



**Cisco**

## **Exam Questions 350-701**

Implementing and Operating Cisco Security Core Technologies

### NEW QUESTION 1

- (Exam Topic 2)

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

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

**Answer: B**

### NEW QUESTION 2

- (Exam Topic 2)

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

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

**Answer: D**

#### Explanation:

Reference:

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

### NEW QUESTION 3

- (Exam Topic 2)

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

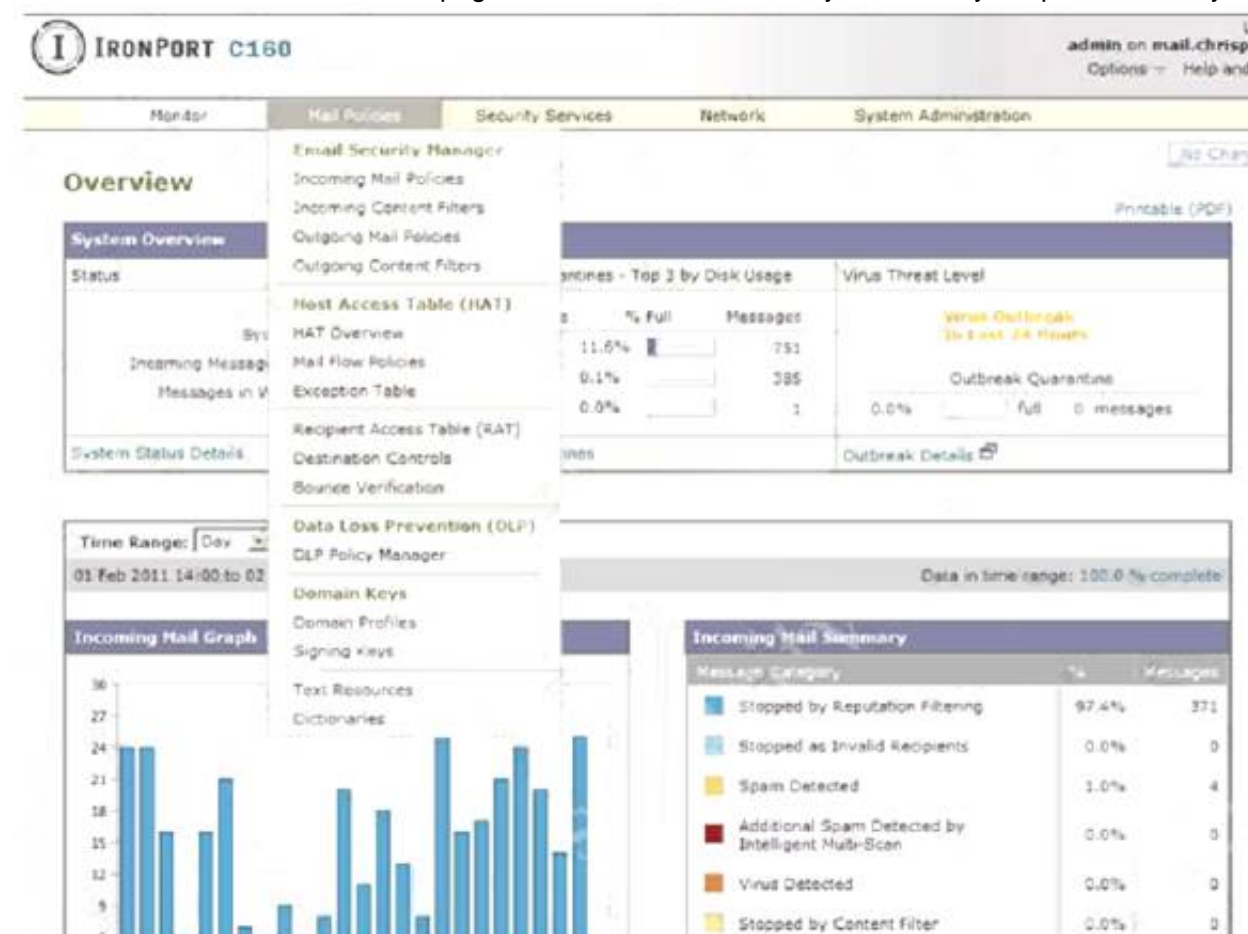
What must be configured to accomplish this?

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

**Answer: D**

#### Explanation:

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



### NEW QUESTION 4

- (Exam Topic 2)

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

- A. Ethos Engine to perform fuzzy fingerprinting
- B. Tetra Engine to detect malware when the endpoint is connected to the cloud

- C. Clam AV Engine to perform email scanning
- D. Spero Engine with machine learning to perform dynamic analysis

**Answer:** A

**Explanation:**

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

**NEW QUESTION 5**

- (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 6**

- (Exam Topic 2)

What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?

- A. Cisco Cloudlock
- B. Cisco Umbrella
- C. Cisco AMP
- D. Cisco App Dynamics

**Answer:** A

**Explanation:**

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

**NEW QUESTION 7**

- (Exam Topic 2)

What is managed by Cisco Security Manager?

- A. access point
- B. WSA
- C. ASA
- D. ESA

**Answer:** C

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/products/security/security-manager/index.html>

**NEW QUESTION 8**

- (Exam Topic 2)

What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group?

- A. posture assessment
- B. CoA
- C. external identity source
- D. SNMP probe

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 9**

- (Exam Topic 2)

