

350-701 Dumps

Implementing and Operating Cisco Security Core Technologies

<https://www.certleader.com/350-701-dumps.html>



NEW QUESTION 1

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 2

- (Exam Topic 2)

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

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

IKEv2

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated with low confidence

NEW QUESTION 3

- (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 4

- (Exam Topic 2)

An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco Firepower. Which feature should be used to accomplish this?

- A. NetFlow
- B. Packet Tracer
- C. Network Discovery
- D. Access Control

Answer: A

Explanation:

Reference:

<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper>

NEW QUESTION 5

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 6

- (Exam Topic 2)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A picture containing table Description automatically generated

NEW QUESTION 7

- (Exam Topic 2)

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

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

Answer: CE

Explanation:

Reference:

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

NEW QUESTION 8

- (Exam Topic 2)

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 9

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 10

- (Exam Topic 2)

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

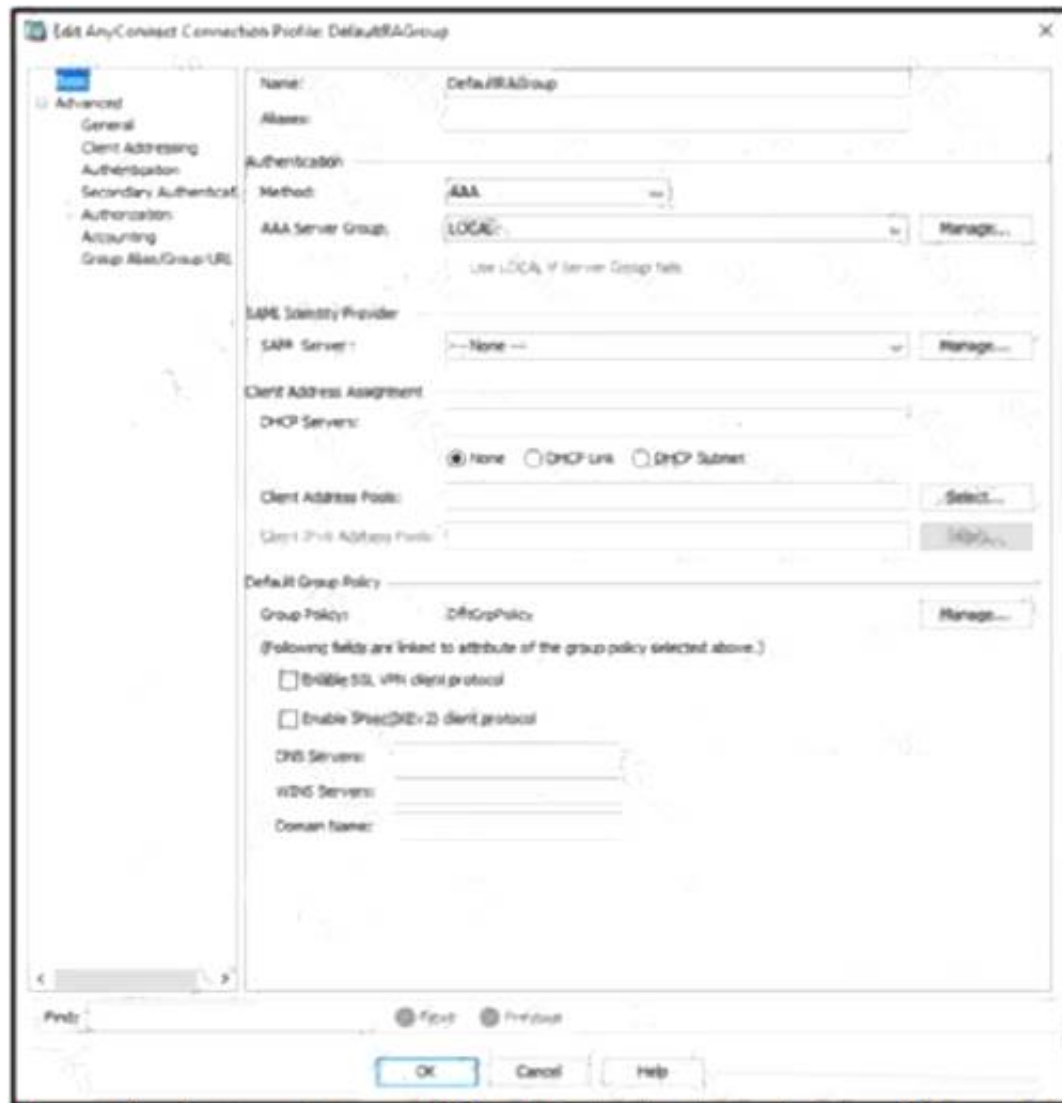
- A. to prevent theft of the endpoints
- B. because defense-in-depth stops at the network
- C. to expose the endpoint to more threats
- D. because human error or insider threats will still exist

