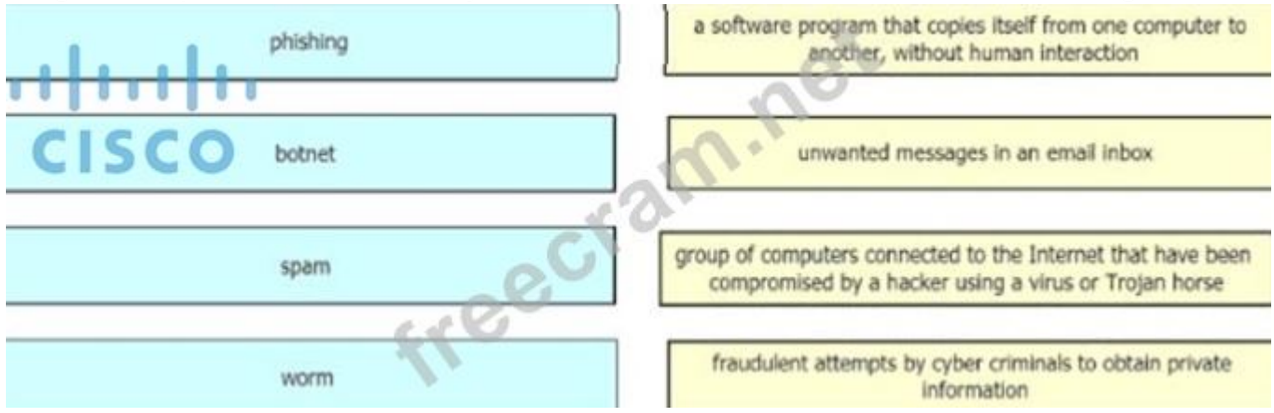
Cisco.350-701.v2022-08-29.q162

Exam Code:	350-701
Exam Name:	Implementing and Operating Cisco Security Core Technologies
Certification Provider:	Cisco
Free Question Number:	162
Version:	v2022-08-29
# of views:	809
# of Questions views:	28787
https://www.freecram.net/torrent/Cisco.350-701.v2022-08-29.q162.html	

NEW QUESTION: 1
Drag and drop the common security threats from the left onto the definitions on the right.



Answer:

NEW QUESTION: 2
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: 3
Which two descriptions of AES encryption are true? (Choose two.)
A. AES can use a 256-bit key for encryption.
B. AES is less secure than 3DES
C. AES can use a 168-bit key for encryption.

D. AES encrypts and decrypts a key three times in sequence
E. AES is more secure than 3DES
Answer: (SHOW ANSWER)

NEW QUESTION: 4
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: (SHOW ANSWER)

NEW QUESTION: 5
Which CLI command is used to register a Cisco FirePower sensor to Firepower Management Center?
A. configure manager add <host><key
B. configure manager delete
C. configure system add <host><key>
D. configure manager <key> add host
Answer: (SHOW ANSWER)

NEW QUESTION: 6
An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?
A. SIEM
B. CASB
C. Adaptive MFA
D. Cisco Cloudlock
Answer: (SHOW ANSWER)
+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy. + Cloudlock is API-based. + Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).
Reference: https://docs.umbrella.com/cloudlock-documentation/docs/endpoints Note: + Security information and event management (SIEM) platforms collect log and event data from security systems, networks and computers, and turn it into actionable security insights. + An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when a condition of an alerting policy has been met.
to identify sensitive information stored in cloud environments in violation of policy.
+ Cloudlock is API-based.

+ Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).
Reference:
Note:
+ Security information and event management (SIEM) platforms collect log and event data from security systems, networks and computers, and turn it into actionable security insights.
+ An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when a
+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy. + Cloudlock is API-based. + Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).
Reference: https://docs.umbrella.com/cloudlock-documentation/docs/endpoints Note: + Security information and event management (SIEM) platforms collect log and event data from security systems, networks and computers, and turn it into actionable security insights. + An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when a condition of an alerting policy has been met.

NEW QUESTION: 7
Which system performs compliance checks and remote wiping?
A. AMP
B. OTP
C. MDM
D. ISE
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Which method is used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources?
A. BYOD on boarding
B. Simple Certificate Enrollment Protocol
C. Client provisioning
D. MAC authentication bypass
Answer: (SHOW ANSWER)
When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network. Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal. Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices. Reference: 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: 9
In which two ways does a system administrator send web traffic transparently to the Web Security Appliance? (Choose two.)
A. reference a Proxy Auto Config file
B. use Web Cache Communication Protocol
C. configure Active Directory Group Policies to push proxy settings
D. configure the proxy IP address in the web-browser settings
E. configure policy-based routing on the network infrastructure
Answer: (SHOW ANSWER)

NEW QUESTION: 10
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: (SHOW ANSWER)
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: 11

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. Send the file to Cisco Threat Grid for dynamic analysis

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

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

D. Upload the hash for the file into the policy

Answer: (SHOW ANSWER)

NEW QUESTION: 12

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

A. type of service byte

B. class of service bits

C. Layer 4 protocol type

D. destination port

E. output logical interface

Answer: (SHOW ANSWER)

Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share seven values which define a unique key for the flow:

+ Ingress interface (SNMP ifIndex)
+ Source IP address
+ Destination IP address
+ IP protocol
+ Source port for UDP or TCP, 0 for other protocols
+ Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
+ IP Type of Service

Note: A flow is a unidirectional series of packets between a given source and destination.

NEW QUESTION: 13

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

A. insecure implementation of API

B. misconfiguration of infrastructure, which allows unauthorized access

C. intermittent connection to the cloud connectors

D. vulnerabilities within protocol

Answer: (SHOW ANSWER)

NEW QUESTION: 14

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: (SHOW ANSWER)
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: 15
Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or Microsoft vSwitch?
A. intra-EPG isolation
B. inter-EPG isolation
C. placement in separate EPGs
D. inter-VLAN security
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
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: (SHOW ANSWER)
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: 17
Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?
A. Dynamic ARP Inspection
B. multifactor authentication
C. fingerprinting
D. RADIUS-based REAP
Answer: (SHOW ANSWER)

NEW QUESTION: 18
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

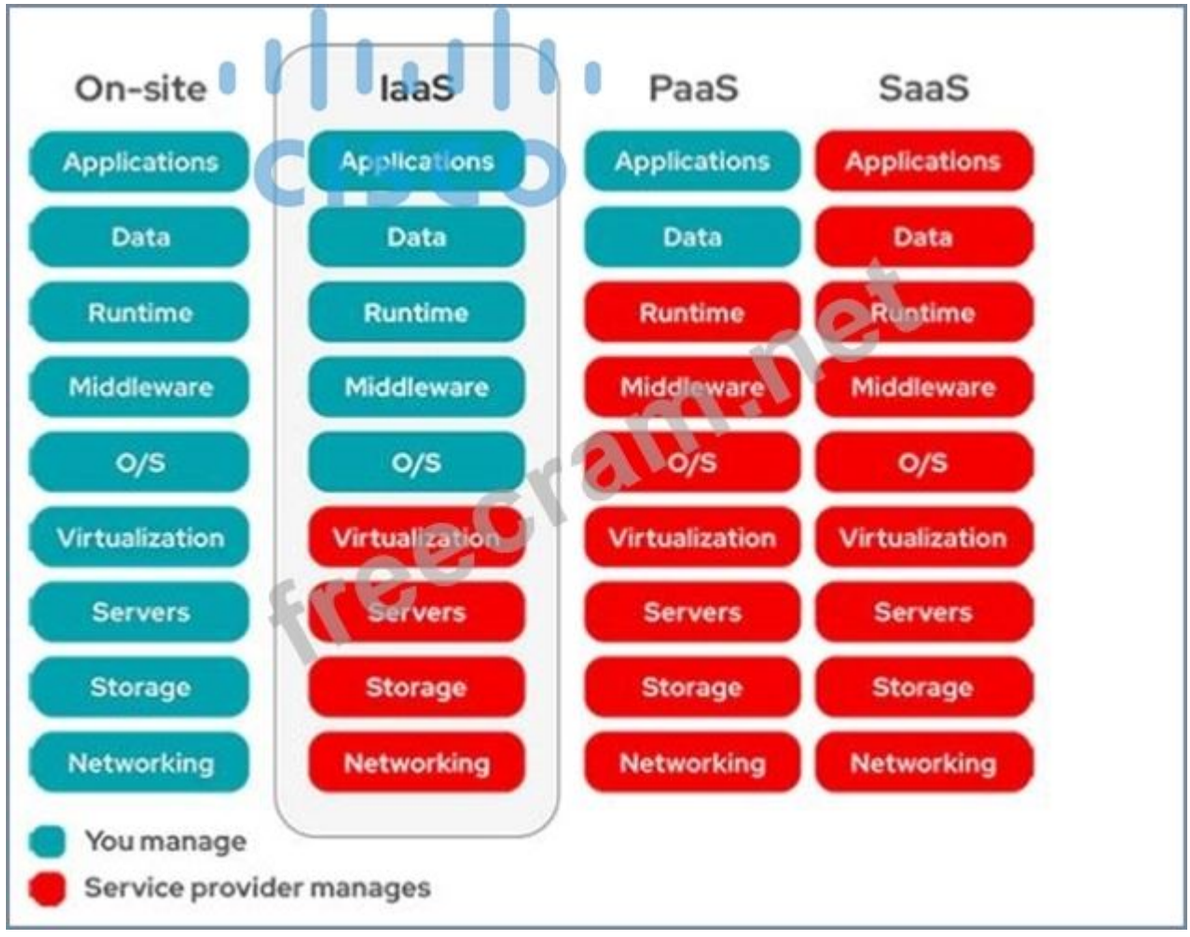
NEW QUESTION: 19
What are two functions of secret key cryptography? (Choose two.)
A. utilization of less memory
B. utilization of different keys for encryption and decryption
C. provides the capability to only know the key on one side
D. utilization of large prime number iterations
E. key selection without integer factorization
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Using Cisco Firepower's Security Intelligence policies, upon which two criteria is Firepower block based?
(Choose two)

