Cisco.350-701.v2023-03-16.q221

Exam Code:	350-701
Exam Name:	Implementing and Operating Cisco Security Core Technologies
Certification Provider:	Cisco
Free Question Number:	221
Version:	v2023-03-16
# of views:	2041
# of Questions views:	2210
https://www.freepdfdumps.com/Cisco.350-701.v2023-03-16.q221.html	

NEW QUESTION: 1
Which option is the main function of Cisco Firepower impact flags?
A. They identify data that the ASA sends to the Firepower module.
B. They correlate data about intrusions and vulnerability.
C. They highlight known and suspected malicious IP addresses in reports.
D. They alert administrators when critical events occur.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
Which two risks is a company vulnerable to if it does not have a well-established patching solution for endpoints? (Choose two)
A. exploits
B. ARP spoofing
C. denial-of-service attacks
D. malware
E. eavesdropping
Answer: A,D (LEAVE A REPLY)
Malware means "malicious software", is any software intentionally designed to cause damage to a computer, server, client, or computer network. The most popular types of malware includes viruses, ransomware and spyware. Virus Possibly the most common type of malware, viruses attach their malicious code to clean code and wait to be run.
Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again.
Spyware is spying software that can secretly record everything you enter, upload, download, and store on your computers or mobile devices. Spyware always tries to keep itself hidden.
An exploit is a code that takes advantage of a software vulnerability or security flaw.

Exploits and malware are two risks for endpoints that are not up to date. ARP spoofing and eavesdropping are attacks against the network while denial-of-service attack is based on the flooding of IP packets.

NEW QUESTION: 3
An administrator is adding a new Cisco ISE node to an existing deployment. What must be done to ensure that the addition of the node will be successful when inputting the FQDN?
A. Make the new Cisco ISE node a secondary PAN before registering it with the primary.
B. Add the DNS entry for the new Cisco ISE node into the DNS server
C. Change the IP address of the new Cisco ISE node to the same network as the others.
D. Open port 8905 on the firewall between the Cisco ISE nodes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
What is a key difference between Cisco Firepower and Cisco ASA?
A. Cisco Firepower provides identity-based access control while Cisco ASA does not.
B. Cisco ASA provides SSL inspection while Cisco Firepower does not.
C. Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not.
D. Cisco ASA provides access control while Cisco Firepower does not.
Answer: C (LEAVE A REPLY)

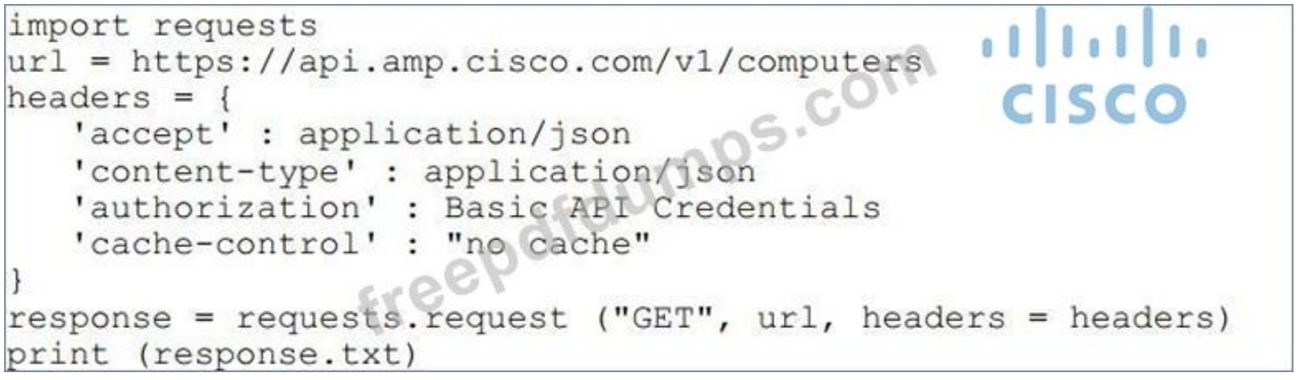
NEW QUESTION: 5
Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two)
A. accounting
B. assurance
C. automation
D. authentication
E. encryption
Answer: B,C (LEAVE A REPLY)
What Cisco DNA Center enables you to do Automate: Save time by using a single dashboard 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: 6

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: D (LEAVE A REPLY)

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: https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1% 2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1 organization that Advanced Malware Protection (AMP) sees Reference:

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: https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1% 2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1

NEW QUESTION: 7

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

A. allow

B. monitor

C. trust

D. block

Answer: B (LEAVE A REPLY)