Answer: D

NEW QUESTION 10

- (Exam Topic 2)

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 15

- (Exam Topic 2)

What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

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

D. Flow-create events are delayed

Answer: B

Explanation:

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

NEW QUESTION 18

- (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 22

- (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 24

- (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 29

- (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 32

- (Exam Topic 1)

What is a commonality between DMVPN and FlexVPN technologies?

- A. FlexVPN and DMVPN use IS-IS routing protocol to communicate with spokes
- B. FlexVPN and DMVPN use the new key management protocol
- C. FlexVPN and DMVPN use the same hashing algorithms
- D. IOS routers run the same NHRP code for DMVPN and FlexVPN

Answer: D

Explanation:

Reference: <https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/>

NEW QUESTION 33

- (Exam Topic 2)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, chat or text message Description automatically generated

NEW QUESTION 35

- (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 37

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 39

- (Exam Topic 2)

An organization has two systems in their DMZ that have an unencrypted link between them for communication.

The organization does not have a defined password policy and uses several default accounts on the systems. The application used on those systems also have not gone through stringent code reviews. Which vulnerability would help an attacker brute force their way into the systems?

- A. weak passwords
- B. lack of input validation
- C. missing encryption

D. lack of file permission

Answer: C

Explanation:

Reference: <https://tools.ietf.org/html/rfc3954>

NEW QUESTION 41

- (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 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 thcrypto 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.](https://www.examttopics.com/discussions/cisco/view/46191-exam-350-701-topic-1-question-71-discussion/#:~:t=Testing%20without%20a%20netmask%20shows%20that%20command%20interpretation%20has%20a%20preference%20for%20%2F16%20and%20%2F24.)

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 45

- (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 instancefamily.+ 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 48

- (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 50

- (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 54

- (Exam Topic 1)

What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?

- A. Cisco Umbrella
- B. External Threat Feeds
- C. Cisco Threat Grid
- D. Cisco Stealthwatch

Answer: C

Explanation:

Reference:

<https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector>

NEW QUESTION 59

- (Exam Topic 1)

Why would a user choose an on-premises ESA versus the CES solution?

- A. Sensitive data must remain onsite.
- B. Demand is unpredictable.
- C. The server team wants to outsource this service.
- D. ESA is deployed inline.

Answer: A

NEW QUESTION 62

- (Exam Topic 1)

Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?

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

Answer: B

NEW QUESTION 65

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 67

- (Exam Topic 1)

Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two)

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

Answer: AC

NEW QUESTION 70

- (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 71

- (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 73

- (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 75

- (Exam Topic 1)

Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

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

Answer: D

Explanation:

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

NEW QUESTION 76

- (Exam Topic 1)

What is the function of the Context Directory Agent?

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

Answer: C

Explanation:

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

NEW QUESTION 80

- (Exam Topic 1)

What is a characteristic of traffic storm control behavior?

- A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
- B. Traffic storm control cannot determine if the packet is unicast or broadcast.
- C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
- D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

Answer: A

NEW QUESTION 84

- (Exam Topic 1)

Which license is required for Cisco Security Intelligence to work on the Cisco Next Generation Intrusion Prevention System?

- A. control
- B. malware
- C. URL filtering
- D. protect

Answer: D

NEW QUESTION 85

- (Exam Topic 1)

Which RADIUS attribute can you use to filter MAB requests in an 802.1 x deployment?

- A. 1
- B. 2
- C. 6
- D. 31

Answer: C

Explanation:

Reference:

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networkingservices/config_

NEW QUESTION 90

- (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 93

- (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 95

- (Exam Topic 1)

Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?

- A. RSA SecureID
- B. Internal Database
- C. Active Directory
- D. LDAP

Answer: C

NEW QUESTION 100

- (Exam Topic 1)

Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two)

- A. Check integer, float, or Boolean string parameters to ensure accurate values.
- B. Use prepared statements and parameterized queries.
- C. Secure the connection between the web and the app tier.
- D. Write SQL code instead of using object-relational mapping libraries.
- E. Block SQL code execution in the web application database login.