A. URLs
B. protocol IDs
C. IP addresses
D. MAC addresses
E. port numbers
Answer: (SHOW ANSWER)
Security Intelligence Sources ... Custom Block lists or feeds (or objects or groups) Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects or groups.) For example, if you become aware of malicious sites or addresses that are not yet blocked by a feed, add these sites to a custom Security Intelligence list and add this custom list to the Block list in the Security Intelligence tab of your access control policy. 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: 21
In which cloud services model is the tenant responsible for virtual machine OS patching?
A. IaaS
B. UCaaS
C. PaaS
D. SaaS
Answer: (SHOW ANSWER)
Only in On-site (on-premises) and IaaS we (tenant) manage O/S (Operating System).



NEW QUESTION: 22
What is a difference between a DoS attack and a DDoS attack?
A. A DoS attack is where a computer is used to flood a server with TCP packets whereas a DDoS attack is where a computer is used to flood a server with UDP packets
B. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where multiple systems target a single system with a DoS attack
C. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where a computer is used to flood multiple servers that are distributed over a LAN
D. A DoS attack is where a computer is used to flood a server with UDP packets whereas a DDoS attack is where a computer is used to flood a server with TCP packets
Answer: (SHOW ANSWER)

NEW QUESTION: 23
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: 24

Refer to the exhibit.

```
import requests
client_id = '<Client id>'
api_key = '<API Key>'
url = 'https://api.amp.cisco.com/v1/computers'
response = requests.get(url, auth=(client_id, api_key))
response_json = response.json()
for computer in response_json['data']
    hostname = computer['hostname']
    print(hostname)
```


What will happen when the Python script is executed?

A. The script will pull all computer hostnames and print them.

B. The script will translate the IP address to FODN and print it

C. The hostname will be printed for the client in the client ID field.

D. The hostname will be translated to an IP address and printed.

Answer: (SHOW ANSWER)

NEW QUESTION: 25

Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two)

A. virtualization

B. middleware

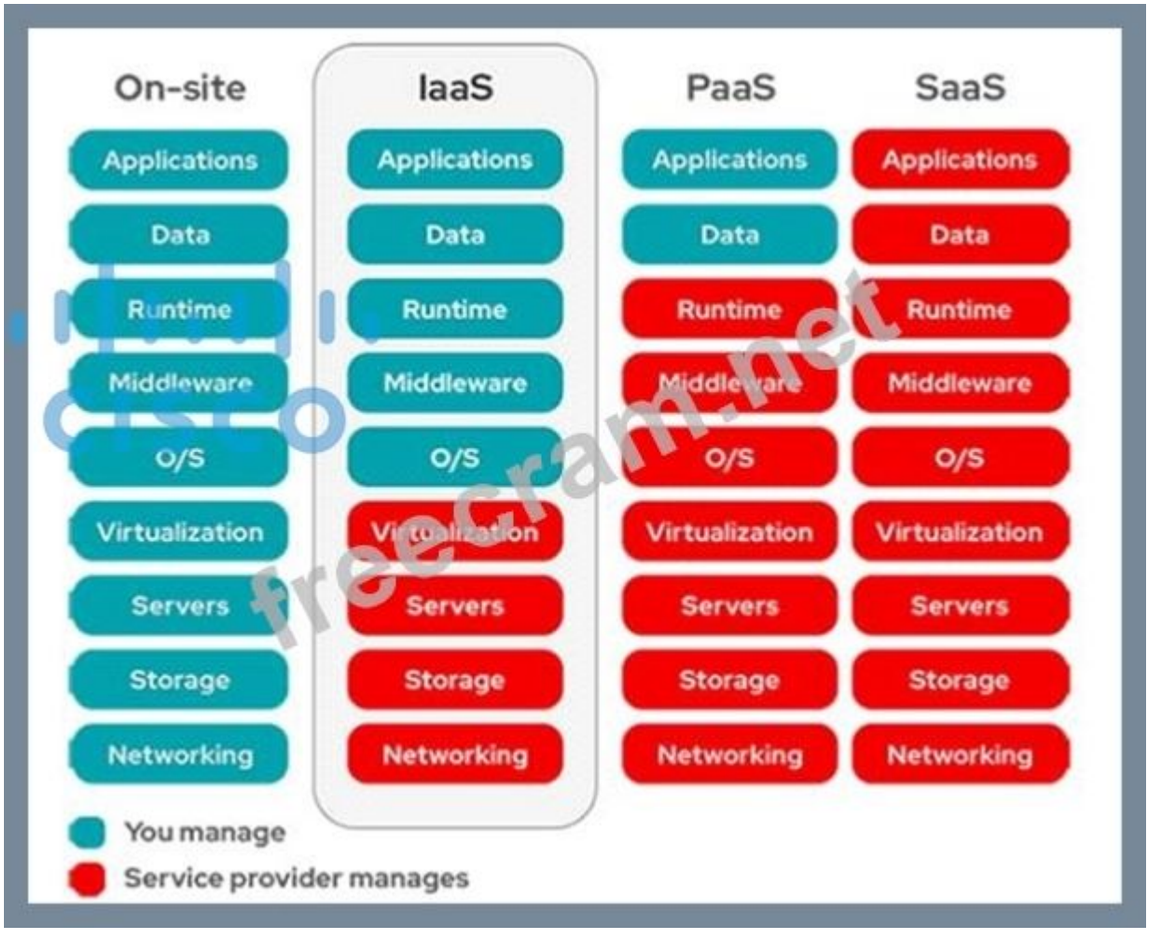
C. operating systems

D. applications

E. data

Answer: (SHOW ANSWER)

Customers must manage applications and data in PaaS.



NEW QUESTION: 26
What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.)
A. Deploy a separate eDirectory server; the dent IP address is recorded in this server.
B. Create an LDAP authentication realm and disable transparent user identification.
C. The eDirectory client must be installed on each client workstation.
D. Create NTLM or Kerberos authentication realm and enable transparent user identification.
E. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.
Answer: (SHOW ANSWER)

NEW QUESTION: 27
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: 28
Which ASA deployment mode can provide separation of management on a shared appliance?
A. DMZ multiple zone mode
B. routed mode
C. multiple context mode
D. transparent firewall mode
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which option is the main function of Cisco Firepower impact flags?
A. They alert administrators when critical events occur.
B. They highlight known and suspected malicious IP addresses in reports.
C. They identify data that the ASA sends to the Firepower module.
D. They correlate data about intrusions and vulnerability.
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Why should organizations migrate to an MFA strategy for authentication?
A. Biometrics authentication leads to the need for MFA due to its ability to be hacked easily.
B. Single methods of authentication can be compromised more easily than MFA.
C. MFA methods of authentication are never compromised.
D. MFA does not require any piece of evidence for an authentication mechanism.
Answer: (SHOW ANSWER)

NEW QUESTION: 31
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. Create an identity policy within Cisco ISE to send all authentication requests to Cisco DUO.
B. Configure Cisco DUO with the external Active Directory connector and tie it to the policy set within Cisco ISE.
C. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE

D. Modify the current policy with the condition MFASourceSequence DUO=true in the authorization conditions within Cisco ISE

Answer: A (LEAVE A REPLY)

NEW QUESTION: 32

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

A. SDN controller and the network elements

B. management console and the SDN controller

C. management console and the cloud

D. SDN controller and the cloud

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 33

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

A. The administrator must upload the file instead of the hash for Cisco AMP to use.

B. Detections for MD5 signatures must be configured in the advanced custom detection policies

C. The APK must be uploaded for the application that the detection is intended

D. The MD5 hash uploaded to the simple detection policy is in the incorrect format

Answer: (SHOW ANSWER)