NEW QUESTION: 8

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

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

NEW QUESTION: 9
Refer to the exhibit. What does this Python script accomplish?
A. It allows authentication with TLSv1 SSL protocol
B. It authenticates to a Cisco ISE with an SSH connection.
C. It authenticates to a Cisco ISE server using the username of ersad
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10
Refer to the exhibit.

```
ASA#  show  service-policy sfr

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


What are two indications of the Cisco Firepower Services Module configuration?
(Choose two.)
A. Traffic is blocked if the module fails.
B. The module is operating in IPS mode.
C. The module fails to receive redirected traffic
D. Traffic continues to flow if the module fails.
E. The module is operating in IDS mode.
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 11
What are two functionalities of SDN Northbound APIs? (Choose two.)
A. Northbound APIs form the interface between the SDN controller and business applications.
B. Northbound APIs form the interface between the SDN controller and the network switches or routers.
C. OpenFlow is a standardized northbound API protocol.
D. Northbound APIs use the NETCONF protocol to communicate with applications.
E. Northbound APIs provide a programmable interface for applications to dynamically configure the network.

Answer: (SHOW ANSWER)

NEW QUESTION: 12
An engineer is adding a Cisco DUO solution to the current TACACS+ deployment using Cisco ISE. The engineer wants to authenticate users using their account when they log into network devices. Which action accomplishes this task?
A. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE
B. Modify the current policy with the condition MFASourceSequence DUO=true in the authorization conditions within Cisco ISE
C. Create an identity policy within Cisco ISE to send all authentication requests to Cisco DUO.
D. Configure Cisco DUO with the external Active Directory connector and tie it to the policy set within Cisco ISE.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
Which feature does the laaS model provide?
A. granular control of data
B. automatic updates and patching of software
C. dedicated, restricted workstations
D. software-defined network segmentation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
Which deployment model is the most secure when considering risks to cloud adoption?
A. private cloud
B. hybrid cloud
C. public cloud
D. community cloud
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
What is a difference between DMVPN and sVTI?
A. DMVPN supports static tunnel establishment, whereas sVTI does not.
B. DMVPN supports tunnel encryption, whereas sVTI does not.
C. DMVPN provides interoperability with other vendors, whereas sVTI does not.
D. DMVPN supports dynamic tunnel establishment, whereas sVTI does not.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
What is a difference between Cisco AMP for Endpoints and Cisco Umbrella?
A. Cisco AMP for Endpoints automatically researches indicators of compromise ..

B. Cisco AMP for Endpoints prevents connections to malicious destinations, and C malware.
C. Cisco AMP for Endpoints is a cloud-based service, and Cisco Umbrella is not.
D. Cisco AMP for Endpoints prevents, detects, and responds to attacks before and against Internet threats.
Answer: (SHOW ANSWER)

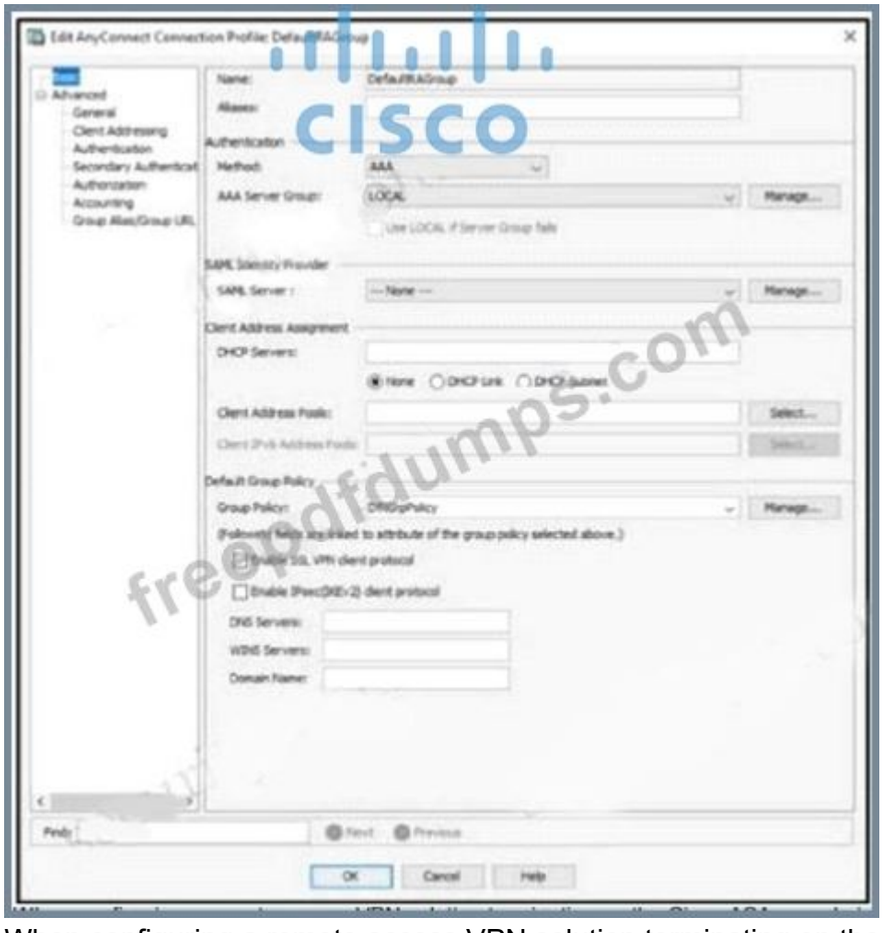
NEW QUESTION: 17
Which two protocols must be configured to authenticate end users to the Web Security Appliance? (Choose two.)
A. NTLMSSP
B. CHAP
C. TACACS+
D. Kerberos
E. RADIUS
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which standard is used to automate exchanging cyber threat information?
A. STIX
B. IoC
C. MITRE
D. TAXII
Answer: (SHOW ANSWER)

NEW QUESTION: 19
An organization has noticed an increase in malicious content downloads and wants to use Cisco Umbrella to prevent this activity for suspicious domains while allowing normal web traffic. Which action will accomplish this task?
A. Set content settings to High
B. Configure the intelligent proxy.
C. Use destination block lists.
D. Configure application block lists.
Answer: B (LEAVE A REPLY)
Obviously, if you allow all traffic to these risky domains, users might access malicious content, resulting in an infection or data leak. But if you block traffic, you can expect false positives, an increase in support inquiries, and

thus, more headaches. By only proxying risky domains, the intelligent proxy delivers more granular visibility and control. The intelligent proxy bridges the gap by allowing access to most known good sites without being proxied and only proxying those that pose a potential risk. The proxy then filters and blocks against specific URLs hosting malware while allowing access to everything else. Reference: https://docs.umbrella.com/deployment-umbrella/docs/what-is-the-intelligent-proxy The intelligent proxy bridges the gap by allowing access to most known good sites without being proxied and only proxying those that pose a potential risk. The proxy then filters and blocks against specific URLs hosting malware while allowing access to everything else.
Obviously, if you allow all traffic to these risky domains, users might access malicious content, resulting in an infection or data leak. But if you block traffic, you can expect false positives, an increase in support inquiries, and thus, more headaches. By only proxying risky domains, the intelligent proxy delivers more granular visibility and control. The intelligent proxy bridges the gap by allowing access to most known good sites without being proxied and only proxying those that pose a potential risk. The proxy then filters and blocks against specific URLs hosting malware while allowing access to everything else. Reference: https://docs.umbrella.com/deployment-umbrella/docs/what-is-the-intelligent-proxy

NEW QUESTION: 20
Refer to the exhibit.



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

A. Group Policy
B. Method
C. SAML Server
D. DHCP Servers
Answer: B (LEAVE A REPLY)
In order to use AAA along with an external token authentication mechanism, set the "Method" as "Both" in the Authentication.

NEW QUESTION: 21
How does the Cisco WSA enforce bandwidth restrictions for web applications?
A. It dynamically creates a scavenger class QoS policy and applies it to each client that connects through the WSA.
B. It sends commands to the uplink router to apply traffic policing to the application traffic.
C. It simulates a slower link by introducing latency into application traffic.
D. It implements a policy route to redirect application traffic to a lower-bandwidth link.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Refer to the exhibit.

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

A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced What is the cause of this issue?
A. The router was not rebooted after the NTP configuration updated.
B. The key was configured in plain text.
C. The hashing algorithm that was used was MD5. which is unsupported.
D. NTP authentication is not enabled.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 23
An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA. Which Cisco ASA command must be used?
A. flow-export destination inside 1.1.1.1 2055
B. ip flow monitor input
C. ip flow-export destination 1.1.1.1 2055
D. flow exporter
Answer: A (LEAVE A REPLY)
The syntax of this command is: flow-export destination interface-name ipv4-address | hostname udp-port This command is used on Cisco ASA to configure Network Secure Event Logging (NSEL) collector to which NetFlow packets are sent. The destination keyword indicates that a NSEL collector is being configured. + The interface-name argument is the name of the ASA and ASA Services Module interface through which the collector is reached.

+ The ipv4-address argument is the IP address of the machine running the collector application. + The hostname argument is the destination IP address or name of the collector. + The udp-port argument is the UDP port number to which NetFlow packets are sent. You can configure a maximum of five collectors. After a collector is configured, template records are automatically sent to all configured NSEL collectors. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/ monitor_nsel.html
This command is used on Cisco ASA to configure Network Secure Event Logging (NSEL) collector to which NetFlow packets are sent. The destination keyword indicates that a NSEL collector is being configured.
+ The interface-name argument is the name of the ASA and ASA Services Module interface through which the collector is reached.
+ The ipv4-address argument is the IP address of the machine running the collector application.
+ The hostname argument is the destination IP address or name of the collector.
+ The udp-port argument is the UDP port number to which NetFlow packets are sent.
You can configure a maximum of five collectors. After a collector is configured, template records are automatically sent to all configured NSEL collectors.
Reference:
The syntax of this command is: flow-export destination interface-name ipv4-address | hostname udp-port This command is used on Cisco ASA to configure Network Secure Event Logging (NSEL) collector to which NetFlow packets are sent. The destination keyword indicates that a NSEL collector is being configured. + The interface-name argument is the name of the ASA and ASA Services Module interface through which the collector is reached. + The ipv4-address argument is the IP address of the machine running the collector application. + The hostname argument is the destination IP address or name of the collector. + The udp-port argument is the UDP port number to which NetFlow packets are sent. You can configure a maximum of five collectors. After a collector is configured, template records are automatically sent to all configured NSEL collectors. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/ monitor_nsel.html

NEW QUESTION: 24
Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using higher-level protocols without readdressing the network?
A. routed mode
B. single context mode
C. transparent mode
D. multiple context mode
Answer: (SHOW ANSWER)

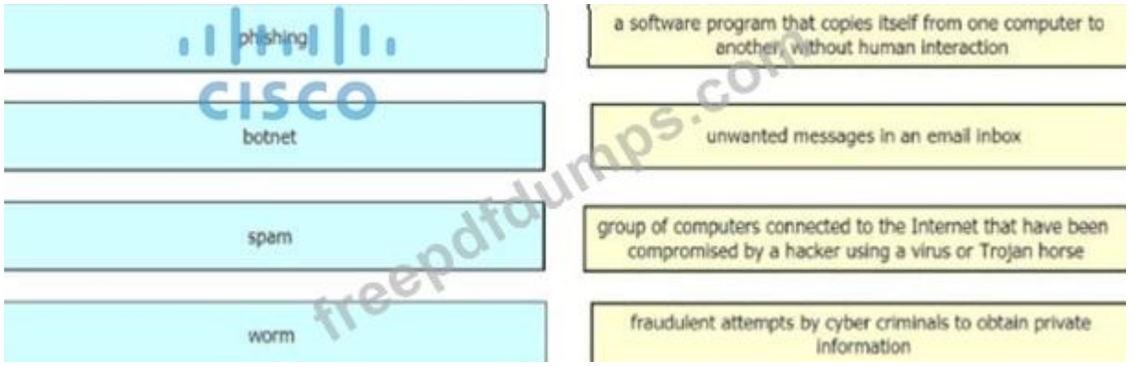
NEW QUESTION: 25
An organization has DHCP servers set up to allocate IP addresses to clients on the LAN. What must be done to ensure the LAN switches prevent malicious DHCP traffic while also distributing IP addresses to the correct endpoints?
A. Configure DHCP snooping and set an untrusted interface for all clients
B. Configure Dynamic ARP Inspection and antispoofing ACLs in the DHCP snooping database
C. Configure Dynamic ARP Inspection and add entries in the DHCP snooping database

D. Configure DHCP snooping and set a trusted interface for the DHCP server

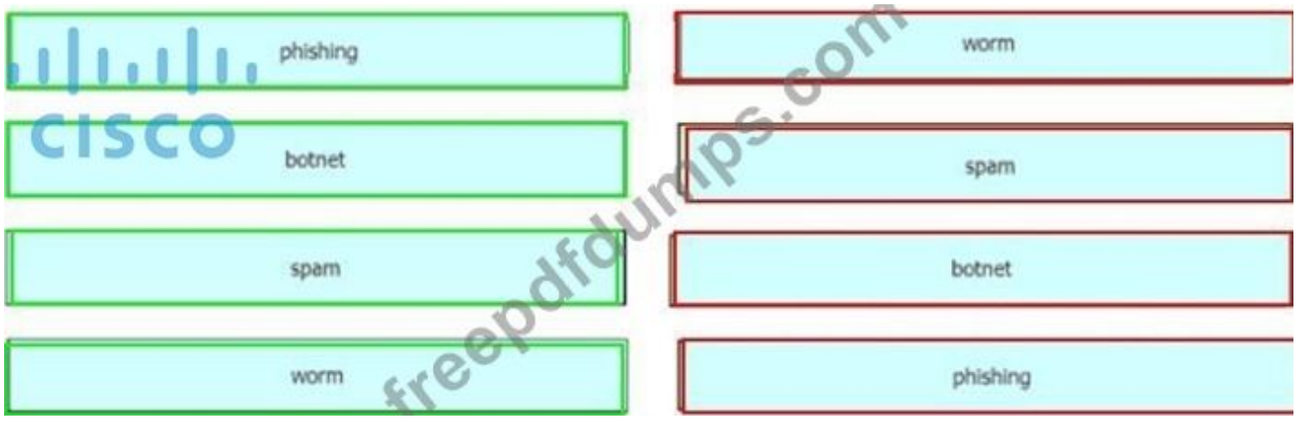
Answer: (SHOW ANSWER)

NEW QUESTION: 26

Drag and drop the common security threats from the left onto the definitions on the right.



Answer:



NEW QUESTION: 27

What is a characteristic of Dynamic ARP Inspection?

A. DAI intercepts all ARP requests and responses on trusted ports only

B. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCP snooping binding database

C. In a typical network, make all ports as trusted except for the ports connecting to switches, which are untrusted.

D. DAI associates a trust state with each switch.

Answer: (SHOW ANSWER)

NEW QUESTION: 28

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

A. It tracks flow-create, flow-teardown, and flow-denied events.

B. It provides stateless IP flow tracking that exports all records of a specific flow.

C. It tracks the flow continuously and provides updates every 10 seconds.

D. Its events match all traffic classes in parallel.

Answer: A (LEAVE A REPLY)

The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs). Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.html The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs).
The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs). Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.html

NEW QUESTION: 29
An administrator is configuring N I P on Cisco ASA via ASDM and needs to ensure that rogue NTP servers cannot insert themselves as the authoritative time source Which two steps must be taken to accomplish this task? (Choose two)
A. Specify the NTP version
B. Choose the interface for syncing to the NTP server
C. Configure the NTP stratum
D. Set the authentication key
E. Set the NTP DNS hostname
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 30
A network engineer is tasked with configuring a Cisco ISE server to implement external authentication against Active Directory. What must be considered about the authentication requirements? (Choose two.)
A. Active Directory supports user and machine authentication by using MSCHAPv2.
B. LDAP communication must be permitted between the ISE server and the domain controller.
C. RADIUS communication must be permitted between the ISE server and the domain controller.
D. The ISE account must be a domain administrator in Active Directory to perform JOIN operations.
E. Active Directory only supports user authentication by using MSCHAPv2.
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 31
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 FTD with Cisco ASDM
D. Cisco Firepower NGFW physical appliance with Cisco. FMC
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?
A. Cisco Umbrella
B. External Threat Feeds
C. Cisco Threat Grid
D. Cisco Stealthwatch
Answer: C (LEAVE A REPLY)
Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector

NEW QUESTION: 33
An engineer is configuring device-hardening on a router in order to prevent credentials from being seen if the router configuration was compromised. Which command should be used?
A. service password-encryption
B. username <username> privilege 15 password <password>
C. service password-recovery
D. username < username> password <password>
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
Which kind of API that is used with Cisco DNA Center provisions SSIDs, QoS policies, and update software versions on switches?
A. Integration
B. Event
C. Intent
D. Multivendor
Answer: C (LEAVE A REPLY)

NEW QUESTION: 35
Which IPS engine detects ARP spoofing?
A. AIC Engine
B. Service Generic Engine
C. Atomic ARP Engine
D. ARP Inspection Engine
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
What is a benefit of using Cisco Umbrella?
A. It prevents malicious inbound traffic.
B. Attacks can be mitigated before the application connection occurs.
C. DNS queries are resolved faster.
D. Files are scanned for viruses before they are allowed to run.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
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 decrypts HTTPS application traffic for unauthenticated users
C. It provides enhanced HTTPS application detection for AsyncOS.
D. It decrypts HTTPS application traffic for authenticated users.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 38
Which type of attack is social engineering?
A. trojan
B. phishing
C. malware
D. MITM
Answer: B (LEAVE A REPLY)
Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem.

NEW QUESTION: 39
An engineer recently completed the system setup on a Cisco WSA Which URL information does the system send to SensorBase Network servers?
A. complete URL,without obfuscating the path segments
B. none because SensorBase Network Participation is disabled by default

C. Summarized server-name information and MD5-hashed path information
D. URL information collected from clients that connect to the Cisco WSA using Cisco AnyConnect
Answer: (SHOW ANSWER)

NEW QUESTION: 40
What Cisco command shows you the status of an 802.1X connection on interface gi0/1?
A. show ver gi0/1
B. show authen sess int gi0/1
C. show authorization status
D. show connection status gi0/1
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
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: 42
What is the benefit of installing Cisco AMP for Endpoints on a network?
A. It provides operating system patches on the endpoints for security.
B. It protects endpoint systems through application control and real-time scanning
C. It enables behavioral analysis to be used for the endpoints.
D. It provides flow-based visibility for the endpoints network connections.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
What are two features of NetFlow flow monitoring? (Choose two)
A. Can track ingress and egress information
B. Include the flow record and the flow importer
C. Copies all ingress flow information to an interface
D. Does not required packet sampling on interfaces
E. Can be used to track multicast, MPLS, or bridged traffic
Answer: A,E (LEAVE A REPLY)

The following are restrictions for Flexible NetFlow: + Traditional NetFlow (TNF) accounting is not supported. + Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported. + Both ingress and egress NetFlow accounting is supported. + Microflow policing feature shares the NetFlow hardware resource with FNF. + Only one flow monitor per interface and per direction is supported. Reference: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html When configuring NetFlow, follow these guidelines and restrictions: + Except in PFC3A mode, NetFlow supports bridged IP traffic. PFC3A mode does not support NetFlow bridged IP traffic. + NetFlow supports multicast IP traffic. Reference: https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.html The Flexible NetFlow - MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow.html

