

Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies



NEW QUESTION 1

- (Exam Topic 2)

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

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

Answer: A

Explanation:

Reference: <https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf> ETHOS = Fuzzy Fingerprinting using static/passive heuristics

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/BRKSEC-2139.pdf>

NEW QUESTION 2

- (Exam Topic 2)

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

standard includes NAT-T	IKEv1
uses six packets in main mode to establish phase 1	
uses four packets to establish phase 1 and phase 2	IKEv2
uses three packets in aggressive mode to establish phase 1	
uses EAP for authenticating remote access clients	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated with low confidence

NEW QUESTION 3

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 4

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 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)

How does Cisco Advanced Phishing Protection protect users?

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

Answer: D

Explanation:

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

NEW QUESTION 8

- (Exam Topic 2)

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

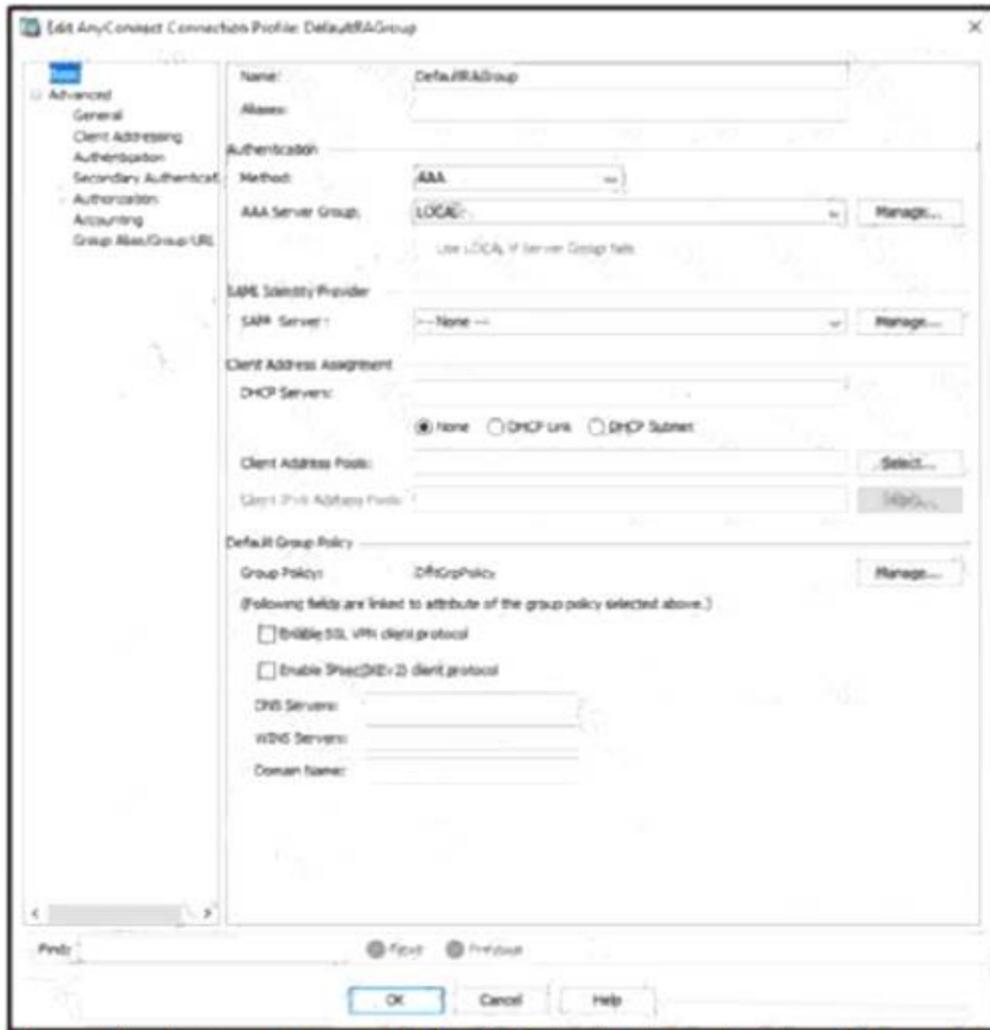
- A. to prevent theft of the endpoints
- B. because defense-in-depth stops at the network
- C. to expose the endpoint to more threats
- D. because human error or insider threats will still exist

Answer: D

NEW QUESTION 9

- (Exam Topic 2)

Refer to the exhibit.