Answer: AB

NEW QUESTION 104

- (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 105

- (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 107

- (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 111

- (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 112

- (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 115

- (Exam Topic 1)

Which two fields are defined in the NetFlow flow? (Choose two)

- A. type of service byte
- B. class of service bits
- C. Layer 4 protocol type
- D. destination port
- E. output logical interface

Answer: AD

Explanation:

Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share seven values which define a unique key for the flow: + Ingress interface (SNMP ifIndex) + Source IP address + Destination IP address + IP protocol + Source port for UDP or TCP, 0 for other protocols + Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols + IP Type of Service Note: A flow is a unidirectional series of packets between a given source and destination.

NEW QUESTION 120

- (Exam Topic 1)

What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services? (Choose two)

- A. multiple factor auth
- B. local web auth
- C. single sign-on
- D. central web auth
- E. TACACS+

Answer: BD

NEW QUESTION 122

- (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 123

- (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 124

- (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 125

- (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 an 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 Wanna Cry 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 129

- (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-guide60/> Refere 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 131

- (Exam Topic 1)

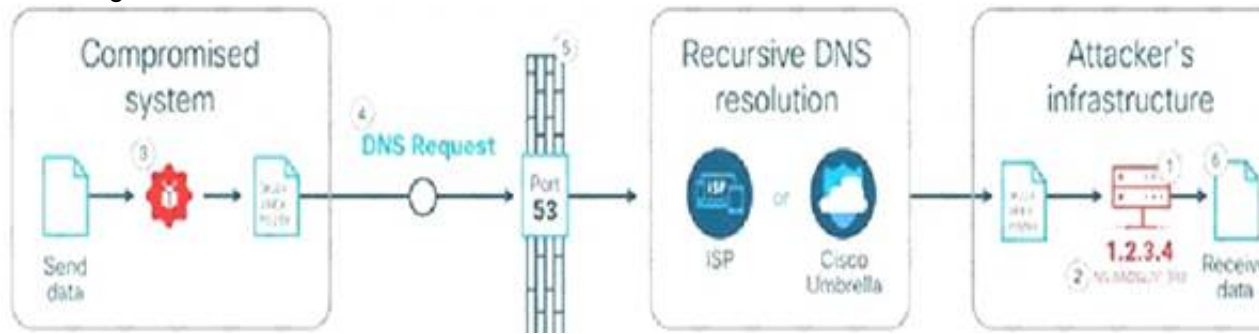
How is DNS tunneling used to exfiltrate data out of a corporate network?

- 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 DNSnameserver (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 134

- (Exam Topic 1)

The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the ASA be added on the Cisco UC Manager platform?

- A. Certificate Trust List
- B. Endpoint Trust List
- C. Enterprise Proxy Service
- D. Secured Collaboration Proxy

Answer: A

NEW QUESTION 136

- (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 139

- (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 144

- (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 147

- (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 152

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 154

- (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 159

- (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 163

- (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 164

- (Exam Topic 1)

Which attack is commonly associated with C and C++ programming languages?

- A. cross-site scripting
- B. water holing
- C. DDoS
- D. buffer overflow

Answer: D

Explanation:

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's allotted memory space. This happens quite frequently in the case of arrays.

NEW QUESTION 166

- (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

NEW QUESTION 168

- (Exam Topic 1)

Refer to the exhibit.

```
def add_device_to_dnac(dnac_ip, device_ip, snmp_version,
    snmp_ro_community, snmp_rw_community,
    snmp_retry, snmp_timeout,
    cli_transport, username, password, enable_password):
    device_object = {
        'ipAddress': [
            device_ip
        ],
        'type': 'NETWORK_DEVICE',
        'computeDevice': False,
        'snmpVersion': snmp_version,
        'snmpROCommunity': snmp_ro_community,
        'snmpRWCommunity': snmp_rw_community,
        'snmpRetry': snmp_retry,
        'snmpTimeout': snmp_timeout,
        'cliTransport': cli_transport,
        'userName': username,
        'password': password,
        'enablePassword': enable_password
    }
    response = requests.post(
        'https://{}/dna/intent/api/v1/network-
device'.format(dnac_ip),
        data=json.dumps(device_object),
        headers={
            'X-Auth-Token': '{}'.format(token),
            'Content-type': 'application/json'
        },
        verify=False
    )
    return response.json()
```

What is the result of this Python script of the Cisco DNA Center API?