+ Traditional NetFlow (TNF) accounting is not supported.
+ Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported.
+ Both ingress and egress NetFlow accounting is supported.
+ Microflow policing feature shares the NetFlow hardware resource with FNF.
+ Only one flow monitor per interface and per direction is supported.

Reference:
consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html
When configuring NetFlow, follow these guidelines and restrictions:

+ Except in PFC3A mode, NetFlow supports bridged IP traffic. PFC3A mode does not support NetFlow bridged IP traffic.
+ NetFlow supports multicast IP traffic.

The Flexible NetFlow - MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN The following are restrictions for Flexible NetFlow: + Traditional NetFlow (TNF) accounting is not supported. + Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported. + Both ingress and egress NetFlow accounting is supported. + Microflow policing feature shares the NetFlow hardware resource with FNF. + Only one flow monitor per interface and per direction is supported. Reference: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html When configuring NetFlow, follow these guidelines and restrictions: + Except in PFC3A mode, NetFlow supports bridged IP traffic. PFC3A mode does not support NetFlow bridged IP traffic. + NetFlow supports multicast IP traffic. Reference: https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.html The Flexible NetFlow - MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the

same VPN Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow.html

NEW QUESTION: 44
Why is it important to implement MFA inside of an organization?
A. To prevent man-the-middle attacks from being successful.
B. To prevent phishing attacks from being successful.
C. To prevent DoS attacks from being successful.
D. To prevent brute force attacks from being successful.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 45
Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?
A. fingerprinting
B. multifactor authentication
C. Dynamic ARP Inspection
D. RADIUS-based REAP
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Using Cisco Cognitive Threat Analytics, which platform automatically blocks risky sites, and test unknown sites for hidden advanced threats before allowing users to click them?
A. Cisco Advanced Stealthwatch Appliance
B. Cisco Identity Services Engine
C. Cisco Enterprise Security Appliance
D. Cisco Web Security Appliance
Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.

Answer:

NEW QUESTION: 48

What is a commonality between DMVPN and FlexVPN technologies?

A. FlexVPN and DMVPN use IS-IS routing protocol to communicate with spokes

B. FlexVPN and DMVPN use the new key management protocol

C. FlexVPN and DMVPN use the same hashing algorithms

D. IOS routers run the same NHRP code for DMVPN and FlexVPN

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 49

A mall provides security services to customers with a shared appliance. The mall wants separation of management on the shared appliance. Which ASA deployment mode meets these needs?

A. transparent mode

B. multiple zone mode

C. routed mode

D. multiple context mode

Answer: (SHOW ANSWER)

NEW QUESTION: 50

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

A. aaa server radius dynamic-author

B. auth-type all

C. aaa new-model

D. ip device-tracking

Answer: C (LEAVE A REPLY)

NEW QUESTION: 51

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 has an additional module that can be installed to provide multiple blocking capabilities, whereas Cisco FTD does not.

B. Cisco ASA because it allows for interactive blocking and blocking with reset to be configured via the GUI, whereas Cisco FTD does not.

C. Cisco FTD because it enables interactive blocking and blocking with reset natively, whereas Cisco ASA does not

D. Cisco FTD because it supports system rate level traffic blocking, whereas Cisco ASA does not

Answer: (SHOW ANSWER)

NEW QUESTION: 52

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

A. RSA is an asymmetric key establishment algorithm intended to output symmetric keys

B. RSA is a symmetric key establishment algorithm intended to output asymmetric keys

C. DH is a symmetric key establishment algorithm intended to output asymmetric keys

D. DH is on asymmetric key establishment algorithm intended to output symmetric keys

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 53

What is a characteristic of an EDR solution and not of an EPP solution?

A. retrospective analysis

B. stops all ransomware attacks

C. decrypts SSL traffic for better visibility

D. performs signature-based detection

Answer: A (LEAVE A REPLY)

NEW QUESTION: 54
Which type of data exfiltration technique encodes data in outbound DNS requests to specific servers and can be stopped by Cisco Umbrella?
A. DNS hijacking
B. cache poisoning
C. DNS tunneling
D. DNS flood attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
A malicious user gained network access by spoofing printer connections that were authorized using MAB on four different switch ports at the same time. What two catalyst switch security features will prevent further violations? (Choose two)
A. DHCP Snooping
B. 802.1AE MacSec
C. IP Device track
D. Port security
E. Private VLANs
F. Dynamic ARP inspection
Answer: A,F (LEAVE A REPLY)

NEW QUESTION: 56
What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?
A. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously
B. It discovers and controls cloud apps that are connected to a company's corporate environment
C. It deletes any application that does not belong in the network
D. It sends the application information to an administrator to act on
Answer: B (LEAVE A REPLY)

NEW QUESTION: 57
Which functions of an SDN architecture require southbound APIs to enable communication?
A. SDN controller and the network elements
B. management console and the SDN controller
C. management console and the cloud
D. SDN controller and the cloud
Answer: (SHOW ANSWER)
The Southbound API is used to communicate between Controllers and network devices

NEW QUESTION: 58
What are two recommended approaches to stop DNS tunneling for data exfiltration and command and control call backs? (Choose two.)

A. Use next generation firewalls.
B. Use intrusion prevention system.
C. Block all TXT DNS records.
D. Use Cisco Umbrella.
E. Enforce security over port 53.
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 59
What provides the ability to program and monitor networks from somewhere other than the DNAC GUI?
A. API
B. ASDM
C. NetFlow
D. desktop client
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
What is a characteristic of a bridge group in ASA Firewall transparent mode?
A. It includes multiple interfaces and access rules between interfaces are customizable
B. It is a Layer 3 segment and includes one port and customizable access rules
C. It allows ARP traffic with a single access rule
D. It has an IP address on its BVI interface and is used for management traffic
Answer: A (LEAVE A REPLY)
A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place. Each bridge group includes a Bridge Virtual Interface (BVI). The ASA uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported. You can include multiple interfaces per bridge group. If you use more than 2 interfaces per bridge group, you can control communication between multiple segments on the same network, and not just between inside and outside. For example, if you have three inside segments that you do not want to communicate with each other, you can put each segment on a separate interface, and only allow them to communicate with the outside interface. Or you can customize the access rules between interfaces to allow only as much access as desired. Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.html
Note: BVI interface is not used for management purpose. But we can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA.
supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place.
Each bridge group includes a Bridge Virtual Interface (BVI). The ASA uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the

bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.
You can include multiple interfaces per bridge group. If you use more than 2 interfaces per bridge group, you can control communication between multiple segments on the same network, and not just between inside and outside. For example, if you have three inside segments that you do not want to communicate with each other, you can put each segment on a separate interface, and only allow them to communicate with the outside interface. Or you can customize the access rules between interfaces to allow only as much access as desired.
Reference:
A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place. Each bridge group includes a Bridge Virtual Interface (BVI). The ASA uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported. You can include multiple interfaces per bridge group. If you use more than 2 interfaces per bridge group, you can control communication between multiple segments on the same network, and not just between inside and outside. For example, if you have three inside segments that you do not want to communicate with each other, you can put each segment on a separate interface, and only allow them to communicate with the outside interface. Or you can customize the access rules between interfaces to allow only as much access as desired. Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.html
Note: BVI interface is not used for management purpose. But we can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA.

NEW QUESTION: 61
What is the difference between EPP and EDR?
A. EDR focuses solely on prevention at the perimeter.
B. Having an EPP solution allows an engineer to detect, investigate, and remediate modern threats.
C. Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior.
D. EPP focuses primarily on threats that have evaded front-line defenses that entered the environment.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 62

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

A. to expose the endpoint to more threats

B. because human error or insider threats will still exist

C. to prevent theft of the endpoints

D. because defense-in-depth stops at the network

Answer: B (LEAVE A REPLY)

NEW QUESTION: 63

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

A. virtual machine

B. network

C. hypervisor

D. application

Answer: D (LEAVE A REPLY)

NEW QUESTION: 64

What is a benefit of using Cisco Tetration?

A. It collects telemetry data from servers and then uses software sensors to analyze flow information.

B. It collects policy compliance data and process details.

C. It collects enforcement data from servers and collects interpacket variation.

D. It collects near-real time data from servers and inventories the software packages that exist on servers.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 65

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

A. outbreakconfig

B. websecurity advancedconfig

C. webadvancedconfig

D. websecurity config

Answer: B (LEAVE A REPLY)

NEW QUESTION: 66

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: 67
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:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html
++ 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:

++ 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:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html

NEW QUESTION: 68
How does Cisco Umbrella archive logs to an enterprise owned storage?
A. by using the Application Programming Interface to fetch the logs
B. by sending logs via syslog to an on-premises or cloud-based syslog server
C. by the system administrator downloading the logs from the Cisco Umbrella web portal
D. by being configured to send logs to a self-managed AWS S3 bucket
Answer: D (LEAVE A REPLY)
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. Reference: https://docs.umbrella.com/deployment-umbrella/docs/manage-logs By having your organizations' logs uploaded to an S3 bucket, you can then download logs automatically to keep in perpetuity in backup storage.
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. Reference: https://docs.umbrella.com/deployment-umbrella/docs/manage-logs

NEW QUESTION: 69
Which action controls the amount of URI text that is stored in Cisco WSA logs files?
A. Configure the advancedproxyconfig command with the HTTPS subcommand
B. Configure a small log-entry size.
C. Configure a maximum packet size.
D. Configure the datasecurityconfig command
Answer: A (LEAVE A REPLY)

NEW QUESTION: 70

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

A. Create an IP block list for the website from which the file was downloaded

B. Block the application that the file was using to open

C. Send the file to Cisco Threat Grid for dynamic analysis

D. Upload the hash for the file into the policy

Answer: (SHOW ANSWER)

NEW QUESTION: 71

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

NEW QUESTION: 72

Which form of attack is launched using botnets?

A. EIDDOS

B. virus

C. DDOS

D. TCP flood

Answer: (SHOW ANSWER)

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

NEW QUESTION: 73

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. organization owned root

B. third-party

C. SubCA

D. self-signed

Answer: (SHOW ANSWER)

NEW QUESTION: 74

Which capability is exclusive to a Cisco AMP public cloud instance as compared to a private cloud instance?

A. RBAC

B. TETRA detection engine

C. SPERO detection engine

D. ETHOS detection engine

Answer: (SHOW ANSWER)

NEW QUESTION: 75

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

A. STIX

B. XMPP

C. pxGrid

D. SMTP

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 76

Refer to the exhibit.

Interface	MAC Address	Method	Domain	Status	Fg	Session I
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth		0A021982000
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth		0A021982000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth		0A021982000
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth		0A021982000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth		0A021982000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth		0A021982000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth		0A021982000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth		0A021982000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth		0A021982000
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth		0A021982000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth		0A021982000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth		0A021982000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth		0A021982000
Gi7/4	54ee.75d3.d766	dot1x	DATA	Auth		0A021982000
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth		0A021982000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth		0A021982000
Gi9/22	0007.b00c.8c35	mab	DATA	Auth		0A021982000

Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

A. show authentication registrations

B. show authentication method

C. show dot1x all

D. show authentication sessions

Answer: (SHOW ANSWER)

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137 Displaying the Summary of All Auth Manager Sessions on the Switch Enter the following:

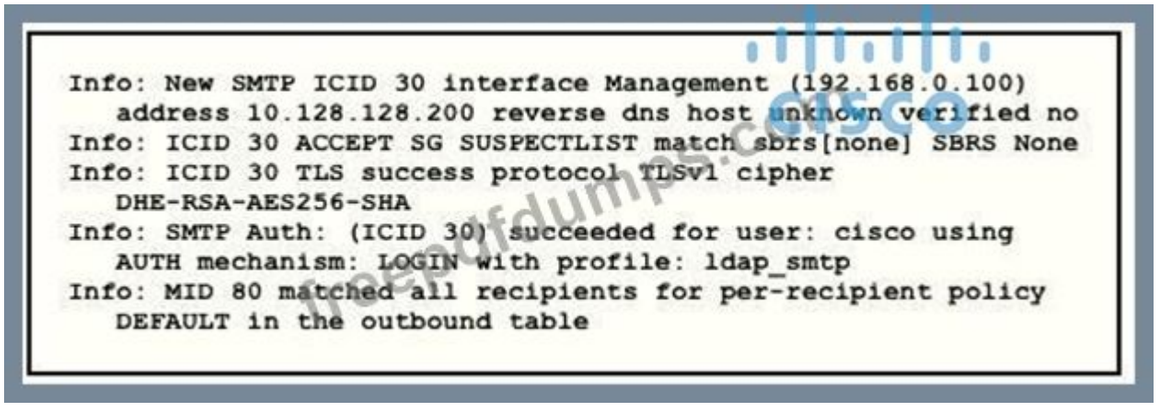
Switch# show authentication sessions

Interface MAC Address Method Domain Status Session ID

Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58 Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

NEW QUESTION: 77

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: (SHOW ANSWER)

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: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118844-technoteesa-00.html The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

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 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: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118844-technoteesa-00.html The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

NEW QUESTION: 78

A network administrator is using the Cisco ESA with AMP to upload files to the cloud for analysis. The network is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?

A. AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.

B. The file is queued for upload when connectivity is restored.

C. The file upload is abandoned.
D. The ESA immediately makes another attempt to upload the file.
Answer: C (LEAVE A REPLY)
The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more. Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technoteesa-00.html In this question, it stated "the network is congested" (not the file analysis server was overloaded) so the appliance will not try to upload the file again.
connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.
Reference:
In this question, it stated "the network is congested" (not the file analysis server was overloaded) so the The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more. Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technoteesa-00.html In this question, it stated "the network is congested" (not the file analysis server was overloaded) so the appliance will not try to upload the file again.

NEW QUESTION: 79
When NetFlow is applied to an interface, which component creates the flow monitor cache that is used to collect traffic based on the key and nonkey fields in the configured record?
