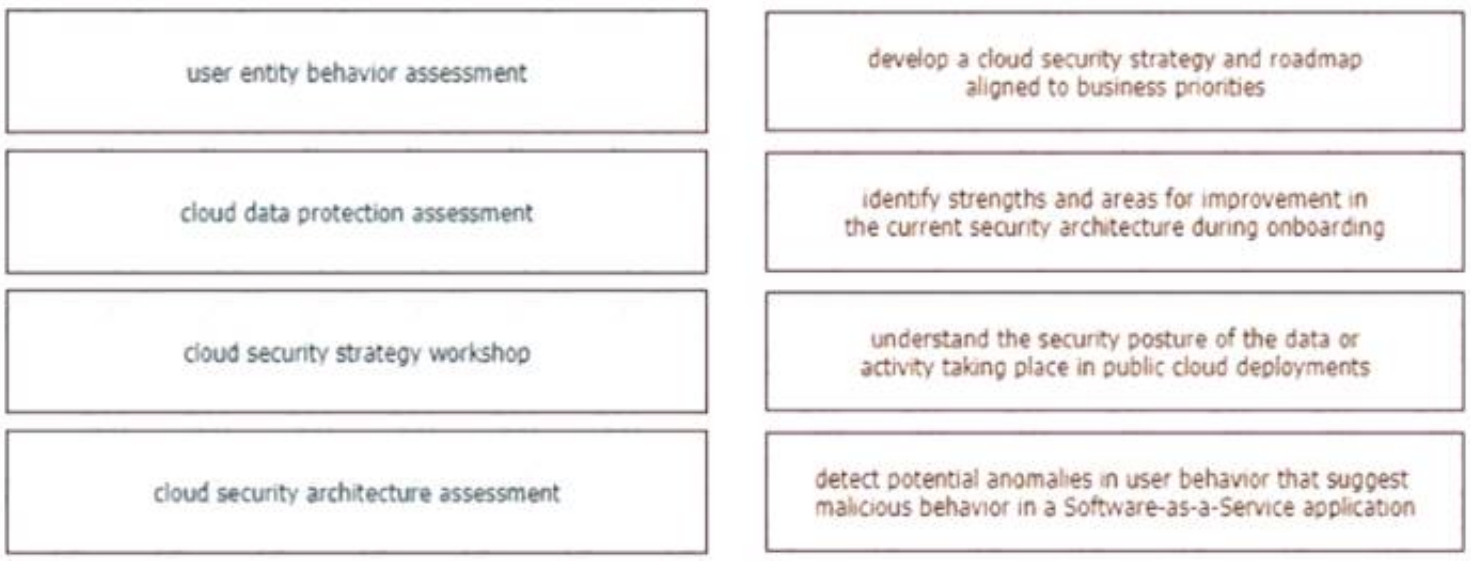
**NEW QUESTION 318**
- (Exam Topic 3)
An engineer has been tasked with configuring a Cisco FTD to analyze protocol fields and detect anomalies in the traffic from industrial systems. What must be done to meet these requirements?

A. Implement pre-filter policies for the CIP preprocessor
B. Enable traffic analysis in the Cisco FTD
C. Configure intrusion rules for the DNP3 preprocessor
D. Modify the access control policy to trust the industrial traffic

**Answer:** C

**Explanation:**
"configure INTRUSION RULES for DNP3" -> Documentation states, that enabling INTRUSION RULES is mandatory for CIP to work + required preprocessors (in Network Access Policy - NAP) will be enabled automatically:
"If you want the CIP preprocessor rules listed in the following table to generate events, you MUST enable them. See Setting Intrusion Rule States for information on enabling rules."
"If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings, although the preprocessor remains disabled in the web interface for the corresponding network analysis policy."
[1]
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada