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

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

**Answer:** D

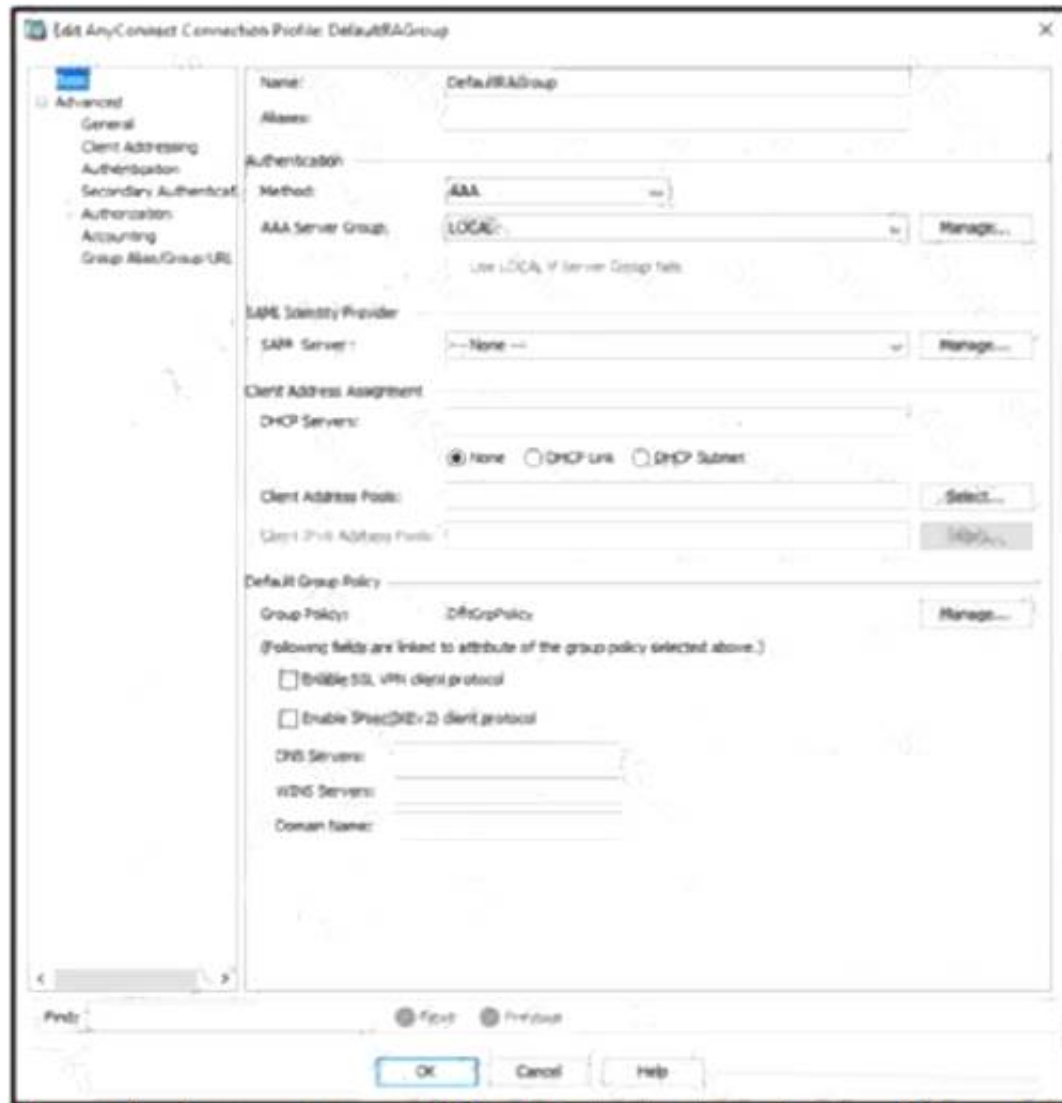
#### Explanation:

Reference: <https://docs.umbrella.com/cloudlock-documentation/docs/endpoints>Note: + Security information and event management (SIEM) platforms collect log and event data from 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 10

- (Exam Topic 2)

Refer to the exhibit.



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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 10

- (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 15

- (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 20

- (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 24

- (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 26

- (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 30

- (Exam Topic 1)

An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the endpoint to apply a new or updated policy from ISE. Which CoA type achieves this goal?

- A. Port Bounce
- B. CoA Terminate
- C. CoA Reauth
- D. CoA Session Query

**Answer:** C

#### NEW QUESTION 33

- (Exam Topic 1)