A. flow exporter
B. flow sampler
C. records
D. flow monitor
Answer: A (LEAVE A REPLY)

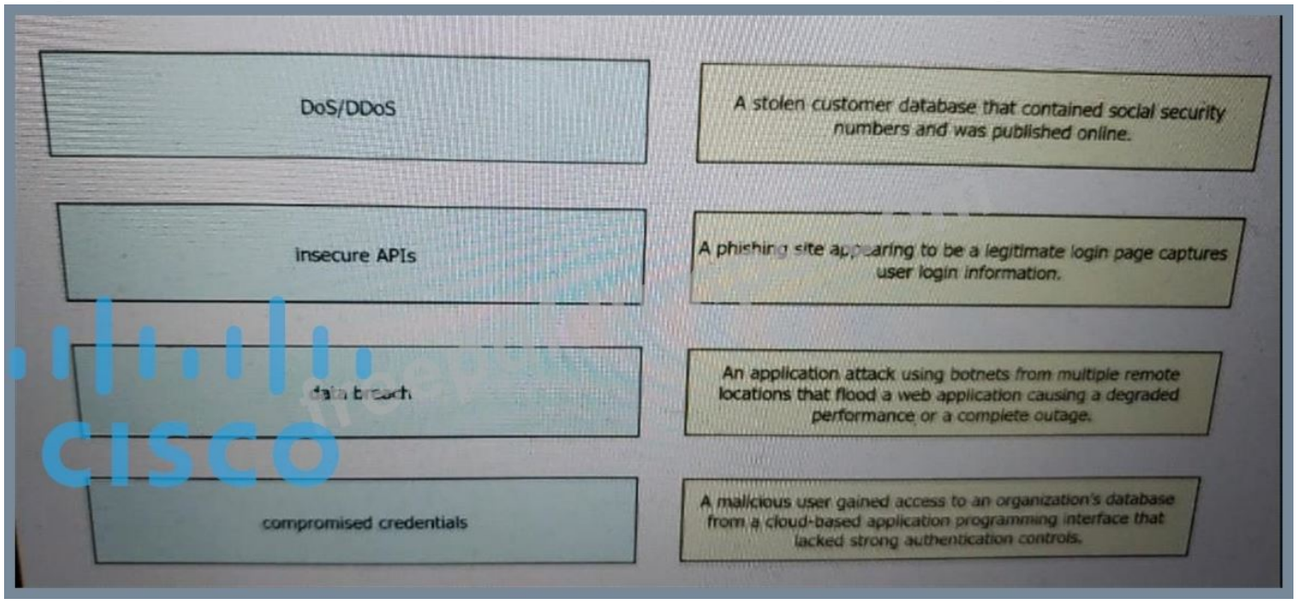
NEW QUESTION: 80
Which technology provides a combination of endpoint protection endpoint detection, and response?
A. Cisco Threat Grid
B. Cisco AMP
C. Cisco Talos
D. Cisco Umbrella
Answer: B (LEAVE A REPLY)

NEW QUESTION: 81
An engineer must modify a policy to block specific addresses using Cisco Umbrell a. The policy is created already and is actively u: of the default policy elements. What else must be done to accomplish this task?
A. Add the specified addresses to the identities list and create a block action.
B. Use content categories to block or allow specific addresses.
C. Create a destination list for addresses to be allowed or blocked.

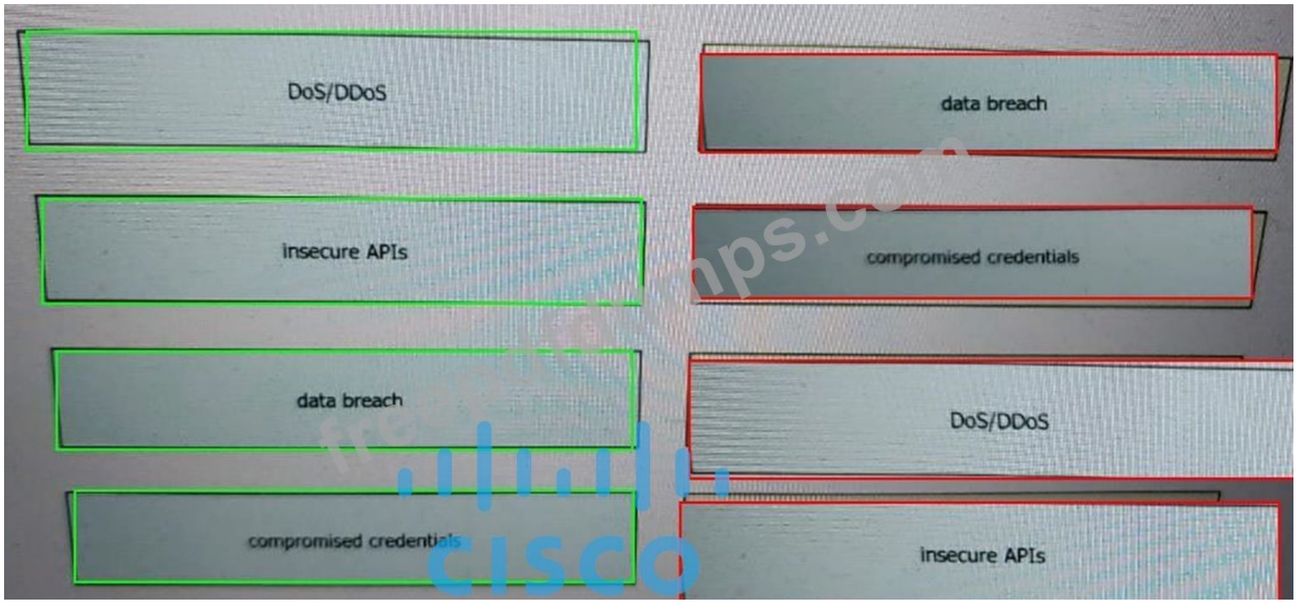
D. Modify the application settings to allow only applications to connect to required addresses.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 82
Which technology limits communication between nodes on the same network segment to individual applications?
A. machine-to-machine firewalling
B. SaaS deployment
C. microsegmentation
D. serverless infrastructure
Answer: C (LEAVE A REPLY)

NEW QUESTION: 83
Drag and drop the threats from the left onto examples of that threat on the right



Answer:



NEW QUESTION: 84
What are two benefits of using an MDM solution? (Choose two.)
A. provides simple and streamlined login experience for multiple applications and users
B. grants administrators a way to remotely wipe a lost or stolen device
C. encrypts data that is stored on endpoints
D. allows for centralized management of endpoint device applications and configurations
E. native integration that helps secure applications across multiple cloud platforms or on-premises environments
Answer: (SHOW ANSWER)

NEW QUESTION: 85
What are the two most commonly used authentication factors in multifactor authentication? (Choose two)
A. biometric factor
B. time factor
C. confidentiality factor
D. knowledge factor
E. encryption factor
Answer: (SHOW ANSWER)
Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource. MFA requires means of verification that unauthorized users won't have. Proper multi-factor authentication uses factors from at least two different categories. MFA methods: + Knowledge - usually a password - is the most commonly used tool in MFA solutions. However, despite their simplicity, passwords have become a security problem and slow down productivity. + Physical factors - also called possession factors-use tokens, such as a USB dongle or a portable device, that generate a temporary QR (quick response) code. Mobile phones are commonly used, as they have the advantage of being readily available in most situations. + Inherent - This category includes biometrics like fingerprint, face, and retina scans. As technology advances, it may also include voice ID or other behavioral inputs like keystroke metrics. Because inherent factors are reliably unique, always present, and secure, this category shows promise. + Location-based and time-based - Authentication systems can use GPS coordinates, network parameters, and metadata for the network in use, and device recognition for MFA. Adaptive authentication combines these data points with historical or contextual user data. A time factor in conjunction with a location factor could detect an attacker attempting to authenticate in Europe when the user was last authenticated in California an hour prior, for example. + Time-based one-time password (TOTP) - This is generally used in 2FA but could apply to any MFA method where a second step is introduced dynamically at login upon completing a first step. The wait for a second step-in which temporary passcodes are sent by SMS or email-is usually brief, and the process is easy to use for a wide range of users and devices. This method is currently widely used. + Social media - In this case a user grants permission for a website to use their social media username and password for login. This provide an easy login process, and one generally available to all users. + Risk-based authentication - Sometimes called adaptive multi-factor authentication, this method combines adaptive authentication and algorithms that calculate risk and observe the context of specific login requests. The goal of this method is to reduce redundant logins and provide a more user-friendly workflow. + Push-based 2FA - Push-based 2FA improves on SMS and TOTP 2FA by adding additional layers of security while

improving ease of use. It confirms a user's identity with multiple factors of authentication that other methods cannot. Because push-based 2FA sends notifications through data networks like cellular or Wi-Fi, users must have data access on their mobile devices to use the 2FA functionality. Reference: https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html The two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint, face, and retina scans. Biometrics is used commonly in mobile devices).
verification factors to gain access to a resource. MFA requires means of verification that unauthorized users won't have.
Proper multi-factor authentication uses factors from at least two different categories.
MFA methods:
+ Knowledge - usually a password - is the most commonly used tool in MFA solutions. However, despite their simplicity, passwords have become a security problem and slow down productivity.
+ Physical factors - also called possession factors-use tokens, such as a USB dongle or a portable device, that generate a temporary QR (quick response) code. Mobile phones are commonly used, as they have the advantage of being readily available in most situations.
+ Inherent - This category includes biometrics like fingerprint, face, and retina scans. As technology advances, it may also include voice ID or other behavioral inputs like keystroke metrics. Because inherent factors are reliably unique, always present, and secure, this category shows promise.
+ Location-based and time-based - Authentication systems can use GPS coordinates, network parameters, and metadata for the network in use, and device recognition for MFA. Adaptive authentication combines these data points with historical or contextual user data.
A time factor in conjunction with a location factor could detect an attacker attempting to authenticate in Europe when the user was last authenticated in California an hour prior, for example.
+ Time-based one-time password (TOTP) - This is generally used in 2FA but could apply to any MFA method where a second step is introduced dynamically at login upon completing a first step. The wait for a second step-in which temporary passcodes are sent by SMS or email-is usually brief, and the process is easy to use for a wide range of users and devices. This method is currently widely used.
+ Social media - In this case a user grants permission for a website to use their social media username and password for login. This provide an easy login process, and one generally available to all users.
+ Risk-based authentication - Sometimes called adaptive multi-factor authentication, this method combines adaptive authentication and algorithms that calculate risk and observe the context of specific login requests.
The goal of this method is to reduce redundant logins and provide a more user-friendly workflow.
+ Push-based 2FA - Push-based 2FA improves on SMS and TOTP 2FA by adding additional layers of security while improving ease of use. It confirms a user's identity with multiple factors of authentication that other methods cannot. Because push-based 2FA sends notifications through data networks like cellular or Wi-Fi, users must have data access on their mobile devices to use the 2FA functionality.
Reference:
The two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint, Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource. MFA requires means of verification that unauthorized users won't have.
Proper multi-factor authentication uses factors from at least two different categories. MFA methods: + Knowledge -

usually a password - is the most commonly used tool in MFA solutions. However, despite their simplicity, passwords have become a security problem and slow down productivity. + Physical factors - also called possession factors-use tokens, such as a USB dongle or a portable device, that generate a temporary QR (quick response) code. Mobile phones are commonly used, as they have the advantage of being readily available in most situations. + Inherent - This category includes biometrics like fingerprint, face, and retina scans. As technology advances, it may also include voice ID or other behavioral inputs like keystroke metrics. Because inherent factors are reliably unique, always present, and secure, this category shows promise. + Location-based and time-based - Authentication systems can use GPS coordinates, network parameters, and metadata for the network in use, and device recognition for MFA. Adaptive authentication combines these data points with historical or contextual user data. A time factor in conjunction with a location factor could detect an attacker attempting to authenticate in Europe when the user was last authenticated in California an hour prior, for example. + Time-based one-time password (TOTP) - This is generally used in 2FA but could apply to any MFA method where a second step is introduced dynamically at login upon completing a first step. The wait for a second step-in which temporary passcodes are sent by SMS or email-is usually brief, and the process is easy to use for a wide range of users and devices. This method is currently widely used. + Social media - In this case a user grants permission for a website to use their social media username and password for login. This provide an easy login process, and one generally available to all users. + Risk-based authentication - Sometimes called adaptive multi-factor authentication, this method combines adaptive authentication and algorithms that calculate risk and observe the context of specific login requests. The goal of this method is to reduce redundant logins and provide a more user-friendly workflow. + Push-based 2FA - Push-based 2FA improves on SMS and TOTP 2FA by adding additional layers of security while improving ease of use. It confirms a user's identity with multiple factors of authentication that other methods cannot. Because push-based 2FA sends notifications through data networks like cellular or Wi-Fi, users must have data access on their mobile devices to use the 2FA functionality. Reference: https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html The two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint, face, and retina scans. Biometrics is used commonly in mobile devices).

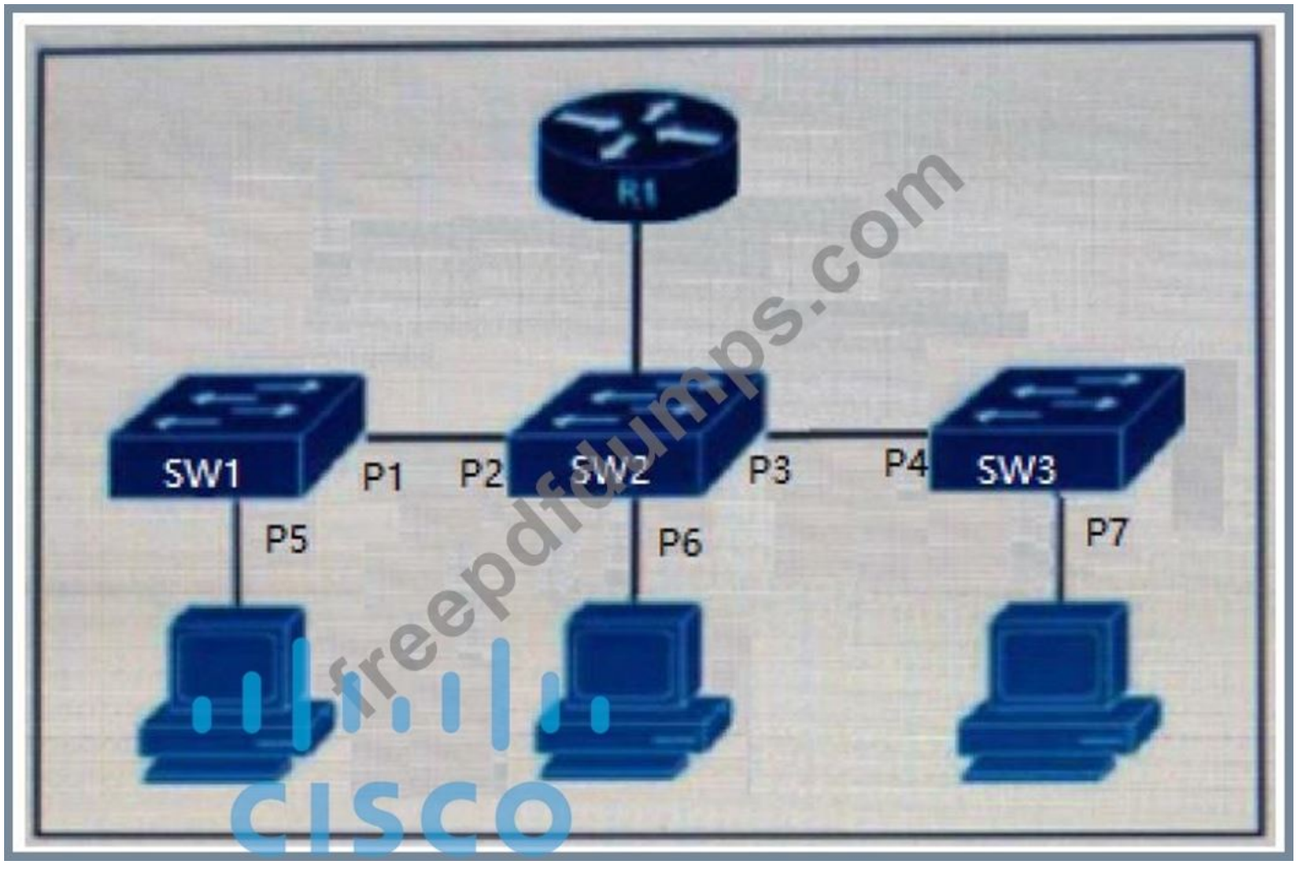
NEW QUESTION: 86
Which ESA implementation method segregates inbound and outbound email?
A. one listener on a single physical Interface
B. one listener on one logical IPv4 address on a single logical interface
C. pair of logical IPv4 listeners and a pair Of IPv6 listeners on two physically separate interfaces
D. pair of logical listeners on a single physical interface with two unique logical IPv4 addresses and one IPv6 address
Answer: B (LEAVE A REPLY)

NEW QUESTION: 87
When configuring ISAKMP for IKEv1 Phase1 on a Cisco IOS router, an administrator needs to input the command crypto isakmp key cisco address 0.0.0.0. The administrator is not sure what the IP addressing in this command issued for. What would be the effect of changing the IP address from 0.0.0.0 to 1.2.3.4?
A. The key server that is managing the keys for the connection will be at 1.2.3.4

B. The remote connection will only be allowed from 1.2.3.4
C. The address that will be used as the crypto validation authority
D. All IP addresses other than 1.2.3.4 will be allowed
Answer: (SHOW ANSWER)
The command crypto isakmp key cisco address 1.2.3.4 authenticates the IP address of the 1.2.3.4 peer by using the key cisco. The address of "0.0.0.0" will authenticate any address with this key.

NEW QUESTION: 88
How does Cisco Workload Optimization Manager help mitigate application performance issues?
A. It deploys an AWS Lambda system
B. It automates resource resizing
C. It optimizes a flow path
D. It sets up a workload forensic score
Answer: C (LEAVE A REPLY)
Cisco Workload Optimization Manager provides specific real-time actions that ensure workloads get the resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software). Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software).
Cisco Workload Optimization Manager provides specific real-time actions that ensure workloads get the resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software). Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf

NEW QUESTION: 89
Refer to the exhibit.



The DHCP snooping database resides on router R1, and dynamic ARP inspection is configured only on switch SW2. Which ports must be configured as untrusted so that dynamic ARP inspection operates normally?

A. P2 and P3 only

B. P5, P6, and P7 only

C. P1, P2, P3, and P4 only

D. P2, P3, and P6 only

Answer: D (LEAVE A REPLY)

NEW QUESTION: 90

An engineer has enabled LDAP accept queries on a listener. Malicious actors must be prevented from quickly identifying all valid recipients. What must be done on the Cisco ESA to accomplish this goal?

A. Configure incoming content filters

B. Use Bounce Verification

C. Configure Directory Harvest Attack Prevention

D. Bypass LDAP access queries in the recipient access table

Answer: C (LEAVE A REPLY)

A Directory Harvest Attack (DHA) is a technique used by spammers to find valid/existent email addresses at a domain either by using Brute force or by guessing valid e-mail addresses at a domain using different permutations of common username. Its easy for attackers to get hold of a valid email address if your organization uses standard format for official e-mail alias (for example: jsmith@example.com). We can configure DHA Prevention to prevent malicious actors from quickly identifying valid recipients.

Note: Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email programs use to look up contact information from a server, such as ClickMail Central Directory. For example, here's an LDAP search translated into plain English: "Search for all people located in Chicago who's name contains "Fred" that have an email address. Please return their full name, email, title, and description.

NEW QUESTION: 91
What is the most commonly used protocol for network telemetry?
A. NctFlow
B. SMTP
C. TFTP
D. SNMP
Answer: (SHOW ANSWER)

NEW QUESTION: 92
What provides total management for mobile and PC including managing inventory and device tracking, remote view, and live troubleshooting using the included native remote desktop support?
A. mobile application management
B. mobile content management
C. mobile device management
D. mobile access management
Answer: C (LEAVE A REPLY)

NEW QUESTION: 93
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. CoA Reauth
B. CoA Session Query
C. Port Bounce
D. CoA Terminate
Answer: A (LEAVE A REPLY)

NEW QUESTION: 94
Which two characteristics of messenger protocols make data exfiltration difficult to detect and prevent?

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

NEW QUESTION: 95
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. PAC file
B. Bridge mode
C. Forward file
D. Transparent mode
Answer: A (LEAVE A REPLY)

NEW QUESTION: 96
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: (SHOW ANSWER)
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: 97
What is the process In DevSecOps where all changes In the central code repository are merged and synchronized?
A. CD
B. CI
C. QA

D. EP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 98
Which two conditions are prerequisites for stateful failover for IPsec? (Choose two)
A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically
B. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.
C. The IPsec configuration that is set up on the active device must be duplicated on the standby device
D. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically.
E. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device
Answer: (SHOW ANSWER)
Stateful failover for IP Security (IPsec) enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This failover process is transparent to users and does not require adjustment or reconfiguration of any remote peer.
Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators.
Prerequisites for Stateful Failover for IPsec
Complete, Duplicate IPsec and IKE Configuration on the Active and Standby Devices This document assumes that you have a complete IKE and IPsec configuration. The IKE and IPsec configuration that is set up on the active device must be duplicated on the standby device. That is, the crypto configuration must be identical with respect to Internet Security Association and Key Management Protocol (ISAKMP) policy, ISAKMP keys (preshared), IPsec profiles, IPsec transform sets, all crypto map sets that are used for stateful failover, all access control lists (ACLs) that are used in match address statements on crypto map sets, all AAA configurations used for crypto, client configuration groups, IP local pools used for crypto, and ISAKMP profiles. Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpnavailability-15-mt-book/sec-state-fail-ipsec.html Although the prerequisites only stated that "Both routers should be the same type of device" but in the "Restrictions for Stateful Failover for IPsec" section of the link above, it requires "Both the active and standby devices must run the identical version of the Cisco IOS software" so answer E is better than answer B.