NEW QUESTION: 34

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. Dynamic ARP inspection

D. Port security

E. Private VLANs

F. IP Device track

Answer: (SHOW ANSWER)

NEW QUESTION: 35
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: 36
What is a characteristic of Dynamic ARP Inspection?
A. DAI intercepts all ARP requests and responses on trusted ports only
B. DAI associates a trust state with each switch.
C. In a typical network, make all ports as trusted except for the ports connecting to switches, which are untrusted.
D. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCP snooping binding database
Answer: (SHOW ANSWER)

NEW QUESTION: 37
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: (SHOW ANSWER)
An example of configuring a NetFlow exporter is shown below:
flow exporter Exporter
destination 192.168.100.22
transport udp 2055

NEW QUESTION: 38
Which command enables 802.1X globally on a Cisco switch?
A. dot1x system-auth-control
B. aaa new-model
C. dot1x pae authenticator
D. authentication port-control aut

Answer: (SHOW ANSWER)

NEW QUESTION: 39
What is the primary role of the Cisco Email Security Appliance?
A. Mail Submission Agent
B. Mail Transfer Agent
C. Mail Delivery Agent
D. Mail User Agent
Answer: (SHOW ANSWER)
Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay. Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/Cisco_SBA_BN_EmailSecurityUsingCiscoESADeploymentGuide-Feb2013.pdf by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay.
Reference:
Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay. Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/Cisco_SBA_BN_EmailSecurityUsingCiscoESADeploymentGuide-Feb2013.pdf

NEW QUESTION: 40
Which attack is preventable by Cisco ESA but not by the Cisco WSA?
A. buffer overflow
B. DoS
C. SQL injection
D. phishing
Answer: (SHOW ANSWER)
The following are the benefits of deploying Cisco Advanced Phishing Protection on the Cisco Email Security Gateway: Prevents the following: + Attacks that use compromised accounts and social engineering. + Phishing, ransomware, zero-day attacks and spoofing. + BEC with no malicious payload or URL. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html Gateway:
Prevents the following:
+ Attacks that use compromised accounts and social engineering.
+ Phishing, ransomware, zero-day attacks and spoofing.

+ BEC with no malicious payload or URL.
Reference:
The following are the benefits of deploying Cisco Advanced Phishing Protection on the Cisco Email Security Gateway: Prevents the following: + Attacks that use compromised accounts and social engineering. + Phishing, ransomware, zero-day attacks and spoofing. + BEC with no malicious payload or URL. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html

NEW QUESTION: 41
Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?
A. STIX
B. CybOX
C. OpenIOC
D. OpenC2
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which Cisco security solution protects remote users against phishing attacks when they are not connected to the VPN?
A. Cisco Stealthwatch
B. Cisco Umbrella
C. Cisco Firepower
D. NGIPS
Answer: (SHOW ANSWER)
Cisco Umbrella protects users from accessing malicious domains by proactively analyzing and blocking unsafe destinations - before a connection is ever made. Thus it can protect from phishing attacks by blocking suspicious domains when users click on the given links that an attacker sent. Cisco Umbrella roaming protects your employees even when they are off the VPN.

NEW QUESTION: 43
Which two tasks allow NetFlow on a Cisco ASA 5500 Series firewall? (Choose two.)
A. Create an ACL to allow UDP traffic on port 9996.
B. Create a class map to match interesting traffic.
C. Define a NetFlow collector by using the flow-export command.
D. Apply NetFlow Exporter to the outside interface in the inbound direction.
E. Enable NetFlow Version 9.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
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 provides flow-based visibility for the endpoints network connections.
C. It enables behavioral analysis to be used for the endpoints.
D. It protects endpoint systems through application control and real-time scanning
Answer: D (LEAVE A REPLY)

NEW QUESTION: 45
An engineer is configuring Cisco Umbrella and has an identity that references two different policies. Which action ensures that the..... use takes precedence over the second one?
A. Make the correct policy first in the policy order.
B. Place the policy with the most-specific configuration last in the policy order.
C. Configure the default policy to redirect the requests to the correct policy.
D. Configure only the policy with the most recently changed timestamp.
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Which Cisco cloud security software centrally manages policies on multiple platforms such as Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS?
A. Cisco DNAC
B. Cisco Defense Orchestrator
C. Cisco Secureworks
D. Cisco Configuration Professional
Answer: (SHOW ANSWER)

NEW QUESTION: 47
After deploying a Cisco ESA on your network, you notice that some messages fail to reach their destinations. Which task can you perform to determine where each message was lost?
A. Configure the trackingconfig command to enable message tracking.
B. Generate a system report.
C. Review the log files.
D. Perform a trace.
Answer: (SHOW ANSWER)
Message tracking helps resolve help desk calls by giving a detailed view of message flow. For example, if a message was not delivered as expected, you can determine if it was found to contain a virus or placed in a

spam quarantine - or if it is located somewhere else in the mail stream. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_011110.html Reference: Message tracking helps resolve help desk calls by giving a detailed view of message flow. For example, if a message was not delivered as expected, you can determine if it was found to contain a virus or placed in a spam quarantine - or if it is located somewhere else in the mail stream. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_011110.html

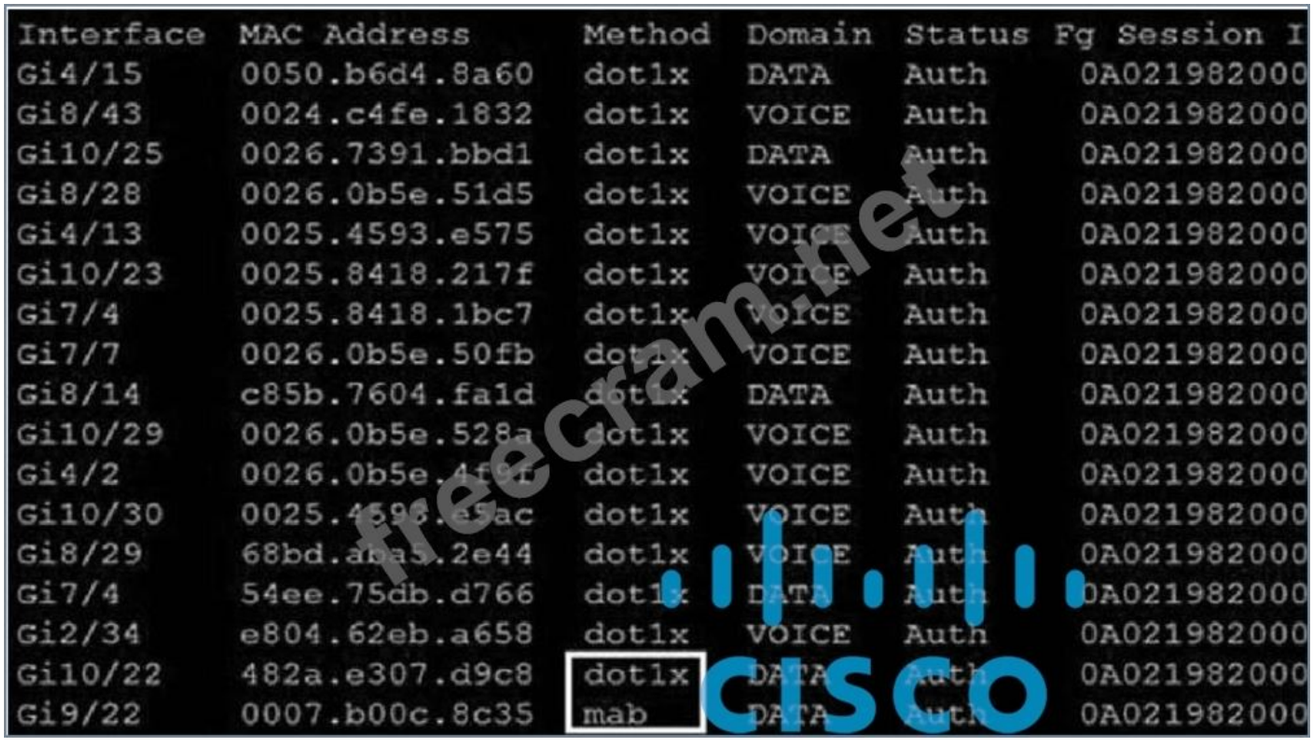
NEW QUESTION: 48
When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, which name is used?
A. Common Security Exploits
B. Common Vulnerabilities and Exposures
C. Common Exploits and Vulnerabilities
D. Common Vulnerabilities, Exploits and Threats
Answer: (SHOW ANSWER)
CVE is an industry-wide standard. CVE is sponsored by US-CERT, the office of Cybersecurity and Communications at the U.S. Department of Homeland Security.
The goal of CVE is to make it's easier to share data across tools, vulnerability repositories, and security services.