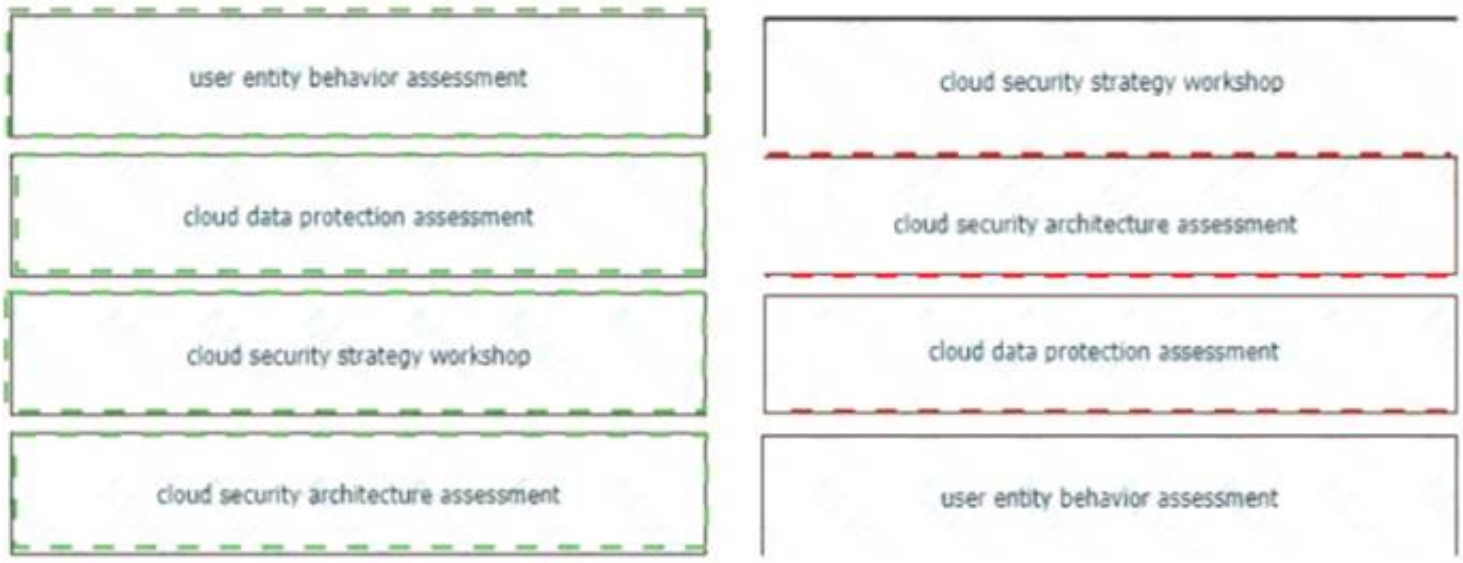
**NEW QUESTION 321**
- (Exam Topic 3)
Drag and drop the cloud security assessment components from the left onto the definitions on the right.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 322**
- (Exam Topic 3)
Refer to the exhibit.

```
interface GigabitEthernet1/0/18
switchport access vlan 41
switchport mode access
switchport voice vlan 44
device-tracking attach-policy IPDT_MAX_10
authentication periodic
authentication timer reauthenticate server
access-session host-mode multi-domain
access-session port-control auto
dot1x pae authenticator
dot1x timeout tx-period 7
dot1x max-reauth-req 3
spanning-tree portfast
```

Refer to the exhibit. A Cisco ISE administrator adds a new switch to an 802.1X deployment and has difficulty with some endpoints gaining access.
Most PCs and IP phones can connect and authenticate using their machine certificate credentials. However printer and video cameras cannot base d on the interface configuration provided, what must be to get these devices on to the network using Cisco ISE for authentication and authorization while maintaining security controls?

A. Change the default policy in Cisco ISE to allow all devices not using machine authentication .
B. Enable insecure protocols within Cisco ISE in the allowed protocols configuration.
C. Configure authentication event fail retry 2 action authorize vlan 41 on the interface
D. Add mab to the interface configuration.

**Answer:** D

**NEW QUESTION 324**
- (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 326**
- (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 329**
- (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 334**
- (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 338**
- (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