This document assumes that you have a complete IKE and IPsec configuration.
The IKE and IPsec configuration that is set up on the active device must be duplicated on the standby device.
That is, the crypto configuration must be identical with respect to Internet Security Association and Key Management Protocol (ISAKMP) policy, ISAKMP keys (preshared), IPsec profiles, IPsec transform sets, all crypto map sets that are used for stateful failover, all access control lists (ACLs) that are used in match address statements on crypto map sets, all AAA configurations used for crypto, client configuration groups, IP local pools used for crypto, and ISAKMP profiles.

Reference:
Although the prerequisites only stated that "Both routers should be the same type of device" but in the Complete, Duplicate IPsec and IKE Configuration on the Active and Standby Devices This document assumes that you have a complete IKE and IPsec configuration. The IKE and IPsec configuration that is set up on the active device must be duplicated on the standby device. That is, the crypto configuration must be identical with respect to Internet Security Association and Key Management Protocol (ISAKMP) policy, ISAKMP keys (preshared), IPsec profiles, IPsec transform sets, all crypto map sets that are used for stateful failover, all access control lists (ACLs) that are used in match address statements on crypto map sets, all AAA configurations used for crypto, client configuration groups, IP local pools used for crypto, and ISAKMP profiles. Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpnavailability-15-mt-book/sec-state-fail-ipsec.html Although the prerequisites only stated that "Both routers should be the same type of device" but in the "Restrictions for Stateful Failover for IPsec" section of the link above, it requires "Both the active and standby devices must run the identical version of the Cisco IOS software" so answer E is better than answer B.

NEW QUESTION: 99
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: 100
An organization has a requirement to collect full metadata information about the traffic going through their AWS cloud services They want to use this information for behavior analytics and statistics Which two actions must be taken to implement this requirement? (Choose two.)
A. Configure Cisco Stealthwatch Cloud to ingest AWS information
B. Configure Cisco ACI to ingest AWS information.
C. Configure Cisco Thousand Eyes to ingest AWS information.
D. Send VPC Flow Logs to Cisco Stealthwatch Cloud.
E. Send syslog from AWS to Cisco Stealthwatch Cloud.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 101
Refer to the exhibit.

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

What is the result of using this authentication protocol in the configuration?

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

NEW QUESTION: 102
Which CLI command is used to register a Cisco FirePower sensor to Firepower Management Center?
A. configure system add <host><key>
B. configure manager <key> add host
C. configure manager delete
D. configure manager add <host><key
Answer: D (LEAVE A REPLY)

NEW QUESTION: 103
Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?
A. Cisco Stealthwatch
B. Cisco AMP for Endpoints
C. Cisco ISE
D. Cisco Umbrella
Answer: C (LEAVE A REPLY)

NEW QUESTION: 104
Cisco SensorBase gaihers threat information from a variety of Cisco products and services and performs analytics to find patterns on threats Which term describes this process?
A. sharing
B. deployment
C. authoring
D. consumption
Answer: B (LEAVE A REPLY)

NEW QUESTION: 105
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. ip host vpn.sohoroutercompany.eom <VPN Peer IP Address>

C. crypto isakmp identity hostname
D. Add the dynamic keyword to the existing crypto map command
E. ip name-server <DNS Server IP Address>
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Which type of DNS abuse exchanges data between two computers even when there is no direct connection?
A. Malware installation
B. Command-and-control communication
C. Network footprinting
D. Data exfiltration
Answer: D (LEAVE A REPLY)
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. Reference: https://www.netsurion.com/articles/5-types-of-dns-attacks-and-how-to-detect-them 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.
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. Reference: https://www.netsurion.com/articles/5-types-of-dns-attacks-and-how-to-detect-them

NEW QUESTION: 107
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: A (LEAVE A REPLY)
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:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_byod.html 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:
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: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_byod.html

NEW QUESTION: 108
What must be enabled to secure SaaS-based applications?
A. modular policy framework
B. two-factor authentication
C. end-to-end encryption
D. application security gateway
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
What are two things to consider when using PAC files with the Cisco WSA? (Choose two.)
A. If the WSA host port is changed, the default port redirects web traffic to the correct port automatically.
B. The WSA hosts PAC files on port 6001 by default.
C. By default, they direct traffic through a proxy when the PC and the host are on the same subnet.
D. The WSA hosts PAC files on port 9001 by default.
E. PAC files use if-else statements to determine whether to use a proxy or a direct connection for traffic between the PC and the host.
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Which function is performed by certificate authorities but is a limitation of registration authorities?
A. CRL publishing
B. certificate re-enrollment
C. verifying user identity
D. accepts enrollment requests
Answer: C (LEAVE A REPLY)

NEW QUESTION: 111
Which threat intelligence standard contains malware hashes?
A. open command and control
B. structured threat information expression
C. advanced persistent threat
D. trusted automated exchange or indicator information
Answer: (SHOW ANSWER)

NEW QUESTION: 112

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

A. buffer overflow

B. browser WGET

C. cross-site scripting

D. SQL injection

Answer: C (LEAVE A REPLY)

NEW QUESTION: 113

What is the benefit of integrating Cisco ISE with a MDM solution?

A. It provides compliance checks for access to the network

B. It provides the ability to update other applications on the mobile device

C. It provides the ability to add applications to the mobile device through Cisco ISE

D. It provides network device administration access

Answer: A (LEAVE A REPLY)

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperability_mdm.html

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperability_mdm.html

NEW QUESTION: 114

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

A. 5

B. 12

C. 10

D. 3

Answer: B (LEAVE A REPLY)

NEW QUESTION: 115

Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?

A. Docker

B. SDLC

C. Contiv

D. Lambda

Answer: (SHOW ANSWER)

NEW QUESTION: 116

A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address Error! Hyperlink reference not valid. IP>/capure/CAPI/pcap/test.pcap, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

A. Enable the HTTPS server for the device platform policy

B. Disable the HTTPS server and use HTTP instead
C. Disable the proxy setting on the browser
D. Use the Cisco FTD IP address as the proxy server setting on the browser
Answer: A (LEAVE A REPLY)

NEW QUESTION: 117
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: A,D (LEAVE A REPLY)
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: 118
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 DNAC
C. Cisco Defense Orchestrator
D. Cisco Secureworks
Answer: C (LEAVE A REPLY)

NEW QUESTION: 119
How is data sent out to the attacker during a DNS tunneling attack?
A. as part of the UDP'53 packet payload
B. as part of the DNS response packet
C. as part of the domain name
D. as part of the TCP/53 packet header
Answer: C (LEAVE A REPLY)

NEW QUESTION: 120
A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?
A. Use MAB with profiling
B. Use MAB with posture assessment.
C. Use 802.1X with posture assessment.
D. Use 802.1X with profiling.
Answer: (SHOW ANSWER)
As the new device does not have a supplicant, we cannot use 802.1X. MAC Authentication Bypass (MAB) is a fallback option for devices that don't support 802.1x. It is virtually always used in deployments in some way shape or form. MAB works by having the authenticator take the connecting device's MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or Access-Reject just like it would with 802.1x. Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles. Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their corporate workstation but be granted limited network access when accessing the network from their personal iPhone. Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456
MAC Authentication Bypass (MAB) is a fallback option for devices that don't support 802.1x. It is virtually always used in deployments in some way shape or form. MAB works by having the authenticator take the connecting device's MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or Access-Reject just like it would with 802.1x.
Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles.
Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their

corporate workstation but be granted limited network access when accessing the network from their personal iPhone.
As the new device does not have a supplicant, we cannot use 802.1X. MAC Authentication Bypass (MAB) is a fallback option for devices that don't support 802.1x. It is virtually always used in deployments in some way shape or form. MAB works by having the authenticator take the connecting device's MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or Access-Reject just like it would with 802.1x. Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles. Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their corporate workstation but be granted limited network access when accessing the network from their personal iPhone. Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456

NEW QUESTION: 121
Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?
A. TLSv1.2
B. TLSv1.1
C. BJTLSv1
D. DTLSv1
Answer: (SHOW ANSWER)
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: 122

Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?

A. PaaS

B. XaaS

C. IaaS

D. SaaS

Answer: A (LEAVE A REPLY)

Cloud computing can be broken into the following three basic models:

+ Infrastructure as a Service (IaaS): IaaS describes a cloud solution where you are renting infrastructure. You purchase virtual power to execute your software as needed. This is much like running a virtual server on your own equipment, except you are now running a virtual server on a virtual disk. This model is similar to a utility company model because you pay for what you use.

+ Platform as a Service (PaaS): PaaS provides everything except applications. Services provided by this model include all phases of the system development life cycle (SDLC) and can use application programming interfaces (APIs), website portals, or gateway software. These solutions tend to be proprietary, which can cause problems if the customer moves away from the provider's platform.

+ Software as a Service (SaaS): SaaS is designed to provide a complete packaged solution. The software is rented out to the user. The service is usually provided through some type of front end or web portal. While the end user is free to use the service from anywhere, the company pays a peruse fee.

NEW QUESTION: 123

Which endpoint protection and detection feature performs correlation of telemetry, files, and intrusion events that are flagged as possible active breaches?

A. indication of compromise

B. file trajectory

C. elastic search

D. retrospective detection

Answer: (SHOW ANSWER)

NEW QUESTION: 124

Which Cisco Firewall solution requires zone definition?

A. Cisco AMP

B. Cisco ASA

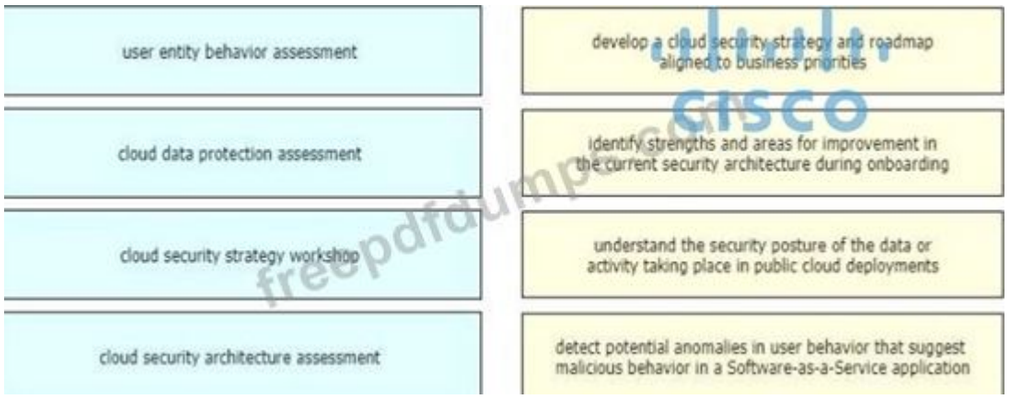
C. CBAC

D. ZBFW

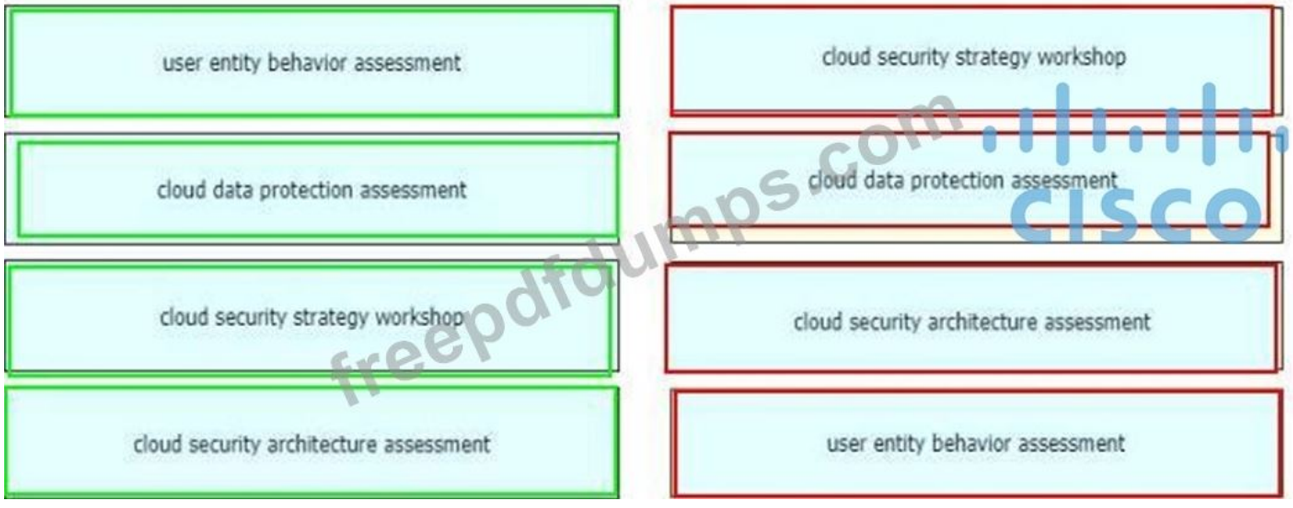
Answer: D (LEAVE A REPLY)

NEW QUESTION: 125

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



Answer:



NEW QUESTION: 126

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

A. impact flags

B. health monitoring

C. URL filtering

D. security intelligence

Answer: A (LEAVE A REPLY)

NEW QUESTION: 127

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 Security Compiance Solution

B. Cisco SDN

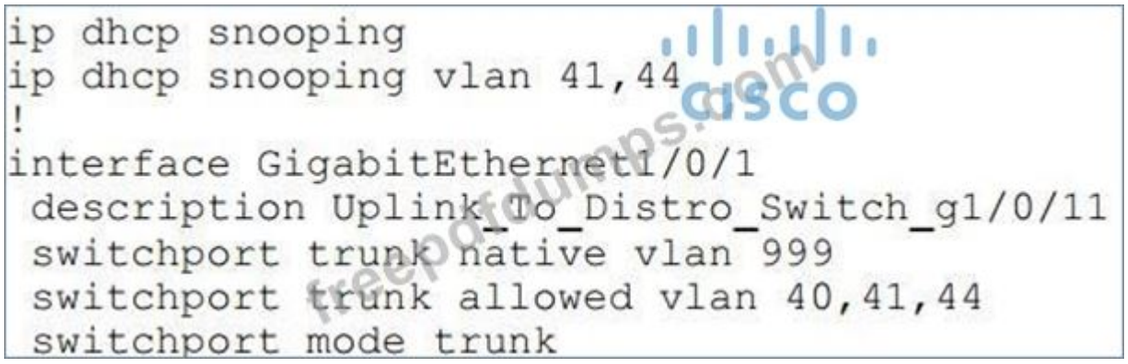
C. Cisco DNA Center

D. Cisco ISE

Answer: (SHOW ANSWER)

NEW QUESTION: 128

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: 129

A network administrator configures Dynamic ARP Inspection on a switch. After Dynamic ARP Inspection is applied, all users on that switch are unable to communicate with any destination. The network administrator checks the interface status of all interfaces, and there is no err-disabled interface. What is causing this problem?

A. DHCP snooping has not been enabled on all VLANs.

B. The ip arp inspection limit command is applied on all interfaces and is blocking the traffic of all users.

C. Dynamic ARP Inspection has not been enabled on all VLANs
D. The no ip arp inspection trust command is applied on all user host interfaces
Answer: D (LEAVE A REPLY)
Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. After enabling DAI, all ports become untrusted ports.

NEW QUESTION: 130
Which Cisco DNA Center Intent API action is used to retrieve the number of devices known to a DNA Center?
A. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/network-device
B. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/network-device/count
C. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/networkdevice?parameter1=value&parameter2=value&....
D. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v 1/networkdevice/startIndex/recordsToReturn
Answer: (SHOW ANSWER)

NEW QUESTION: 131
What is the difference between deceptive phishing and spear phishing?
A. Deceptive phishing is an attacked aimed at a specific user in the organization who holds a C-level role.
B. A spear phishing campaign is aimed at a specific person versus a group of people.
C. Spear phishing is when the attack is aimed at the C-level executives of an organization.
D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.
Answer: B (LEAVE A REPLY)
In deceptive phishing, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.
Spear phishing is carefully designed to get a single recipient to respond. Criminals select an individual target within an organization, using social media and other public information - and craft a fake email tailored for that person.

NEW QUESTION: 132
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: https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F
+ 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:
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: https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F

NEW QUESTION: 133
Which Cisco WSA feature supports access control using URL categories?
A. transparent user identification
B. web usage controls
C. user session restrictions
D. SOCKS proxy services
Answer: A (LEAVE A REPLY)

NEW QUESTION: 134
An administrator configures a new destination list in Cisco Umbrella so that the organization can block specific domains for its devices. What should be done to ensure that all subdomains of domain.com are blocked?
A. Configure the *.com address in the block list.
B. Configure the *.domain.com address in the block list
C. Configure the domain.com address in the block list
D. Configure the *.domain.com address in the block list
Answer: (SHOW ANSWER)

NEW QUESTION: 135
What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?
A. Multiple NetFlow collectors are supported
B. Advanced NetFlow v9 templates and legacy v5 formatting are supported
C. Secure NetFlow connections are optimized for Cisco Prime Infrastructure
D. Flow-create events are delayed
Answer: D (LEAVE A REPLY)
The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions: ... - Delays the export of flow-create events. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.pdf
...
- Delays the export of flow-create events.
The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions: ... - Delays the export of flow-create events. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.pdf

NEW QUESTION: 136
Which two configurations must be made on Cisco ISE and on Cisco TrustSec devices to force a session to be adjusted after a policy change is made? (Choose two)
A. aaa server radius dynamic-author
B. tacacs-server host 10.1.1.250 key password
C. CoA
D. aaa authorization exec default local
E. posture assessment
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 137
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. Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesignGuide-AUG13.pdf 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.
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. Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesignGuide-AUG13.pdf

