Cisco.350-701.v2023-09-13.q261

Exam Code:	350-701
Exam Name:	Implementing and Operating Cisco Security Core Technologies
Certification Provider:	Cisco
Free Question Number:	261
Version:	v2023-09-13
# of views:	1518
# of Questions views:	2610
https://www.freepdfdumps.com/Cisco.350-701.v2023-09-13.q261.html	

NEW QUESTION: 1
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. No other applications except Cisco Umbrella can write to the S3 bucket
B. It can grant third-party SIEM integrations write access to the S3 bucket
C. It is included m the license cost for the multi-org console of Cisco Umbrella
D. Data can be stored offline for 30 days.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
A network engineer is configuring DMVPN and entered the crypto isakmp key cisc0380739941 address 0.0.0.0 command on host A.
The tunnel is not being established to hostB. What action is needed to authenticate the VPN?
A. Enter the same command on hostB.
B. Enter the command with a different password on hostB.
C. Change isakmp to ikev2 in the command on hostA.
D. Change the password on hostA to the default password.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
What must be used to share data between multiple security products?
A. Cisco Stealthwatch Cloud
B. Cisco Platform Exchange Grid
C. Cisco Rapid Threat Containment
D. Cisco Advanced Malware Protection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4

Which feature does the IaaS model provide?
A. automatic updates and patching of software
B. software-defined network segmentation
C. dedicated, restricted workstations
D. granular control of data
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which feature is used in a push model to allow for session identification, host reauthentication, and session termination?
A. AAA attributes
B. AV pair
C. carrier-grade NAT
D. CoA request
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?
A. It alerts users when the WSA decrypts their traffic.
B. It provides enhanced HTTPS application detection for AsyncOS.
C. It decrypts HTTPS application traffic for authenticated users.
D. It decrypts HTTPS application traffic for unauthenticated users
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
An organization wants to implement a cloud-delivered and SaaS-based solution to provide visibility and threat detection across the AWS network. The solution must be deployed without software agents and rely on AWS VPC flow logs instead. Which solution meets these requirements?
A. Cisco Umbrella
B. Cisco Cloudlock
C. Cisco Stealthwatch Cloud
D. NetFlow collectors
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
Which parameter is required when configuring a Netflow exporter on a Cisco Router?
A. DSCP value
B. Source interface
C. Exporter name
D. Exporter description
Answer: C (LEAVE A REPLY)
An example of configuring a NetFlow exporter is shown below:
flow exporter Exporter

destination 192.168.100.22
transport udp 2055

NEW QUESTION: 9
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 (LEAVE A REPLY)
https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Secure_Managed_Endpoint.pdf

NEW QUESTION: 10
In which scenario is endpoint-based security the solution?
A. inspecting a password-protected archive
B. performing signature-based application control
C. device profiling and authorization
D. inspecting encrypted traffic
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?
A. It verifies that the endpoint has the latest Microsoft security patches installed.
B. It allows the endpoint to authenticate with 802.1xor MAB.
C. It adds endpoints to identity groups dynamically.
D. It allows CoA to be applied if the endpoint status is compliant.
Answer: (SHOW ANSWER)

NEW QUESTION: 12
What is the purpose of the My Devices Portal in a Cisco ISE environment?
A. to register new laptops and mobile devices
B. to request a newly provisioned mobile device
C. to provision userless and agentless systems
D. to manage and deploy antivirus definitions and patches on systems owned by the end user
Answer: (SHOW ANSWER)
Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network.

NEW QUESTION: 13
What is a functional difference between Cisco AMP for Endpoints and Cisco Umbrella Roaming Client?
A. The Umbrella Roaming Client authenticates users and provides segmentation, and AMP for Endpoints allows only for VPN connectivity

B. The Umbrella Roaming client stops and tracks malicious activity on hosts, and AMP for Endpoints tracks only URL-based threats.
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 (LEAVE A REPLY)

NEW QUESTION: 14
Refer to the exhibit.
What is a result of the configuration?
A. Traffic from the DMZ network is redirected
B. Traffic from the inside network is redirected
C. All TCP traffic is redirected
D. Traffic from the inside and DMZ networks is redirected
Answer: D (LEAVE A REPLY)
The purpose of above commands is to redirect traffic that matches the ACL "redirect-acl" to the Cisco FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and any other actions that are applied by policy are performed, the traffic is returned to the ASA for further processing and ultimate transmission. The command "service-policy global_policy global" applies the policy to all of the interfaces. Reference: https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.html FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and any other actions that are applied by policy are performed, the traffic is returned to the ASA for further processing and ultimate transmission.
The command "service-policy global_policy global" applies the policy to all of the interfaces.
The purpose of above commands is to redirect traffic that matches the ACL "redirect-acl" to the Cisco FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and any other actions that are applied by policy are performed, the traffic is returned to the ASA for further processing and ultimate transmission. The command "service-policy global_policy global" applies the policy to all of the interfaces. Reference: https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.html

NEW QUESTION: 15
Refer to the exhibit.
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 (LEAVE A REPLY)
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: 16
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: (SHOW ANSWER)
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: 17
An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices. The default management port conflicts with other communications on the network and must be changed. What must be done to ensure that all devices can communicate together?
A. Manually change the management port on Cisco FMC and all managed Cisco FTD devices
B. Set the tunnel to go through the Cisco FTD
C. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices
D. Set the tunnel port to 8305
Answer: (SHOW ANSWER)
The FMC and managed devices communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305.
Cisco strongly recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate with each other.

NEW QUESTION: 18
Which kind of API that is used with Cisco DNA Center provisions SSIDs, QoS policies, and update software versions on switches?
A. Intent
B. Event
C. Integration
D. Multivendor
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
How does Cisco Umbrella protect clients when they operate outside of the corporate network?
A. by using the Cisco Umbrella roaming client
B. by modifying the registry for DNS lookups
C. by using Active Directory group policies to enforce Cisco Umbrella DNS servers
D. by forcing DNS queries to the corporate name servers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 20
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 (LEAVE A REPLY)

NEW QUESTION: 21
What are two benefits of using Cisco Duo as an MFA solution? (Choose two.)
A. encrypts data that is stored on endpoints
B. allows for centralized management of endpoint device applications and configurations
C. provides simple and streamlined login experience for multiple applications and users
D. native integration that helps secure applications across multiple cloud platforms or on-premises environments
E. grants administrators a way to remotely wipe a lost or stolen device
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 22
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: (SHOW ANSWER)
Spero analysis examines structural characteristics such as metadata and header information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware.
Reference:
-> 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 Threat Grid 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: 23
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. Map sender !P addresses to a host interface.
B. Enable flagged message handling
C. Deploy an encryption appliance.
D. Provision the email appliance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
Why is it important to implement MFA inside of an organization?
A. To prevent brute force attacks from being successful.
B. To prevent DoS attacks from being successful.
C. To prevent man-the-middle attacks from being successful.
D. To prevent phishing attacks from being successful.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
Drag and drop the common security threats from the left onto the definitions on the right.
Answer:

NEW QUESTION: 26
For a given policy in Cisco Umbrella, how should a customer block website based on a custom list?
A. by adding the website IP addresses to the Cisco Umbrella blocklist
B. by specifying blocked domains in me policy settings
C. by specifying the websites in a custom blocked category
D. by adding the websites to a blocked type destination list
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which Talos reputation center allows for tracking the reputation of IP addresses for email and web traffic?
A. IP Slock List Center
B. AMP Reputation Center
C. File Reputation Center

D. IP and Domain Reputation Center
Answer: D (LEAVE A REPLY)

NEW QUESTION: 28
Why should organizations migrate to an MFA strategy for authentication?
A. Single methods of authentication can be compromised more easily than MFA.
B. Biometrics authentication leads to the need for MFA due to its ability to be hacked easily.
C. MFA does not require any piece of evidence for an authentication mechanism.
D. MFA methods of authentication are never compromised.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
Which Cisco ISE service checks the compliance of endpoints before allowing the endpoints to connect to the network?
A. profiler
B. posture
C. Threat Centric NAC
D. Cisco TrustSec
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
Refer to the exhibit.
The DHCP snooping database resides on router R1, and dynamic ARP inspection is configured only on switch SW2. Which ports must be configured as untrusted so that dynamic ARP inspection operates normally?
A. P5, P6, and P7 only
B. P2 and P3 only
C. P2, P3, and P6 only
D. P1, P2, P3, and P4 only
Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
Which feature requires a network discovery policy on the Cisco Firepower Next Generation Intrusion Prevention System?
A. security intelligence
B. impact flags
C. URL filtering
D. health monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which function is included when Cisco AMP is added to web security?
A. multifactor, authentication-based user identity
B. phishing detection on emails
C. threat prevention on an infected endpoint
D. detailed analytics of the unknown file's behavior
Answer: D (LEAVE A REPLY)

NEW QUESTION: 33
Which two Cisco ISE components must be configured for BYOD? (Choose two.)
A. central WebAuth
B. dual
C. guest
D. null WebAuth
E. local WebAuth
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 34
What are two functions of TAXII in threat intelligence sharing? (Choose two.)
A. determines the "what" of threat intelligence
B. exchanges trusted anomaly intelligence information
C. determines how threat intelligence information is relayed
D. Supports STIX information
E. allows users to describe threat motivations and abilities
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 35
A network engineer entered the snmp-server user asmith myv7 auth sha cisco priv aes 256 cisc0xxxxxxxxx command and needs to send SNMP information to a host at 10.255.255.1. Which command achieves this goal?
A. snmp-server host inside 10.255.255.1 snmpv3 myv7
B. snmp-server host inside 10.255.255.1 snmpv3 asmith
C. snmp-server host inside 10.255.255.1 version 3 myv7
D. snmp-server host inside 10.255.255.1 version 3 asmith
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36

An MDM provides which two advantages to an organization with regards to device management? (Choose two.)
A. critical device management
B. allowed application management
C. network device management
D. Active Directory group policy management
E. asset inventory management
Answer: (SHOW ANSWER)

NEW QUESTION: 37
What are two security benefits of an MDM deployment? (Choose two.)
A. distributed software upgrade
B. on-device content management
C. privacy control checks
D. distributed dashboard
E. robust security policy enforcement
Answer: (SHOW ANSWER)

NEW QUESTION: 38
What is a function of the Layer 4 Traffic Monitor on a Cisco WSA?
A. decrypts SSL traffic to monitor for malicious content
B. monitors suspicious traffic across all the TCP/UDP ports
C. blocks traffic from URL categories that are known to contain malicious content
D. prevents data exfiltration by searching all the network traffic for specified sensitive information
Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
Which type of DNS abuse exchanges data between two computers even when there is no direct connection?
A. Malware installation
B. Command-and-control communication
C. Network footprinting
D. Data exfiltration
Answer: (SHOW ANSWER)
Malware installation: This may be done by hijacking DNS queries and responding with malicious IP addresses.
Command & Control communication: As part of lateral movement, after an initial compromise, DNS communications is abused to communicate with a C2 server. This typically involves making periodic DNS queries from a computer in the target network for a domain controlled by the adversary. The responses contain encoded messages that may be used to perform unauthorized actions in the target network.
Network footprinting: Adversaries use DNS queries to build a map of the network. Attackers live off the terrain so developing a map is important to them.
Data theft (exfiltration): Abuse of DNS to transfer data; this may be performed by tunneling other protocols like FTP, SSH through DNS queries and responses. Attackers make multiple DNS queries from a compromised computer to a domain owned by the adversary. DNS tunneling can also be used for executing commands and transferring malware into the target network.