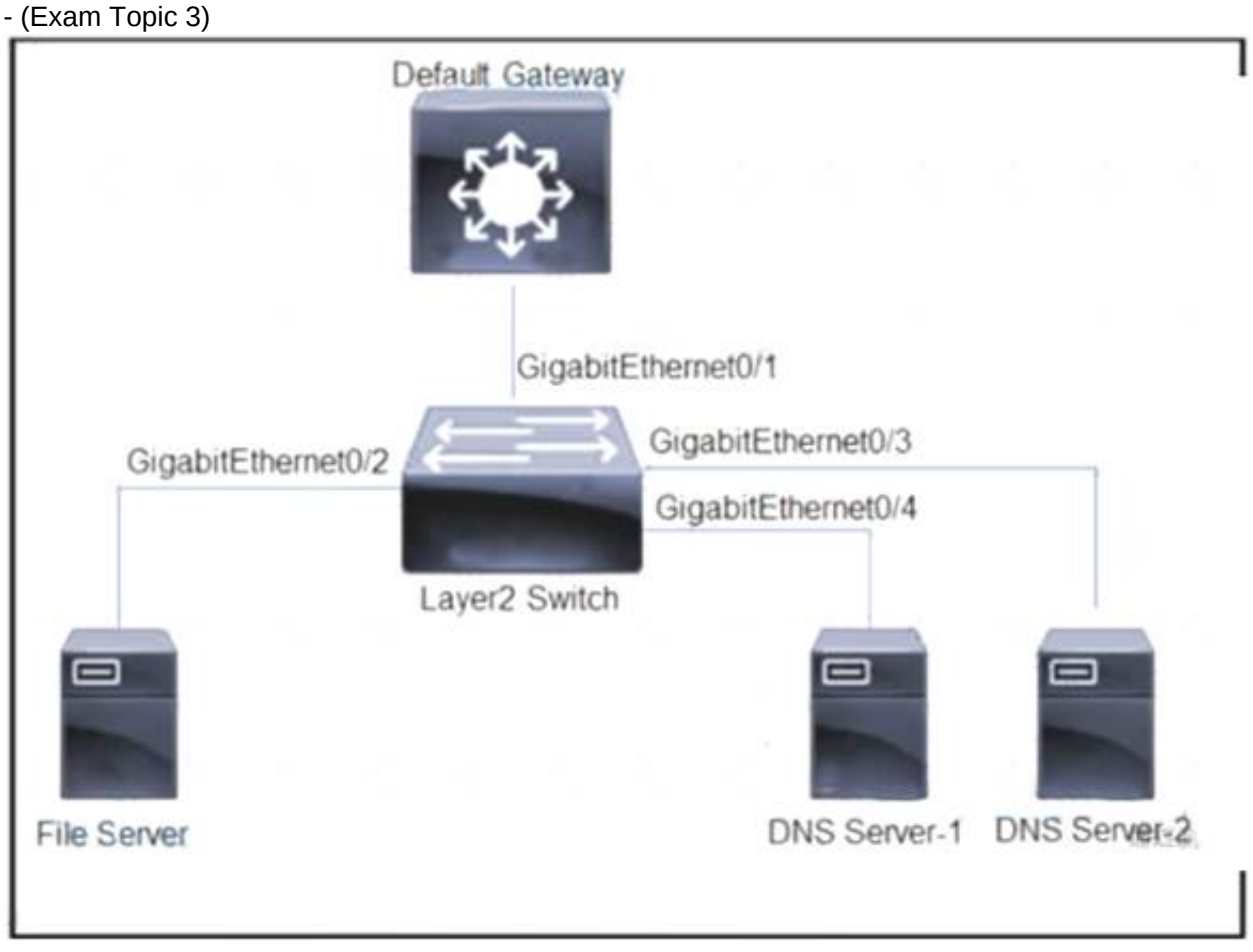
**Answer:** B

**NEW QUESTION 341**
- (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 345**
- (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 347**
- (Exam Topic 3)
Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks? (Choose two.)

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

**Answer:** CE

**NEW QUESTION 352**
- (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 354**
- (Exam Topic 3)
An organization wants to implement a cloud-delivered and SaaS-based solution to provide visibility and threat detection across the AWS network. The solution must be deployed without software agents and rely on AWS VPC flow logs instead. Which solution meets these requirements?

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

**Answer:** A

**NEW QUESTION 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:**


**NEW QUESTION 360**
- (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 363**
- (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 364**
- (Exam Topic 3)
A hacker initiated a social engineering attack and stole username and passwords of some users within a company. Which product should be used as a solution to this problem?

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

**Answer:** D

**NEW QUESTION 366**
- (Exam Topic 3)
Which statement describes a serverless application?

A. The application delivery controller in front of the server farm designates on which server the application runs each time.
B. The application runs from an ephemeral, event-triggered, and stateless container that is fully managed by a cloud provider.
C. The application is installed on network equipment and not on physical servers.
D. The application runs from a containerized environment that is managed by Kubernetes or Docker Swarm.

**Answer:** B

**NEW QUESTION 369**
- (Exam Topic 3)
An engineer needs to configure a Cisco Secure Email Gateway (SEG) to prompt users to enter multiple forms of identification before gaining access to the SEG. The SEG must also join a cluster using the preshared key of cisc421555367. What steps must be taken to support this?

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

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

**Answer:** C

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

**NEW QUESTION 373**
- (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 378**
- (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 381**
- (Exam Topic 3)
A network engineer must migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vMotion. What is a requirement for both physical hosts?

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

**Answer:** C

**NEW QUESTION 386**
- (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 391**
- (Exam Topic 3)
Which solution supports high availability in routed or transparent mode as well as in northbound and southbound deployments?

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

**Answer:** B

**NEW QUESTION 396**
- (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 399**
- (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 404**
- (Exam Topic 3)
Which two actions does the Cisco Identity Services Engine posture module provide that ensures endpoint security? (Choose two.)

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

**Answer:** AD

**NEW QUESTION 405**
- (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 407**
- (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 410**
- (Exam Topic 3)
What is the concept of CI/CD pipelining?