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

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

Answer: B

Explanation:

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

NEW QUESTION 10

- (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 10

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 14

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 15

- (Exam Topic 2)

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 17

- (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 20

- (Exam Topic 1)

Which feature is supported when deploying Cisco ASAv within AWS public cloud?

- A. multiple context mode
- B. user deployment of Layer 3 networks
- C. IPv6
- D. clustering

Answer: B

Explanation:

The ASAv on AWS supports the following features: + Support for Amazon EC2 C5 instances, the next generation of the Amazon EC2 Compute Optimized instance family. + Deployment in the Virtual Private Cloud (VPC) + Enhanced networking (SR-IOV) where available + Deployment from Amazon Marketplace + Maximum of four vCPUs per instance + User deployment of L3 networks + Routed mode (default) Note: The Cisco Adaptive Security Virtual Appliance (ASAv) runs the same software as physical Cisco ASAs to deliver proven security functionality in a virtual form factor. The ASAv can be deployed in the public AWS cloud. It can then be configured to protect virtual and physical data center workloads that expand, contract, or shift their location over time. Reference:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96_qsg/asavaws.html

NEW QUESTION 23

- (Exam Topic 1)

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 26

- (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 27

- (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 28

- (Exam Topic 1)

Refer to the exhibit.

```
*Jun 30 16:52:33.795: ISAKMP:(1002): retransmission skipped for phase 1 (time
since last transmission 504)
R1#
*Jun 30 16:52:40.183: ISAKMP:(1001):purging SA., sa=68CEE058, delme=68CEE058
R1#
*Jun 30 16:52:43.291: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:43.291: ISAKMP (1002): incrementing error counter on sa, attempt 5
of 5: retransmit phase 1
*Jun 30 16:52:43.295: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002): sending packet to 10.10.12.2 my_port 500
peer_port 500 (I) MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002):Sending an IKE IPv4 Packet.
R1#
*Jun 30 16:52:53.299: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:53.299: ISAKMP:(1002):peer does not do paranoid keepalives.

*Jun 30 16:52:53.299: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.303: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.307: ISAKMP: Unlocking peer struct 0x68287318 for
isadb_mark_sa_deleted(), count 0
*Jun 30 16:52:53.307: ISAKMP: Deleting peer node by peer_reap for 10.10.12.2:
68287318
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node 79875537 error FALSE reason "IKE
deleted"
R1#
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node -484575753 error FALSE reason
"IKE deleted"
*Jun 30 16:52:53.315: ISAKMP:(1002):Input = IKE_MSG_INTERNAL, IKE_PHASE1_DEL
*Jun 30 16:52:53.319: ISAKMP:(1002):Old State = IKE_I_MM5 New State = IKE_DEST_SA
```

A network administrator configured a site-to-site VPN tunnel between two Cisco IOS routers, and hosts are unable to communicate between two sites of VPN. The network administrator runs the debug crypto isakmp sa command to track VPN status. What is the problem according to this command output?

- A. hashing algorithm mismatch
- B. encryption algorithm mismatch
- C. authentication key mismatch
- D. interesting traffic was not applied

Answer: C

NEW QUESTION 32

- (Exam Topic 1)

What are two reasons for implementing a multifactor authentication solution such as Duo Security provide to an organization? (Choose two)

- A. flexibility of different methods of 2FA such as phone callbacks, SMS passcodes, and push notifications
- B. single sign-on access to on-premises and cloud applications
- C. integration with 802.1x security using native Microsoft Windows supplicant
- D. secure access to on-premises and cloud applications
- E. identification and correction of application vulnerabilities before allowing access to resources

Answer: AD

Explanation:

Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a second factor (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password. Note: Single sign-on (SSO) is a property of identity and access management that enables users to securely authenticate with multiple applications and websites by logging in only once with just one set of credentials (username and password). With SSO, the application or website that the user is trying to access relies on a trusted third party to verify that users are who they say they are.