NEW QUESTION: 40
Refer to the exhibit.
Which command was used to display this output?
A. show dot1x
B. show dot1x all
C. show dot1x all summary
D. show dot1x interface gi1/0/12
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
What are two reasons for implementing a multifactor authentication solution such as Duo Security provide to an organization? (Choose two)
A. flexibility of different methods of 2FA such as phone callbacks, SMS passcodes, and push notifications
B. single sign-on access to on-premises and cloud applications
C. integration with 802.1x security using native Microsoft Windows supplicant
D. secure access to on-premises and cloud applications
E. identification and correction of application vulnerabilities before allowing access to resources
Answer: A,D (LEAVE A REPLY)
Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a second factor (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password.
Note: Single sign-on (SSO) is a property of identity and access management that enables users to securely authenticate with multiple applications and websites by logging in only once with just one set of credentials (username and password). With SSO, the application or website that the user is trying to access relies on a trusted third party to verify that users are who they say they are.

NEW QUESTION: 42
An organization has two machines hosting web applications. Machine 1 is vulnerable to SQL injection while machine 2 is vulnerable to buffer overflows.
What action would allow the attacker to gain access to machine 1 but not machine 2?
A. sniffing the packets between the two hosts
B. overflowing the buffer's memory
C. inserting malicious commands into the database
D. sending continuous pings
Answer: (SHOW ANSWER)

NEW QUESTION: 43
Which Cisco Firewall solution requires zone definition?
A. CBAC
B. Cisco ASA
C. ZBFW
D. Cisco AMP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 44

What Cisco command shows you the status of an 802.1X connection on interface gi0/1?
A. show authorization status
B. show connection status gi0/1
C. show ver gi0/1
D. show authen sess int gi0/1
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two)
A. virtualization
B. middleware
C. operating systems
D. applications
E. data
Answer: D,E (LEAVE A REPLY)
Customers must manage applications and data in PaaS.

NEW QUESTION: 46
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 (LEAVE A REPLY)
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: 47
A company identified a phishing vulnerability during a pentest What are two ways the company can protect employees from the attack? (Choose two.)
A. using Cisco FTD
B. using Cisco ESA
C. using Cisco ISE
D. using an inline IPS/IDS in the network
E. using Cisco Umbrella

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 48
Where are individual sites specified to be blacklisted in Cisco Umbrella?
A. application settings
B. content categories
C. security settings
D. destination lists
Answer: (SHOW ANSWER)
A destination list is a list of internet destinations that can be blocked or allowed based on the administrative preferences for the policies applied to the identities within your organization. A destination is an IP address (IPv4), URL, or fully qualified domain name. You can add a destination list to Umbrella at any time; however, a destination list does not come into use until it is added to a policy.

NEW QUESTION: 49
Drag and drop the cryptographic algorithms for IPsec from the left onto the cryptographic processes on the right.
Answer:

NEW QUESTION: 50
A network engineer has entered the snmp-server user andy myv3 auth sha cisco priv aes 256 cisc0380739941 command and needs to send SNMP information to a host at 10.255.254.1. Which command achieves this goal?
A. snmp-server host inside 10.255.254.1 version 3 andy
B. snmp-server host inside 10.255.254.1 version 3 myv3
C. snmp-server host inside 10.255.254.1 snmpv3 andy
D. snmp-server host inside 10.255.254.1 snmpv3 myv3
Answer: A (LEAVE A REPLY)
The command "snmp-server user user-name group-name [remote ip-address [udp-port port]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]" adds a new user (in this case "andy") to an SNMPv3 group (in this case group name "myv3") and configures a password for the user.
In the "snmp-server host" command, we need to:
+ Specify the SNMP version with key word "version {1 | 2 | 3}"
+ Specify the username ("andy"), not group name ("myv3").
Note: In "snmp-server host inside ..." command, "inside" is the interface name of the ASA interface through which the NMS (located at 10.255.254.1) can be reached.

NEW QUESTION: 51
An engineer configures new features within the Cisco Umbrella dashboard and wants to identify and proxy traffic that is categorized as risky domains and may contain safe and malicious content. Which action accomplishes these objectives?
A. Upload the threat intelligence database to Cisco Umbrella for the most current information on reputations and to have the destination lists block them.
B. Create a new site within Cisco Umbrella to block requests from those categories so they can be sent to the proxy device.
C. Configure intelligent proxy within Cisco Umbrella to intercept and proxy the requests for only those categories.
D. Configure URL filtering within Cisco Umbrella to track the URLs and proxy the requests for those categories and below.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 52
Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)
A. Cisco ISE
B. Cisco TrustSec
C. Cisco DNA Center
D. Cisco Umbrella
E. Cisco Duo Security
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats?
A. PSIRT
B. Talos
C. CSIRT
D. DEVNET
Answer: B (LEAVE A REPLY)
Talos Threat Source is a regular intelligence update from Cisco Talos, highlighting the biggest threats each week and other security news.

NEW QUESTION: 54
Which two activities can be done using Cisco DNA Center? (Choose two)
A. DHCP
B. Design
C. Accounting
D. DNS
E. Provision
Answer: B,E (LEAVE A REPLY)
Cisco DNA Center has four general sections aligned to IT workflows: Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site. Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need. Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task. The profiles (called scalable group tags or

"SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups. Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work. The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- dna-center-so-cte-en.html Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site.
Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need.
Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task.
The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups.
Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work.
The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks.
Cisco DNA Center has four general sections aligned to IT workflows: Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site. Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need.
Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task. The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated

and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups. Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work. The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- dna-center-so-cte-en.html

NEW QUESTION: 55
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 service provider manages the operating system
C. Infrastructure as a Service because the customer manages the operating system
D. Platform as a Service because the service provider manages the operating system
Answer: (SHOW ANSWER)

NEW QUESTION: 56
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. fqdn vpn.sohoroutercompany.com <VPN Peer IP Address>
B. Add the dynamic keyword to the existing crypto map command
C. ip name-server <DNS Server IP Address>
D. crypto isakmp identity hostname
E. ip host vpn.sohoroutercompany.eom <VPN Peer IP Address>
Answer: (SHOW ANSWER)

NEW QUESTION: 57
What does Cisco ISE use to collect endpoint attributes that are used in profiling?
A. probes
B. posture assessment
C. Cisco pxGrid
D. Cisco AnyConnect Secure Mobility Client
Answer: A (LEAVE A REPLY)

NEW QUESTION: 58
What is the benefit of installing Cisco AMP for Endpoints on a network?
A. It protects endpoint systems through application control and real-time scanning
B. It provides flow-based visibility for the endpoints network connections.

C. It provides operating system patches on the endpoints for security.
D. It enables behavioral analysis to be used for the endpoints.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
What are two characteristics of Cisco DNA Center APIs? (Choose two.)
A. They do not support Python scripts.
B. They view the overall health of the network
C. They quickly provision new devices.
D. Postman is required to utilize Cisco DNA Center API calls.
E. They are Cisco proprietary.
Answer: (SHOW ANSWER)

NEW QUESTION: 60
How does Cisco AMP for Endpoints provide next-generation protection?
A. It integrates with Cisco FTD devices.
B. It leverages an endpoint protection platform and endpoint detection and response.
C. It encrypts data on user endpoints to protect against ransomware.
D. It utilizes Cisco pxGrid, which allows Cisco AMP to pull threat feeds from threat intelligence centers.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 61
What is a prerequisite when integrating a Cisco ISE server and an AD domain?
A. Place the Cisco ISE server and the AD server in the same subnet
B. Configure a common administrator account
C. Configure a common DNS server
D. Synchronize the clocks of the Cisco ISE server and the AD server
Answer: D (LEAVE A REPLY)
The following are the prerequisites to integrate Active Directory with Cisco ISE.
+ Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI.
+ If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation.
+ You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE.
Reference:
/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F

NEW QUESTION: 62
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. private VLANs
C. Dynamic ARP Inspection
D. Reverse ARP
Answer: (SHOW ANSWER)

NEW QUESTION: 63
What is a characteristic of Firepower NGIPS inline deployment mode?
A. ASA with Firepower module cannot be deployed.
B. It must have inline interface pairs configured.
C. It cannot take actions such as blocking traffic.
D. It is out-of-band from traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
A company recently discovered an attack propagating throughout their Windows network via a file named abc428565580xyz exe The malicious file was uploaded to a Simple Custom Detection list in the AMP for Endpoints Portal and the currently applied policy for the Windows clients was updated to reference the detection list Verification testing scans on known infected systems shows that AMP for Endpoints is not detecting the presence of this file as an indicator of compromise What must be performed to ensure detection of the malicious file?
A. Upload the SHA-256 hash for the file to the Simple Custom Detection List
B. Use an Advanced Custom Detection List instead of a Simple Custom Detection List
C. Upload the malicious file to the Blocked Application Control List
D. Check the box in the policy configuration to send the file to Cisco Threat Grid for dynamic analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
What are two Trojan malware attacks? (Choose two)
A. frontdoor
B. smurf
C. sync
D. backdoor
E. rootkit

Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 66
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 Reauth
C. CoA Terminate
D. CoA Session Query
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?
A. OpenIOC
B. CybOX
C. OpenC2
D. STIX
Answer: D (LEAVE A REPLY)

NEW QUESTION: 68
Under which two circumstances is a CoA issued? (Choose two)
A. A new authentication rule was added to the policy on the Policy Service node.
B. An endpoint is deleted on the Identity Service Engine server.
C. A new Identity Source Sequence is created and referenced in the authentication policy.
D. An endpoint is profiled for the first time.
E. A new Identity Service Engine server is added to the deployment with the Administration persona
Answer: B,D (LEAVE A REPLY)
The profiling service issues the change of authorization in the following cases:
- Endpoint deleted-When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network.
An exception action is configured-If you have an exception action configured per profile that leads to an unusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to the corresponding static profile by issuing a CoA.
- An endpoint is profiled for the first time-When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.
+ An endpoint identity group has changed-When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.
The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:
++ The endpoint identity group changes for endpoints when they are dynamically profiled
++ The endpoint identity group changes when the static assignment flag is set to true for a dynamic endpoint - An endpoint profiling policy has changed and the policy is used in an authorization policy-When an endpoint profiling policy changes, and the policy is included in a logical profile that is used in an authorization policy. The endpoint profiling policy may change due to the profiling policy match or when an endpoint is statically assigned to an endpoint

profiling policy, which is associated to a logical profile. In both the cases, the profiling service issues a CoA, only when the endpoint profiling policy is used in an authorization policy.
Reference:
b_ise_admin_guide_20_chapter_010100.html

NEW QUESTION: 69
How is Cisco Umbrella configured to log only security events?
A. per policy
B. in the Reporting settings
C. in the Security Settings section
D. per network in the Deployments section
Answer: A (LEAVE A REPLY)
The logging of your identities' activities is set per-policy when you first create a policy. By default, logging is on and set to log all requests an identity makes to reach destinations. At any time after you create a policy, you can change what level of identity activity Umbrella logs.
From the Policy wizard, log settings are:
Log All Requests-For full logging, whether for content, security or otherwise Log Only Security Events-For security logging only, which gives your users more privacy-a good setting for people with the roaming client installed on personal devices Don't Log Any Requests-Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on.