Refer to the exhibit.



```
Sysauthcontrol      Enabled
Dot1x Protocol Version      3

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

Which command was used to display this output?

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

**Answer:** A

#### NEW QUESTION 36

- (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 39

- (Exam Topic 1)

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

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

**Answer:** BD

#### NEW QUESTION 42

- (Exam Topic 1)

What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?

- A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
- B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
- C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
- D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX

**Answer:** C

#### Explanation:

Configure a Crypto ISAKMP Key

In order to configure a preshared

configuration mode:

authentication key, enter the crypto isakmp key

command in global

crypto isakmp key cisco123 address 172.16.1.1

<https://community.cisco.com/t5/vpn/isakmp-with-0-0-0-0-dmvpn/td-p/4312380>

It is a bad practice but it is valid. 172.16.0.0/16 the full range will be accepted as possible PEER

<https://www.examttopics.com/discussions/cisco/view/46191-exam-350-701-topic-1-question-71-discussion/#:~:t> Testing without a netmask shows that command interpretation has a preference for /16 and /24.  
CSR-1(config)#crypto isakmp key cisco123 address 172.16.0.0  
CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.0.0 [255.255.0.0] cisco123  
CSR-1(config)#no crypto isakmp key cisco123 address 172.16.0.0 CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.0 CSR-1(config)#do show crypto isakmp key | i cisco  
default 172.16.1.0 [255.255.255.0] cisco123  
CSR-1(config)#no crypto isakmp key cisco123 address 172.16.1.0 CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.128  
CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.1.128 cisco123 CSR-1(config)#

#### NEW QUESTION 47

- (Exam Topic 1)

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

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

**Answer:** AD

#### Explanation:

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

#### NEW QUESTION 51

- (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 IKEv2 implementations. 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 52

- (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 54

- (Exam Topic 1)

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

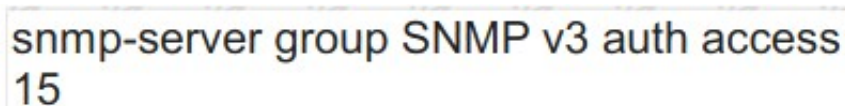
- A. Windows service
- B. computer identity
- C. user identity
- D. Windows firewall
- E. default browser

**Answer:** AD

#### NEW QUESTION 58

- (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 61**

- (Exam Topic 1)

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

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

**Answer:** C

**NEW QUESTION 62**

- (Exam Topic 1)

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

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

**Answer:** A

**NEW QUESTION 63**

- (Exam Topic 1)

Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?

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

**Answer:** C

**NEW QUESTION 64**

- (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 69**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**



Reference:

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

#### NEW QUESTION 74

- (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 75

- (Exam Topic 1)

When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

- A. Application Control
- B. Security Category Blocking
- C. Content Category Blocking
- D. File Analysis

**Answer:** B

#### NEW QUESTION 77

- (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 82

- (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 83

- (Exam Topic 1)

What provides visibility and awareness into what is currently occurring on the network?

- A. CMX
- B. WMI
- C. Prime Infrastructure
- D. Telemetry

**Answer:** D

#### Explanation:

Reference: [https://www.cisco.com/c/dam/en\\_us/about/doing\\_business/legal/service\\_descriptions/docs/activethreat-analytics](https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/activethreat-analytics)

#### NEW QUESTION 85

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 86

- (Exam Topic 1)

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

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

**Answer:** BC

#### NEW QUESTION 91

- (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 93

- (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 94

- (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 96

- (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 99

- (Exam Topic 1)

An engineer wants to automatically assign endpoints that have a specific OUI into a new endpoint group.

Which probe must be enabled for this type of profiling to work?

- A. NetFlow
- B. NMAP
- C. SNMP
- D. DHCP

**Answer:** B

#### Explanation:

Reference:  
<http://www.network-node.com/blog/2016/1/2/ise-20-profiling>

#### NEW QUESTION 102

- (Exam Topic 1)

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

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

**Answer:** BE

#### NEW QUESTION 106

- (Exam Topic 1)

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

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

**Answer:** AC

#### Explanation:

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

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

#### File Condition

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

Description **Cisco Predefined Check: Micro**

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

Compliance Module **Any version**

\* File Type **FileVersion**

\* File Path **SYSTEM\_32**

\* Operator **LaterThan**

\* File Version **10.0.10240.17318**

Cancel

#### NEW QUESTION 109

- (Exam Topic 1)

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

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

**Answer:** B

#### Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide/v60/> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload the whole 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 is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that

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

#### NEW QUESTION 113

- (Exam Topic 1)

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 114

- (Exam Topic 1)

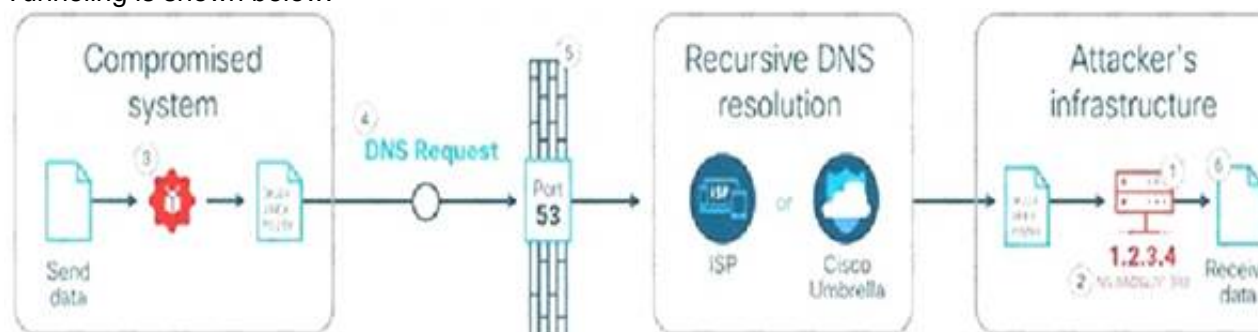
How is DNS tunneling used to exfiltrate data out of a corporate network?

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

**Answer: B**

#### Explanation:

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



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

#### NEW QUESTION 117

- (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 118

- (Exam Topic 1)

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

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

**Answer:** CE

**NEW QUESTION 120**

- (Exam Topic 1)

Which Cisco AMP file disposition valid?

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