- A. adds authentication to a switch
- B. adds a switch to Cisco DNA Center
- C. receives information about a switch
- D. deletes a switch from Cisco DNA Center

Answer: B

NEW QUESTION 173

- (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 174

- (Exam Topic 1)

Which action controls the amount of URI text that is stored in Cisco WSA logs files?

- A. Configure the datasecurityconfig command
- B. Configure the advancedproxyconfig command with the HTTPS subcommand
- C. Configure a small log-entry size.
- D. Configure a maximum packet size.

Answer: B

NEW QUESTION 178

- (Exam Topic 1)

Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware? (Choose two)

- A. Sophos engine
- B. white list
- C. RAT
- D. outbreak filters
- E. DLP

Answer: AD

NEW QUESTION 182

- (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 186

- (Exam Topic 1)

Elliptic curve cryptography is a stronger more efficient cryptography method meant to replace which current encryption technology?

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

Answer: B

Explanation:

Compared to RSA, the prevalent public-key cryptography of the Internet today, Elliptic Curve Cryptography (ECC) offers smaller key sizes, faster computation, as well as memory, energy and bandwidth savings and is thus better suited for small devices.

NEW QUESTION 187

- (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 global configuration mode), we must type this command: (config)#privilege exec level 5 configure terminal. Without 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 190

- (Exam Topic 1)

An administrator wants to ensure that all endpoints are compliant before users are allowed access on the corporate network. The endpoints must have the corporate antivirus application installed and be running the latest build of Windows 10.

What must the administrator implement to ensure that all devices are compliant before they are allowed on the network?

- A. Cisco Identity Services Engine and AnyConnect Posture module
- B. Cisco Stealthwatch and Cisco Identity Services Engine integration
- C. Cisco ASA firewall with Dynamic Access Policies configured
- D. Cisco Identity Services Engine with PxGrid services enabled

Answer: A

NEW QUESTION 194

- (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 198

- (Exam Topic 1)

On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed devices?

- A. health policy
- B. system policy
- C. correlation policy
- D. access control policy
- E. health awareness policy

Answer: A

NEW QUESTION 201

- (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 203

- (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 204

- (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 207

- (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 210

- (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 212

- (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 214

- (Exam Topic 1)

How does Cisco Stealthwatch Cloud provide security for cloud environments?

- A. It delivers visibility and threat detection.
- B. It prevents exfiltration of sensitive data.
- C. It assigns Internet-based DNS protection for clients and servers.
- D. It facilitates secure connectivity between public and private networks.

Answer: A

Explanation:

Cisco Stealthwatch Cloud: Available as an SaaS product offer to provide visibility and threat detection within public cloud infrastructures such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

NEW QUESTION 217

- (Exam Topic 1)

Which type of attack is social engineering?

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

Answer: B

Explanation:

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

NEW QUESTION 219

- (Exam Topic 1)

Which two capabilities does TAXII support? (Choose two)

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

Answer: AB

Explanation:

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

NEW QUESTION 222

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 226

- (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 231

- (Exam Topic 1)

Which feature requires a network discovery policy on the Cisco Firepower Next Generation Intrusion Prevention System?

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

Answer: B

NEW QUESTION 236

- (Exam Topic 1)

Which form of attack is launched using botnets?

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

Answer: C

Explanation:

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

NEW QUESTION 238

- (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 241

- (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 243

- (Exam Topic 3)

During a recent security audit a Cisco IOS router with a working IPSEC configuration using IKEv1 was flagged for using a wildcard mask with the crypto isakmp key command The VPN peer is a SOHO router with a dynamically assigned IP address Dynamic DNS has been configured on the SOHO router to map the dynamic IP address to the host name of vpn sohoroutercompany.com In addition to the command crypto isakmp key Cisc425007536 hostname vpn.sohoroutercompany.com what other two commands are now required on the Cisco IOS router for the VPN to continue to function after the wildcard command is removed? (Choose two)

- A. ip host vpn.sohoroutercompany.eom <VPN Peer IP Address>
- B. crypto isakmp identity hostname
- C. Add the dynamic keyword to the existing crypto map command
- D. fqdn vpn.sohoroutercompany.com <VPN Peer IP Address>
- E. ip name-server <DNS Server IP Address>

Answer: BC

NEW QUESTION 247

- (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 252

- (Exam Topic 3)

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

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

Answer: CD

NEW QUESTION 255

- (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 257

- (Exam Topic 3)

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

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

D. It simulates a slower link by introducing latency into application traffic.

Answer: C

NEW QUESTION 262

- (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 266

- (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 269

- (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 271

- (Exam Topic 3)

Which algorithm is an NGE hash function?