A. The project is split into several phases where one phase cannot start before the previous phase finishes successfully.
B. The project code is centrally maintained and each code change should trigger an automated build and test sequence
C. The project is split into time-limited cycles and focuses on pair programming for continuous code review
D. Each project phase is independent from other phases to maintain adaptiveness and continual improvement

**Answer:** A

**NEW QUESTION 411**
- (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 413**
- (Exam Topic 3)
A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https://<FMC IP>/capure/CAPI/pcap/test.pcap, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

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

**Answer:** D

**NEW QUESTION 415**
- (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 420**
- (Exam Topic 3)
A network engineer entered the snmp-server user asmith myv7 auth sha cisco priv aes 256 cisc0xxxxxxxxx command and needs to send SNMP information to a host at 10.255.255.1. Which
command achieves this goal?

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

**Answer:** C

**NEW QUESTION 423**
- (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 425**
- (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 427**
- (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 429**
- (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 ASAdoes 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 432**
- (Exam Topic 3)
An engineer is configuring IPsec VPN and needs an authentication protocol that is reliable and supports ACK and sequence. Which protocol accomplishes this goal?

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

**Answer:** D

**NEW QUESTION 437**
- (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 [redacted]  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 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

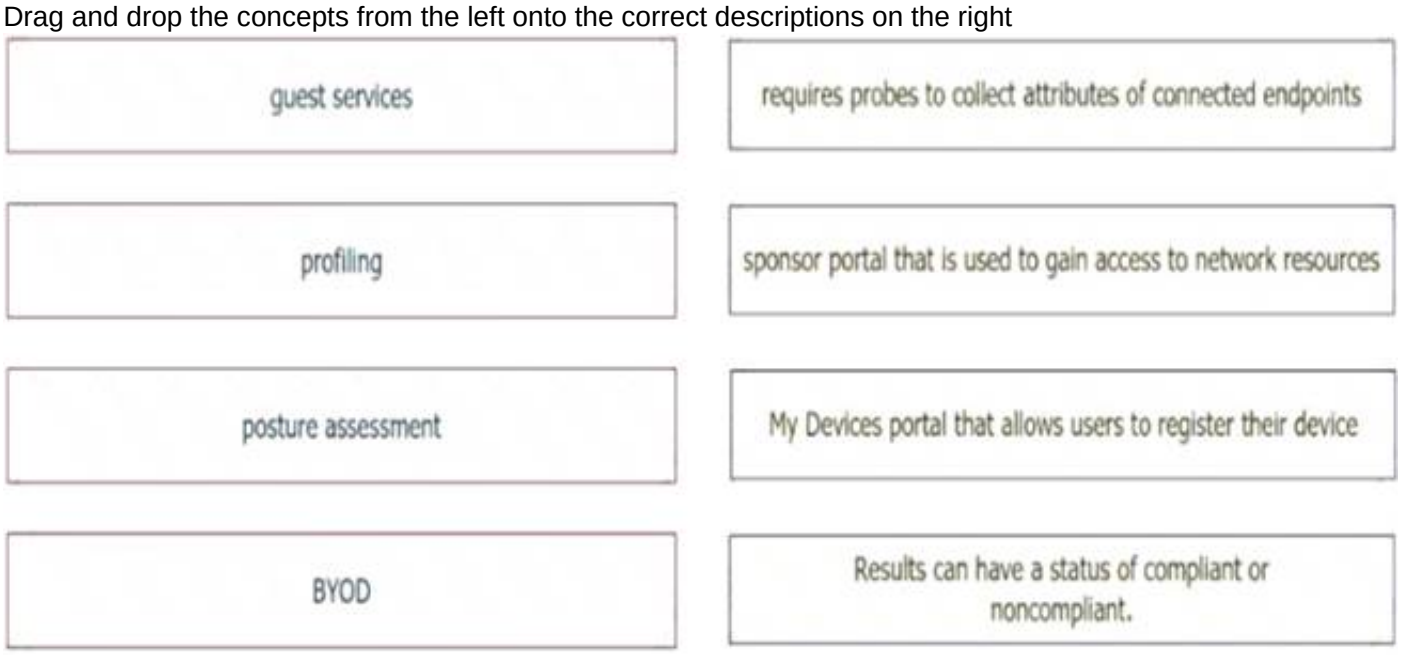
**NEW QUESTION 447**
- (Exam Topic 3)
An engineer needs to detect and quarantine a file named abc424400664 zip based on the MD5 signature of the file using the Outbreak Control list feature within Cisco Advanced Malware Protection (AMP) for Endpoints The configured detection method must work on files of unknown disposition Which Outbreak Control list must be configured to provide this?