**Answer:** B

**NEW QUESTION 124**

- (Exam Topic 1)

What is a characteristic of Firepower NGIPS inline deployment mode?

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

**Answer:** D

**NEW QUESTION 129**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 133**

- (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 137**

- (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 142**

- (Exam Topic 1)

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

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

**Answer:** A



**Explanation:**

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

**NEW QUESTION 143**

- (Exam Topic 1)

What is a characteristic of a bridge group in ASA Firewall transparent mode?

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

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 148**

- (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 151**

- (Exam Topic 1)

Refer to the exhibit.

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

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

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

**Answer:** D

**NEW QUESTION 155**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 159**

- (Exam Topic 1)

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

- A. A new authentication rule was added to the policy on the Policy Service node.
- B. An endpoint is deleted on the Identity Service Engine server.
- C. A new Identity Source Sequence is created and referenced in the authentication policy.

- D. An endpoint is profiled for the first time.
- E. A new Identity Service Engine server is added to the deployment with the Administration persona

**Answer:** BD

**Explanation:**

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

Reference:

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

**NEW QUESTION 163**

- (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 167**

- (Exam Topic 1)

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

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

**Answer:** BE

**Explanation:**

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

**NEW QUESTION 168**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 170**

- (Exam Topic 1)

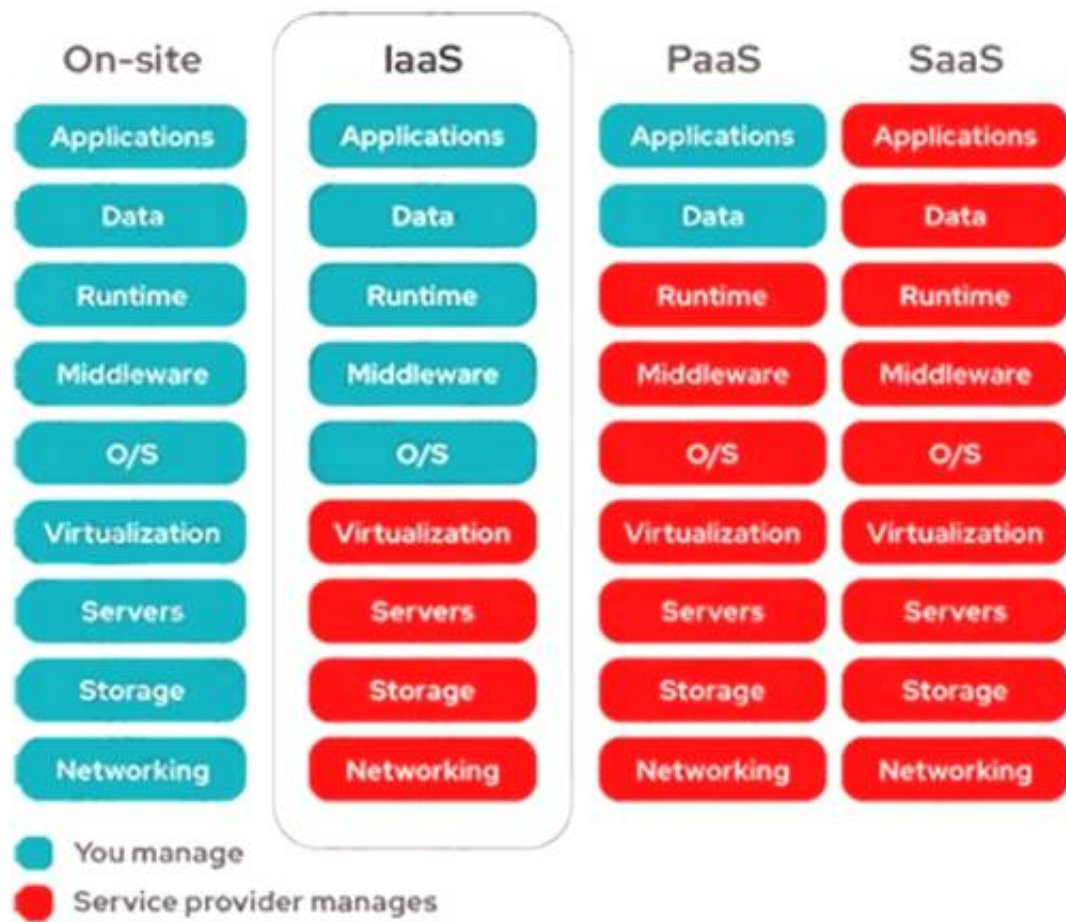
In which cloud services model is the tenant responsible for virtual machine OS patching?

- 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 173

- (Exam Topic 1)

Which command enables 802.1X globally on a Cisco switch?

- A. dot1x system-auth-control
- B. dot1x pae authenticator
- C. authentication port-control aut
- D. aaa new-model

**Answer:** A

#### NEW QUESTION 175

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 177

- (Exam Topic 1)

Which two are valid suppression types on a Cisco Next Generation Intrusion Prevention System? (Choose two)

- A. Port
- B. Rule
- C. Source
- D. Application
- E. Protocol

**Answer:** BC

#### NEW QUESTION 178

- (Exam Topic 1)

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

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

**Answer:** BD

#### Explanation:

Ping of Death (PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command. A correctly-formed ping packet is typically 56 bytes in size, or 64 bytes when the ICMP header is considered, and 84 including Internet Protocol version 4 header. However, any IPv4 packet (including pings) may be as large as 65,535 bytes. Some

computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented. Like other large but well-formed packets, a ping of death is fragmented into groups of 8 octets before transmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code.

#### NEW QUESTION 180

- (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 184

- (Exam Topic 1)

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

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

**Answer:** AC

#### NEW QUESTION 188

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 192

- (Exam Topic 1)

Which API is used for Content Security?

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

**Answer:** D

#### NEW QUESTION 195

- (Exam Topic 1)

Which algorithm provides encryption and authentication for data plane communication?

- A. AES-GCM
- B. SHA-96
- C. AES-256
- D. SHA-384

**Answer:** A

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html>

#### NEW QUESTION 197

- (Exam Topic 1)

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

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

**Answer:** A

#### Explanation:



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

#### NEW QUESTION 201

- (Exam Topic 1)

What is the difference between deceptive phishing and spear phishing?

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

**Answer: B**

#### Explanation:

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

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

#### NEW QUESTION 202

- (Exam Topic 1)

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

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

**Answer: D**

#### NEW QUESTION 204

- (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 208

- (Exam Topic 1)

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

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

**Answer: CE**

#### Explanation:

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

Reference:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_vpn/configuration/15-mt/sec-vpn-availability-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](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpn/configuration/15-mt/sec-vpn-availability-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 209

- (Exam Topic 1)

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

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



E. Cisco FTDv configured in routed mode and IPv6 configured

**Answer:** AC

#### NEW QUESTION 213

- (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 217

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 222

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 225

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 227

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 229

- (Exam Topic 3)

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

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

**Answer:** D

#### Explanation:

Reference:

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

#### NEW QUESTION 234

- (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 237

- (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 241

- (Exam Topic 3)

Why is it important to patch endpoints consistently?

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

**Answer:** B

#### NEW QUESTION 244

- (Exam Topic 3)

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

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

**Answer:**

D

#### NEW QUESTION 249

- (Exam Topic 3)

Which algorithm is an NGE hash function?

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

**Answer:** D

#### NEW QUESTION 250

- (Exam Topic 3)