NEW QUESTION: 70
Which risk is created when using an Internet browser to access cloud-based service?
A. vulnerabilities within protocol
B. insecure implementation of API
C. misconfiguration of infrastructure, which allows unauthorized access
D. intermittent connection to the cloud connectors
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71
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 (LEAVE A REPLY)
The command "crypto isakmp identity address 172.19.20.24" is not valid. We can only use "crypto isakmp identity {address | hostname}. The following example uses preshared keys at two peers and sets both their ISAKMP identities to the IP address.
At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified:
crypto isakmp identity address
crypto isakmp key sharedkeystring address 192.168.1.33

At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified:
crypto isakmp identity address
crypto isakmp key sharedkeystring address 10.0.0.1
Reference:
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 ca identity CA-Server" -> Answer A is not correct.
Only answer B is the best choice left.

NEW QUESTION: 72
Which two authentication protocols are supported by the Cisco WSA? (Choose two.)
A. NTLM
B. SSL
C. LDAP
D. TLS
E. WCCP
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 73
Which technology reduces data loss by identifying sensitive information stored in public computing environments?
A. Cisco HyperFlex
B. Cisco SDA
C. Cisco Cloudlock
D. Cisco Firepower
Answer: C (LEAVE A REPLY)

NEW QUESTION: 74
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 (LEAVE A REPLY)
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: 75
Refer to the exhibit.

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

A. NTP authentication is not enabled.

B. The router was not rebooted after the NTP configuration updated.

C. The key was configured in plain text.

D. The hashing algorithm that was used was MD5. which is unsupported.

Answer: (SHOW ANSWER)

NEW QUESTION: 76

Which Cisco AMP file disposition valid?

A. malware

B. non malicious

C. dirty

D. pristine

Answer: A (LEAVE A REPLY)

NEW QUESTION: 77

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 (LEAVE A REPLY)

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 forsmall devices.

NEW QUESTION: 78

Which technology provides a combination of endpoint protection endpoint detection, and response?

A. Cisco AMP

B. Cisco Threat Grid

C. Cisco Umbrella

D. Cisco Talos

Answer: A (LEAVE A REPLY)

NEW QUESTION: 79

Refer to the exhibit.
Which statement about the authentication protocol used in the configuration is true?
A. The authentication request contains only a password
B. The authentication request contains only a username
C. The authentication and authorization requests are grouped in a single packet
D. There are separate authentication and authorization request packets
Answer: C (LEAVE A REPLY)
This command uses RADIUS which combines authentication and authorization in one function (packet).

NEW QUESTION: 80
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: B,C (LEAVE A REPLY)
What Cisco DNA Center enables you to do Automate: Save time by using a single dashboard to manage and automate your network. Quickly scale your business with intuitive workflows and reusable templates. Configure and provision thousands of network devices across your enterprise in minutes, not hours. Secure policy: Deploy group-based secure access and network segmentation based on business needs. With Cisco DNA Center, you apply policy to users and applications instead of to your network devices. Automation reduces manual operations and the costs associated with human errors, resulting in more uptime and improved security. Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent. Assurance: Monitor, identify, and react in real time to changing network and wireless conditions. Cisco DNA Center uses your network's wired and wireless devices to create sensors everywhere, providing real-time feedback based on actual network conditions. The Cisco DNA Assurance engine correlates network sensor insights with streaming telemetry and compares this with the current context of these data sources. With a quick check of the health scores on the Cisco DNA Center dashboard, you can see where there is a performance issue and identify the most likely cause in minutes. Extend ecosystem: With the new Cisco DNA Center platform, IT can now integrate Cisco solutions and thirdparty technologies into a single network operation for streamlining IT workflows and increasing business value and innovation. Cisco DNA Center allows you to run the network with open interfaces with IT and business applications, integrates across IT operations and technology domains, and can manage heterogeneous network devices. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- cisco-dna-center-aag-cte-en.html Automate: Save time by using a single dashboard to manage and automate your network. Quickly scale your business with intuitive workflows and reusable templates. Configure and provision thousands of network devices across your enterprise in minutes, not hours.
Secure policy: Deploy group-based secure access and network segmentation based on business needs. With Cisco DNA Center, you apply policy to users and applications instead of to your network devices. Automation reduces manual operations and the costs associated with human errors, resulting in more uptime and improved security. Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent.
Assurance: Monitor, identify, and react in real time to changing network and wireless conditions. Cisco DNA Center uses your network's wired and wireless devices to create sensors everywhere, providing real-time feedback based on actual network conditions. The Cisco DNA Assurance engine correlates network sensor insights with streaming telemetry and compares this with the current context of these data sources. With a quick check of the health scores on the Cisco DNA Center dashboard, you can see where there is a performance issue and identify the most likely cause in minutes.

Extend ecosystem: With the new Cisco DNA Center platform, IT can now integrate Cisco solutions and thirdparty technologies into a single network operation for streamlining IT workflows and increasing business value and innovation. Cisco DNA Center allows you to run the network with open interfaces with IT and business applications, integrates across IT operations and technology domains, and can manage heterogeneous network devices.
What Cisco DNA Center enables you to do Automate: Save time by using a single dashboard to manage and automate your network. Quickly scale your business with intuitive workflows and reusable templates. Configure and provision thousands of network devices across your enterprise in minutes, not hours. Secure policy: Deploy group-based secure access and network segmentation based on business needs. With Cisco DNA Center, you apply policy to users and applications instead of to your network devices. Automation reduces manual operations and the costs associated with human errors, resulting in more uptime and improved security. Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent. Assurance: Monitor, identify, and react in real time to changing network and wireless conditions. Cisco DNA Center uses your network's wired and wireless devices to create sensors everywhere, providing real-time feedback based on actual network conditions. The Cisco DNA Assurance engine correlates network sensor insights with streaming telemetry and compares this with the current context of these data sources. With a quick check of the health scores on the Cisco DNA Center dashboard, you can see where there is a performance issue and identify the most likely cause in minutes. Extend ecosystem: With the new Cisco DNA Center platform, IT can now integrate Cisco solutions and thirdparty technologies into a single network operation for streamlining IT workflows and increasing business value and innovation. Cisco DNA Center allows you to run the network with open interfaces with IT and business applications, integrates across IT operations and technology domains, and can manage heterogeneous network devices. 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: 81
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: (SHOW ANSWER)
Reference:
The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

NEW QUESTION: 82
An administrator is configuring a DHCP server to better secure their environment. They need to be able to ratelimit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?
A. Set a trusted interface for the DHCP server
B. Set the DHCP snooping bit to 1
C. Add entries in the DHCP snooping database
D. Enable ARP inspection for the required VLAN
Answer: A (LEAVE A REPLY)
To understand DHCP snooping we need to learn about DHCP spoofing attack first.
DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle".

The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.
DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.
Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.

NEW QUESTION: 83
What is a feature of NetFlow Secure Event Logging?
A. It supports v5 and v8 templates.
B. It filters NSEL events based on the traffic and event type through RSVP.
C. It exports only records that indicate significant events in a flow.
D. It delivers data records to NSEL collectors through NetFlow over TCP only.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 84
Which security solution is used for posture assessment of the endpoints in a BYOD solution?
A. Cisco ASA
B. Cisco ISE
C. Cisco FTD
D. Cisco Umbrella
Answer: B (LEAVE A REPLY)

NEW QUESTION: 85
Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?
A. IP and Domain Reputation Center
B. File Reputation Center
C. AMP Reputation Center
D. IP Blacklist Center
Answer: (SHOW ANSWER)

NEW QUESTION: 86
Which direction do attackers encode data in DNS requests during exfiltration using DNS tunneling?
A. outbound
B. inbound
C. north-south
D. east-west
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which action must be taken in the AMP for Endpoints console to detect specific MD5 signatures on endpoints and then quarantine the files?

A. Configure a simple custom detection list
B. Configure an IP Block & Allow custom detection list
C. Configure an application custom detection list
D. Configure an advanced custom detection list.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 88
What must be enabled to secure SaaS-based applications?
A. application security gateway
B. end-to-end encryption
C. two-factor authentication
D. modular policy framework
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.)
A. Create NTLM or Kerberos authentication realm and enable transparent user identification.
B. Create an LDAP authentication realm and disable 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 dent IP address is recorded in this server.
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Which metric is used by the monitoring agent to collect and output packet loss and jitter information?
A. OTCP performance
B. RTP performance
C. WSAv performance
D. AVC performance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 91
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. Put all company users in the trusted segment of NGFW and put all servers to the DMZ segment of the Cisco NGFW. ni
B. Segment different departments to different IP blocks and enable Dynamic ARp inspection on all VLANs
C. Ensure that a user cannot enter the network of another department.
D. Perform a posture check to allow only network access to (hose Windows devices that are already patched.
E. Ensure that noncompliant endpoints are segmented off to contain any potential damage.
Answer: (SHOW ANSWER)

NEW QUESTION: 92
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 key 1 primary
C. ntp server 192.168.1.110 key 1 prefer
D. ntp peer 192.168.1.110 prefer key 1
Answer: A (LEAVE A REPLY)

NEW QUESTION: 93
Which Cisco solution integrates Encrypted Traffic Analytics to perform enhanced visibility, promote compliance, shorten response times, and provide administrators with the information needed to provide educated and automated decisions to secure the environment?
A. Cisco DNA Center
B. Cisco ISE
C. Cisco Security Compliance Solution
D. Cisco SDN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94
Which cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group?
A. Hybrid
B. Community
C. Private
D. Public
Answer: (SHOW ANSWER)
Community Cloud allows system and services to be accessible by group of organizations. It shares the infrastructure between several organizations from a specific community. It may be managed internally by organizations or by the third-party.