A. Blocked Application

B. Simple Custom Detection
C. Advanced Custom Detection
D. Android Custom Detection

**Answer:** C

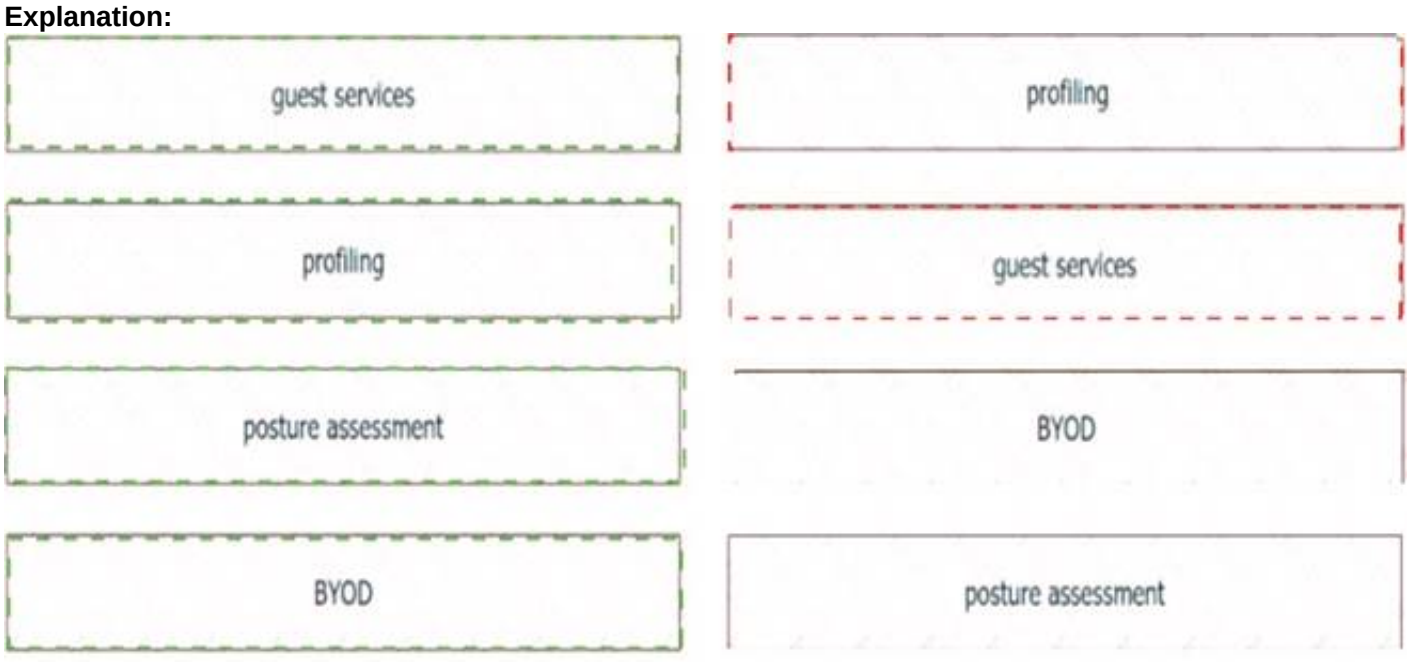
**NEW QUESTION 451**
- (Exam Topic 3)
Drag and drop the concepts from the left onto the correct descriptions on the right




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 453**
- (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 458**
- (Exam Topic 3)
What are two benefits of using Cisco Duo as an MFA solution? (Choose two.)

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

**Answer:** BC

**NEW QUESTION 463**

- (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 468**
- (Exam Topic 3)
How is data sent out to the attacker during a DNS tunneling attack?

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

**Answer:** A

**NEW QUESTION 469**
- (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 474**
- (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 479**
- (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 481**
- (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