NEW QUESTION: 138
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 ISE
B. using Cisco ESA
C. using Cisco Umbrella
D. using Cisco FTD
E. using an inline IPS/IDS in the network
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 139
Refer to the exhibit. What is the function of the Python script code snippet for the Cisco ASA REST API?
A. deletes a global rule from policies
B. obtains the saved configuration of the Cisco ASA firewall
C. changes the hostname of the Cisco ASA
D. adds a global rule into policies
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
Which statement describes a traffic profile on a Cisco Next Generation Intrusion Prevention System?

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

NEW QUESTION: 141
Refer to the exhibit.

Consider that any feature of DNS requests, such as the length off the domain name and the number of subdomains, can be used to construct models of expected behavior to which observed values can be compared. Which type of malicious attack are these values associated with?
A. Spectre Worm
B. Heartbleed SSL Bug
C. Eternal Blue Windows
D. W32/AutoRun worm
Answer: D (LEAVE A REPLY)

NEW QUESTION: 142
An engineer adds a custom detection policy to a Cisco AMP deployment and encounters issues with the configuration The simple detection mechanism is configured, but the dashboard indicates that the hash is not 64 characters and is non-zero What is the issue?
A. The engineer is attempting to upload a file instead of a hash
B. The file being uploaded is incompatible with simple detections and must use advanced detections
C. The engineer is attempting to upload a hash created using MD5 instead of SHA-256

D. The hash being uploaded is part of a set in an incorrect format
Answer: C (LEAVE A REPLY)

NEW QUESTION: 143
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: 144
Refer to the exhibit

When configuring this access control rule in Cisco FMC, what happens with the traffic destined to the DMZjnside zone once the configuration is deployed?
A. No traffic will be allowed through to the DMZ_inside zone regardless of if it's trusted or not
B. No traffic will be allowed through to the DMZ_inside zone unless it's already trusted
C. All traffic from any zone will be allowed to the DMZ_inside zone only after inspection
D. All traffic from any zone to the DMZ_inside zone will be permitted with no further inspection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 145
Which encryption algorithm provides highly secure VPN communications?
A. AES 256

B. 3DES
C. AES 128
D. DES
Answer: A (LEAVE A REPLY)

NEW QUESTION: 146
Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?
A. Nexus
B. Firepower
C. Stealthwatch
D. Tetration
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Which Cisco solution extends network visibility, threat detection, and analytics to public cloud environments?
A. Cisco Stealthwatch Cloud
B. Cisco Appdynamics
C. Cisco Umbrella
D. Cisco CloudLock
Answer: A (LEAVE A REPLY)

NEW QUESTION: 148
Which two capabilities does an MDM provide? (Choose two.)
A. unified management of Android and Apple devices from a centralized dashboard
B. unified management of mobile devices, Macs, and PCs from a centralized dashboard
C. delivery of network malware reports to an inbox in a schedule
D. manual identification and classification of client devices
E. enforcement of device security policies from a centralized dashboard
Answer: (SHOW ANSWER)

NEW QUESTION: 149
Which two capabilities does TAXII support? (Choose two)
A. Exchange
B. Pull messaging
C. Binding
D. Correlation
E. Mitigating
Answer: B,C (LEAVE A REPLY)
The Trusted Automated eXchangeof Indicator Information (TAXII) specifies mechanisms for exchanging structured cyber threat information between parties over the network.
TAXII exists to provide specific capabilities to those interested in sharing structured cyber threat information.

TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilities that this version of TAXII supports: push messaging, pull messaging, and discovery.
Although there is no "binding" capability in the list but it is the best answer here.

NEW QUESTION: 150
Which technology is used to improve web traffic performance by proxy caching?
A. ASA
B. WSA
C. FireSIGHT
D. Firepower
Answer: (SHOW ANSWER)

NEW QUESTION: 151
Which two key and block sizes are valid for AES? (Choose two)
A. 64-bit block size, 112-bit key length
B. 64-bit block size, 168-bit key length
C. 128-bit block size, 192-bit key length
D. 128-bit block size, 256-bit key length
E. 192-bit block size, 256-bit key length
Answer: C,D (LEAVE A REPLY)
The AES encryption algorithm encrypts and decrypts data in blocks of 128 bits (block size). It can do this using 128-bit, 192-bit, or 256-bit keys

NEW QUESTION: 152
What is a benefit of using Cisco FMC over Cisco ASDM?
A. Cisco FMC uses Java while Cisco ASDM uses HTML5.
B. Cisco FMC provides centralized management while Cisco ASDM does not.
C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.
D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices
Answer: B (LEAVE A REPLY)
Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide Note: The ASA FirePOWER

module runs on the separately upgraded ASA operating system "You cannot use an FMC to manage ASA firewall functions." Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management. Reference: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheetc78-736775.html the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Reference:
Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system
"You cannot use an FMC to manage ASA firewall functions."
The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management.
Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system "You cannot use an FMC to manage ASA firewall functions." Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management. Reference: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheetc78-736775.html

NEW QUESTION: 153
What is a difference between an XSS attack and an SQL injection attack?
A. SQL injection is a hacking method used to attack SQL databases, whereas XSS attacks can exist in many different types of applications
B. XSS is a hacking method used to attack SQL databases, whereas SQL injection attacks can exist in many different types of applications
C. SQL injection attacks are used to steal information from databases whereas XSS attacks are used to redirect users to websites where attackers can steal data from them
D. XSS attacks are used to steal information from databases whereas SQL injection attacks are used to redirect users to websites where attackers can steal data from them
Answer: C (LEAVE A REPLY)
In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites where attackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POST parameters.

NEW QUESTION: 154
What is the recommendation in a zero-trust model before granting access to corporate applications and resources?
A. to use a wired network, not wireless
B. to disconnect from the network when inactive

C. to use strong passwords
D. to use multifactor authentication
Answer: D (LEAVE A REPLY)

NEW QUESTION: 155
Which Cisco AMP file disposition valid?
A. dirty
B. non malicious
C. pristine
D. malware
Answer: D (LEAVE A REPLY)

NEW QUESTION: 156
Why is it important to patch endpoints consistently?
A. Patching helps to mitigate vulnerabilities.
B. Patching allows for creating a honeypot.
C. Patching reduces the attack surface of the infrastructure.
D. Patching is required per the vendor contract.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 157
Which attack is commonly associated with C and C++ programming languages?
A. cross-site scripting
B. water holing
C. DDoS
D. buffer overflow
Answer: D (LEAVE A REPLY)
A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations. Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's alloted memory space. This happens quite frequently in the case of arrays.

NEW QUESTION: 158
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: A,C (LEAVE A REPLY)

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

...

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.

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

NEW QUESTION: 159

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 is included m the license cost for the multi-org console of Cisco Umbrella

C. It can grant third-party SIEM integrations write access to the S3 bucket

D. Data can be stored offline for 30 days.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 160

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

NEW QUESTION: 161
Which two request of REST API are valid on the Cisco ASA Platform? (Choose two)
A. put
B. options
C. get

D. push
E. connect
Answer: A,C (LEAVE A REPLY)
The ASA REST API gives you programmatic access to managing individual ASAs through a Representational State Transfer (REST) API. The API allows external clients to perform CRUD (Create, Read, Update, Delete) operations on ASA resources; it is based on the HTTPS protocol and REST methodology.
All API requests are sent over HTTPS to the ASA, and a response is returned.
Request Structure
Available request methods are:
GET - Retrieves data from the specified object.
PUT - Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist.
POST - Creates the object with the supplied information.
DELETE - Deletes the specified object
PATCH - Applies partial modifications to the specified object. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html PATCH - Applies partial modifications to the specified object. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html

NEW QUESTION: 162
Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?
A. Group Policy
B. Access Control Policy
C. Device Management Policy
D. Platform Service Policy
Answer: D (LEAVE A REPLY)
Cisco Firepower deployments can take advantage of platform settings policies. A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. Examples of these platform settings policies are time and date settings, external authentication, and other common administrative features. A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device. For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/platform_settings_policies_for_managed_devices.html Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best answer here so we have to choose it.
administrative features.

A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device.
For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.
Reference:
Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best Cisco Firepower deployments can take advantage of platform settings policies. A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. Examples of these platform settings policies are time and date settings, external authentication, and other common administrative features. A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device. For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/platform_settings_policies_for_managed_devices.html Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best answer here so we have to choose it.

NEW QUESTION: 163
Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two.)
A. RADIUS
B. sFlow
C. TACACS+
D. SMTP
E. DHCP
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 164
What is a feature of the open platform capabilities of Cisco DNA Center?
A. application adapters
B. automation adapters
C. domain integration
D. intent-based APIs
Answer: D (LEAVE A REPLY)

NEW QUESTION: 165
How is ICMP used an exfiltration technique?
A. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address
B. by overwhelming a targeted host with ICMP echo-request packets
C. by flooding the destination host with unreachable packets
D. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host
Answer: D (LEAVE A REPLY)

NEW QUESTION: 166
When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?
A. Spero analysis
B. dynamic analysis
C. sandbox analysis
D. malware analysis
Answer: B (LEAVE A REPLY)
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: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Reference_a_wrapper_Chapter_topic_here.html -> 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.
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 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:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Reference_a_wrapper_Chapter_topic_here.html -> 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: 167

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

A. Cisco ISE

B. Cisco NAC

C. Cisco WSA

D. Cisco TACACS+

Answer: A (LEAVE A REPLY)

NEW QUESTION: 168

A network engineer is deciding whether to use stateful or stateless failover when configuring two ASAs for high availability. What is the connection status in both cases?

A. need to be reestablished with both stateful and stateless failover

B. preserved with stateful failover and need to be reestablished with stateless failover

C. need to be reestablished with stateful failover and preserved with stateless failover

D. preserved with both stateful and stateless failover

Answer: (SHOW ANSWER)

NEW QUESTION: 169

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

A. IP Slock List Center

B. IP and Domain Reputation Center

C. File Reputation Center

D. AMP Reputation Center

Answer: (SHOW ANSWER)

NEW QUESTION: 170

Which two mechanisms are used to control phishing attacks? (Choose two.)

A. Revoke expired CRL of the websites

B. Enable browser alerts for fraudulent websites

C. Use antispyware software

D. Implement email filtering techniques

E. Define security group memberships

Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 171

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: 172
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. public cloud
B. private cloud
C. community cloud
D. hybrid cloud
Answer: (SHOW ANSWER)

NEW QUESTION: 173
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. Change the password on hostA to the default password.
B. Enter the command with a different password on hostB.
C. Enter the same command on hostB.
D. Change isakmp to ikev2 in the command on hostA.
Answer: (SHOW ANSWER)

NEW QUESTION: 174
Which license is required for Cisco Security Intelligence to work on the Cisco Next Generation Intrusion Prevention System?
A. protect
B. control
C. URL filtering
D. malware
Answer: A (LEAVE A REPLY)

NEW QUESTION: 175
What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?
A. EDR focuses on network security, and EPP focuses on device security.
B. EPP focuses on network security, and EDR 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: (SHOW ANSWER)

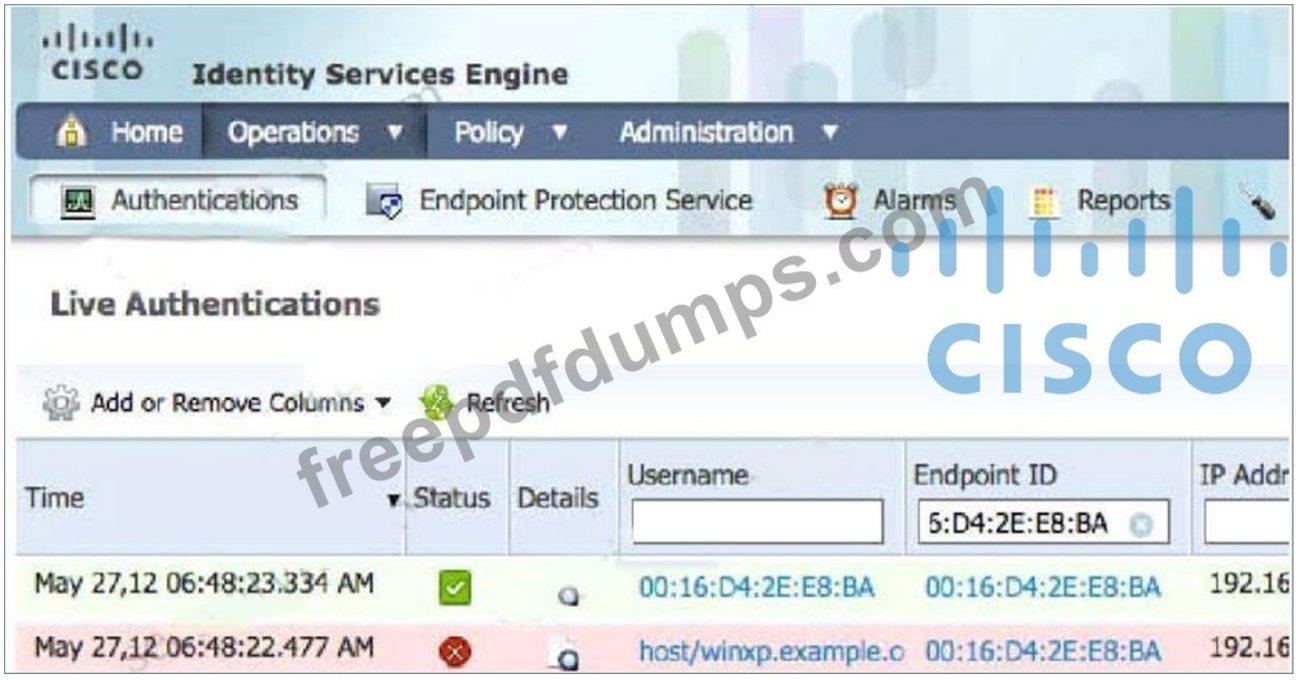
NEW QUESTION: 176

Which feature is leveraged by advanced antimalware capabilities to be an effective endpomt protection platform?
A. blocklisting
B. storm centers
C. sandboxing
D. big data
Answer: C (LEAVE A REPLY)

NEW QUESTION: 177
Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)
A. It must have been signed by an internal CA.
B. it must contain a SAN.
C. It must reside in the trusted store of the WSA.
D. It must reside in the trusted store of the endpoint.
E. It must include the current date.
Answer: (SHOW ANSWER)

NEW QUESTION: 178
Which Cisco security solution integrates with cloud applications like Dropbox and Office 365 while protecting data from being exfiltrated?
A. Cisco Umbrella Investigate
B. Cisco Cloudlock
C. Cisco Tajos
D. Cisco Steaithwatch Cloud
Answer: B (LEAVE A REPLY)

NEW QUESTION: 179
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: D (LEAVE A REPLY)
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: 180
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: B (LEAVE A REPLY)
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: 181
What is the purpose of joining Cisco WSAs to an appliance group?
A. The group supports improved redundancy
B. It simplifies the task of patching multiple appliances.
C. All WSAs in the group can view file analysis results.
D. It supports cluster operations to expedite the malware analysis process.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 182
An organization wants to improve its cybersecurity processes and to add intelligence to its data The organization wants to utilize the most current intelligence data for URL filtering, reputations, and vulnerability information that can be integrated with the Cisco FTD and Cisco WSA What must be done to accomplish these objectives?
A. Download the threat intelligence feed from the IETF and import it into the Cisco FTD and Cisco WSA databases
B. Create a Cisco pxGrid connection to NIST to import this information into the security products for policy use
C. Create an automated download of the Internet Storm Center intelligence feed into the Cisco FTD and Cisco WSA databases to tie to the dynamic access control policies.
D. Configure the integrations with Talos Intelligence to take advantage of the threat intelligence that it provides.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 183
When planning a VPN deployment, for which reason does an engineer opt for an active/active FlexVPN configuration as opposed to DMVPN?
A. Traffic is distributed statically by default.
B. Floating static routes are required.
C. HSRP is used for faliover.
D. Multiple routers or VRFs are required.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 184
Refer to the exhibit.

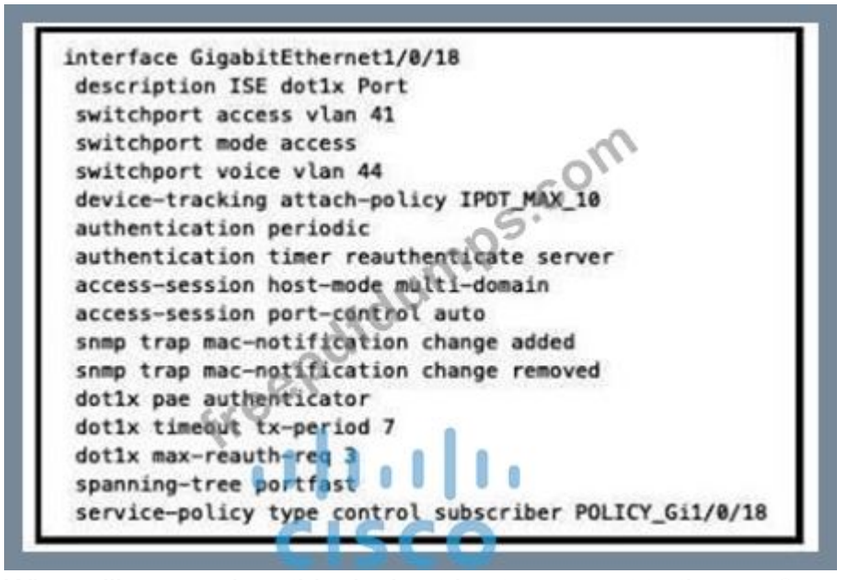
```
Sysauthcontrol              Enabled
Dot1x Protocol Version      3