NEW QUESTION: 49
Which IPS engine detects ARP spoofing?
A. Service Generic Engine
B. AIC Engine
C. Atomic ARP Engine
D. ARP Inspection Engine
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
What are two benefits of Flexible NetFlow records? (Choose two)
A. They allow the user to configure flow information to perform customized traffic identification
B. They provide attack prevention by dropping the traffic
C. They provide accounting and billing enhancements
D. They converge multiple accounting technologies into one accounting mechanism
E. They provide monitoring of a wider range of IP packet information from Layer 2 to 4
Answer: (SHOW ANSWER)
NetFlow is typically used for several key customer applications, including the following: ... Billing and accounting. NetFlow data provides fine-grained metering (for instance, flow data includes details such as IP addresses, packet and byte counts, time stamps, type of service (ToS), and application ports) for highly

flexible and detailed resource utilization accounting. Service providers may use the information for billing based on time of day, bandwidth usage, application usage, quality of service, and so on. Enterprise customers may use the information for departmental charge back or cost allocation for resource utilization. Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnffnetflow.html If the predefined Flexible NetFlow records are not suitable for your traffic requirements, you can create a userdefined (custom) record using the Flexible NetFlow collect and match commands. Before you can create a customized record, you must decide the criteria that you are going to use for the key and nonkey fields. Reference: https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413d9.html#wp1057997 Note: Traditional NetFlow allows us to monitor from Layer 2 to 4 but Flexible NetFlow goes beyond these layers.
...
Billing and accounting. NetFlow data provides fine-grained metering (for instance, flow data includes details such as IP addresses, packet and byte counts, time stamps, type of service (ToS), and application ports) for highly flexible and detailed resource utilization accounting. Service providers may use the information for billing based on time of day, bandwidth usage, application usage, quality of service, and so on. Enterprise customers may use the information for departmental charge back or cost allocation for resource utilization. Reference:
If the predefined Flexible NetFlow records are not suitable for your traffic requirements, you can create a userdefined (custom) record using the Flexible NetFlow collect and match commands. Before you can create a customized record, you must decide the criteria that you are going to use for the key and nonkey fields. cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413d9.html#wp1057997 Note: Traditional NetFlow allows us to monitor from Layer 2 to 4 but Flexible NetFlow goes beyond these NetFlow is typically used for several key customer applications, including the following: ... Billing and accounting. NetFlow data provides fine-grained metering (for instance, flow data includes details such as IP addresses, packet and byte counts, time stamps, type of service (ToS), and application ports) for highly flexible and detailed resource utilization accounting. Service providers may use the information for billing based on time of day, bandwidth usage, application usage, quality of service, and so on. Enterprise customers may use the information for departmental charge back or cost allocation for resource utilization. Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnffnetflow.html If the predefined Flexible NetFlow records are not suitable for your traffic requirements, you can create a userdefined (custom) record using the Flexible NetFlow collect and match commands. Before you can create a customized record, you must decide the criteria that you are going to use for the key and nonkey fields. Reference: https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon_external_docbase_0900e4b18055d0d2_4container_external_docbase_0900e4b181b413d9.html#wp1057997 Note: Traditional NetFlow allows us to monitor from Layer 2 to 4 but Flexible NetFlow goes beyond these layers.

NEW QUESTION: 51
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.75db.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: 52

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

A. SPERO detection engine

B. TETRA detection engine

C. ETHOS detection engine

D. RBAC

Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
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: (SHOW ANSWER)

NEW QUESTION: 54
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: (SHOW ANSWER)
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: 55
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: (SHOW ANSWER)
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: 56
On which part of the IT environment does DevSecOps focus?
A. data center
B. perimeter network
C. wireless network
D. application development

Answer: (SHOW ANSWER)

NEW QUESTION: 57
A customer has various external HTTP resources available including Intranet Extranet and Internet, with a proxy configuration running in explicit mode. Which method allows the client desktop browsers to be configured to select when to connect direct or when to use the proxy?
A. Transport mode
B. Forward file
C. PAC file
D. Bridge mode
Answer: (SHOW ANSWER)
A Proxy Auto-Configuration (PAC) file is a JavaScript function definition that determines whether web browser requests (HTTP, HTTPS, and FTP) go direct to the destination or are forwarded to a web proxy server.
PAC files are used to support explicit proxy deployments in which client browsers are explicitly configured to send traffic to the web proxy. The big advantage of PAC files is that they are usually relatively easy to create and maintain.

NEW QUESTION: 58
What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?
A. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA.
B. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA
C. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA
D. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not
Answer: (SHOW ANSWER)

NEW QUESTION: 59
Which Dos attack uses fragmented packets to crash a target machine?
A. smurf
B. MITM
C. teardrop
D. LAND
Answer: (SHOW ANSWER)
A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

NEW QUESTION: 60

Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?

A. Threat Intelligence Director
B. Encrypted Traffic Analytics
C. Cisco Talos Intelligence
D. Cognitive Threat Analytics
Answer: (SHOW ANSWER)

NEW QUESTION: 61

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 AnyConnect
B. Cisco Tetration
C. Cisco AMP for Network
D. Cisco ISE?
Answer: (SHOW ANSWER)

NEW QUESTION: 62

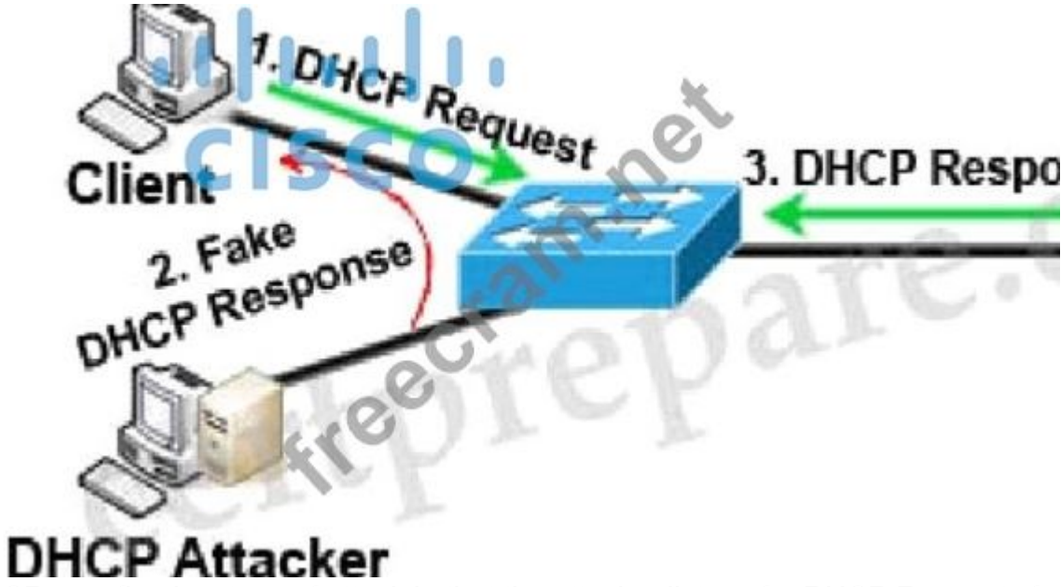
Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?
A. interpacket variation
B. software package variation
C. flow insight variation
D. process details variation
Answer: (SHOW ANSWER)

The telemetry information consists of three types of data: + Flow information: This information contains details about endpoints, protocols, ports, when the flow started, how long the flow was active, etc. + Interpacket variation: This information captures any interpacket variations within the flow. Examples include variation in Time To Live (TTL), IP and TCP flags, payload length, etc + Context details: Context information is derived outside the packet header. It includes details about variation in buffer utilization, packet drops within a flow, association with tunnel endpoints, etc. Reference:

https://www.cisco.com/c/dam/global/en_uk/products/switches/cisco_nexus_9300_ex_platform_switches_white_paper_uki.pdf
+ Flow information: This information contains details about endpoints, protocols, ports, when the flow started, how long the flow was active, etc.
+ Interpacket variation: This information captures any interpacket variations within the flow. Examples include variation in Time To Live (TTL), IP and TCP flags, payload length, etc
+ Context details: Context information is derived outside the packet header. It includes details about variation in buffer utilization, packet drops within a flow, association with tunnel endpoints, etc.
Reference:
The telemetry information consists of three types of data: + Flow information: This information contains details about endpoints, protocols, ports, when the flow started, how long the flow was active, etc. + Interpacket variation: This information captures any interpacket variations within the flow. Examples include variation in Time To Live (TTL), IP and TCP flags, payload length, etc + Context details: Context information is derived outside the packet header. It includes details about variation in buffer utilization, packet drops within a flow, association with tunnel endpoints, etc. Reference:
https://www.cisco.com/c/dam/global/en_uk/products/switches/cisco_nexus_9300_ex_platform_switches_white_paper_uki.pdf