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

Answer: D

NEW QUESTION 275

- (Exam Topic 3)

Which solution stops unauthorized access to the system if a user's password is compromised?

- A. VPN
- B. MFA
- C. AMP
- D. SSL

Answer: B

NEW QUESTION 276

- (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 279

- (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 280

- (Exam Topic 3)

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

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

Answer: AE

NEW QUESTION 284

- (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 285

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 288

- (Exam Topic 3)

Which cloud service offering allows customers to access a web application that is being hosted, managed, and maintained by a cloud service provider?

- A. IaC
- B. SaaS
- C. IaaS
- D. PaaS

Answer: B

NEW QUESTION 290

- (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 294

- (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=Pow> 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 296

- (Exam Topic 3)

Which two capabilities does an MDM provide? (Choose two.)

- A. delivery of network malware reports to an inbox in a schedule
- B. unified management of mobile devices, Macs, and PCs from a centralized dashboard
- C. enforcement of device security policies from a centralized dashboard
- D. manual identification and classification of client devices
- E. unified management of Android and Apple devices from a centralized dashboard

Answer: BC

NEW QUESTION 298

- (Exam Topic 3)

Which solution is more secure than the traditional use of a username and password and encompasses at least two of the methods of authentication?

- A. single-sign on
- B. RADIUS/LDAP authentication
- C. Kerberos security solution
- D. multifactor authentication

Answer: D

NEW QUESTION 301

- (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 303

- (Exam Topic 3)

Which ESA implementation method segregates inbound and outbound email?

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

Answer: D

NEW QUESTION 304

- (Exam Topic 3)

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

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

Answer: A

Explanation:

Reference:

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/2-6/admin_guide

NEW QUESTION 308

- (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 313

- (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 315

- (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 318

- (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 319

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 324

- (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 329

- (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 331

- (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. antispooofing programs

Answer: AB

NEW QUESTION 334

- (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 336

- (Exam Topic 3)

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

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

Answer: AC

NEW QUESTION 340

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 342

- (Exam Topic 3)

Which metric is used by the monitoring agent to collect and output packet loss and jitter information?

- A. WSAv performance
- B. AVC performance
- C. OTCP performance
- D. RTP performance

Answer: D

NEW QUESTION 345

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 350

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 351

- (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 355

- (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 358

- (Exam Topic 3)

An organization has DHCP servers set up to allocate IP addresses to clients on the LAN. What must be done to ensure the LAN switches prevent malicious DHCP traffic while also distributing IP addresses to the correct endpoints?

- A. Configure Dynamic ARP inspection and add entries in the DHCP snooping database.
- B. Configure DHCP snooping and set trusted interfaces for all client connections.
- C. Configure Dynamic ARP inspection and antispoofing ACLs in the DHCP snooping database.
- D. Configure DHCP snooping and set a trusted interface for the DHCP server.

Answer: B

Explanation:

Reference: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration

NEW QUESTION 361

- (Exam Topic 3)

What is an advantage of the Cisco Umbrella roaming client?

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

Answer: C

NEW QUESTION 363

- (Exam Topic 3)

Which Cisco security solution provides patch management in the cloud?

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

Answer: C

NEW QUESTION 367

- (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 371

- (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 375

- (Exam Topic 3)

What do tools like Jenkins, Octopus Deploy, and Azure DevOps provide in terms of application and infrastructure automation?

- A. continuous integration and continuous deployment
- B. cloud application security broker
- C. compile-time instrumentation
- D. container orchestration

Answer: A

NEW QUESTION 376

- (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 380

- (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 381

- (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 385

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 387

- (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 390

- (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 395

- (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 400

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 405

- (Exam Topic 3)

Refer to the exhibit. When creating an access rule for URL filtering, a network engineer adds certain categories and individual URLs to block. What is the result of the configuration?

- A. Only URLs for botnets with reputation scores of 1-3 will be blocked.
- B. Only URLs for botnets with a reputation score of 3 will be blocked.
- C. Only URLs for botnets with reputation scores of 3-5 will be blocked.
- D. Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked.

Answer: A

NEW QUESTION 407

- (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

NEW QUESTION 408

- (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 413

- (Exam Topic 3)

Which standard is used to automate exchanging cyber threat information?