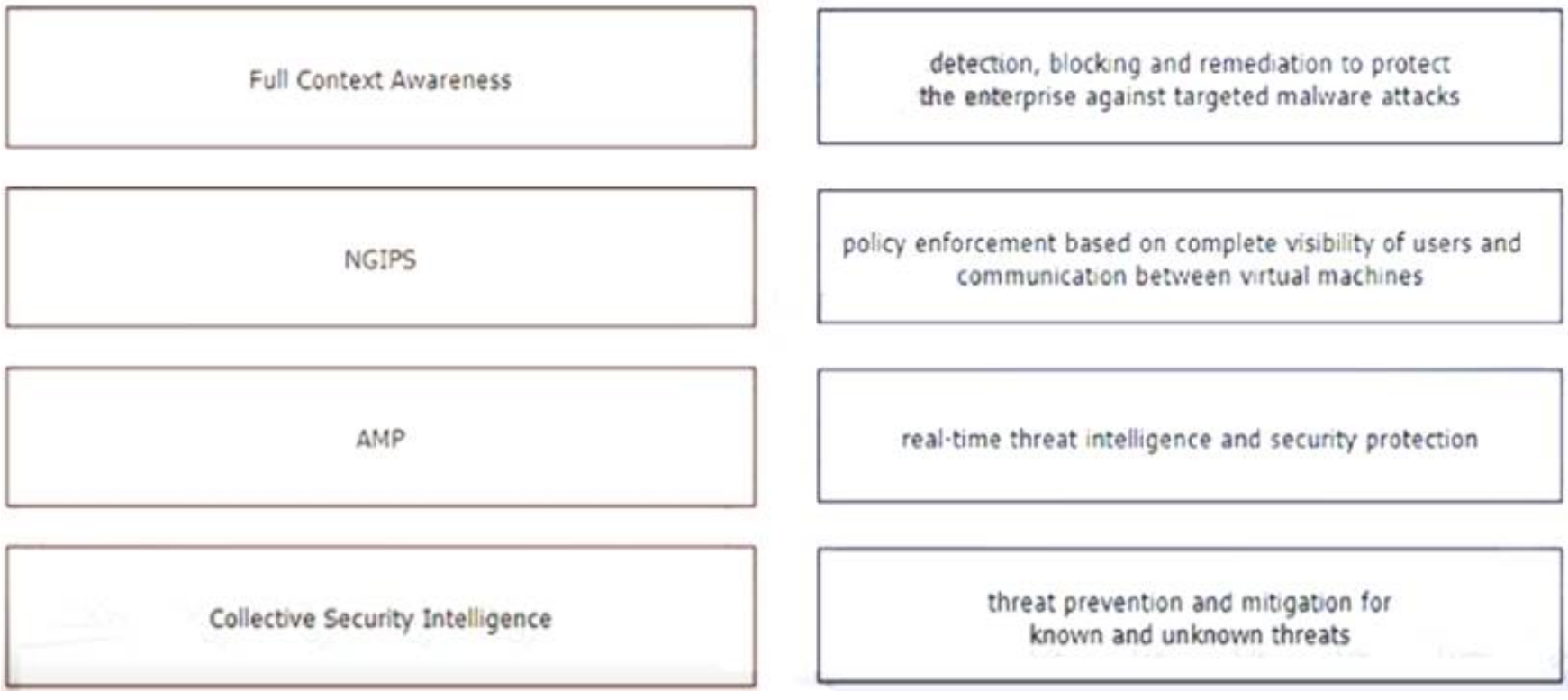
**Answer:** B

**NEW QUESTION 484**
- (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 487**
- (Exam Topic 3)
Drag and drop the features of Cisco ASA with Firepower from the left onto the benefits on the right.




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 491**
- (Exam Topic 3)
Which type of attack is MFA an effective deterrent for?

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

**Answer:** B

**NEW QUESTION 492**
- (Exam Topic 3)
An engineer must configure Cisco AMP for Endpoints so that it contains a list of files that should not be executed by users. These files must not be quarantined.
Which action meets this configuration requirement?

A. Identity the network IPs and place them in a blocked list.
B. Modify the advanced custom detection list to include these files.
C. Create an application control blocked applications list.
D. Add a list for simple custom detection.

**Answer:** C

**NEW QUESTION 495**
- (Exam Topic 3)
Which two commands are required when configuring a flow-export action on a Cisco ASA? (Choose two.)

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

**Answer:** AB

**NEW QUESTION 498**
- (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 502**
- (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 !P addresses to a host interface.
D. Enable flagged message handling

**Answer:** D

**NEW QUESTION 505**
- (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 507**
- (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