Which solution for remote workers enables protection, detection, and response on the endpoint against known and unknown threats?

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

**Answer:** A

#### NEW QUESTION 254

- (Exam Topic 3)

Which open source tool does Cisco use to create graphical visualizations of network telemetry on Cisco IOS XE devices?

- A. InfluxDB
- B. Splunk
- C. SNMP
- D. Grafana

**Answer:** D

#### NEW QUESTION 255

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 260

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 263

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 267

- (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 272

- (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 275

- (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 277

- (Exam Topic 3)

Which Cisco DNA Center Intent API action is used to retrieve the number of devices known to a DNA Center?

- A. GET <https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/network-device/count>
- B. GET <https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/network-device>
- C. GET <https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/networkdevice?parameter1=value&parameter2=v>
- D. GET <https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/networkdevice/startIndex/recordsToReturn>

**Answer:** A

#### NEW QUESTION 282

- (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."

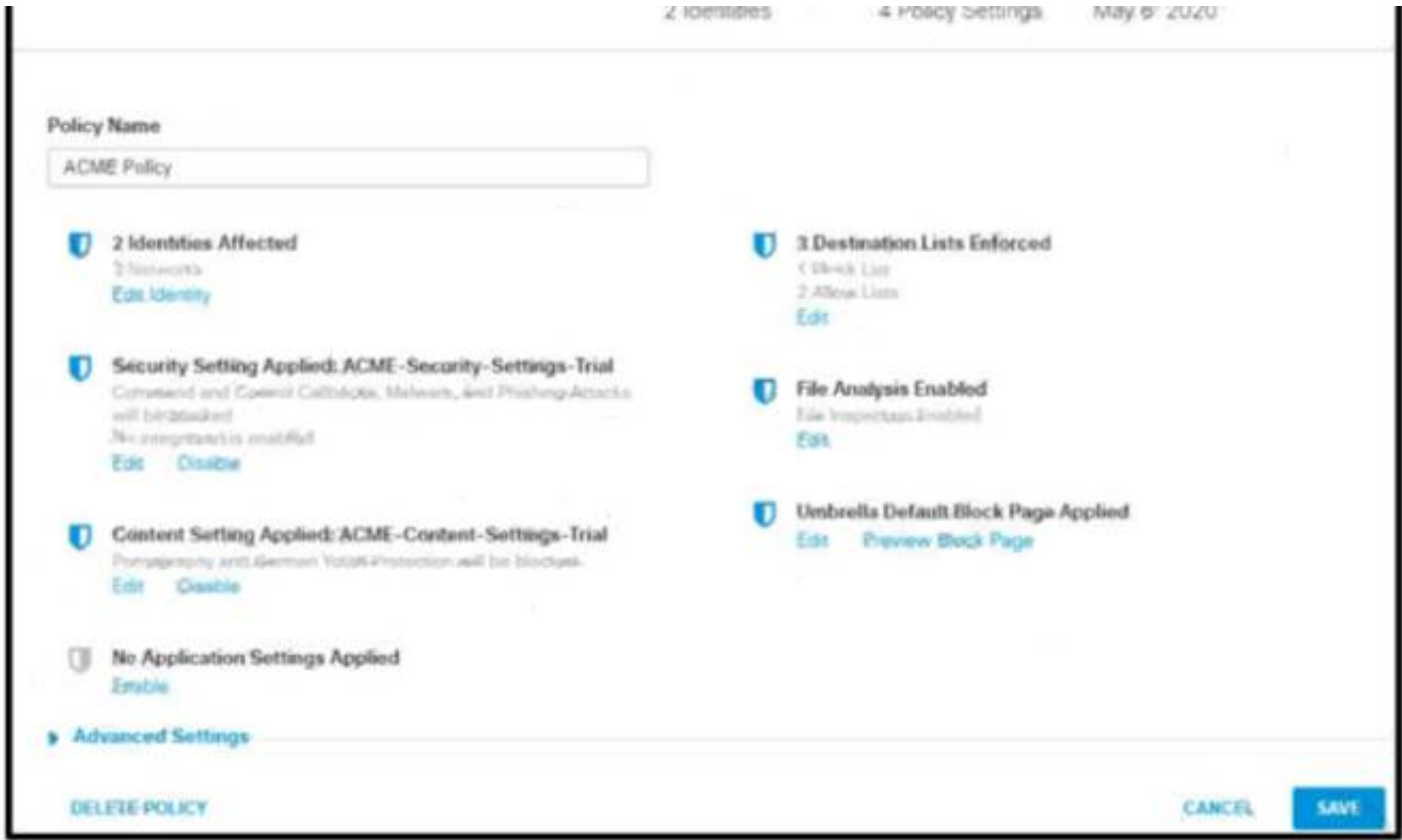
[1]  
<https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada>

#### NEW QUESTION 283

- (Exam Topic 3)

Refer to the exhibit.





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

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

Answer: B

NEW QUESTION 286

- (Exam Topic 3)

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

- A. Cisco AMP for Endpoints is a cloud-based service, and Cisco Umbrella is not.
- B. Cisco AMP for Endpoints prevents connections to malicious destinations, and C malware.
- C. Cisco AMP for Endpoints automatically researches indicators of compromise ..
- D. Cisco AMP for Endpoints prevents, detects, and responds to attacks before and against Internet threats.

Answer: D

Explanation:

https://learn-umbrella.cisco.com/i/802005-umbrella-security-report/3? https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html#:~:text=Power Cisco Advanced Malware Protection (AMP) for endpoints can be seen as a replacement for the traditional antivirus solution. It is a next generation, cloud delivered endpoint protection platform (EPP), and advanced endpoint detection and response (EDR). Providing Protection – Detection Response  
While Cisco Umbrella can enforce security at the DNS-, IP-, and HTTP/S-layer, this report does not require that blocking is enabled and only monitors your DNS activity. Any malicious domains requested and IPs resolved are indicators of compromise (IOC).  
Any malicious domains requested and IPs resolved are indicators of compromise IO( C)

NEW QUESTION 291

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:





#### NEW QUESTION 295

- (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 296

- (Exam Topic 3)

A company discovered an attack propagating through their network via a file. A custom file policy was created in order to track this in the future and ensure no other endpoints execute the infected file. In addition, it was discovered during testing that the scans are not detecting the file as an indicator of compromise. What must be done in order to ensure that the created is functioning as it should?

- A. Create an IP block list for the website from which the file was downloaded
- B. Block the application that the file was using to open
- C. Upload the hash for the file into the policy
- D. Send the file to Cisco Threat Grid for dynamic analysis

**Answer: C**

#### NEW QUESTION 301

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 306

- (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 310

- (Exam Topic 3)

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

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

**Answer:** A

#### Explanation:

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

Reference:

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

#### NEW QUESTION 315

- (Exam Topic 3)

Which Talos reputation center allows for tracking the reputation of IP addresses for email and web traffic?

- A. IP and Domain Reputation Center
- B. File Reputation Center
- C. IP Slock List Center
- D. AMP Reputation Center

**Answer:** A

#### NEW QUESTION 318

- (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 323

- (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 326

- (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 331

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 336

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 338

- (Exam Topic 3)

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

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

**Answer:** AB

#### NEW QUESTION 340

- (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 341

- (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 345

- (Exam Topic 3)

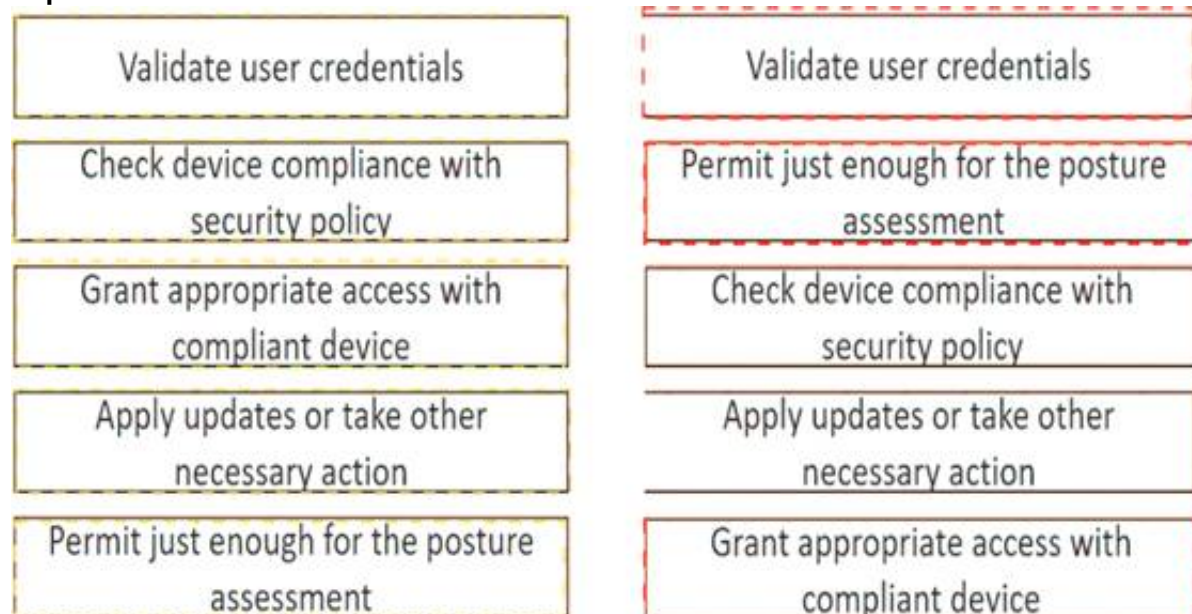
Drag and drop the posture assessment flow actions from the left into a sequence on the right.

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 349**

- (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 351**

- (Exam Topic 3)

What is the process in DevSecOps where all changes in the central code repository are merged and synchronized?

- A. CD
- B. EP
- C. CI
- D. QA

**Answer:** C

**NEW QUESTION 354**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 355**

- (Exam Topic 3)

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

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

**Answer:** AE

**NEW QUESTION 357**

- (Exam Topic 3)

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

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



**Answer:** C

#### NEW QUESTION 360

- (Exam Topic 3)

A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address <https://<FMC IP>/capture/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 362

- (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 366

- (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 367

- (Exam Topic 3)

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

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

**Answer:** CD

#### NEW QUESTION 372

- (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 377

- (Exam Topic 3)

An organization wants to provide visibility and to identify active threats in its network using a VM. The organization wants to extract metadata from network packet flow while ensuring that payloads are not retained or transferred outside the network. Which solution meets these requirements?

- A. Cisco Umbrella Cloud
- B. Cisco Stealthwatch Cloud PNM
- C. Cisco Stealthwatch Cloud PCM
- D. Cisco Umbrella On-Premises

**Answer:** B

**Explanation:**



Reference:

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

#### NEW QUESTION 381

- (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 382

- (Exam Topic 3)

Refer to the exhibit.