NEW QUESTION: 95
Which two preventive measures are used to control cross-site scripting? (Choose two.)
A. Disable cookie inspection in the HTML inspection engine.
B. Run untrusted HTML input through an HTML sanitization engine.
C. Enable client-side scripts on a per-domain basis.

D. SameSite cookie attribute should not be used.
E. Incorporate contextual output encoding/escaping.
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 96
Refer to the exhibit.
Which type of authentication is in use?
A. LDAP authentication for Microsoft Outlook
B. POP3 authentication
C. SMTP relay server authentication
D. external user and relay mail authentication
Answer: A (LEAVE A REPLY)
The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.
Reference:
The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

NEW QUESTION: 97
Which two descriptions of AES encryption are true? (Choose two.)
A. AES can use a 256-bit key for encryption.
B. AES is more secure than 3DES
C. AES can use a 168-bit key for encryption.
D. AES encrypts and decrypts a key three times in sequence
E. AES is less secure than 3DES
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 98
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. Isolation
B. Simple Custom Detection
C. Blocked Application
D. Advanced Custom Detection
Answer: (SHOW ANSWER)

NEW QUESTION: 99
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 reputation scores of 3-5 will be blocked.
C. Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked.
D. Only URLs for botnets with a reputation score of 3 will be blocked.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100
An organization must add new firewalls to its infrastructure and wants to use Cisco ASA or Cisco FTD.
The chosen firewalls must provide methods of blocking traffic that include offering the user the option to bypass the block for certain sites after displaying a warning page and to reset the connection. Which solution should the organization choose?
A. Cisco ASA because it allows for interactive blocking and blocking with reset to be configured via the GUI, whereas Cisco FTD does not.
B. Cisco FTD because it enables interactive blocking and blocking with reset natively, whereas Cisco ASA does not
C. Cisco ASA because it has an additional module that can be installed to provide multiple blocking capabilities, whereas Cisco FTD does not.
D. Cisco FTD because it supports system rate level traffic blocking, whereas Cisco ASA does not
Answer: (SHOW ANSWER)

NEW QUESTION: 101
Which algorithm is an NGE hash function?
A. SISHA-2
B. SHA-1
C. HMAC
D. MD5
Answer: (SHOW ANSWER)

NEW QUESTION: 102
How does the Cisco WSA enforce bandwidth restrictions for web applications?
A. It sends commands to the uplink router to apply traffic policing to the application traffic.
B. It implements a policy route to redirect application traffic to a lower-bandwidth link.
C. It simulates a slower link by introducing latency into application traffic.
D. It dynamically creates a scavenger class QoS policy and applies it to each client that connects through the WSA.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 103
Drag and drop the deployment models from the left onto the explanations on the right.
Answer:

NEW QUESTION: 104
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 (LEAVE A REPLY)
Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco's Firepower next generation firewall. The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure. In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet. In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions. Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/ white-paper-c11-740505.html The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure.
In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet.
In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions.
Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco's Firepower next generation firewall. The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure. In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet. In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions. Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/ white-paper-c11-740505.html

NEW QUESTION: 105
What features does Cisco FTDv provide over ASAv?
A. Cisco FTDv runs on VMWare while ASAv does not
B. Cisco FTDv supports URL filtering while ASAv does not
C. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not
D. Cisco FTDv runs on AWS while ASAv does not
Answer: B (LEAVE A REPLY)

NEW QUESTION: 106
The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?
A. SDN controller and the management solution
B. SDN controller and the cloud
C. management console and the SDN controller
D. management console and the cloud
Answer: A (LEAVE A REPLY)

NEW QUESTION: 107
What is a difference between DMVPN and sVTI?
A. DMVPN supports dynamic tunnel establishment, whereas sVTI does not.
B. DMVPN provides interoperability with other vendors, whereas sVTI does not.
C. DMVPN supports static tunnel establishment, whereas sVTI does not.
D. DMVPN supports tunnel encryption, whereas sVTI does not.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
What is a characteristic of an EDR solution and not of an EPP solution?
A. retrospective analysis
B. stops all ransomware attacks
C. performs signature-based detection
D. decrypts SSL traffic for better visibility
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.
Answer:

NEW QUESTION: 110
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. Endpoint Trust List
B. Secured Collaboration Proxy
C. Enterprise Proxy Service
D. Certificate Trust List
Answer: D (LEAVE A REPLY)

NEW QUESTION: 111
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 (LEAVE A REPLY)
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: 112
After a recent breach, an organization determined that phishing was used to gain initial access to the network before regaining persistence. The information gained from the phishing attack was a result of users visiting known malicious websites. What must be done in order to prevent this from happening in the future?
A. Modify an access policy
B. Modify identification profiles
C. Modify outbound malware scanning policies
D. Modify web proxy settings
Answer: D (LEAVE A REPLY)
URL conditions in access control rules allow you to limit the websites that users on your network can access. This feature is called URL filtering. There are two ways you can use access control to specify URLs you want to block (or, conversely, allow):
- With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic.
- With a URL Filtering license, you can also control access to websites based on the URL's general classification, or category, and risk level, or reputation. The system displays this category and reputation data in connection logs, intrusion events, and application details.
Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies.

NEW QUESTION: 113
An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1 1 11 using the flow record Stea! thwatch406397954 command Which additional command is required to complete the flow record?
A. destination 1.1.1.1
B. match ipv4 ttl
C. transport udp 2055
D. cache timeout active 60
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
Which ESA implementation method segregates inbound and outbound email?
A. pair of logical listeners on a single physical interface with two unique logical IPv4 addresses and one IPv6 address
B. pair of logical IPv4 listeners and a pair Of IPv6 listeners on two physically separate interfaces
C. one listener on a single physical Interface
D. one listener on one logical IPv4 address on a single logical interface
Answer: D (LEAVE A REPLY)

NEW QUESTION: 115
What is a characteristic of Dynamic ARP Inspection?
A. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCP snooping binding database
B. In a typical network, make all ports as trusted except for the ports connecting to switches, which are untrusted.
C. DAI associates a trust state with each switch.

D. DAI intercepts all ARP requests and responses on trusted ports only
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps.
Which two actions must be taken to ensure that interfaces are put back into service? (Choose two)
A. Have Cisco Prime Infrastructure issue an SNMP set command to re-enable the ports after the pre configured interval.
B. Use EEM to have the ports return to service automatically in less than 300 seconds.
C. Enter the shutdown and no shutdown commands on the interfaces.
D. Enable the snmp-server enable traps command and wait 300 seconds
E. Ensure that interfaces are configured with the error-disable detection and recovery feature
Answer: (SHOW ANSWER)
You can also bring up the port by using these commands:
+ The "shutdown" interface configuration command followed by the "no shutdown" interface configuration command restarts the disabled port.
+ The "errdisable recovery cause ..." global configuration command enables the timer to automatically recover error-disabled state, and the "errdisable recovery interval interval" global configuration command specifies the time to recover error-disabled state.

NEW QUESTION: 117
What provides visibility and awareness into what is currently occurring on the network?
A. CMX
B. WMI
C. Prime Infrastructure
D. Telemetry
Answer: (SHOW ANSWER)
Telemetry - Information and/or data that provides awareness and visibility into what is occurring on the network at any given time from networking devices, appliances, applications or servers in which the core function of the device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks.

NEW QUESTION: 118
Which threat involves software being used to gain unauthorized access to a computer system?
A. NTP amplification
B. virus
C. ping of death
D. HTTP flood
Answer: (SHOW ANSWER)

NEW QUESTION: 119
Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?
A. File Analysis
B. SafeSearch
C. SSL Decryption

D. Destination Lists
Answer: (SHOW ANSWER)
SSL Decryption is an important part of the Umbrella Intelligent Proxy. he feature allows the Intelligent Proxy to go beyond simply inspecting normal URLs and actually proxy and inspect traffic that's sent over HTTPS. The SSL Decryption feature does require the root certificate be installed.

NEW QUESTION: 120
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 (LEAVE A REPLY)
Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay.
Reference:
Cisco_SBA_BN_EmailSecurityUsingCiscoESADeploymentGuide-Feb2013.pdf

NEW QUESTION: 121
What is the target in a phishing attack?
A. web server
B. endpoint
C. IPS
D. perimeter firewall
Answer: B (LEAVE A REPLY)

NEW QUESTION: 122
Which attribute has the ability to change during the RADIUS CoA?
A. NTP
B. Authorization
C. Accessibility
D. Membership
Answer: B (LEAVE A REPLY)
The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated.

Reference:
sy-book/sec-rad-coa.html

NEW QUESTION: 123
Which two capabilities of Integration APIs are utilized with Cisco DNA center? (Choose two)
A. Create new SSIDs on a wireless LAN controller
B. Third party reporting
C. Connect to ITSM platforms
D. Automatically deploy new virtual routers
E. Upgrade software on switches and routers
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 124
I I
An engineer musiet up 200 new laptops on a network and wants to prevent the users from moving their laptops around to simplify administration Which switch port MAC address security setting must be used?
A. static
B. maximum
C. aging
D. sticky
Answer: (SHOW ANSWER)

NEW QUESTION: 125
What is the function of SDN southbound API protocols?
A. to allow for the dynamic configuration of control plane applications
B. to enable the controller to make changes
C. to enable the controller to use REST
D. to allow for the static configuration of control plane applications
Answer: (SHOW ANSWER)
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs. Reference:
https://www.ciscopress.com/articles/article.asp?p=3004581&seqNum=2 scalability needs.
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs. Reference:
https://www.ciscopress.com/articles/article.asp?p=3004581&seqNum=2
Note: Southbound APIs helps us communicate with data plane (not control plane) applications

NEW QUESTION: 126
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 ransom ware infection? (Choose two)
A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.
B. Set up a profiling policy in Cisco Identity Service Engine to check and endpoint patch level before allowing access on the network.
C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.

D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.
E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.
Answer: A,C (LEAVE A REPLY)
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.

NEW QUESTION: 127
Which benefit does endpoint security provide the overall security posture of an organization?
A. It allows the organization to mitigate web-based attacks as long as the user is active in the domain
B. It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.
C. It allows the organization to detect and respond to threats at the edge of the network
D. It streamlines the incident response process to automatically perform digital forensics on the endpoint
Answer: B (LEAVE A REPLY)

NEW QUESTION: 128
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 (LEAVE A REPLY)
The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:
+ Shell code execution: Looks for the patterns used by shell code.
+ Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.
+ Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts.
Using these, it can detect Meltdown, Spectre, and other cache-timing attacks.
+ Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping).
+ User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods.
+ Interesting file access: Cisco Tetration platform can be armed to look at sensitive files.
+ File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user.
+ Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform.