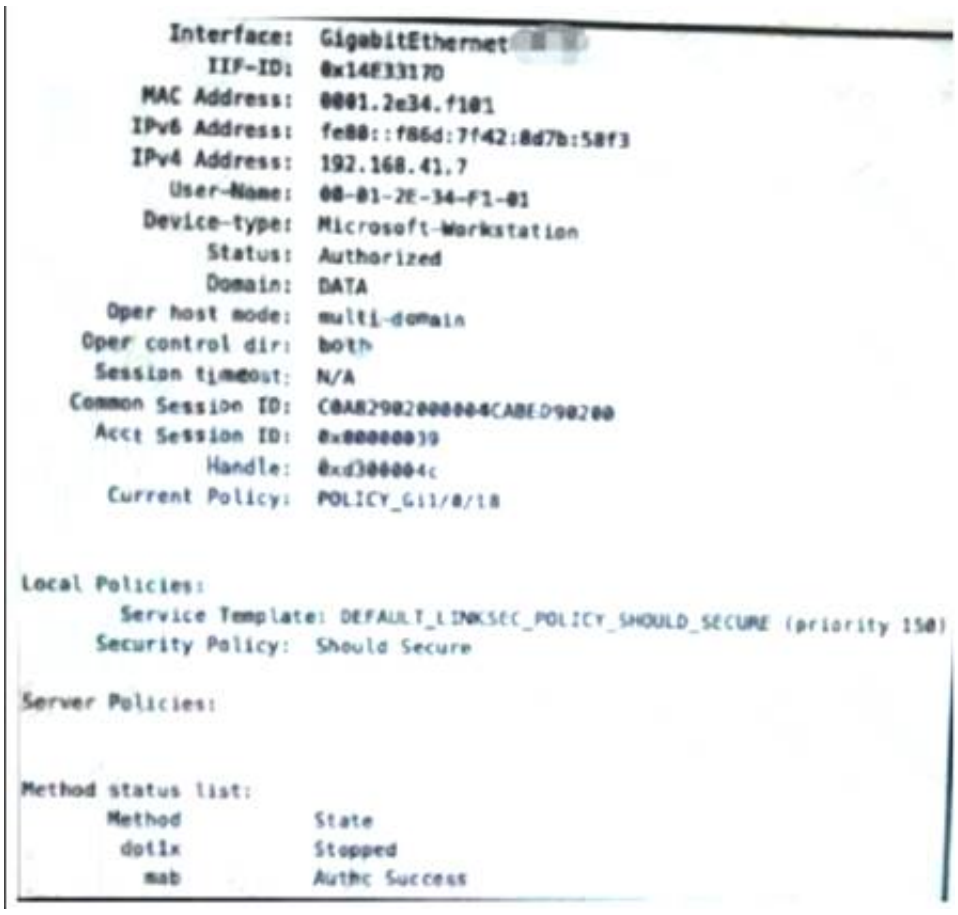
**Answer:** D

**NEW QUESTION 510**
- (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 511**
- (Exam Topic 3)
Refer to the exhibit.




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

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

**Answer:** C

**NEW QUESTION 514**
- (Exam Topic 3)
Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

A. OpenC2
B. OpenlOC
C. CybOX
D. STIX

**Answer:** D

**NEW QUESTION 517**
- (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 519**
- (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-lP 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 521**
- (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 526**
- (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 530**
- (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 532**
- (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 534**
- (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. lf 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 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)
Which security solution protects users leveraging DNS-layer security?

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

**Answer:** C

**NEW QUESTION 544**
- (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 toredirect 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 546**
- (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 me 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

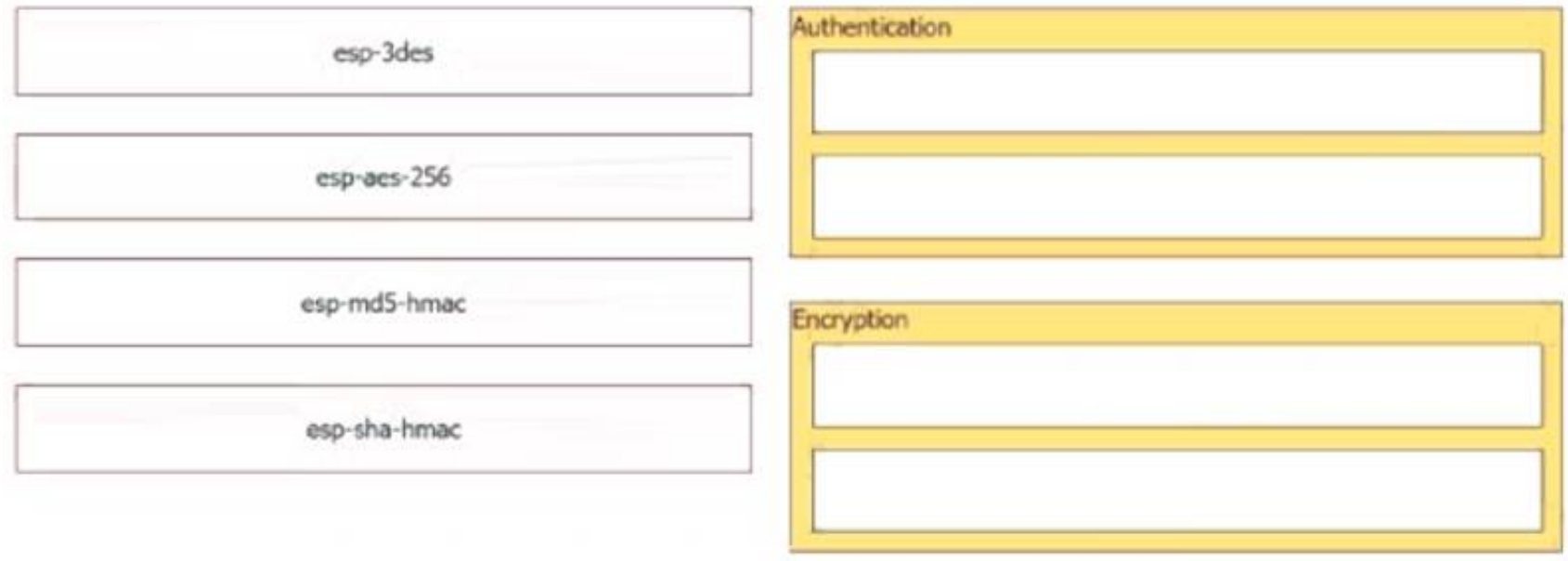
**Answer:** C

**NEW QUESTION 547**
- (Exam Topic 3)
Which feature does the laaS model provide?

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

**Answer:** C

**NEW QUESTION 550**
- (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 553**
- (Exam Topic 3)
A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to
ensure that bandwidth is available for VPN users needing access to corporate resources on the10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the
network?