NEW QUESTION 33

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

Answer: A

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_A

NEW QUESTION 35

- (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 37

- (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 39

- (Exam Topic 1)

An engineer is configuring AMP for endpoints and wants to block certain files from executing. Which outbreak control method is used to accomplish this task?

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

Answer: C

NEW QUESTION 42

- (Exam Topic 1)

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

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

Answer: D

Explanation:

Reference:

https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_

NEW QUESTION 43

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 48

- (Exam Topic 1)

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

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

Answer: AB

NEW QUESTION 52

- (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 54

- (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

NEW QUESTION 59

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 63

- (Exam Topic 1)

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

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

Answer: CE

NEW QUESTION 66

- (Exam Topic 1)

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

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

Answer: AD

Explanation:

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

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

NEW QUESTION 71

- (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 72

- (Exam Topic 1)

Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two)

- A. packet decoder
- B. SIP
- C. modbus
- D. inline normalization
- E. SSL

Answer: BE

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Applic> uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

NEW QUESTION 74

- (Exam Topic 1)

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

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

Answer: A

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_nsel.h

NEW QUESTION 76

- (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 81

- (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 82

- (Exam Topic 1)

What are two list types within AMP for Endpoints Outbreak Control? (Choose two)

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

Answer: BD

Explanation:

Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists. A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine. Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company Reference: <https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf>

NEW QUESTION 85

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 89

- (Exam Topic 1)

In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

- A. Smurf
- B. distributed denial of service
- C. cross-site scripting
- D. rootkit exploit

Answer: C

Explanation:

Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. For example the code below is written in hex: <ahref=javascript:alert(('XSS')>Click Here is equivalent to: Click Here Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form.

NEW QUESTION 93

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 96

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 101

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 104

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 107

- (Exam Topic 1)

Which two request of REST API are valid on the Cisco ASA Platform? (Choose two)

- A. put
- B. options
- C. get
- D. push
- E. connect

Answer: AC

Explanation:

The ASA REST API gives you programmatic access to managing individual ASAs through a Representational State Transfer (REST) API. The API allows external clients to perform CRUD (Create, Read, Update, Delete) operations on ASA resources; it is based on the HTTPS protocol and REST methodology. All API requests are sent over HTTPS to the ASA, and a response is returned. Request Structure Available request methods are: GET – Retrieves data from the specified object. PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist. POST – Creates the object with the supplied information. DELETE – Deletes the specified object

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html>

NEW QUESTION 110

- (Exam Topic 1)

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

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

Answer: AE

NEW QUESTION 112

- (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 117

- (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 120

- (Exam Topic 1)

Refer to the exhibit.

```
HQ_Router(config)#username admin5 privilege 5
HQ_Router(config)#privilege interface level 5
shutdown
HQ_Router(config)#privilege interface level 5 ip
HQ_Router(config)#privilege interface level 5
description
```

A network administrator configures command authorization for the admin5 user. What is the admin5 user able to do on HQ_Router after this configuration?

- A. set the IP address of an interface
- B. complete no configurations
- C. complete all configurations
- D. add subinterfaces

Answer: B

Explanation:

The user "admin5" was configured with privilege level 5. In order to allow configuration (enter globalconfiguration mode), we must type this command:(config)#privilege exec level 5 configure terminalWithout this command, this user cannot do any configuration.Note: Cisco IOS supports privilege levels from 0 to 15, but the privilege levels which are used by default are privilege level 1 (user EXEC) and level privilege 15 (privilege EXEC)

NEW QUESTION 122

- (Exam Topic 1)

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

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

Answer: AB

NEW QUESTION 123

- (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 126

- (Exam Topic 1)

How is ICMP used as an exfiltration technique?

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

Answer: C

NEW QUESTION 128

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 130

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 132

- (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 133

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 136

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 138

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 142

- (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 146

- (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 151

- (Exam Topic 3)

Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)

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

Answer: AB

NEW QUESTION 156

- (Exam Topic 3)

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

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

Answer: AE

NEW QUESTION 157

- (Exam Topic 3)

What is the difference between a vulnerability and an exploit?