NEW QUESTION: 63
An administrator is adding a new switch onto the network and has configured AAA for network access control. When testing the configuration, the RADIUS authenticates to Cisco ISE but is being rejected. Why is the ip radius source-interface command needed for this configuration?
A. Encrypted RADIUS authentication requires the RADIUS source interface be defined
B. Only requests that originate from a configured NAS IP are accepted by a RADIUS server
C. RADIUS requests are generated only by a router if a RADIUS source interface is defined.
D. The RADIUS authentication key is transmitted only from the defined RADIUS source interface
Answer: (SHOW ANSWER)

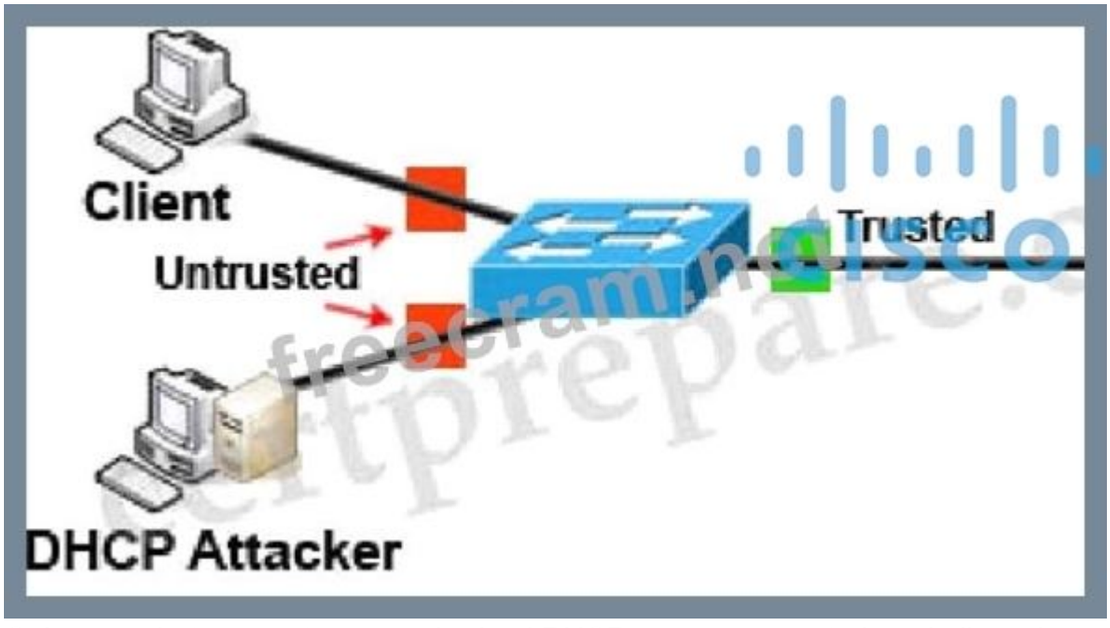
NEW QUESTION: 64
An administrator is configuring a DHCP server to better secure their environment. They need to be able to ratelimit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?
A. Set a trusted interface for the DHCP server
B. Set the DHCP snooping bit to 1
C. Add entries in the DHCP snooping database
D. Enable ARP inspection for the required VLAN
Answer: (SHOW ANSWER)
To understand DHCP snooping we need to learn about DHCP spoofing attack first.



DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle".

The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.

DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.



Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.

NEW QUESTION: 65

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.

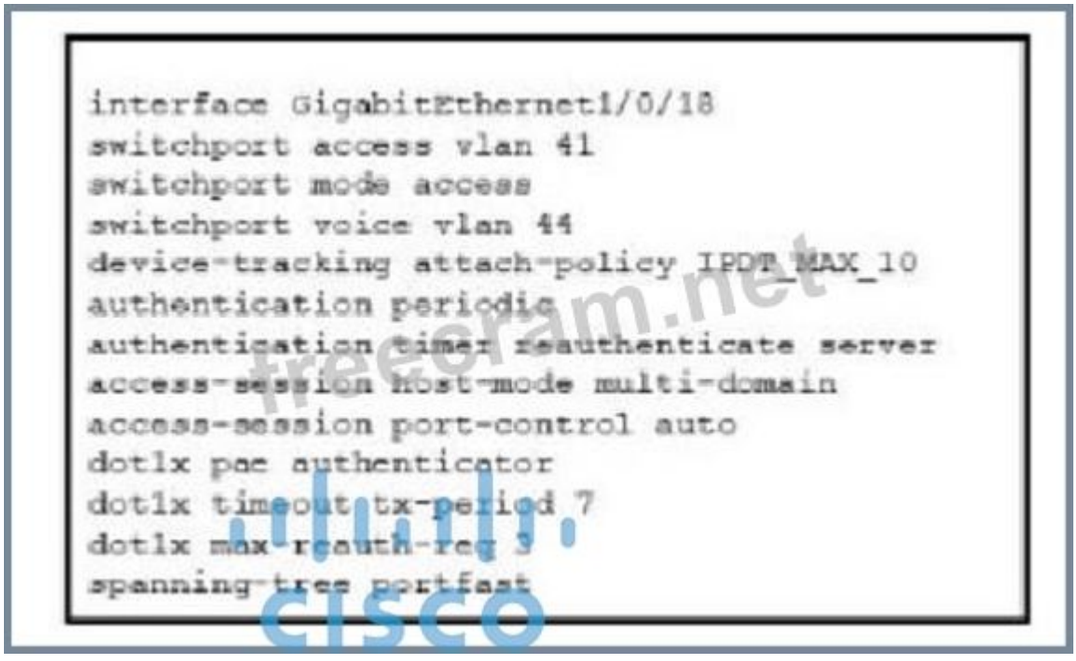
In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet.

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: 66

Refer to the exhibit.



Refer to the exhibit. A Cisco ISE administrator adds a new switch to an 802.1X deployment and has difficulty with some endpoints gaining access.

Most PCs and IP phones can connect and authenticate using their machine certificate credentials. However printer and video cameras cannot base d on the interface configuration provided, what must be to get these devices on to the network using Cisco ISE for authentication and authorization while maintaining security controls?

A. Configure authentication event fail retry 2 action authorize vlan 41 on the interface

B. Add mab to the interface configuration.

C. Enable insecure protocols within Cisco ISE in the allowed protocols configuration.

D. Change the default policy in Cisco ISE to allow all devices not using machine authentication .

Answer: (SHOW ANSWER)

NEW QUESTION: 67

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

A. DHCP

B. Design

C. Accounting

D. DNS

E. Provision

Answer: (SHOW ANSWER)

Cisco DNA Center has four general sections aligned to IT workflows: Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by

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

Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need. Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task.

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

NEW QUESTION: 68

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

A. set the password to be used for SNMPv3 authentication

B. map SNMPv3 users to SNMP views

C. define the encryption algorithm to be used by SNMPv3

D. specify the UDP port used by SNMP

Answer: (SHOW ANSWER)

NEW QUESTION: 69

An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?

A. Cisco Defense Orchestrator

B. Cisco Secureworks

C. Cisco DNA Center

D. Cisco Configuration Professional

Answer: (SHOW ANSWER)

Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms. Cisco Defense Orchestrator features: .... Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms. Reference: https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html and device configurations with ease across multiple Cisco and cloud-native security platforms. Cisco Defense Orchestrator features:

....

Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms.

Reference:

Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms. Cisco Defense Orchestrator features: .... Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms. Reference: https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html

NEW QUESTION: 70

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

A. when there is a need for traditional anti-malware detection

B. when there is no need to have the solution centrally managed

C. when there is no firewall on the network

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

NEW QUESTION: 71
Which endpoint solution protects a user from a phishing attack?
A. Cisco Identity Services Engine
B. Cisco AnyConnect with Umbrella Roaming Security module
C. Cisco AnyConnect with Network Access Manager module
D. Cisco AnyConnect with ISE Posture module
Answer: (SHOW ANSWER)

NEW QUESTION: 72
An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems. Why should the organization select either Platform as a Service or Infrastructure as a Service for this environment?
A. Infrastructure as a Service because the service provider manages the operating system
B. Platform as a Service because the customer manages the operating system
C. Platform as a Service because the service provider manages the operating system
D. Infrastructure as a Service because the customer manages the operating system
Answer: (SHOW ANSWER)

NEW QUESTION: 73
On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed devices?
A. correlation policy
B. access control policy
C. health awareness policy
D. system policy
E. health policy

Answer: (SHOW ANSWER)