```
ASA# show service-policy sfr

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

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

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

**Answer:** AE

#### Explanation:

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

#### NEW QUESTION 387

- (Exam Topic 3)

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

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

**Answer:** B

#### Explanation:

Reference:

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

#### NEW QUESTION 391

- (Exam Topic 3)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 396

- (Exam Topic 3)

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

- A. an infection spreading across the network
- 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 399

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 403

- (Exam Topic 3)

When MAB is configured for use within the 802.1X environment, an administrator must create a policy that allows the devices onto the network. Which information is used for the username and password?

- A. The MAB uses the IP address as username and password.
- B. The MAB uses the call-station-ID as username and password.
- C. Each device must be set manually by the administrator.
- D. The MAB uses the MAC address as username and password.

**Answer:** D

#### NEW QUESTION 404

- (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 407

- (Exam Topic 3)

An engineer is configuring Cisco WSA and needs to deploy it in transparent mode. Which configuration component must be used to accomplish this goal?

- A. MDA on the router
- B. PBR on Cisco WSA
- C. WCCP on switch
- D. DNS resolution on Cisco WSA

**Answer:** C

#### NEW QUESTION 410

- (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 414

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 418

- (Exam Topic 3)

Which role is a default guest type in Cisco ISE?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 422

- (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 425

- (Exam Topic 3)

Which benefit does DMVPN provide over GETVPN?

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

**Answer:** D

#### NEW QUESTION 428

- (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 430

- (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 432

- (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 437

- (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 442

- (Exam Topic 3)

Drag and drop the exploits from the left onto the type of security vulnerability on the right.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 447

- (Exam Topic 3)

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

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

Answer: D



#### NEW QUESTION 450

- (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 452

- (Exam Topic 3)

What is the purpose of the Cisco Endpoint loC feature?

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

**Answer:** C

#### Explanation:

[https://www.cisco.com/c/dam/en\\_us/about/doing\\_business/legal/service\\_descriptions/docs/Cisco\\_Secure\\_Manageable\\_Endpoint\\_LoC.pdf](https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Secure_Manageable_Endpoint_LoC.pdf)

#### NEW QUESTION 456

- (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 457

- (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?

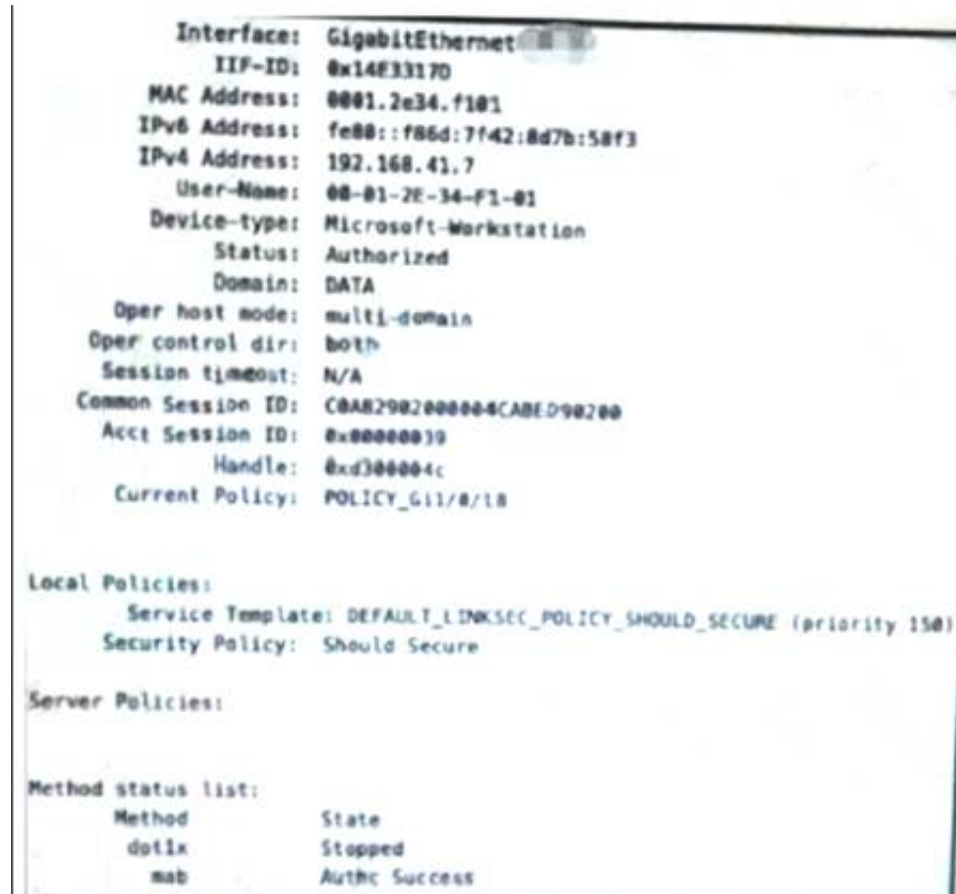
- A. VMware APIC
- B. VMwarevRealize
- C. VMware fusion
- D. VMware horizons

**Answer:** B

#### NEW QUESTION 462

- (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 465

- (Exam Topic 3)

Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)

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

**Answer:** AE

#### NEW QUESTION 466

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 467

- (Exam Topic 3)

Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

- A. OpenC2
- B. OpenIOC
- C. CybOX
- D. STIX

**Answer:** D

#### NEW QUESTION 469

- (Exam Topic 3)

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

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

**Answer:** BE

#### NEW QUESTION 473

- (Exam Topic 3)

What are two workloaded security models? (Choose two)

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

**Answer:** CD

#### NEW QUESTION 477

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 481**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 483**

- (Exam Topic 3)

An organization deploys multiple Cisco FTD appliances and wants to manage them using one centralized solution. The organization does not have a local VM but does have existing Cisco ASAs that must migrate over to Cisco FTDs. Which solution meets the needs of the organization?

- A. Cisco FMC
- B. CSM
- C. Cisco FDM
- D. CDO

**Answer:** B

**NEW QUESTION 484**

- (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 486**

- (Exam Topic 3)

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

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

**Answer:** BE

**NEW QUESTION 487**

- (Exam Topic 3)

What is the result of the ACME-Router(config)#login block-for 100 attempts 4 within 60 command on a Cisco IOS router?

- A. If four log in attempts fail in 100 seconds, wait for 60 seconds to next log in prompt.
- B. After four unsuccessful log in attempts, the line is blocked for 100 seconds and only permit IP addresses are permitted in ACL
- C. After four unsuccessful log in attempts, the line is blocked for 60 seconds and only permit IP addresses are permitted in ACL1
- D. If four failures occur in 60 seconds, the router goes to quiet mode for 100 seconds.

**Answer:** D

**NEW QUESTION 489**

- (Exam Topic 3)

Refer to the exhibit.

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

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

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

Answer: B

#### NEW QUESTION 491

- (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 495

- (Exam Topic 3)

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

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

Answer: C

#### Explanation:

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

#### NEW QUESTION 496

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Reference:

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

#### NEW QUESTION 501

- (Exam Topic 3)

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

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

Answer: C

#### NEW QUESTION 506

- (Exam Topic 3)

What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?

- A. trusted automated exchange
- B. Indicators of Compromise
- C. The Exploit Database

D. threat intelligence

**Answer:** D

#### NEW QUESTION 509

- (Exam Topic 3)

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

esp-3des	Authentication
esp-aes-256	
esp-md5-hmac	
esp-sha-hmac	Encryption

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Diagram Description automatically generated

#### NEW QUESTION 513

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 514

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 516

- (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 520

- (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 523

- (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 526

- (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 527

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 531

- (Exam Topic 3)

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

- A. L2TP is an IP packet encapsulation protocol, and GRE over IPsec is a tunneling protocol.
- B. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701.



- C. GRE over IPsec adds its own header, and L2TP does not.
- D. GRE over IPsec cannot be used as a standalone protocol, and L2TP can.