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

Which command was used to display this output?
A. show dot1x all summary
B. show dot1x all
C. show dot1x interface gi1/0/12
D. show dot1x
Answer: (SHOW ANSWER)

NEW QUESTION: 185
Which Cisco platform processes behavior baselines, monitors for deviations, and reviews for malicious processes in data center traffic and servers while performing software vulnerability detection?
A. Cisco Tetration
B. Cisco ISE?
C. Cisco AMP for Network
D. Cisco AnyConnect
Answer: (SHOW ANSWER)

NEW QUESTION: 186
How does a WCCP-configured router identify if the Cisco WSA is functional?
A. The WSA sends a Here-I-Am message every 10 seconds, and the router acknowledges with an ISee-You message.
B. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the WSA.
C. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the router.
D. The router sends a Here-I-Am message every 10 seconds, and the WSA acknowledges with an ISee-You message.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 187
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 will work and the device will be allowed on the network
C. 802 1X and MAB will both be used and ISE can use policy to determine the access level

D. 802.1X will not work and the device will not be allowed network access
Answer: C (LEAVE A REPLY)

NEW QUESTION: 188
An engineer musi set 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. sticky
C. maximum
D. aging
Answer: B (LEAVE A REPLY)

NEW QUESTION: 189
Which two descriptions of AES encryption are true? (Choose two.)
A. AES can use a 168-bit key for encryption.
B. AES is more secure than 3DES
C. AES is less secure than 3DES
D. AES can use a 256-bit key for encryption.
E. AES encrypts and decrypts a key three times in sequence
Answer: (SHOW ANSWER)

NEW QUESTION: 190
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: C,E (LEAVE A REPLY)
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: 191
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: 192

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: C (LEAVE A REPLY)

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. Reference: https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-IntelligentProxy 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. Reference: https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-IntelligentProxy

NEW QUESTION: 193

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: (SHOW ANSWER)

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: 194

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

A. If four log in attempts fail in 100 seconds, wait for 60 seconds to next log in prompt.

B. If four failures occur in 60 seconds, the router goes to quiet mode for 100 seconds.

C. After four unsuccessful log in attempts, the line is blocked for 100 seconds and only permit IP addresses are permitted in ACL

D. After four unsuccessful log in attempts, the line is blocked for 60 seconds and only permit IP addresses are permitted in ACL1

Answer: A (LEAVE A REPLY)

NEW QUESTION: 195

Which Cisco ASA Platform mode disables the threat detection features except for Advanced Threat Statistics?