- A. TAXII
- B. MITRE
- C. IoC
- D. STIX

Answer: A

NEW QUESTION 418

- (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 420

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 422

- (Exam Topic 3)

What is a feature of container orchestration?

- A. ability to deploy Amazon ECS clusters by using the Cisco Container Platform data plane
- B. ability to deploy Amazon EKS clusters by using the Cisco Container Platform data plane
- C. ability to deploy Kubernetes clusters in air-gapped sites
- D. automated daily updates

Answer: C

NEW QUESTION 427

- (Exam Topic 3)

Drag and drop the features of Cisco ASA with Firepower from the left onto the benefits on the right.

Full Context Awareness	detection, blocking and remediation to protect the enterprise against targeted malware attacks
NGIPS	policy enforcement based on complete visibility of users and communication between virtual machines
AMP	real-time threat intelligence and security protection
Collective Security Intelligence	threat prevention and mitigation for known and unknown threats

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Full Context Awareness - policy enforcement NGIPS - threat prevention

AMP - real-time

Collective Sec Intel - Detection, blocking an remediation

NEW QUESTION 428

- (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 429

- (Exam Topic 3)

What is the purpose of the Cisco Endpoint IoC 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_Manage.pdf

NEW QUESTION 432

- (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 435

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 440

- (Exam Topic 3)

Which two commands are required when configuring a flow-export action on a Cisco ASA? (Choose two.)

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

Answer: AB

NEW QUESTION 441

- (Exam Topic 3)

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

- A. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where multiple systems target a single system with a DoS attack
- B. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where a computer is used to flood multiple servers that are distributed over a LAN
- C. A DoS attack is where a computer is used to flood a server with UDP packets whereas a DDoS attack is where a computer is used to flood a server with TCP packets
- D. A DoS attack is where a computer is used to flood a server with TCP packets whereas a DDoS attack is where a computer is used to flood a server with UDP packets

Answer: A

NEW QUESTION 444

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 446

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 449

- (Exam Topic 3)

Which endpoint solution protects a user from a phishing attack?

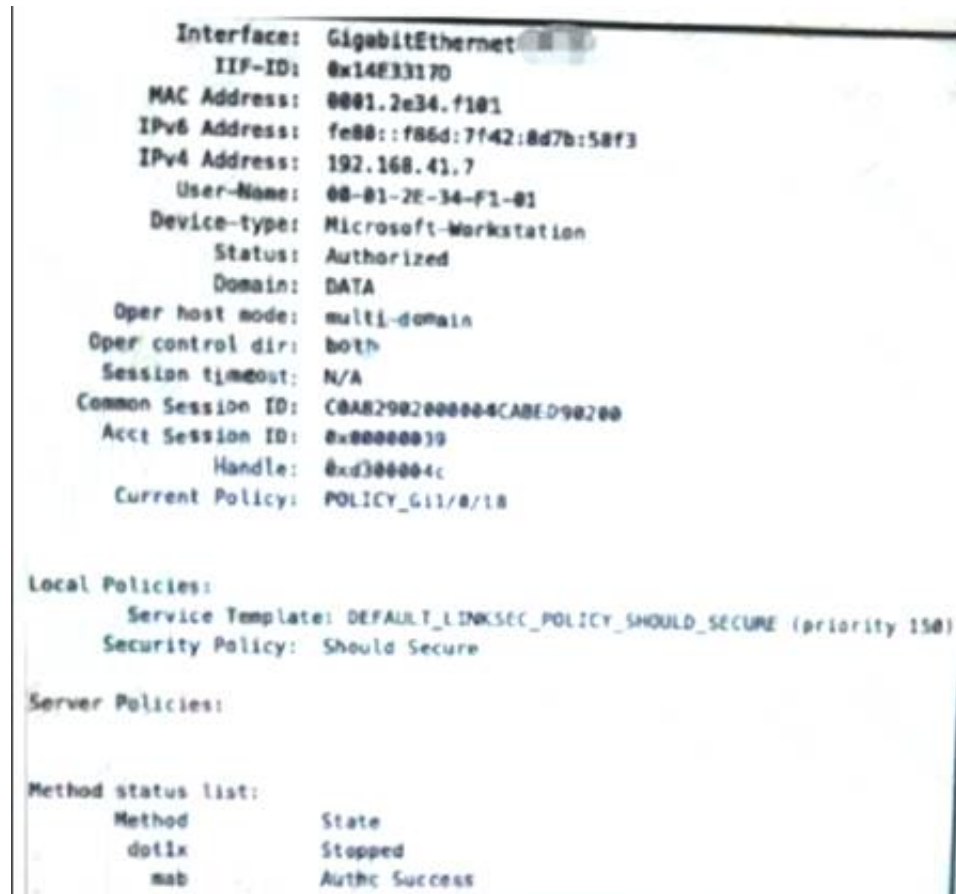
- A. Cisco Identity Services Engine
- B. Cisco AnyConnect with ISE Posture module
- C. Cisco AnyConnect with Network Access Manager module
- D. Cisco AnyConnect with Umbrella Roaming Security module