NEW QUESTION: 74
A Cisco ESA administrator has been tasked with configuring the Cisco ESA to ensure there are no viruses before quarantined emails are delivered. In addition, delivery of mail from known bad mail servers must be prevented. Which two actions must be taken in order to meet these requirements? (Choose two)
A. Use outbreak filters from SenderBase
B. Enable a message tracking service
C. Configure a recipient access table
D. Deploy the Cisco ESA in the DMZ
E. Scan quarantined emails using AntiVirus signatures
Answer: (SHOW ANSWER)
We should scan emails using AntiVirus signatures to make sure there are no viruses attached in emails. Note: A virus signature is the fingerprint of a virus. It is a set of unique data, or bits of code, that allow it to be identified. Antivirus software uses a virus signature to find a virus in a computer file system, allowing to detect, quarantine, and remove the virus. SenderBase is an email reputation service designed to help email administrators research senders, identify legitimate sources of email, and block spammers. When the Cisco ESA receives messages from known or highly reputable senders, it delivers them directly to the end user without any content scanning. However, when the Cisco ESA receives email messages from unknown or less reputable senders, it performs antispam and antivirus scanning. Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/
b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html -> Therefore Outbreak filters can be used to block emails from bad mail servers. Web servers and email gateways are generally located in the DMZ so Note: The recipient access table (RAT), not to be confused with remote-access Trojan (also RAT), is a Cisco ESA term that defines which recipients are accepted by a public listener.
Note: A virus signature is the fingerprint of a virus. It is a set of unique data, or bits of code, that allow it to be identified. Antivirus software uses a virus signature to find a virus in a computer file system, allowing to detect, quarantine, and remove the virus.
SenderBase is an email reputation service designed to help email administrators research senders, identify legitimate sources of email, and block spammers. When the Cisco ESA receives messages from known or highly reputable senders, it delivers them directly to the end user without any content scanning. However, when the Cisco ESA receives email messages from unknown or less reputable senders, it performs antispam and antivirus scanning.
Reference:
b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html
-> Therefore Outbreak filters can be used to block emails from bad mail servers.
Web servers and email gateways are generally located in the DMZ so
We should scan emails using AntiVirus signatures to make sure there are no viruses attached in emails. Note: A virus signature is the fingerprint of a virus. It is a set of unique data, or bits of code, that allow it to be identified. Antivirus software uses a virus signature to find a virus in a computer file system, allowing to detect, quarantine, and remove the virus. SenderBase is an email reputation service designed to help email

administrators research senders, identify legitimate sources of email, and block spammers. When the Cisco ESA receives messages from known or highly reputable senders, it delivers them directly to the end user without any content scanning. However, when the Cisco ESA receives email messages from unknown or less reputable senders, it performs antispam and antivirus scanning. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100100.html -> Therefore Outbreak filters can be used to block emails from bad mail servers. Web servers and email gateways are generally located in the DMZ so Note: The recipient access table (RAT), not to be confused with remote-access Trojan (also RAT), is a Cisco ESA term that defines which recipients are accepted by a public listener.

NEW QUESTION: 75
What features does Cisco FTDv provide over ASAv?
A. Cisco FTDv runs on AWS while ASAv does not
B. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not
C. Cisco FTDv runs on VMWare while ASAv does not
D. Cisco FTDv supports URL filtering while ASAv does not
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Refer to the exhibit.

```
ip dhcp snooping
ip dhcp snooping vlan 41,44
!
interface GigabitEthernet1/0/1
 description Uplink_To_Distro_Switch_g1/0/11
 switchport trunk native vlan 999
 switchport trunk allowed vlan 40,41,44
 switchport mode trunk
```


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: (SHOW ANSWER)
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: 77
Drag and drop the VPN functions from the left onto the description on the right.

Answer:

NEW QUESTION: 78
Which feature is leveraged by advanced antimalware capabilities to be an effective endpomt protection platform?
A. blocklisting
B. sandboxing
C. storm centers
D. big data
Answer: (SHOW ANSWER)

NEW QUESTION: 79
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: (SHOW ANSWER)
TAXII (Trusted Automated Exchange of Indicator Information) is a standard that provides a transport

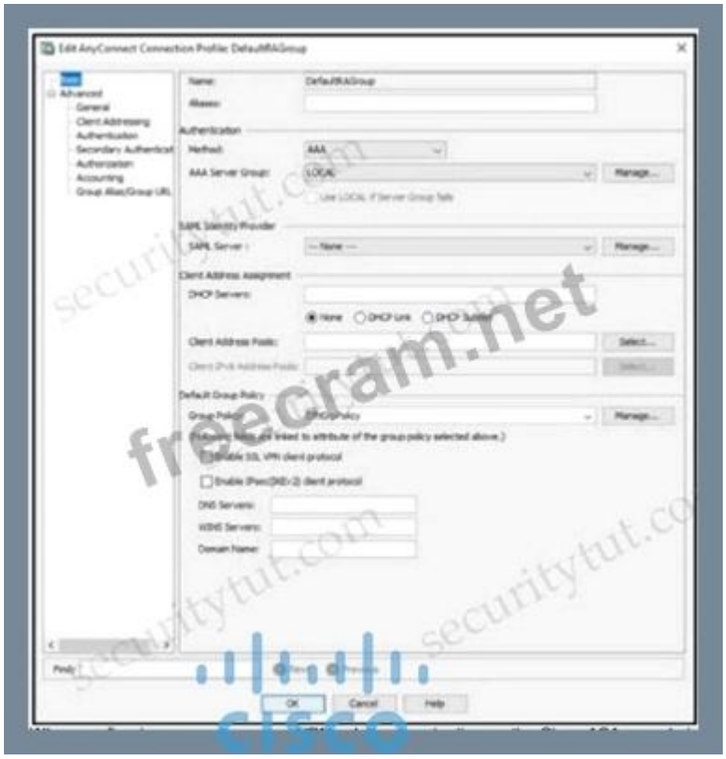
NEW QUESTION: 80
An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?
A. Cisco Umbrella
B. Cisco Cloud Email Security
C. Cisco NGFW
D. Cisco Cloudlock
Answer: (SHOW ANSWER)
Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform. Reference:

https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45-738565.pdf Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform. Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45-738565.pdf

NEW QUESTION: 81
A network engineer is configuring DMVPN and entered the crypto isakmp key cisc0380739941 address 0.0.0.0 command on host
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. Change isakmp to ikev2 in the command on hostA.
D. Enter the same command on hostB.
Answer: (SHOW ANSWER)

NEW QUESTION: 82
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: (SHOW ANSWER)
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: 83
Refer to the exhibit.



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

A. Group Policy

B. Method

C. SAML Server

D. DHCP Servers

Answer: (SHOW ANSWER)

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

NEW QUESTION: 84

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

A. Patch management remediation is performed.

B. The latest antivirus updates are applied before access is allowed.

C. A centralized management solution is deployed.

D. Assignments to endpoint groups are made dynamically, based on endpoint attributes.

E. Endpoint supplicant configuration is deployed.

Answer: (SHOW ANSWER)

NEW QUESTION: 85

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

A. TACACS+
B. central web auth
C. multiple factor auth
D. single sign-on
E. local web auth
Answer: (SHOW ANSWER)

NEW QUESTION: 86
A network engineer has entered the snmp-server user andy myv3 auth sha cisco priv aes 256 cisc0380739941 command and needs to send SNMP information to a host at 10.255.254.1. Which command achieves this goal?
A. snmp-server host inside 10.255.254.1 version 3 andy
B. snmp-server host inside 10.255.254.1 version 3 myv3
C. snmp-server host inside 10.255.254.1 snmpv3 andy
D. snmp-server host inside 10.255.254.1 snmpv3 myv3
Answer: (SHOW ANSWER)
The command "snmp-server user user-name group-name [remote ip-address [udp-port port]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]" adds a new user (in this case "andy") to an SNMPv3 group (in this case group name "myv3") and configures a password for the user.
In the "snmp-server host" command, we need to:
+ Specify the SNMP version with key word "version {1 | 2 | 3}"
+ Specify the username ("andy"), not group name ("myv3").
Note: In "snmp-server host inside ..." command, "inside" is the interface name of the ASA interface through which the NMS (located at 10.255.254.1) can be reached.

NEW QUESTION: 87
What is a benefit of performing device compliance?
A. Device classification and authorization
B. Providing multi-factor authentication
C. Providing attribute-driven policies
D. Verification of the latest OS patches
Answer: (SHOW ANSWER)

NEW QUESTION: 88
An organization wants to secure data in a cloud environment. Its security model requires that all users be authenticated and authorized. Security configuration and posture must be continuously validated before access is granted or maintained to applications and dat a. There is also a need to allow certain application traffic and deny all other traffic by default. Which technology must be used to implement these requirements?
A. Virtual routing and forwarding
B. Microsegmentation
C. Access control policy

D. Virtual LAN

Answer: (SHOW ANSWER)

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.

The Zero Trust model uses microsegmentation - a security technique that involves dividing perimeters into small zones to maintain separate access to every part of the network - to contain attacks.

NEW QUESTION: 89

What is a benefit of using a multifactor authentication strategy?

A. It provides secure remote access for applications.

B. It provides an easy, single sign-on experience against multiple applications

C. It provides visibility into devices to establish device trust.

D. It protects data by enabling the use of a second validation of identity.

Answer: (SHOW ANSWER)

NEW QUESTION: 90

A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an undetermined verdict. What is causing this issue?