A. routed

B. multiple context

C. transparent

D. cluster
Answer: (SHOW ANSWER)

NEW QUESTION: 196
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: (SHOW ANSWER)
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. Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management 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.
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. Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management

NEW QUESTION: 197
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: (SHOW ANSWER)
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: 198
An organization deploys multiple Cisco FTD appliances and wants to manage them using one centralized solution. The organization does not have a local VM but does have existing Cisco ASAs that must migrate over to Cisco FTDs. Which solution meets the needs of the organization?
A. CSM
B. Cisco FMC
C. Cisco FDM
D. CDO
Answer: B (LEAVE A REPLY)

NEW QUESTION: 199

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

A. Configure a Cisco FMC to send syslogs to Cisco Stealthwatch Cloud

B. Deploy the Cisco Stealthwatch Cloud PNM sensor that sends data to Cisco Stealthwatch Cloud

C. Deploy a Cisco FTD sensor to send network events to Cisco Stealthwatch Cloud

D. Configure a Cisco FMC to send NetFlow to Cisco Stealthwatch Cloud

Answer: (SHOW ANSWER)

The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems. Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.

The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems. Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf

NEW QUESTION: 200

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

A. Cisco WSAV

B. Cisco ASAV

C. Cisco Stealthwatch Cloud

D. Cisco Cloud Orchestrator

Answer: (SHOW ANSWER)

NEW QUESTION: 201

Which type of protection encrypts RSA keys when they are exported and imported?

A. passphrase

B. nonexportable

C. file

D. NGE

Answer: A (LEAVE A REPLY)

NEW QUESTION: 202

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: 203

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. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html

+ 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.
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. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html

NEW QUESTION: 204
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)
A. Patch for cross-site scripting.
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.
D. Install a spam and virus email filter.
E. Protect systems with an up-to-date antimalware program
Answer: D,E (LEAVE A REPLY)
Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

NEW QUESTION: 205
Which cryptographic process provides origin confidentiality, integrity, and origin authentication for packets?
A. AH
B. IKEv1
C. IKEv2
D. ESP
Answer: (SHOW ANSWER)

NEW QUESTION: 206
Which security product enables administrators to deploy Kubernetes clusters in air-gapped sites without needing Internet access?
A. Cisco Container Controller

B. Cisco Cloud Platform
C. Cisco Container Platform
D. Cisco Content Platform
Answer: (SHOW ANSWER)

NEW QUESTION: 207
A Cisco Firepower administrator needs to configure a rule to allow a new application that has never been seen on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose two)
A. permit
B. trust
C. reset
D. allow
E. monitor
Answer: B,E (LEAVE A REPLY)
Each rule also has an action, which determines whether you monitor, trust, block, or allow matching traffic.
Note: With action "trust", Firepower does not do any more inspection on the traffic. There will be no intrusion protection and also no file-policy on this traffic.

NEW QUESTION: 208
An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation. What must be un solution?
A. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701.
B. GRE over IPsec cannot be used as a standalone protocol, and L2TP can.
C. L2TP is an IP packet encapsulation protocol, and GRE over IPsec is a tunneling protocol.
D. GRE over IPsec adds its own header, and L2TP does not.
Answer: (SHOW ANSWER)

NEW QUESTION: 209
Which direction do attackers encode data in DNS requests during exfiltration using DNS tunneling?
A. outbound
B. north-south
C. inbound
D. east-west
Answer: A (LEAVE A REPLY)

NEW QUESTION: 210
An engineer is implementing DHCP security mechanisms and needs the ability to add additional attributes to profiles that are created within Cisco ISE Which action accomplishes this task?
A. Define MAC-to-IP address mappings in the switch to ensure that rogue devices cannot get an IP address
B. Modify the DHCP relay and point the IP address to Cisco ISE.

C. Use DHCP option 82 to ensure that the request is from a legitimate endpoint and send the information to Cisco ISE
D. Configure DHCP snooping on the switch VLANs and trust the necessary interfaces
Answer: D (LEAVE A REPLY)

NEW QUESTION: 211
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: A (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. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html
- 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.
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. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html

NEW QUESTION: 212
Which two parameters are used to prevent a data breach in the cloud? (Choose two.)
A. DLP solutions
B. antispoofing programs
C. encryption
D. strong user authentication
E. complex cloud-based web proxies
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 213
What are two rootkit types? (Choose two)
A. registry
B. virtual
C. bootloader
D. user mode
E. buffer mode
Answer: (SHOW ANSWER)
The term 'rootkit' originally comes from the Unix world, where the word 'root' is used to describe a user with the highest possible level of access privileges, similar to an 'Administrator' in Windows. The word 'kit' refers to the software that grants root-level access to the machine. Put the two together and you get 'rootkit', a program that gives someone - with legitimate or malicious intentions - privileged access to a computer.
There are four main types of rootkits: Kernel rootkits, User mode rootkits, Bootloader rootkits, Memory rootkits

NEW QUESTION: 214
What is an attribute of the DevSecOps process?
A. mandated security controls and check lists
B. security scanning and theoretical vulnerabilities
C. development security
D. isolated security team
Answer: C (LEAVE A REPLY)
DevSecOps (development, security, and operations) is a concept used in recent years to describe how to move security activities to the start of the development life cycle and have built-in security practices in the continuous integration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer to IT and business objectives.
Three key things make a real DevSecOps environment:
+ Security testing is done by the development team.
+ Issues found during that testing is managed by the development team.
+ Fixing those issues stays within the development team.

NEW QUESTION: 215
Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?
A. OpenC2
B. OpenIOC
C. CybOX
D. STIX
Answer: B (LEAVE A REPLY)

NEW QUESTION: 216
Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two)
A. DDoS
B. antispam
C. antivirus
D. encryption
E. DLP
Answer: D,E (LEAVE A REPLY)
Cisco Hybrid Email Security is a unique service offering that combines a cloud-based email security deployment with an appliance-based email security deployment (on premises) to provide maximum choice and control for your organization. The cloud-based infrastructure is typically used for inbound email cleansing, while the onpremises appliances provide granular control - protecting sensitive information with data loss prevention (DLP) and encryption technologies. Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf with an appliance-based email security deployment (on premises) to provide maximum choice and control for your organization. The cloud-based infrastructure is typically

used for inbound email cleansing, while the onpremises appliances provide granular control - protecting sensitive information with data loss prevention (DLP) and encryption technologies.
Reference:
Cisco Hybrid Email Security is a unique service offering that combines a cloud-based email security deployment with an appliance-based email security deployment (on premises) to provide maximum choice and control for your organization. The cloud-based infrastructure is typically used for inbound email cleansing, while the onpremises appliances provide granular control - protecting sensitive information with data loss prevention (DLP) and encryption technologies. Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

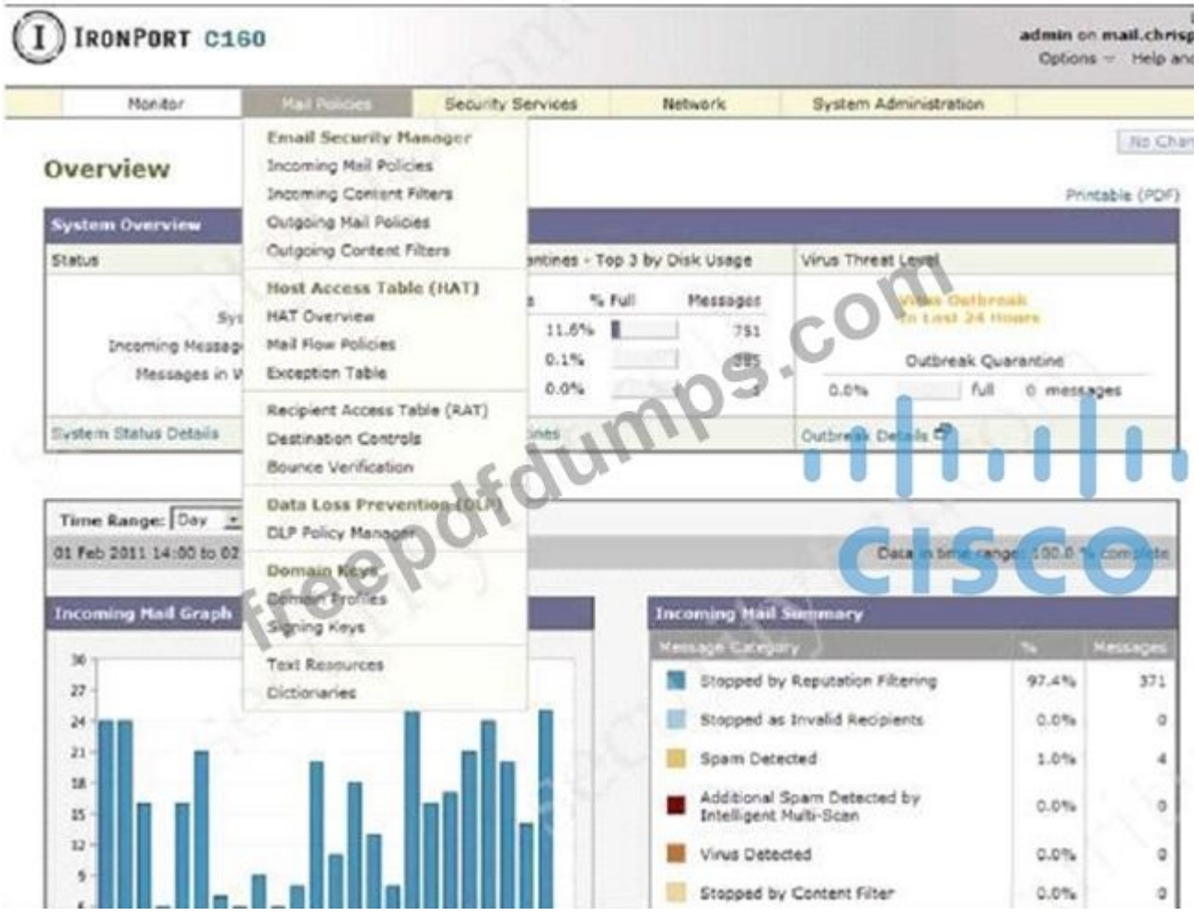
NEW QUESTION: 217
An organization wants to use Cisco FTD or Cisco ASA devices. Specific URLs must be blocked from being accessed via the firewall which requires that the administrator input the bad URL categories that the organization wants blocked into the access policy. Which solution should be used to meet this requirement?
A. Cisco ASA because it includes URL filtering in the access control policy capabilities, whereas Cisco FTD does not
B. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not
C. Cisco ASA because it enables URL filtering and blocks malicious URLs by default, whereas Cisco FTD does not
D. Cisco FTD because it includes URL filtering in the access control policy capabilities, whereas Cisco ASA does not
Answer: (SHOW ANSWER)

NEW QUESTION: 218
What are two security benefits of an MDM deployment? (Choose two.)
A. distributed software upgrade
B. distributed dashboard
C. privacy control checks
D. robust security policy enforcement
E. on-device content management
Answer: (SHOW ANSWER)

NEW QUESTION: 219
How many interfaces per bridge group does an ASA bridge group deployment support?
A. up to 2
B. up to 4
C. up to 8
D. up to 16
Answer: (SHOW ANSWER)
Each of the ASAs interfaces need to be grouped into one or more bridge groups. Each of these groups acts as an independent transparent firewall. It is not possible for one bridge group to communicate with another bridge group without assistance from an external router.

As of 8.4(1) upto 8 bridge groups are supported with 2-4 interface in each group. Prior to this only one bridge group was supported and only 2 interfaces.
Up to 4 interfaces are permitted per bridge-group (inside, outside, DMZ1, DMZ2)

NEW QUESTION: 220
An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically.
What must be configured to accomplish this?
A. Configure the Cisco WSA to modify policies based on the traffic seen
B. Configure the Cisco ESA to receive real-time updates from Talos
C. Configure the Cisco WSA to receive real-time updates from Talos
D. Configure the Cisco ESA to modify policies based on the traffic seen
Answer: D (LEAVE A REPLY)
The Mail Policies menu is where almost all of the controls related to email filtering happens. All the security and content filtering policies are set here, so it's likely that, as an ESA administrator, the pages on this menu are where you are likely to spend most of your time.



NEW QUESTION: 221
Which benefit does DMVPN provide over GETVPN?
A. DMVPN is a tunnel-less VPN, and GETVPN is tunnel-based.

B. DMVPN supports QoS, multicast, and routing, and GETVPN supports only QoS.
C. DMVPN supports non-IP protocols, and GETVPN supports only IP protocols.
D. DMVPN can be used over the public Internet, and GETVPN requires a private network.
Answer: D (LEAVE A REPLY)