NEW QUESTION: 129
Why is it important for the organization to have an endpoint patching strategy?
A. so the internal PSIRT organization is aware of the latest bugs
B. so the latest security fixes are installed on the endpoints
C. so the network administrator is notified when an existing bug is encountered
D. so the organization can identify endpoint vulnerabilities

Answer: (SHOW ANSWER)

NEW QUESTION: 130
What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?
A. Indicators of Compromise
B. trusted automated exchange
C. The Exploit Database
D. threat intelligence
Answer: D (LEAVE A REPLY)

NEW QUESTION: 131
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 with PxGrid services enabled
B. Cisco Stealthwatch and Cisco Identity Services Engine integration
C. Cisco ASA firewall with Dynamic Access Policies configured
D. Cisco Identity Services Engine and AnyConnect Posture module
Answer: D (LEAVE A REPLY)

NEW QUESTION: 132
Which endpoint protection and detection feature performs correlation of telemetry, files, and intrusion events that are flagged as possible active breaches?
A. elastic search
B. file trajectory
C. indication of compromise
D. retrospective detection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 133
Which feature enables a Cisco ISR to use the default bypass list automatically for web filtering?
A. company key
B. group key
C. filters
D. connector
Answer: D (LEAVE A REPLY)

NEW QUESTION: 134
Which RADIUS feature provides a mechanism to change the AAA attributes of a session after it is authenticated?
A. Accounting
B. Authorization

C. CoA
D. Authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 135
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: (SHOW ANSWER)
Because MAB uses the MAC address as a username and password, you should make sure that the RADIUS server can differentiate MAB requests from other types of requests for network access. This precaution will prevent other clients from attempting to use a MAC address as a valid credential. Cisco switches uniquely identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB Access-Request message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server.

NEW QUESTION: 136
What is the term for the concept of limiting communication between applications or containers on the same node?
A. microservicing
B. microsegmentation
C. container orchestration
D. software-defined access
Answer: (SHOW ANSWER)

NEW QUESTION: 137
Which Cisco cloud security software centrally manages policies on multiple platforms such as Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS?
A. Cisco Configuration Professional
B. Cisco Defense Orchestrator
C. Cisco Secureworks
D. Cisco DNAC
Answer: B (LEAVE A REPLY)

NEW QUESTION: 138
Which feature within Cisco ISE verifies the compliance of an endpoint before providing access to the network?
A. pxGrid

B. Profiling
C. Posture
D. MAB
Answer: (SHOW ANSWER)

NEW QUESTION: 139
What is a capability of Cisco ASA Netflow?
A. It filters NSEL events based on traffic
B. It generates NSEL events even if the MPF is not configured
C. It logs all event types only to the same collector
D. It sends NetFlow data records from active and standby ASAs in an active standby failover pair
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01101.html Policy Order The order in which policies are listed in a policy table determines the priority with which they are applied to Web requests. Web requests are checked against policies beginning at the top of the table and ending at the first policy matched. Any policies below that point in the table are not processed. If no user-defined policy is matched against a Web request, then the global policy for that policy type is applied. Global policies are always positioned last in Policy tables and cannot be re-ordered.

NEW QUESTION: 140
Which type of data does the Cisco Stealthwatch system collect and analyze from routers, switches, and firewalls?
A. NetFlow
B. SNMP
C. syslog
D. NTP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 141
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 (LEAVE A REPLY)

NEW QUESTION: 142
Using Cisco Firepower's Security Intelligence policies, upon which two criteria is Firepower block based?
(Choose two)
A. URLs
B. protocol IDs
C. IP addresses

D. MAC addresses
E. port numbers
Answer: (SHOW ANSWER)
Security Intelligence Sources
...
Custom Block lists or feeds (or objects or groups)
Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects or groups.)
For example, if you become aware of malicious sites or addresses that are not yet blocked by a feed, add these sites to a custom Security Intelligence list and add this custom list to the Block list in the Security Intelligence tab of your access control policy.

NEW QUESTION: 143
Which IETF attribute is supported for the RADIUS CoA feature?
A. 81 Message-Authenticator
B. 42 Acct-Session-ID
C. 30 Calling-Station-ID
D. 24 State
Answer: D (LEAVE A REPLY)

NEW QUESTION: 144
Which command enables 802.1X globally on a Cisco switch?
A. aaa new-model
B. dot1x pae authenticator
C. dot1x system-auth-control
D. authentication port-control aut
Answer: C (LEAVE A REPLY)

NEW QUESTION: 145
Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.
Answer:

NEW QUESTION: 146
Which two statements about a Cisco WSA configured in Transparent mode are true? (Choose two.)
A. It requires a PAC file for the client web browser.
B. It can handle explicit HTTP requests.
C. WCCP v2-enabled devices can automatically redirect traffic destined to port 80.
D. It requires a proxy for the client web browser.
E. Layer 4 switches can automatically redirect traffic destined to port 80.
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 147
Which two protocols must be configured to authenticate end users to the Cisco WSA? (Choose two.)

A. CHAP
B. NTLMSSP
C. RADIUS
D. TACACS+
E. Kerberos
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 148
An engineer is trying to decide whether to use Cisco Umbrella, Cisco CloudLock, Cisco Stealthwatch, or Cisco AppDynamics Cloud Monitoring for visibility into data transfers as well as protection against data exfiltration Which solution best meets these requirements?
A. Cisco Umbrella
B. Cisco AppDynamics Cloud Monitoring
C. Cisco CloudLock
D. Cisco Stealthwatch
Answer: D (LEAVE A REPLY)

NEW QUESTION: 149
Which CLI command is used to register a Cisco FirePower sensor to Firepower Management Center?
A. configure manager <key> add host
B. configure manager add <host><key
C. configure manager delete
D. configure system add <host><key>
Answer: B (LEAVE A REPLY)

NEW QUESTION: 150
When network telemetry is implemented, what is important to be enabled across all network infrastructure devices to correlate different sources?
A. DNS
B. CDP
C. NTP
D. syslog
Answer: C (LEAVE A REPLY)

NEW QUESTION: 151
How does a WCCP-configured router identify if the Cisco WSA is functional?
A. The router sends a Here-I-Am message every 10 seconds, and the WSA acknowledges with an ISee-You message.
B. The WSA sends a Here-I-Am message every 10 seconds, and the router acknowledges with an ISee-You message.
C. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the WSA.
D. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the router.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 152
Which solution for remote workers enables protection, detection, and response on the endpoint against known and unknown threats?
A. Cisco Duo
B. Cisco AMP for Endpoints
C. Cisco AnyConnect
D. Cisco Umbrella
Answer: B (LEAVE A REPLY)

NEW QUESTION: 153
Which information is required when adding a device to Firepower Management Center?
A. encryption method
B. username and password
C. device serial number
D. registration key
Answer: D (LEAVE A REPLY)

NEW QUESTION: 154
What is the most common type of data exfiltration that organizations currently experience?
A. HTTPS file upload site
B. SQL database injections
C. encrypted SMTP
D. Microsoft Windows network shares
Answer: D (LEAVE A REPLY)

NEW QUESTION: 155
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: (SHOW ANSWER)
A trusted CA is the only entity that can issue trusted digital certificates. This is extremely important because while PKI manages more of the encryption side of these certificates, authentication is vital to understanding which entities own what keys. Without a trusted CA, anyone can issue their own keys, authentication goes out the window and chaos ensues.

NEW QUESTION: 156

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 (LEAVE A REPLY)
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: 157
An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?
A. HAT
B. BAT
C. SAT
D. RAT
Answer: D (LEAVE A REPLY)

NEW QUESTION: 158
Which technology enables integration between Cisco ISE and other platforms to gather and share network and vulnerability data and SIEM and location information?
A. NetFlow
B. SNMP
C. Cisco Talos
D. pxGrid
Answer: D (LEAVE A REPLY)

NEW QUESTION: 159
Refer to the exhibit.
An engineer must configure a Cisco switch to perform PPP authentication via a TACACS server located at IP address 10.1.1.10. Authentication must fall back to the local database using the username LocalUser and password C1Sc0451069341l if the TACACS server is unreachable.
Drag and drop the commands from the left onto the corresponding configuration steps on the right.
Answer:

NEW QUESTION: 160
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. RADIUS/LDAP authentication
B. single-sign on
C. Kerberos security solution
D. multifactor authentication

Answer: (SHOW ANSWER)

NEW QUESTION: 161
An engineer is trying to securely connect to a router and wants to prevent insecure algorithms from being used.
However, the connection is failing. Which action should be taken to accomplish this goal?
A. Disable telnet using the no ip telnet command.
B. Enable the SSH server using the ip ssh server command.
C. Configure the port using the ip ssh port 22 command.
D. Generate the RSA key using the crypto key generate rsa command.
Answer: (SHOW ANSWER)
In this question, the engineer was trying to secure the connection so maybe he was trying to allow SSH to the device. But maybe something went wrong so the connection was failing (the connection used to be good). So maybe he was missing the "crypto key generate rsa" command.

NEW QUESTION: 162
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: (SHOW ANSWER)
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: 163
In which two ways does a system administrator send web traffic transparently to the Web Security Appliance?
(Choose two)
A. configure policy-based routing on the network infrastructure
B. configure Active Directory Group Policies to push proxy settings
C. reference a Proxy Auto Config file
D. use Web Cache Communication Protocol
E. configure the proxy IP address in the web-browser settings
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 164
What is a benefit of performing device compliance?
A. Device classification and authorization
B. Verification of the latest OS patches
C. Providing multi-factor authentication
D. Providing attribute-driven policies

Answer: B (LEAVE A REPLY)

NEW QUESTION: 165
Which Dos attack uses fragmented packets to crash a target machine?
A. smurf
B. MITM
C. teardrop
D. LAND
Answer: (SHOW ANSWER)
A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

NEW QUESTION: 166
What is the difference between EPP and EDR?
A. EDR focuses solely on prevention at the perimeter.
B. EPP focuses primarily on threats that have evaded front-line defenses that entered the environment.
C. Having an EPP solution allows an engineer to detect, investigate, and remediate modern threats.
D. Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior.
Answer: (SHOW ANSWER)

NEW QUESTION: 167
Which two commands are required when configuring a flow-export action on a Cisco ASA? (Choose two.)
A. flow-export template timeout-rate 15
B. access-list
C. flow-export event-type
D. policy-map
E. access-group
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 168
What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?
A. Activate SSL decryption
B. Activate the Advanced Malware Protection license
C. Enable Intelligent Proxy

D. Enable IP Layer enforcement
Answer: C (LEAVE A REPLY)

NEW QUESTION: 169
Which feature must be configured before implementing NetFlow on a router?
A. syslog
B. VRF
C. IP routing
D. SNMPv3
Answer: (SHOW ANSWER)

NEW QUESTION: 170
Drag and drop the posture assessment flow actions from the left into a sequence on the right.
Answer:

NEW QUESTION: 171
Refer to the exhibit. What function does the API key perform while working with https://api.amp.cisco.com/v1/computers?
A. imports requests
B. plays dent ID
C. HTTP authentication
D. HTTP authorization
Answer: C (LEAVE A REPLY)

NEW QUESTION: 172
DoS attacks are categorized as what?
A. virus attacks
B. phishing attacks
C. flood attacks
D. trojan attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 173
Refer to the exhibit.
An engineer is implementing a certificate based VPN. What is the result of the existing configuration?
A. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER
B. The OU of the IKEv2 peer certificate is set to MANGLER
C. Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully
D. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 174

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

A. Set the sftunnel port to 8305.

B. Set the sftunnel to go through the Cisco FTD

C. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices

D. Manually change the management port on Cisco FMC and all managed Cisco FTD devices

Answer: (SHOW ANSWER)

NEW QUESTION: 175

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 uses HTTP to send a request to a web service.