A. Use split tunneling to tunnel traffic for the 10.0.0.0/24 network only.

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

**Answer:** A

**NEW QUESTION 555**
- (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 557**
- (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 562**
- (Exam Topic 3)
What is a function of the Layer 4 Traffic Monitor on a Cisco WSA?

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

**Answer:** C

**NEW QUESTION 563**
- (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 565**
- (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 566**
- (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 570**
- (Exam Topic 3)
What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?

A. Telemetry uses a pull mehod, which makes it more reliable than SNMP
B. Telemetry uses push and pull, which makes it more scalable than SNMP
C. Telemetry uses push and pull which makes it more secure than SNMP
D. Telemetry uses a push method which makes it faster than SNMP

**Answer:** D

**Explanation:**
SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts.The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data.Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc.Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics.
Referfence: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming telemetry

**NEW QUESTION 575**
- (Exam Topic 3)
What is a characteristic of an EDR solution and not of an EPP solution?

A. stops all ransomware attacks
B. retrospective analysis

C. decrypts SSL traffic for better visibility
D. performs signature-based detection

**Answer:** B

**NEW QUESTION 576**
- (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 580**
- (Exam Topic 3)
Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using higher-level protocols without readdressing the network?

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

**Answer:** B

**NEW QUESTION 585**
- (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 590**
- (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 594**
- (Exam Topic 3)
What is the benefit of integrating Cisco ISE with a MDM solution?

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

**Answer:** A

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

**NEW QUESTION 597**
- (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 602**
- (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 603**
- (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 606**
- (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 607**
- (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 610**
- (Exam Topic 3)
Why should organizations migrate to a multifactor authentication strategy?

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

**Answer:** D

**NEW QUESTION 613**
- (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 618**
- (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 623**
- (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 626**
- (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 630**
- (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 631**
- (Exam Topic 3)
What are two functions of IKEv1 but not IKEv2? (Choose two)

A. NAT-T is supported in IKEv1 but rot 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 633**
- (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)
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 638**
- (Exam Topic 3)
Which solution detects threats across a private network, public clouds, and encrypted traffic?

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

**Answer:** A

**NEW QUESTION 643**
- (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 646**
- (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 650**
- (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 655**
- (Exam Topic 3)
Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?

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

**Answer:** C

**NEW QUESTION 656**
- (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 660**
- (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 661**
- (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 663**
- (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 665**
- (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

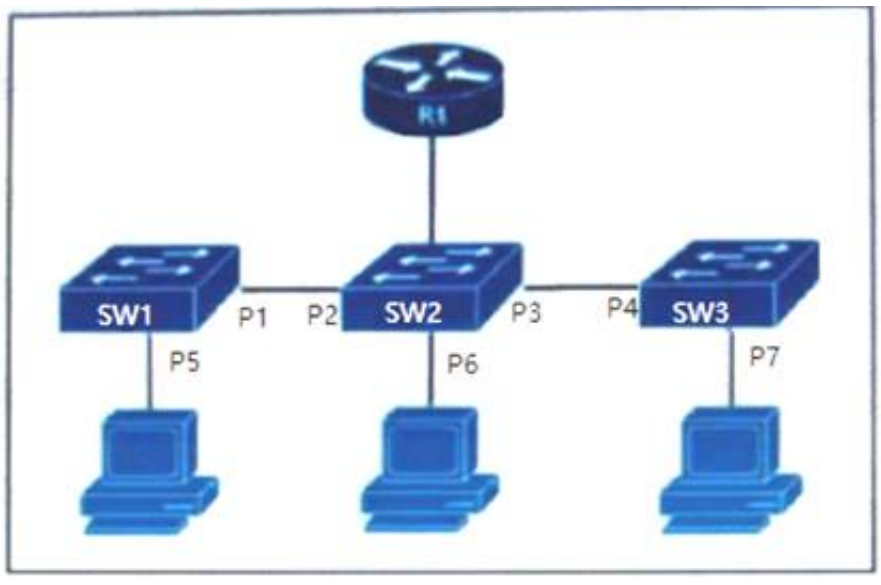
**NEW QUESTION 668**
- (Exam Topic 3)
What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.) The eDirectory client must be installed on each client workstation.

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

**Answer:** AB

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

**NEW QUESTION 671**
- (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 674**
- (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 675**
- (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 677**
- (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 681**
- (Exam Topic 3)
Which two actions does the Cisco identity Services Engine posture module provide that ensures endpoint security?(Choose two.)

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

**Answer:** AD

**NEW QUESTION 684**

.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons 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 FirstTry

* 350-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year