**Answer:** D

#### NEW QUESTION 533

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 537

- (Exam Topic 3)

What is the purpose of CA in a PKI?

- A. To issue and revoke digital certificates
- B. To validate the authenticity of a digital certificate
- C. To create the private key for a digital certificate
- D. To certify the ownership of a public key by the named subject

**Answer:** A

#### Explanation:

Reference: <https://cheapsslsecurity.com/blog/understanding-the-role-of-certificate-authorities-in-pki/>

#### NEW QUESTION 538

- (Exam Topic 3)

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

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

**Answer:** B

#### Explanation:

Reference:

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

#### NEW QUESTION 540

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 545

- (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 547

- (Exam Topic 3)

Which Cisco Firewall solution requires zone definition?

- A. CBAC

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

**Answer:** C

**NEW QUESTION 549**

- (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 550**

- (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 554**

- (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 559**

- (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 564**

- (Exam Topic 3)

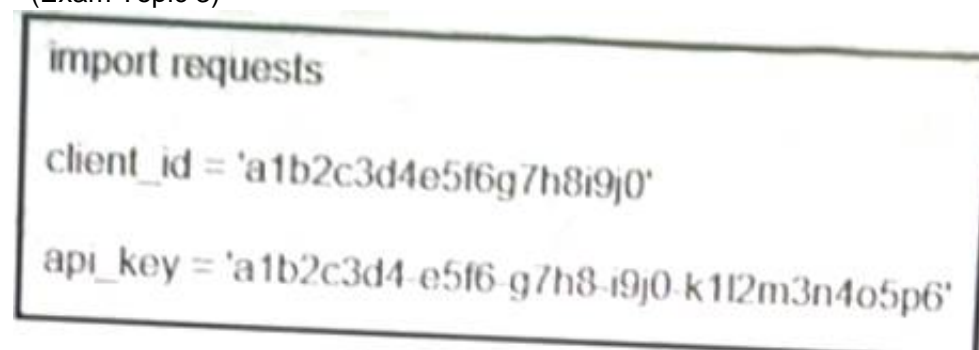
Which solution detects threats across a private network, public clouds, and encrypted traffic?

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

**Answer:** A

**NEW QUESTION 567**

- (Exam Topic 3)



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 570

- (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 575

- (Exam Topic 3)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 580

- (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 582

- (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 583

- (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 587

- (Exam Topic 3)

A network engineer must configure a Cisco ESA to prompt users to enter two forms of information before gaining access The Cisco ESA must also join a cluster machine using preshared keys What must be configured to meet these requirements?

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

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

**Answer:** A

#### NEW QUESTION 592

- (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 593

- (Exam Topic 3)

An organization wants to secure data in a cloud environment. Its security model requires that all users be authenticated and authorized. Security configuration and posture must be continuously validated before access is granted or maintained to applications and data. There is also a need to allow certain application traffic and deny all other traffic by default. Which technology must be used to implement these requirements?

- A. Virtual routing and forwarding
- B. Microsegmentation
- C. Access control policy
- D. Virtual LAN

**Answer:** C

#### Explanation:

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location. The Zero Trust model uses microsegmentation — a security technique that involves dividing perimeters into small zones to maintain separate access to every part of the network — to contain attacks.

#### NEW QUESTION 595

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 599

- (Exam Topic 3)

What is a function of Cisco AMP for Endpoints?

- A. It detects DNS attacks
- B. It protects against web-based attacks
- C. It blocks email-based attacks
- D. It automates threat responses of an infected host

**Answer:** D

#### NEW QUESTION 604

- (Exam Topic 3)

What is an advantage of network telemetry over SNMP pulls?

- A. accuracy
- B. encapsulation
- C. security
- D. scalability

**Answer:** D

#### NEW QUESTION 606

- (Exam Topic 3)

What is the intent of a basic SYN flood attack?

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

**Answer:** B

**NEW QUESTION 608**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 611**

- (Exam Topic 3)

What is a description of microsegmentation?

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

**Answer:** B

**NEW QUESTION 612**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 615**

- (Exam Topic 3)

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

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

**Answer:** DE

**NEW QUESTION 620**

- (Exam Topic 3)

What are two advantages of using Cisco Any connect over DMVPN? (Choose two)

- A. It provides spoke-to-spoke communications without traversing the hub
- B. It allows different routing protocols to work over the tunnel
- C. It allows customization of access policies based on user identity
- D. It allows multiple sites to connect to the data center
- E. It enables VPN access for individual users from their machines

**Answer:** CE

**NEW QUESTION 622**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 623**

- (Exam Topic 3)

Which portion of the network do EPP solutions solely focus on and EDR solutions do not?



- A. server farm
- B. perimeter
- C. core
- D. East-West gateways

**Answer:** B

#### NEW QUESTION 627

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 629

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 634

- (Exam Topic 3)

Which MDM configuration provides scalability?

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

**Answer:** C

#### NEW QUESTION 639

- (Exam Topic 3)

Refer to the exhibit.

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

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

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

**Answer:** B

#### NEW QUESTION 641

- (Exam Topic 3)

Which feature must be configured before implementing NetFlow on a router?

- A. SNMPv3
- B. syslog
- C. VRF

D. IP routing

**Answer:** D

**NEW QUESTION 642**

- (Exam Topic 3)

Which Cisco AMP feature allows an engineer to look back to trace past activities, such as file and process activity on an endpoint?

- A. endpoint isolation
- B. advanced search
- C. advanced investigation
- D. retrospective security

**Answer:** D

**NEW QUESTION 646**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 650**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 652**

- (Exam Topic 3)

When NetFlow is applied to an interface, which component creates the flow monitor cache that is used to collect traffic based on the key and nonkey fields in the configured record?

- A. records
- B. flow exporter
- C. flow sampler
- D. flow monitor

**Answer:** D

**NEW QUESTION 653**

- (Exam Topic 3)

Which category includes DoS Attacks?

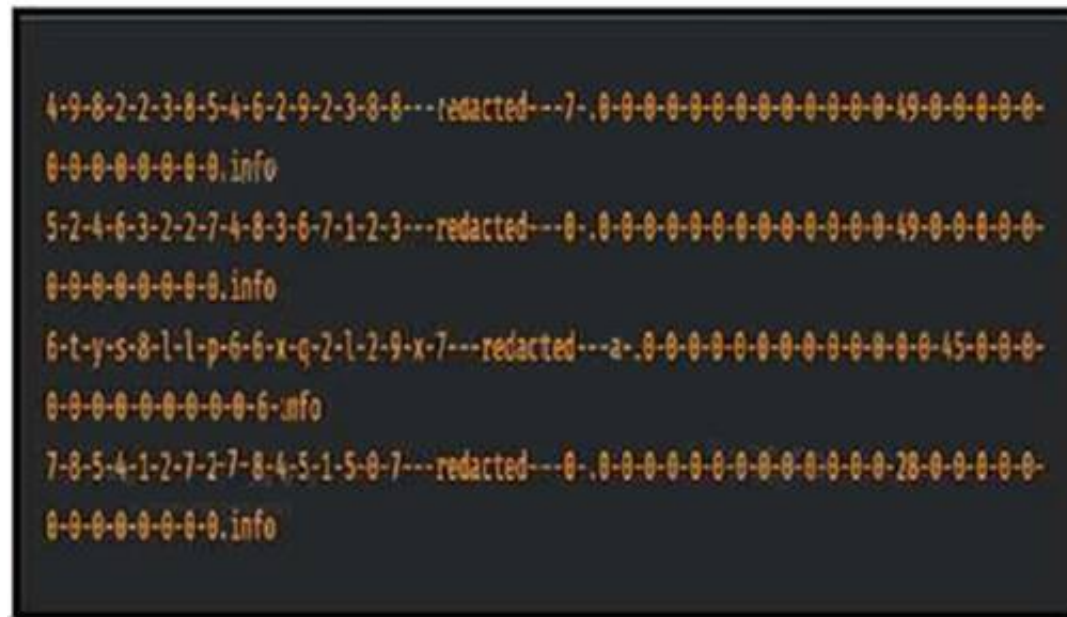
- A. Virus attacks
- B. Trojan attacks
- C. Flood attacks
- D. Phishing attacks