Answer: D

NEW QUESTION 452

- (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 454

- (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 457

- (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 461

- (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 462

- (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 467

- (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 471

- (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 472

- (Exam Topic 3)

Which feature is used in a push model to allow for session identification, host reauthentication, and session termination?

- A. AAA attributes
- B. CoA request
- C. AV pair
- D. carrier-grade NAT

Answer: C

NEW QUESTION 476

- (Exam Topic 3)

What is a benefit of flexible NetFlow records?

- A. They are used for security
- B. They are used for accounting
- C. They monitor a packet from Layer 2 to Layer 5
- D. They have customized traffic identification

Answer: D

Explanation:

<https://confluence.netvizura.com/display/NVUG/Traditional+vs.+Flexible+NetFlow>

NEW QUESTION 479

- (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 481

- (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 482

- (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 485

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 488

- (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 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 492

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 497

- (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 499

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 500

- (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 504

- (Exam Topic 3)

What is the purpose of the Cisco Endpoint IoC feature?

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

Answer: A

Explanation:

Reference: <https://docs.amp.cisco.com/Cisco%20Endpoint%20IOC%20Attributes.pdf>

The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

NEW QUESTION 507

- (Exam Topic 3)

What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?

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

Answer: D

Explanation:

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

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

NEW QUESTION 508

- (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 513

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 514

- (Exam Topic 3)

An administrator is configuring NTP on Cisco ASA via ASDM and needs to ensure that rogue NTP servers cannot insert themselves as the authoritative time source Which two steps must be taken to accomplish this task? (Choose two)

- A. Specify the NTP version
- B. Configure the NTP stratum
- C. Set the authentication key
- D. Choose the interface for syncing to the NTP server
- E. Set the NTP DNS hostname

Answer: CD

NEW QUESTION 516

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 517

- (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 521

- (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 523

- (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 527

- (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 530

- (Exam Topic 3)

Which system performs compliance checks and remote wiping?

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

Answer: A

NEW QUESTION 531

- (Exam Topic 3)

An engineer is adding a Cisco router to an existing environment. NTP authentication is configured on all devices in the environment with the command `ntp authentication-key 1 md5 Clsc427128380`. There are two routers on the network that are configured as NTP servers for redundancy, 192.168.1.110 and 192.168.1.111. 192.168.1.110 is configured as the authoritative time source. What command must be configured on the new router to use 192.168.1.110 as its primary time source without the new router attempting to offer time to existing devices?

- A. `ntp server 192.168.1.110 primary key 1`
- B. `ntp peer 192.168.1.110 prefer key 1`
- C. `ntp server 192.168.1.110 key 1 prefer`
- D. `ntp peer 192.168.1.110 key 1 primary`

Answer: A

NEW QUESTION 536

- (Exam Topic 3)

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

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

Answer: BE

NEW QUESTION 539

- (Exam Topic 3)

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

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

Answer: CE

NEW QUESTION 543

- (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 545

- (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 549

- (Exam Topic 3)

Why is it important to have a patching strategy for endpoints?

- A. to take advantage of new features released with patches
- B. so that functionality is increased on a faster scale when it is used
- C. so that known vulnerabilities are targeted and having a regular patch cycle reduces risks
- D. so that patching strategies can assist with disabling nonsecure protocols in applications

Answer: C

NEW QUESTION 550

- (Exam Topic 3)

What is an advantage of the Cisco Umbrella roaming client?

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

Answer: C

NEW QUESTION 551

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 554

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 558

- (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 561

- (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 562

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 565

- (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 568

- (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 569

- (Exam Topic 3)

An engineer needs to configure an access control policy rule to always send traffic for inspection without using the default action. Which action should be configured for this rule?