C. REST is a Linux platform-based architecture.

D. The POST action replaces existing data at the URL path.

E. REST codes can be compiled with any programming language.

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 176

What is the role of Cisco Umbrella Roaming when it is installed on an endpoint?

A. To protect the endpoint against malicious file transfers

B. To ensure that assets are secure from malicious links on and off the corporate network

C. To establish secure VPN connectivity to the corporate network

D. To enforce posture compliance and mandatory software

Answer: B (LEAVE A REPLY)

Umbrella Roaming is a cloud-delivered security service for Cisco's next-generation firewall. It protects your employees even when they are off the VPN.

NEW QUESTION: 177

Which two features of Cisco Email Security can protect your organization against email threats? (Choose two)

A. Time-based one-time passwords

B. Data loss prevention

C. Heuristic-based filtering

D. Geolocation-based filtering

E. NetFlow

Answer: (SHOW ANSWER)

Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution.

Cisco Email Security appliance can now handle incoming mail connections and incoming messages from specific geolocations and perform appropriate actions on them, for example:

- Prevent email threats coming from specific geographic regions.
- Allow or disallow emails coming from specific geographic regions.

Reference:

b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_00.html

NEW QUESTION: 178
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 (LEAVE A REPLY)
Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to).
CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices.
Reference:
cda_oveviw.html

NEW QUESTION: 179
An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?
A. Cisco Umbrella
B. Cisco Cloud Email Security
C. Cisco NGFW
D. Cisco Cloudlock
Answer: (SHOW ANSWER)
Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform. Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45- 738565.pdf Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform. Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45- 738565.pdf

NEW QUESTION: 180
Which solution supports high availability in routed or transparent mode as well as in northbound and southbound deployments?
A. Cisco FTD with Cisco FMC
B. Cisco Firepower NGFW Virtual appliance with Cisco FMC
C. Cisco Firepower NGFW physical appliance with Cisco. FMC
D. Cisco FTD with Cisco ASDM
Answer: (SHOW ANSWER)

NEW QUESTION: 181
What limits communication between applications or containers on the same node?
A. microsegmentation

B. microservicing
C. Software-Defined Access
D. container orchestration
Answer: (SHOW ANSWER)

NEW QUESTION: 182
Which statement describes a serverless application?
A. The application runs from a containerized environment that is managed by Kubernetes or Docker Swarm.
B. The application delivery controller in front of the server farm designates on which server the application runs each time.
C. The application is installed on network equipment and not on physical servers.
D. The application runs from an ephemeral, event-triggered, and stateless container that is fully managed by a cloud provider.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 183
Refer to the exhibit.
What is the function of the Python script code snippet for the Cisco ASA REST API?
A. changes the hostname of the Cisco ASA
B. obtains the saved configuration of the Cisco ASA firewall
C. adds a global rule into policies
D. deletes a global rule from policies
Answer: C (LEAVE A REPLY)

NEW QUESTION: 184
Refer to the exhibit.
An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained.
Which command should be configured on the switch interface in order to provide the user with network connectivity?
A. ip dhcp snooping verify mac-address
B. ip dhcp snooping limit 41
C. ip dhcp snooping vlan 41
D. ip dhcp snooping trust
Answer: D (LEAVE A REPLY)
To understand DHCP snooping we need to learn about DHCP spoofing attack first.
DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle".

The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.
DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.
Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.
The port connected to a DHCP server should be configured as trusted port with the "ip dhcp snooping trust" command. Other ports connecting to hosts are untrusted ports by default.
In this question, we need to configure the uplink to "trust" (under interface Gi1/0/1) as shown below.

NEW QUESTION: 185
A Cisco ISE engineer configures Central Web Authentication (CWA) for wireless guest access and must have the guest endpoints redirect to the guest portal for authentication and authorization. While testing the policy, the engineer notices that the device is not redirected and instead gets full guest access. What must be done for the redirect to work?
A. Add the DACL name for the Airespace ACL configured on the WLC in the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.
B. Create an advanced attribute setting of Cisco:cisco-gateway-id=guest within the authorization profile for the authorization policy line that the unauthenticated devices hit.
C. Tag the guest portal in the CWA part of the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.
D. Use the track movement option within the authorization profile for the authorization policy line that the unauthenticated devices hit.
Answer: (SHOW ANSWER)

NEW QUESTION: 186
Refer to the exhibit.
What will happen when this Python script is run?
A. The compromised computers and malware trajectories will be received from Cisco AMP
B. The list of computers and their current vulnerabilities will be received from Cisco AMP
C. The compromised computers and what compromised them will be received from Cisco AMP
D. The list of computers, policies, and connector statuses will be received from Cisco AMP
Answer: (SHOW ANSWER)
The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across your organization that Advanced Malware Protection (AMP) sees Reference:
2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1

NEW QUESTION: 187
What is the difference between a vulnerability and an exploit?
A. An exploit is a hypothetical event that causes a vulnerability in the network
B. A vulnerability is a hypothetical event for an attacker to exploit
C. An exploit is a weakness that can cause a vulnerability in the network
D. A vulnerability is a weakness that can be exploited by an attacker

Answer: D (LEAVE A REPLY)

NEW QUESTION: 188
Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?
A. url
B. terminal
C. profile
D. selfsigned
Answer: C (LEAVE A REPLY)
A trustpoint enrollment mode, which also defines the trustpoint authentication mode, can be performed via 3 main methods: 1. Terminal Enrollment - manual method of performing trustpoint authentication and certificate enrolment using copy-paste in the CLI terminal. 2. SCEP Enrollment - Trustpoint authentication and enrollment using SCEP over HTTP. 3. Enrollment Profile - Here, authentication and enrollment methods are defined separately. Along with terminal and SCEP enrollment methods, enrollment profiles provide an option to specify HTTP/TFTP commands to perform file retrieval from the Server, which is defined using an authentication or enrollment url under the profile. Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/211333-IOSPKI-Deployment-Guide-Initial-Design.html
1. Terminal Enrollment - manual method of performing trustpoint authentication and certificate enrolment using copy-paste in the CLI terminal.
2. SCEP Enrollment - Trustpoint authentication and enrollment using SCEP over HTTP.
3. Enrollment Profile - Here, authentication and enrollment methods are defined separately. Along with terminal and SCEP enrollment methods, enrollment profiles provide an option to specify HTTP/TFTP commands to perform file retrieval from the Server, which is defined using an authentication or enrollment url under the profile.
A trustpoint enrollment mode, which also defines the trustpoint authentication mode, can be performed via 3 main methods: 1. Terminal Enrollment - manual method of performing trustpoint authentication and certificate enrolment using copy-paste in the CLI terminal. 2. SCEP Enrollment - Trustpoint authentication and enrollment using SCEP over HTTP. 3. Enrollment Profile - Here, authentication and enrollment methods are defined separately. Along with terminal and SCEP enrollment methods, enrollment profiles provide an option to specify HTTP/TFTP commands to perform file retrieval from the Server, which is defined using an authentication or enrollment url under the profile. Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/211333-IOSPKI-Deployment-Guide-Initial-Design.html

NEW QUESTION: 189
Refer to the exhibit.
What does the API key do while working with https://api.amp.cisco.com/v1/computers?
A. Imports requests
B. HTTP authentication
C. displays client ID
D. HTTP authorization
Answer: (SHOW ANSWER)

NEW QUESTION: 190
Drag and drop the concepts from the left onto the correct descriptions on the right
Answer:

NEW QUESTION: 191
Refer to the exhibit.
An administrator is adding a new Cisco FTD device to their network and wants to manage it with Cisco FMC.
The Cisco FTD is not behind a NAT device. Which command is needed to enable this on the Cisco FTD?
A. configure manager add DONTRESOLVE kregistration key>
B. configure manager add <FMC IP address> <registration key> 16
C. configure manager add DONTRESOLVE <registration key> FTD123
D. configure manager add <FMC IP address> <registration key>
Answer: (SHOW ANSWER)
To let FMC manages FTD, first we need to add manager from the FTD and assign a register key of your choice. The command configure manager add 1.1.1.2 the_registration_key_you_want, where 1.1.1.2 is the IP address of the FMC, you need to use the same registration key in FMC when adding this FTD as a managed device.

NEW QUESTION: 192
Why is it important to patch endpoints consistently?
A. Patching allows for creating a honeypot.
B. Patching helps to mitigate vulnerabilities.
C. Patching is required per the vendor contract.
D. Patching reduces the attack surface of the infrastructure.
Answer: (SHOW ANSWER)

NEW QUESTION: 193
What is provided by the Secure Hash Algorithm in a VPN?
A. integrity
B. key exchange
C. encryption
D. authentication
Answer: A (LEAVE A REPLY)
The HMAC-SHA-1-96 (also known as HMAC-SHA-1) encryption technique is used by IPSec to ensure that a message has not been altered. (-> Therefore answer "integrity" is the best choice). HMAC-SHA-1 uses the SHA-1 specified in FIPS-190-1, combined with HMAC (as per RFC 2104), and is described in RFC 2404.