- A. A vulnerability is a hypothetical event for an attacker to exploit
- B. A vulnerability is a weakness that can be exploited by an attacker
- C. An exploit is a weakness that can cause a vulnerability in the network
- D. An exploit is a hypothetical event that causes a vulnerability in the network

Answer: B

NEW QUESTION 158

- (Exam Topic 3)

How does Cisco Workload Optimization Manager help mitigate application performance issues?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 159

- (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 163

- (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 165

- (Exam Topic 3)

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

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

Answer: BD

NEW QUESTION 169

- (Exam Topic 3)

An engineer is configuring their router to send NetFlow data to Stealthwatch which has an IP address of 1.1.1.1 using the flow record Stealthwatch406397954 command. Which additional command is required to complete the flow record?

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

Answer: B

NEW QUESTION 172

- (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 177

- (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 179

- (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 183

- (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¶meter2=v>
- D. GET <https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/networkdevice/startIndex/recordsToReturn>

Answer: A

NEW QUESTION 187

- (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 188

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 191

- (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 192

- (Exam Topic 3)

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

- A. Cisco CTA

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

Answer: B

NEW QUESTION 197

- (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 199

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 203

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 207

- (Exam Topic 3)

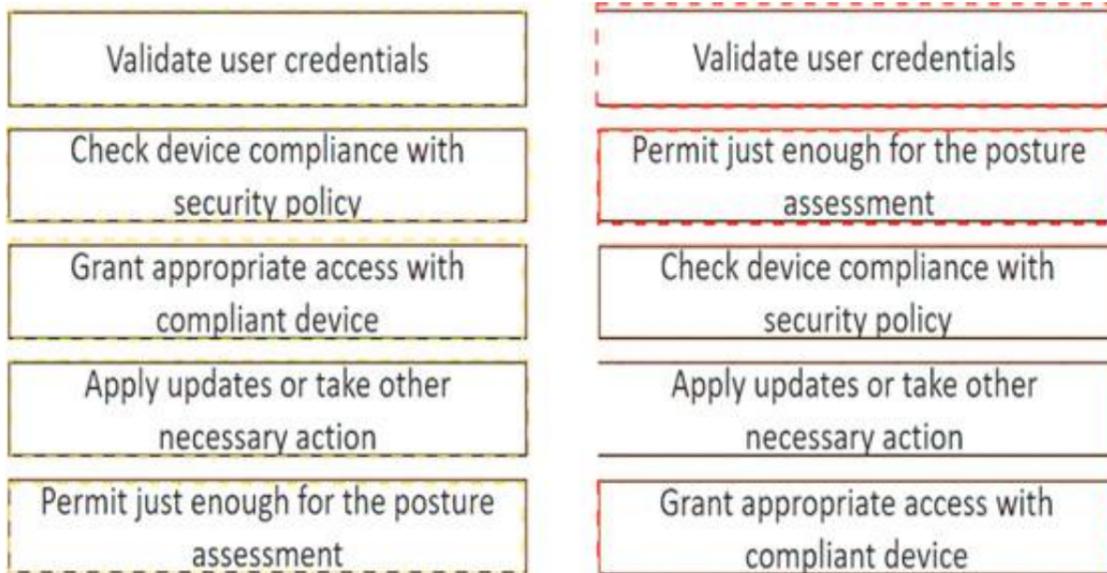
Drag and drop the posture assessment flow actions from the left into a sequence on the right.

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 211

- (Exam Topic 3)

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

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

Answer: AC

NEW QUESTION 213

- (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 215

- (Exam Topic 3)

What is the concept of CI/CD pipelining?

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

Answer: A

NEW QUESTION 219

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 220

- (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 222

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 227

- (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 229

- (Exam Topic 3)

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

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

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

Answer: D

NEW QUESTION 233

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 237

- (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 238

- (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 241

- (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 242

- (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 245

- (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 247

- (Exam Topic 3)

Which IETF attribute is supported for the RADIUS CoA feature?