A. The policy was created to send a message to quarantine instead of drop

B. The file has a reputation score that is above the threshold

C. The file has a reputation score that is below the threshold

D. The policy was created to disable file analysis

Answer: (SHOW ANSWER)

Maybe the "newly installed service" in this Qmentions about Advanced Malware Protection (AMP) which can be used along with ESA. AMP allows superior protection across the attack continuum.

+ File Reputation - captures a fingerprint of each file as it traverses the ESA and sends it to AMP's cloudbased intelligence network for a reputation verdict. Given these results, you can automatically block malicious files and apply administrator-defined policy.

+ File Analysis - provides the ability to analyze unknown files that are traversing the ESA. A highly secure sandbox environment enables AMP to glean precise details about the file's behavior and to combine that data with detailed human and machine analysis to determine the file's threat level. This disposition is then fed into AMP cloud-based intelligence network and used to dynamically update and expand the AMP cloud data set for enhanced protection

NEW QUESTION: 91

What are two DDoS attack categories? (Choose two)

A. sequential

B. protocol
C. database
D. volume-based
E. screen-based
Answer: (SHOW ANSWER)
There are three basic categories of attack: + volume-based attacks, which use high traffic to inundate the network bandwidth + protocol attacks, which focus on exploiting server resources + application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks Reference: https://www.esecurityplanet.com/networks/types-of-ddos-attacks/
+ volume-based attacks, which use high traffic to inundate the network bandwidth
+ protocol attacks, which focus on exploiting server resources
There are three basic categories of attack: + volume-based attacks, which use high traffic to inundate the network bandwidth + protocol attacks, which focus on exploiting server resources + application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks Reference: https://www.esecurityplanet.com/networks/types-of-ddos-attacks/

NEW QUESTION: 92
An organization has a Cisco Stealthwatch Cloud deployment in their environment. Cloud logging is working as expected, but logs are not being received from the on-premise network, what action will resolve this issue?
A. Configure security appliances to send syslogs to Cisco Stealthwatch Cloud
B. Configure security appliances to send NetFlow to Cisco Stealthwatch Cloud
C. Deploy a Cisco FTD sensor to send events to Cisco Stealthwatch Cloud
D. Deploy a Cisco Stealthwatch Cloud sensor on the network to send data to Cisco Stealthwatch Cloud
Answer: (SHOW ANSWER)
You can also monitor on-premises networks in your organizations using Cisco Stealthwatch Cloud. In order to do so, you need to deploy at least one Cisco Stealthwatch Cloud Sensor appliance (virtual or physical appliance).

NEW QUESTION: 93
When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?
A. Spero analysis
B. dynamic analysis
C. sandbox analysis

D. malware analysis

Answer: (SHOW ANSWER)

Spero analysis examines structural characteristics such as metadata and header information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware. Reference: 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: 94
What is a description of microsegmentation?
A. Environments deploy centrally managed host-based firewall rules on each server or container
B. Environments implement private VLAN segmentation to group servers with similar applications.
C. Environments deploy a container orchestration platform, such as Kubernetes, to manage the application delivery
D. Environments apply a zero-trust model and specify how applications on different servers or containers can communicate
Answer: (SHOW ANSWER)

NEW QUESTION: 95
Refer to the exhibit. What is the result of the Python script?
A. It uses the GET HTTP method to obtain a username and password to be used for authentication
B. It uses the POST HTTP method to obtain a token to be used for authentication.
C. It uses the GET HTTP method to obtain a token to be used for authentication.
D. It uses the POST HTTP method to obtain a username and password to be used for authentication.
Answer: (SHOW ANSWER)

NEW QUESTION: 96
What is a characteristic of traffic storm control behavior?
A. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.
B. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.

C. Traffic storm control cannot determine if the packet is unicast or broadcast.
D. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 97
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: (SHOW ANSWER)
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: 98
Which algorithm provides asymmetric encryption?
A. RC4
B. 3DES
C. RSA
D. AES
Answer: (SHOW ANSWER)

NEW QUESTION: 99
Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?
A. Advanced Malware Protection
B. Platform Exchange Grid
C. Multifactor Platform Integration
D. Firepower Threat Defense
Answer: (SHOW ANSWER)

With Cisco pxGrid (Platform Exchange Grid), your multiple security products can now share data and work together. This open, scalable, and IETF standards-driven platform helps you automate security to get answers and contain threats faster.

NEW QUESTION: 100

What is provided by the Secure Hash Algorithm in a VPN?

A. integrity

B. key exchange

C. encryption

D. authentication

Answer: (SHOW ANSWER)

The HMAC-SHA-1-96 (also known as HMAC-SHA-1) encryption technique is used by IPSec to ensure that a message has not been altered. (-> Therefore answer "integrity" is the best choice). HMAC-SHA-1 uses the SHA-1 specified in FIPS-190-1, combined with HMAC (as per RFC 2104), and is described in RFC 2404. Reference: https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=4 The HMAC-SHA-1-96 (also known as HMAC-SHA-1) encryption technique is used by IPSec to ensure that a message has not been altered. (-> Therefore answer "integrity" is the best choice). HMAC-SHA-1 uses the SHA-1 specified in FIPS-190-1, combined with HMAC (as per RFC 2104), and is described in RFC 2404. Reference: https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=4

NEW QUESTION: 101

Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?

A. It verifies that the endpoint has the latest Microsoft security patches installed.

B. It adds endpoints to identity groups dynamically.

C. It allows the endpoint to authenticate with 802.1xor MAB.

D. It allows CoA to be applied if the endpoint status is compliant.

Answer: (SHOW ANSWER)

NEW QUESTION: 102

What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.) The eDirectory client must be installed on each client workstation.

A. Create NTLM or Kerberos authentication realm and enable transparent user identification

B. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.

C. Deploy a separate eDirectory server: the client IP address is recorded in this server

D. Create an LDAP authentication realm and disable transparent user identification.

Answer: (SHOW ANSWER)

NEW QUESTION: 103

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

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

NEW QUESTION: 104
An engineer wants to automatically assign endpoints that have a specific OUI into a new endpoint group. Which probe must be enabled for this type of profiling to work?
A. NetFlow
B. NMAP
C. SNMP
D. DHCP
Answer: (SHOW ANSWER)
Cisco ISE can determine the type of device or endpoint connecting to the network by performing "profiling." Profiling is done by using DHCP, SNMP, Span, NetFlow, HTTP, RADIUS, DNS, or NMAP scans to collect as much metadata as possible to learn the device fingerprint. NMAP ("Network Mapper") is a popular network scanner which provides a lot of features. One of them is the OUI (Organizationally Unique Identifier) information. OUI is the first 24 bit or 6 hexadecimal value of the MAC address. Note: DHCP probe cannot collect OUIs of endpoints. NMAP scan probe can collect these endpoint attributes: + EndPointPolicy + LastNmapScanCount + NmapScanCount + OUI + Operating-system Reference: http://www.network-node.com/blog/2016/1/2/ise-20-profiling Profiling is done by using DHCP, SNMP, Span, NetFlow, HTTP, RADIUS, DNS, or NMAP scans to collect as much metadata as possible to learn the device fingerprint. NMAP ("Network Mapper") is a popular network scanner which provides a lot of features. One of them is the OUI (Organizationally Unique Identifier) information. OUI is the first 24 bit or 6 hexadecimal value of the MAC address.
Note: DHCP probe cannot collect OUIs of endpoints. NMAP scan probe can collect these endpoint attributes:
+ EndPointPolicy
+ LastNmapScanCount
+ NmapScanCount
+ OUI
+ Operating-system
Cisco ISE can determine the type of device or endpoint connecting to the network by performing "profiling." Profiling is done by using DHCP, SNMP, Span, NetFlow, HTTP, RADIUS, DNS, or NMAP scans to collect as much metadata as possible to learn the device fingerprint. NMAP ("Network Mapper") is a popular network scanner which provides a lot of features. One of them is the OUI (Organizationally Unique Identifier) information. OUI is the first 24 bit or 6 hexadecimal value of the MAC address. Note: DHCP probe cannot collect OUIs of endpoints. NMAP scan probe can collect these endpoint attributes: + EndPointPolicy + LastNmapScanCount + NmapScanCount + OUI + Operating-system Reference: http://www.network-node.com/blog/2016/1/2/ise-20-profiling

NEW QUESTION: 105
Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two)
A. Use prepared statements and parameterized queries.
B. Secure the connection between the web and the app tier.
C. Write SQL code instead of using object-relational mapping libraries.
D. Block SQL code execution in the web application database login.
E. Check integer, float, or Boolean string parameters to ensure accurate values.
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Which attack type attempts to shut down a machine or network so that users are not able to access it?
A. smurf
B. bluesnarfing
C. MAC spoofing
D. IP spoofing
Answer: (SHOW ANSWER)
Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to its intended users.
The Smurf attack is a DDoS attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.