NEW QUESTION: 194
Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?
A. multifactor authentication
B. Dynamic ARP Inspection
C. RADIUS-based REAP
D. fingerprinting
Answer: (SHOW ANSWER)

NEW QUESTION: 195

Which SNMPv3 configuration must be used to support the strongest security possible?
A. asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
B. asa-host(config)#snmp-server group myv3 v3 noauth
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
C. asa-host(config)#snmp-server group myv3 v3 noauth
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
D. asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 196
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: (SHOW ANSWER)
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: 197
Which Cisco security solution stops exfiltration using HTTPS?
A. Cisco FTD
B. Cisco AnyConnect
C. Cisco CTA
D. Cisco ASA
Answer: C (LEAVE A REPLY)
https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf

NEW QUESTION: 198
What is the function of Cisco Cloudlock for data security?
A. user and entity behavior analytics
B. data loss prevention
C. detects anomalies
D. controls malicious cloud apps
Answer: B (LEAVE A REPLY)

NEW QUESTION: 199
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 (LEAVE A REPLY)
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: 200
Which two parameters are used to prevent a data breach in the cloud? (Choose two.)
A. antispoofing programs
B. DLP solutions
C. complex cloud-based web proxies
D. strong user authentication
E. encryption
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 201
Drag and drop the solutions from the left onto the solution's benefits on the right.
Answer:

NEW QUESTION: 202
What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.) The eDirectory client must be installed on each client workstation.
A. Create NTLM or Kerberos authentication realm and enable transparent user identification
B. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.
C. Create an LDAP authentication realm and disable transparent user identification.
D. Deploy a separate eDirectory server: the client IP address is recorded in this server
Answer: A,B (LEAVE A REPLY)

Transparently identify users with authentication realms - This option is available when one or more authentication realms are configured to support transparent identification using one of the following authentication servers:
Active Directory - Create an NTLM or Kerberos authentication realm and enable transparent user identification. In addition, you must deploy a separate Active Directory agent such as Cisco's Context Directory Agent. For more information, see Transparent User Identification with Active Directory.
LDAP - Create an LDAP authentication realm configured as an eDirectory, and enable transparent user identification. For more information, see Transparent User Identification with LDAP.
Details:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01001.html#:~:text=Transparently%20identify%20users%20with%20authentication,User%20Identification%20with%20LDAP.

NEW QUESTION: 203
When a Cisco WSA checks a web request, what occurs if it is unable to match a user-defined policy?
A. It applies the advanced policy.
B. It blocks the request.
C. It applies the next identification profile policy.
D. It applies the global policy.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 204
Which two components do southbound APIs use to communicate with downstream devices? (Choose two.)
A. external application APIs
B. OpenFlow
C. OpFlex
D. services running over the network
E. applications running over the network
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 205
Which two mechanisms are used to control phishing attacks? (Choose two.)
A. Use antispyware software
B. Implement email filtering techniques
C. Define security group memberships
D. Enable browser alerts for fraudulent websites
E. Revoke expired CRL of the websites
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 206
A network administrator is configuring a switch to use Cisco ISE for 802.1X. An endpoint is failing authentication and is unable to access the network.
Where should the administrator begin troubleshooting to verify the authentication details?
A. Adaptive Network Control Policy List
B. Context Visibility

C. Accounting Reports
D. RADIUS Live Logs
Answer: (SHOW ANSWER)
How To Troubleshoot ISE Failed Authentications & Authorizations
Check the ISE Live Logs
Login to the primary ISE Policy Administration Node (PAN).
Go to Operations > RADIUS > Live Logs
(Optional) If the event is not present in the RADIUS Live Logs, go to Operations > Reports > Reports > Endpoints and Users > RADIUS Authentications
Check for Any Failed Authentication Attempts in the Log

NEW QUESTION: 207
For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two.)
A. user identity
B. computer identity
C. Windows firewall
D. Windows service
E. default browser
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 208
Which Cisco security solution provides patch management in the cloud?
A. Cisco Umbrella
B. Cisco ISE
C. Cisco CloudLock
D. Cisco Tetration
Answer: C (LEAVE A REPLY)

NEW QUESTION: 209
An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms.
Which software should be used to accomplish this goal?
A. Cisco Defense Orchestrator
B. Cisco Secureworks
C. Cisco DNA Center
D. Cisco Configuration Professional
Answer: A (LEAVE A REPLY)
Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms.
Cisco Defense Orchestrator features:
....
Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms.

Reference:
736847.html

NEW QUESTION: 210
A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an undetermined verdict. What is causing this issue?
A. The policy was created to send a message to quarantine instead of drop
B. The file has a reputation score that is above the threshold
C. The file has a reputation score that is below the threshold
D. The policy was created to disable file analysis
Answer: D (LEAVE A REPLY)
Maybe the "newly installed service" in this Qmentions about Advanced Malware Protection (AMP) which can be used along with ESA. AMP allows superior protection across the attack continuum.
+ File Reputation - captures a fingerprint of each file as it traverses the ESA and sends it to AMP's cloudbased intelligence network for a reputation verdict. Given these results, you can automatically block malicious files and apply administrator-defined policy.
+ File Analysis - provides the ability to analyze unknown files that are traversing the ESA. A highly secure sandbox environment enables AMP to glean precise details about the file's behavior and to combine that data with detailed human and machine analysis to determine the file's threat level. This disposition is then fed into AMP cloud-based intelligence network and used to dynamically update and expand the AMP cloud data set for enhanced protection

NEW QUESTION: 211
Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?
A. Docker
B. Lambda
C. Contiv
D. SDLC
Answer: A (LEAVE A REPLY)

NEW QUESTION: 212
How does a cloud access security broker function?
A. It acts as a security information and event management solution and receives syslog from other cloud solutions.
B. It scans other cloud solutions being used within the network and identifies vulnerabilities
C. It is an authentication broker to enable single sign-on and multi-factor authentication for a cloud solution
D. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution
Answer: D (LEAVE A REPLY)

NEW QUESTION: 213
Which cryptographic process provides origin confidentiality, integrity, and origin authentication for packets?
A. IKEv2
B. IKEv1
C. ESP
D. AH
Answer: C (LEAVE A REPLY)

NEW QUESTION: 214
Why would a user choose an on-premises ESA versus the CES solution?
A. ESA is deployed inline
B. Demand is unpredictable
C. The server team wants to outsource this service.
D. Sensitive data must remain onsite
Answer: D (LEAVE A REPLY)

NEW QUESTION: 215
Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?
A. transparent
B. redirection
C. forward
D. proxy gateway
Answer: A (LEAVE A REPLY)
There are two possible methods to accomplish the redirection of traffic to Cisco WSA: transparent proxy mode and explicit proxy mode.
In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to Cisco WSA, without any configuration on the client. The transparent proxy deployment is used in this design, and the Cisco ASA firewall is used to redirect traffic to the appliance because all of the outbound web traffic passes through the device and is generally managed by the same operations staff who manage Cisco WSA.

NEW QUESTION: 216
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. The RADIUS authentication key is transmitted only from the defined RADIUS source interface
B. Encrypted RADIUS authentication requires the RADIUS source interface be defined
C. RADIUS requests are generated only by a router if a RADIUS source interface is defined.
D. Only requests that originate from a configured NAS IP are accepted by a RADIUS server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 217
Which endpoint solution protects a user from a phishing attack?

A. Cisco Identity Services Engine
B. Cisco AnyConnect with Network Access Manager module
C. Cisco AnyConnect with Umbrella Roaming Security module
D. Cisco AnyConnect with ISE Posture module
Answer: C (LEAVE A REPLY)

NEW QUESTION: 218
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: (SHOW ANSWER)
In its essence, FlexVPN is the same as DMVPN. Connections between devices are still point-to-point GRE tunnels, spoke-to-spoke connectivity is still achieved with NHRP redirect message, IOS routers even run the same NHRP code for both DMVPN and FlexVPN, which also means that both are Cisco's proprietary technologies.

NEW QUESTION: 219
Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?
A. TLSv1.2
B. TLSv1.1
C. BJTLSv1
D. DTLSv1
Answer: D (LEAVE A REPLY)
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: 220
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: (SHOW ANSWER)
The Cisco Umbrella Multi-Org console has the ability to upload, store, and archive traffic activity logs from your organizations' Umbrella dashboards to the cloud through Amazon S3. CSV formatted Umbrella logs are compressed (gzip) and uploaded every ten minutes so that there's a minimum of delay between traffic from the organization's Umbrella dashboard being logged and then being available to download from an S3 bucket.
By having your organizations' logs uploaded to an S3 bucket, you can then download logs automatically to keep in perpetuity in backup storage.

NEW QUESTION: 221

What are two list types within AMP for Endpoints Outbreak Control? (Choose two)
A. blocked ports
B. simple custom detections
C. command and control
D. allowed applications
E. URL
Answer: (SHOW ANSWER)
Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists.
A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine.
Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf

NEW QUESTION: 222
An engineer is configuring AMP for endpoints and wants to block certain files from executing. Which outbreak control method is used to accomplish this task?
A. application blocking list
B. simple detections
C. advanced custom detections
D. device flow correlation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 223
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. Restrict access to only websites with trusted third-party signed certificates.
C. Modify the user's browser settings to suppress errors from Umbrella.
D. Import the Umbrella root CA into the trusted root store on the user's device.
Answer: (SHOW ANSWER)

NEW QUESTION: 224
Which two parameters are used for device compliance checks? (Choose two.)
A. DNS integrity checks
B. DHCP snooping checks
C. device operating system version
D. Windows registry values
E. endpoint protection software version
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 225

An engineer configured a new network identity in Cisco Umbrella but must verify that traffic is being routed through the Cisco Umbrella network. Which action tests the routing?

A. Ensure that the client computers are pointing to the on-premises DNS servers.

B. Add the public IP address that the client computers are behind to a Core Identity

C. Enable the Intelligent Proxy to validate that traffic is being routed correctly.

D. Browse to http://welcome.umbrella.com/ to validate that the new identity is working

Answer: (SHOW ANSWER)

NEW QUESTION: 226

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 manager

B. file prevalence

C. file discovery

D. file conviction

Answer: B (LEAVE A REPLY)

NEW QUESTION: 227

An engineer has been tasked with configuring a Cisco FTD to analyze protocol fields and detect anomalies in the traffic from industrial systems. What must be done to meet these requirements?

A. Implement pre-filter policies for the CIP preprocessor

B. Enable traffic analysis in the Cisco FTD

C. Configure intrusion rules for the DNP3 preprocessor

D. Modify the access control policy to trust the industrial traffic

Answer: C (LEAVE A REPLY)

"configure INTRUSION RULES for DNP3" -> Documentation states, that enabling INTRUSION RULES is mandatory for CIP to work + required preprocessors (in Network Access Policy - NAP) will be enabled automatically:

"If you want the CIP preprocessor rules listed in the following table to generate events, you MUST enable them. See Setting Intrusion Rule States for information on enabling rules."

"If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings, although the preprocessor remains disabled in the web interface for the corresponding network analysis policy."