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

Answer: A

NEW QUESTION 248

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 251

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 252

- (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 257

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 259

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 261

- (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 265

- (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 269

- (Exam Topic 3)

```
def dnac_login(host, username, password):
    url = "https://{}/api/system/v1/auth/token".format(host)
    response = requests.request("POST", url,
    auth=HTTPBasicAuth(username, password),
                                headers=headers, verify=False)
    return response.json() ["Token"]
```

Refer to the exhibit. What is the result of the Python script?

- A. It uses the POST HTTP method to obtain a username and password to be used for authentication.
- B. It uses the POST HTTP method to obtain a token to be used for authentication.
- C. It uses the GET HTTP method to obtain a token to be used for authentication.
- D. It uses the GET HTTP method to obtain a username and password to be used for authentication

Answer: B

NEW QUESTION 274

- (Exam Topic 3)

Which security solution protects users leveraging DNS-layer security?

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

Answer: C

NEW QUESTION 279

- (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 283

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 287

- (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 288

- (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 289

- (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 294

- (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 297

- (Exam Topic 3)

Which Cisco network security device supports contextual awareness?

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

Answer: D

NEW QUESTION 302

- (Exam Topic 3)

Why should organizations migrate to a multifactor authentication strategy?

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

Answer: D

NEW QUESTION 307

- (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 312

- (Exam Topic 3)

What is the recommendation in a zero-trust model before granting access to corporate applications and resources?

- A. to use multifactor authentication
- B. to use strong passwords
- C. to use a wired network, not wireless
- D. to disconnect from the network when inactive

Answer: A

NEW QUESTION 313

- (Exam Topic 3)

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

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

Answer: CD

NEW QUESTION 317

- (Exam Topic 3)

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

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

Answer: BC

Explanation:

Reference:

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

NEW QUESTION 321

- (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 325

- (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 328

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 329

- (Exam Topic 3)

Refer to the exhibit.



An engineer must configure a Cisco switch to perform PPP authentication via a TACACS server located at IP address 10.1.1.10. Authentication must fall back to the local database using the username LocalUser and password C1Sc0451069341I if the TACACS server is unreachable.

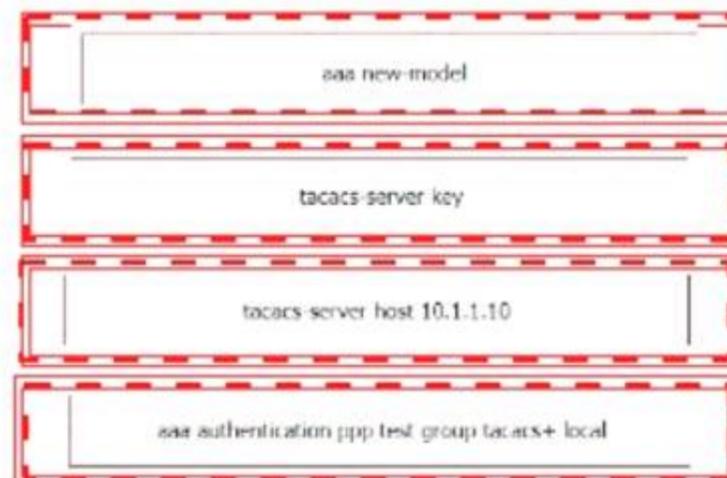
Drag and drop the commands from the left onto the corresponding configuration steps on the right.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 334

- (Exam Topic 3)

Which service allows a user export application usage and performance statistics with Cisco Application Visibility and control?

ntp association detail command indicates that the configured NTP server is unsynchronized and has a stratum of 16. What is the cause of this issue?