**Answer:** C

**NEW QUESTION 656**

- (Exam Topic 3)

Refer to the exhibit.



Consider that any feature of DNS requests, such as the length off the domain name and the number of subdomains, can be used to construct models of expected behavior to which observed values can be compared. Which type of malicious attack are these values associated with?

- A. Spectre Worm
- B. Eternal Blue Windows
- C. Heartbleed SSL Bug
- D. W32/AutoRun worm

**Answer: D**

#### NEW QUESTION 659

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 663

- (Exam Topic 3)

Which Cisco platform onboards the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing the endpoint to gain network access?

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

**Answer: A**

#### NEW QUESTION 664

- (Exam Topic 3)

What is a feature of NetFlow Secure Event Logging?

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

**Answer: A**

#### NEW QUESTION 667

- (Exam Topic 3)

Cisco SensorBase gathers threat information from a variety of Cisco products and services and performs analytics to find patterns on threats Which term describes this process?

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

**Answer: A**

#### NEW QUESTION 669

- (Exam Topic 3)

Which Cisco ISE feature helps to detect missing patches and helps with remediation?

- A. posture assessment
- B. profiling policy
- C. authentication policy
- D. enabling probes

**Answer:** B

#### NEW QUESTION 672

- (Exam Topic 3)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 674

- (Exam Topic 2)

What is a prerequisite when integrating a Cisco ISE server and an AD domain?

- A. Place the Cisco ISE server and the AD server in the same subnet
- B. Configure a common administrator account
- C. Configure a common DNS server
- D. Synchronize the clocks of the Cisco ISE server and the AD server

**Answer:** D

#### Explanation:

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise\\_active\\_directory\\_integration/b\\_ISE\\_AD\\_integration\\_](https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_)

#### NEW QUESTION 675

- (Exam Topic 2)

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

Which mechanism should the engineer configure to accomplish this goal?

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

**Answer:** C

#### NEW QUESTION 679

- (Exam Topic 2)

What are two Trojan malware attacks? (Choose two)

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

**Answer:** BD

#### NEW QUESTION 680

- (Exam Topic 2)

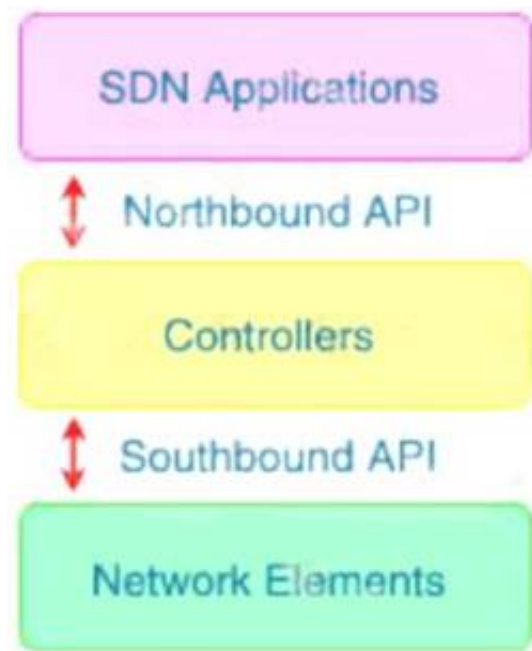
Which type of API is being used when a controller within a software-defined network architecture dynamically makes configuration changes on switches within the network?

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

**Answer:** B

#### Explanation:

Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs.



#### NEW QUESTION 681

- (Exam Topic 2)

How does DNS Tunneling exfiltrate data?

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

**Answer:** A

#### NEW QUESTION 683

- (Exam Topic 2)

Drag and drop the descriptions from the left onto the encryption algorithms on the right.

requires secret keys	<b>Asymmetric</b> <div></div> <div></div>
requires more time	
Diffie-Hellman exchange	<b>Symmetric</b> <div></div> <div></div>
3DES	

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetric encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating. Asymmetric encryption takes relatively more time than the symmetric encryption. Diffie Hellman algorithm is an asymmetric algorithm used to establish a shared secret for a symmetric key algorithm. Nowadays most of the people uses hybrid crypto system i.e, combination of symmetric and asymmetric encryption. Asymmetric Encryption is used as a technique in key exchange mechanism to share secret key and after the key is shared between sender and receiver, the communication will take place using symmetric encryption. The shared secret key will be used to encrypt the communication. Triple DES (3DES), a symmetric-key algorithm for the encryption of electronic data, is the successor of DES (Data Encryption Standard) and provides more secure encryption than DES. Note: Although "requires secret keys" option in this question is a bit unclear but it can only be assigned to Symmetric algorithm.

#### NEW QUESTION 686

- (Exam Topic 2)

An engineer is implementing NTP authentication within their network and has configured both the client and server devices with the command `ntp authentication-key 1 md5 Cisc392368270`. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however it is unable to do so. Which command is required to enable the client to accept the server's authentication key?

- A. `ntp peer 1.1.1.1 key 1`



- B. ntp server 1.1.1.1 key 1
- C. ntp server 1.1.1.2 key 1
- D. ntp peer 1.1.1.2 key 1

**Answer:** B

**Explanation:**

To configure an NTP enabled router to require authentication when other devices connect to it, use the following commands: NTP\_Server(config)#ntp authentication-key 2 md5 securitytutNTP\_Server(config)#ntp authenticateNTP\_Server(config)#ntp trusted-key 2Then you must configure the same authentication-key on the client router: NTP\_Client(config)#ntp authentication-key 2 md5 securitytutNTP\_Client(config)#ntp authenticateNTP\_Client(config)#ntp trusted-key 2NTP\_Client(config)#ntp server 10.10.10.1 key 2Note: To configure a Cisco device as a NTP client, use the command ntp server <IP address>. For example: Router(config)#ntp server 10.10.10.1. This command will instruct the router to query 10.10.10.1 for the time.

**NEW QUESTION 689**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### 350-701 Practice Exam Features:

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

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