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

NEW QUESTION: 228

On which part of the IT environment does DevSecOps focus?
A. perimeter network
B. data center
C. application development
D. wireless network
Answer: (SHOW ANSWER)

NEW QUESTION: 229
Which two actions does the Cisco Identity Services Engine posture module provide that ensures endpoint security?(Choose two.)
A. Assignments to endpoint groups are made dynamically, based on endpoint attributes.
B. Endpoint supplicant configuration is deployed.
C. The latest antivirus updates are applied before access is allowed.
D. Patch management remediation is performed.
E. A centralized management solution is deployed.
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 230
Which feature requires that network telemetry be enabled?
A. SNMP trap notification
B. per-interface stats
C. central syslog system
D. Layer 2 device discovery
Answer: (SHOW ANSWER)

NEW QUESTION: 231
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 Prime Infrastructure
B. Cisco ASAV
C. Cisco NBAR2
D. Account on Resolution
Answer: (SHOW ANSWER)

NEW QUESTION: 232
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: (SHOW ANSWER)

NetFlow is a network protocol developed by Cisco for the collection and monitoring of network traffic flow data generated by NetFlow-enabled routers and switches. The flows do not contain actual packet data, but rather the metadata for communications. It is a standard form of session data that details who, what, when, and where of network traffic -> Answer A is not correct.
Reference:
white-paper-c11-736595.html

NEW QUESTION: 233
In an IaaS cloud services model, which security function is the provider responsible for managing?
A. Internet proxy
B. firewalling virtual machines
C. CASB
D. hypervisor OS hardening
Answer: B (LEAVE A REPLY)
In this IaaS model, cloud providers offer resources to users/machines that include computers as virtual machines, raw (block) storage, firewalls, load balancers, and network devices.
Note: Cloud access security broker (CASB) provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware such as ransomware.

NEW QUESTION: 234
Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?
A. Internal Database
B. RSA SecureID
C. Active Directory
D. LDAP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 235
Which method is used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources?
A. BYOD on boarding
B. Simple Certificate Enrollment Protocol
C. Client provisioning
D. MAC authentication bypass
Answer: (SHOW ANSWER)
When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network.
Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal.
Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices.
Reference:

m_ise_devices_byod.html

NEW QUESTION: 236
For Cisco IOS PKI, which two types of Servers are used as a distribution point for CRLs? (Choose two)
A. SDP
B. LDAP
C. subordinate CA
D. SCP
E. HTTP
Answer: B,E (LEAVE A REPLY)
Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI.
A PKI is composed of the following entities: ...
- A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs)

NEW QUESTION: 237
Drag and drop the capabilities from the left onto the correct technologies on the right.
Answer:

NEW QUESTION: 238
Based on the NIST 800-145 guide, which cloud architecture may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises?
A. private cloud
B. community cloud
C. public cloud
D. hybrid cloud
Answer: B (LEAVE A REPLY)

NEW QUESTION: 239
In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?
A. Smurf
B. distributed denial of service
C. cross-site scripting
D. rootkit exploit
Answer: C (LEAVE A REPLY)
Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.
Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on.
For example the code below is written in hex: <a

href=javascript:alert&#
x28'XSS')>Click Here
is equivalent to:
Click Here
Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form.

NEW QUESTION: 240
Refer to the exhibit.
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 and MAB will both be used and ISE can use policy to determine the access level
C. 802 1X will work and the device will be allowed on the network
D. 802.1X will not work and the device will not be allowed network access
Answer: D (LEAVE A REPLY)

NEW QUESTION: 241
What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two)
A. data exfiltration
B. command and control communication
C. intelligent proxy
D. snort
E. URL categorization
Answer: A,B (LEAVE A REPLY)
Cisco Cognitive Threat Analytics helps you quickly detect and respond to sophisticated, clandestine attacks that are already under way or are attempting to establish a presence within your environment. The solution automatically identifies and investigates suspicious or malicious web-based traffic. It identifies both potential and confirmed threats, allowing you to quickly remediate the infection and reduce the scope and damage of an attack, whether it's a known threat campaign that has spread across multiple organizations or a unique threat you've never seen before.
Detection and analytics features provided in Cognitive Threat Analytics are shown below:
+ Data exfiltration: Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content
+ Command-and-control (C2) communication: Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPSencoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad range of threats
...

NEW QUESTION: 242
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: (SHOW ANSWER)
In order to use AAA along with an external token authentication mechanism, set the "Method" as "Both" in the Authentication.

NEW QUESTION: 243
What are two functionalities of northbound and southbound APIs within Cisco SDN architecture? (Choose two.)
A. Northbound APIs utilize RESTful API methods such as GET, POST, and DELETE.
B. Southbound APIs are used to define how SDN controllers integrate with applications.
C. Northbound interfaces utilize OpenFlow and OpFlex to integrate with network devices.
D. Southbound APIs utilize CLI, SNMP, and RESTCONF.
E. Southbound interfaces utilize device configurations such as VLANs and IP addresses.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 244
Refer to the exhibit. All servers are in the same VLAN/Subnet. DNS Server-1 and DNS Server-2 must communicate with each other, and all servers must communicate with default gateway multilayer switch. Which type of private VLAN ports should be configured to prevent communication between DNS servers and the file server?
A. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as isolated port and GigabitEthernet0/3 and GrgabitEthernet0/4 as community ports
B. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as community port, and GigabitEthernet0/3 and GrgabitEthernet0/4 as isolated ports.
C. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as promiscuous port, Gigabit Ethernet0/3 and GigabitEthernet0/4 as isolated ports
D. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as isolated port, and GigabitEthernet0/3 and GigabitEthernet0/4 as promiscuous ports.
Answer: (SHOW ANSWER)

NEW QUESTION: 245
What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?
A. EPP focuses on network security, and EDR focuses on device security.

B. EDR focuses on network security, and EPP focuses on device security.
C. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.
D. EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 246
Which Cisco platform onboards the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing the endpoint to gain network access?
A. Cisco ISE
B. Cisco WSA
C. Cisco TACACS+
D. Cisco NAC
Answer: (SHOW ANSWER)

NEW QUESTION: 247
Which two kinds of attacks are prevented by multifactor authentication? (Choose two.)
A. DDOS
B. man-in-the-middle
C. tear drop
D. phishing
E. brute force
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 248
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: B,E (LEAVE A REPLY)
Application layer protocols can represent the same data in a variety of ways. The Firepower System provides application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results.
Reference:
FirePower uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

NEW QUESTION: 249
Refer to the exhibit.
What does the API do when connected to a Cisco security appliance?
A. get the process and PID information from the computers in the network

B. create an SNMP pull mechanism for managing AMP
C. gather network telemetry information from AMP for endpoints
D. gather the network interface information about the computers AMP sees
Answer: (SHOW ANSWER)
The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across your organization that Advanced Malware Protection (AMP) sees.
Reference:
2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1

NEW QUESTION: 250
Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?
A. user input validation in a web page or web application
B. Linux and Windows operating systems
C. database
D. web page images
Answer: A (LEAVE A REPLY)
SQL injection usually occurs when you ask a user for input, like their username/userid, but the user gives ("injects") you an SQL statement that you will unknowingly run on your database. For example:
Look at the following example, which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
If user enter something like this: "100 OR 1=1" then the SzQL statement will look like this:
SELECT * FROM Users WHERE UserId = 100 OR 1=1;
The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE. A hacker might get access to all the user names and passwords in this database.

NEW QUESTION: 251
Which solution should be leveraged for secure access of a CI/CD pipeline?
A. Duo Network Gateway
B. SSL WebVPN
C. Cisco FTD network gateway
D. remote access client
Answer: A (LEAVE A REPLY)

NEW QUESTION: 252
Which API method and required attribute are used to add a device into Cisco DNA Center with the native API?
A. POST and name
B. GET and serialNumber
C. userSudiSerlalNos and deviceInfo
D. lastSyncTime and pid

Answer: B (LEAVE A REPLY)

NEW QUESTION: 253
Which threat intelligence standard contains malware hashes?
A. structured threat information expression
B. open command and control
C. trusted automated exchange of indicator information
D. advanced persistent threat
Answer: A (LEAVE A REPLY)

NEW QUESTION: 254
An administrator is adding a new Cisco ISE node to an existing deployment. What must be done to ensure that the addition of the node will be successful when inputting the FQDN?
A. Make the new Cisco ISE node a secondary PAN before registering it with the primary.
B. Change the IP address of the new Cisco ISE node to the same network as the others.
C. Add the DNS entry for the new Cisco ISE node into the DNS server
D. Open port 8905 on the firewall between the Cisco ISE nodes
Answer: C (LEAVE A REPLY)

NEW QUESTION: 255
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: (SHOW ANSWER)
SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts. The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data. Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc. Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Referfence: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming telemetry 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.
SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts. The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data. Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc. Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Referfence: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming telemetry

NEW QUESTION: 256
An engineer is configuring web filtering for a network using Cisco Umbrella Secure Internet Gateway.

The requirement is that all traffic needs to be filtered. Using the SSL decryption feature, which type of certificate should be presented to the end-user to accomplish this goal?

A. third-party

B. SubCA

C. self-signed

D. organization owned root

Answer: D (LEAVE A REPLY)

NEW QUESTION: 257

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

A. GET https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/network-device/count

B. GET https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/network-device

C. GET https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v 1/networkdevice/startIndex/recordsToReturn

D. GET https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/networkdevice?parameter1=value&parameter2=value&....

Answer: A (LEAVE A REPLY)

NEW QUESTION: 258

Refer to the exhibit.

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

A. No split-tunnel policy is defined on the Firepower Threat Defense appliance.

B. The access control policy is not allowing VPN traffic in.

C. Site-to-site VPN peers are using different encryption algorithms.

D. Site-to-site VPN preshared keys are mismatched.

Answer: (SHOW ANSWER)

If sysopt permit-vpn is not enabled then an access control policy must be created to allow the VPN traffic through the FTD device. If sysopt permit-vpn is enabled skip creating an access control policy. Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html

NEW QUESTION: 259

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

A. GET VPN uses multiple security associations for connections

B. GET VPN supports Remote Access VPNs

C. GET VPN interoperates with non-Cisco devices

D. GET VPN natively supports MPLS and private IP networks

Answer: D (LEAVE A REPLY)

NEW QUESTION: 260
What does endpoint isolation in Cisco AMP for Endpoints security protect from?
A. an infection spreading across the network E
B. a malware spreading across the user device
C. an infection spreading across the LDAP or Active Directory domain from a user account
D. a malware spreading across the LDAP or Active Directory domain from a user account
Answer: (SHOW ANSWER)
https://community.cisco.com/t5/endpoint-security/amp-endpoint-isolation/td-p/4086674#:~:text=Isolating%20an%20endpoint%20blocks%20all,your%20IP%20isolation%20allow%20list

NEW QUESTION: 261
Which Cisco ISE feature helps to detect missing patches and helps with remediation?
A. profiling policy
B. enabling probes
C. authentication policy
D. posture assessment
Answer: A (LEAVE A REPLY)