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

Answer: B

NEW QUESTION 356

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 358

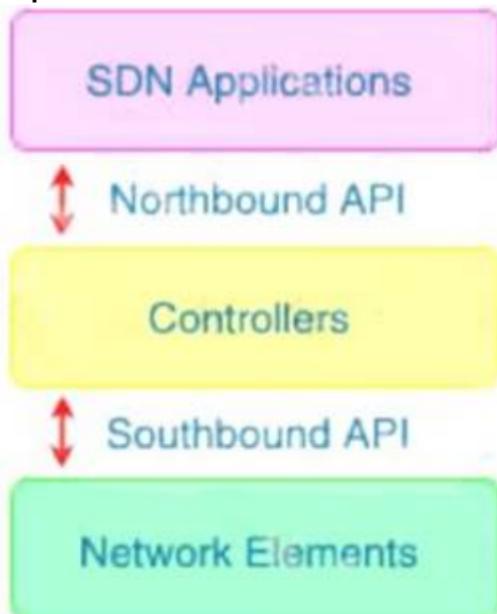
- (Exam Topic 2)

With which components does a southbound API within a software-defined network architecture communicate?

- A. controllers within the network
- B. applications
- C. appliances
- D. devices such as routers and switches

Answer: D

Explanation:



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

NEW QUESTION 361

- (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 365

- (Exam Topic 2)

What is a functional difference between a Cisco ASA and a Cisco IOS router with Zone-based policy firewall?

- A. The Cisco ASA denies all traffic by default whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces
- B. The Cisco IOS router with Zone-Based Policy Firewall can be configured for high availability, whereas the Cisco ASA cannot
- C. The Cisco IOS router with Zone-Based Policy Firewall denies all traffic by default, whereas the Cisco ASA starts out by allowing all traffic until rules are added
- D. The Cisco ASA can be configured for high availability whereas the Cisco IOS router with Zone-Based Policy Firewall cannot

Answer: A

NEW QUESTION 369

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 374

- (Exam Topic 2)

What are two characteristics of Cisco DNA Center APIs? (Choose two)

- A. Postman is required to utilize Cisco DNA Center API calls.
- B. They do not support Python scripts.
- C. They are Cisco proprietary.
- D. They quickly provision new devices.
- E. They view the overall health of the network

Answer: DE

NEW QUESTION 376

- (Exam Topic 2)

What is a difference between DMVPN and sVTI?

- A. DMVPN supports tunnel encryption, whereas sVTI does not.
- B. DMVPN supports dynamic tunnel establishment, whereas sVTI does not.
- C. DMVPN supports static tunnel establishment, whereas sVTI does not.
- D. DMVPN provides interoperability with other vendors, whereas sVTI does not.

Answer: B

NEW QUESTION 378

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 382

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 386

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 387

- (Exam Topic 2)

What are two benefits of Flexible NetFlow records? (Choose two)

- A. They allow the user to configure flow information to perform customized traffic identification
- B. They provide attack prevention by dropping the traffic
- C. They provide accounting and billing enhancements
- D. They converge multiple accounting technologies into one accounting mechanism
- E. They provide monitoring of a wider range of IP packet information from Layer 2 to 4

Answer: AD

Explanation:

Reference: https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon_external_docbase_0_d9.html#wp1057997Note: Traditional NetFlow allows us to monitor from Layer 2 to 4 but Flexible NetFlow goes beyond these layers.

NEW QUESTION 391

- (Exam Topic 2)

An organization is receiving SPAM emails from a known malicious domain. What must be configured in order to prevent the session during the initial TCP communication?

- A. Configure the Cisco ESA to drop the malicious emails
- B. Configure policies to quarantine malicious emails
- C. Configure policies to stop and reject communication
- D. Configure the Cisco ESA to reset the TCP connection

Answer: D

NEW QUESTION 392

- (Exam Topic 2)

What is the function of SDN southbound API protocols?

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

Answer: B

Explanation:

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

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

NEW QUESTION 395

- (Exam Topic 2)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

Cisco TrustSec – software defined segmentation that uses SGTs

Cisco Umbrella – secure internet gateway ion the cloud that provides a security solution

NEW QUESTION 398

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 400

- (Exam Topic 2)

Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.

privilege escalation	Tetration platform learns the normal behavior of users.
user login suspicious behavior	Tetration platform is armed to look at sensitive files.
interesting file access	Tetration platform watches user access failures and methods
file access from a different user	Tetration platform watches for movement in the process lineage tree.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 404

.....

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](#)