- A. monitor
- B. allow
- C. block
- D. trust

Answer: B

Explanation:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/acce> the first three access control rules in the policy—Monitor, Trust, and Block—cannot inspect matching traffic. Monitor rules track and log but do not inspect network traffic, so the system continues to match traffic against additional rules to determine whether to permit or deny it
<https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/acce>

NEW QUESTION 572

- (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 576

- (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 578

- (Exam Topic 3)

Which two actions does the Cisco Identity Services Engine posture module provide that ensures endpoint security? (Choose two.)

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

Answer: AD

NEW QUESTION 580

- (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 584

- (Exam Topic 3)

Refer to the exhibit.

```
"remarks" [],  
"destinationService" {  
  "kind" serviceKind,  
  "value" destinationService,  
},  
"permit" trueORfalse,  
"active" "true",  
"position" "1",  
"sourceAddress" {  
  "kind" sourceAddressKind,  
  "value" sourceAddress,  
}  
}  
  
req = urllib2.Request(url, json.dumps(post_data), headers)  
base64string = base64.encodestring('%s:%s' % (username, password)).replace("\n", "")  
req.add_header("Authorization", "Basic %s" % base64string)  
try  
    f = urllib2.urlopen(req)  
    status_code = f.getcode()  
  
    print "Status code is "+str(status_code)  
    if status_code == 201:  
        print "Operation successful"  
    except urllib2.HTTPError, err:  
        print "Error received from server HTTP Status code "+str(err.code)  
    try  
        json_error = json.loads(err.read())  
    if json_error:  
        print json.dumps(json_error, sort_keys=True, indent=4, separators=(',', ' '))  
    except ValueError:  
        pass  
    finally  
        if f: f.close()
```

What is the function of the Python script code snippet for the Cisco ASA REST API?

- A. adds a global rule into policies
- B. changes the hostname of the Cisco ASA
- C. deletes a global rule from policies
- D. obtains the saved configuration of the Cisco ASA firewall

Answer: A

NEW QUESTION 586

- (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 588

- (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 589

- (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 594

- (Exam Topic 3)

An engineer is configuring Dropbox integration with Cisco Cloudlock. Which action must be taken before granting API access in the Dropbox admin console?

- A. Authorize Dropbox within the Platform settings in the Cisco Cloudlock portal.
- B. Add Dropbox to the Cisco Cloudlock Authentication and API section in the Cisco Cloudlock portal.
- C. Send an API request to Cisco Cloudlock from Dropbox admin portal.
- D. Add Cisco Cloudlock to the Dropbox admin portal.

Answer: A

NEW QUESTION 596

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 598

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 599

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 603

- (Exam Topic 3)

Which Cisco security solution determines if an endpoint has the latest OS updates and patches installed on the system?

- A. Cisco Endpoint Security Analytics
- B. Cisco AMP for Endpoints
- C. Endpoint Compliance Scanner
- D. Security Posture Assessment Service

Answer: A

NEW QUESTION 607

- (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)

Which two parameters are used for device compliance checks? (Choose two.)

- A. endpoint protection software version
- B. Windows registry values
- C. DHCP snooping checks
- D. DNS integrity checks
- E. device operating system version

Answer: CE

NEW QUESTION 617

- (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 620

- (Exam Topic 3)

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

- A. SNORT
- B. NetFlow
- C. SNMP
- D. 802.1X

Answer: B

Explanation:

Application Visibility and control (AVC) supports NetFlow to export application usage and performance statistics. This data can be used for analytics, billing, and security policies.

NEW QUESTION 625

- (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 628

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 632

- (Exam Topic 3)

Which capability is provided by application visibility and control?

- A. reputation filtering
- B. data obfuscation
- C. data encryption
- D. deep packet inspection

Answer: D

NEW QUESTION 637

- (Exam Topic 3)

What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?

- A. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not
- B. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA.
- C. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA
- D. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA

Answer: A

NEW QUESTION 642

- (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 646

- (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 648

- (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 652

- (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 656

- (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 657

- (Exam Topic 3)

What is a benefit of using a multifactor authentication strategy?

- A. It provides visibility into devices to establish device trust.

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

Answer: D

NEW QUESTION 661

- (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 664

- (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 666

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 671

- (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 676

- (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 679

- (Exam Topic 3)

What is a description of microsegmentation?

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

Answer: A

NEW QUESTION 683

- (Exam Topic 2)

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

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

Answer: AD

Explanation:

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

NEW QUESTION 686

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 350-701 Exam with Our Prep Materials Via below:

<https://www.certleader.com/350-701-dumps.html>