NEW QUESTION: 107
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. Modify the application settings to allow only applications to connect to required addresses.
C. Use content categories to block or allow specific addresses.
D. Create a destination list for addresses to be allowed or blocked.
Answer: (SHOW ANSWER)

NEW QUESTION: 108

An administrator configures new authorization policies within Cisco ISE and has difficulty profiling the devices. Attributes for the new Cisco IP phones that are profiled based on the RADIUS authentication are seen however the attributes for CDP or DHCP are not. What should the administrator do to address this issue?
A. Configure the ip dhcp snooping trust command on the DHCP interfaces to get the information to Cisco ISE
B. Configure the authentication port-control auto feature within Cisco ISE to identify the devices that are trying to connect
C. Configure a service template within the switch to standardize the port configurations so that the correct information is sent to Cisco ISE
D. Configure the device sensor feature within the switch to send the appropriate protocol information
Answer: (SHOW ANSWER)
Device sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by Device Sensor can come from the following protocols: + Cisco Discovery Protocol (CDP) + Link Layer Discovery Protocol (LLDP) + Dynamic Host Configuration Protocol (DHCP) Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-ConfigureDevice-Sensor-for-ISE-Profilin.html information collected by Device Sensor can come from the following protocols:
+ Cisco Discovery Protocol (CDP)
+ Link Layer Discovery Protocol (LLDP)
+ Dynamic Host Configuration Protocol (DHCP)
Device sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by Device Sensor can come from the following protocols: + Cisco Discovery Protocol (CDP) + Link Layer Discovery Protocol (LLDP) + Dynamic Host Configuration Protocol (DHCP) Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-ConfigureDevice-Sensor-for-ISE-Profilin.html

NEW QUESTION: 109
What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?
A. Telemetry uses a pull mehod, which makes it more reliable than SNMP
B. Telemetry uses push and pull, which makes it more scalable than SNMP
C. Telemetry uses push and pull which makes it more secure than SNMP
D. Telemetry uses a push method which makes it faster than SNMP
Answer: (SHOW ANSWER)
SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts. The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data. Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc. Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Referfence: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming telemetry The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data.

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

NEW QUESTION: 110

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

A. improper file security
B. unencrypted links for traffic
C. software bugs on applications
D. weak passwords for authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 111
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. LDAP communication must be permitted between the ISE server and the domain controller.
B. Active Directory only supports user authentication by using MSCHAPv2.
C. The ISE account must be a domain administrator in Active Directory to perform JOIN operations.
D. Active Directory supports user and machine authentication by using MSCHAPv2.
E. RADIUS communication must be permitted between the ISE server and the domain controller.
Answer: (SHOW ANSWER)

NEW QUESTION: 112
Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?
A. IP Blacklist Center
B. AMP Reputation Center
C. File Reputation Center
D. IP and Domain Reputation Center
Answer: (SHOW ANSWER)

NEW QUESTION: 113
What are two functions of TAXII in threat intelligence sharing? (Choose two.)
A. Supports STIX information

B. determines the "what" of threat intelligence
C. exchanges trusted anomaly intelligence information
D. determines how threat intelligence information is relayed
E. allows users to describe threat motivations and abilities
Answer: (SHOW ANSWER)

NEW QUESTION: 114
Which Talos reputation center allows for tracking the reputation of IP addresses for email and web traffic?
A. IP and Domain Reputation Center
B. AMP Reputation Center
C. File Reputation Center
D. IP Slock List Center
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which type of protection encrypts RSA keys when they are exported and imported?
A. NGE
B. file
C. passphrase
D. nonexportable
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which type of encryption uses a public key and private Key?
A. symmetric
B. linear
C. asymmetric
D. nonlinear
Answer: (SHOW ANSWER)

NEW QUESTION: 117
In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?
A. man-in-the-middle
B. insecure API
C. cross-site scripting
D. LDAP injection
Answer: (SHOW ANSWER)

NEW QUESTION: 118
What is the purpose of the My Devices Portal in a Cisco ISE environment?

A. to register new laptops and mobile devices
B. to request a newly provisioned mobile device
C. to provision userless and agentless systems
D. to manage and deploy antivirus definitions and patches on systems owned by the end user
Answer: (SHOW ANSWER)
Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html

NEW QUESTION: 119
An engineer needs to add protection for data in transit and have headers in the email message Which configuration is needed to accomplish this goal?
A. Provision the email appliance
B. Deploy an encryption appliance.
C. Map sender !P addresses to a host interface.
D. Enable flagged message handling
Answer: (SHOW ANSWER)

NEW QUESTION: 120
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: (SHOW ANSWER)
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: 121
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: (SHOW ANSWER)

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: 122

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

A. DMVPN

B. FlexVPN

C. IPsec DVTI

D. GET VPN

Answer: (SHOW ANSWER)

Cisco's Group Encrypted Transport VPN (GETVPN) introduces the concept of a trusted group to eliminate point-to-point tunnels and their associated overlay routing. All group members (GMs) share a common security association (SA), also known as a group SA. This enables GMs to decrypt traffic that was encrypted by any other GM. GETVPN provides instantaneous large-scale any-to-any IP connectivity using a group IPsec security paradigm. Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/ GETVPN_DIG_version_2_0_External.pdf

NEW QUESTION: 123

Which type of attack is MFA an effective deterrent for?

A. phishing

B. teardrop

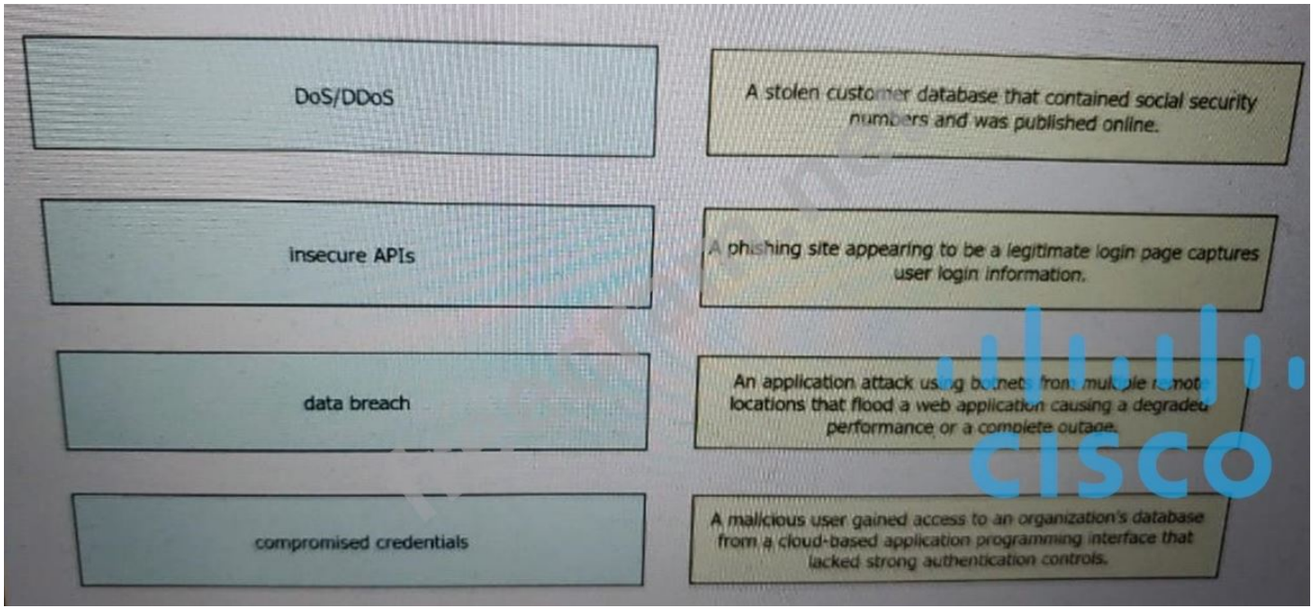
C. ping of death

D. syn flood

Answer: (SHOW ANSWER)

NEW QUESTION: 124

Drag and drop the threats from the left onto examples of that threat on the right



Answer:

NEW QUESTION: 125

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

A. Cisco FTDv with one management interface and two traffic interfaces configured

B. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS

C. Cisco FTDv configured in routed mode and IPv6 configured

D. Cisco FTDv with two management interfaces and one traffic interface configured

E. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises

Answer: (SHOW ANSWER)

NEW QUESTION: 126

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: (SHOW ANSWER)
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: 127
An engineer is configuring Cisco WSA and needs to enable a separated email transfer flow from the Internet and from the LAN. Which deployment mode must be used to accomplish this goal?
A. transparent
B. single interface
C. two-interface
D. multi-context
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
How does a cloud access security broker function?
A. It acts as a security information and event management solution and receives syslog from other cloud solutions.
B. It is an authentication broker to enable single sign-on and multi-factor authentication for a cloud solution
C. It scans other cloud solutions being used within the network and identifies vulnerabilities
D. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution
Answer: (SHOW ANSWER)

NEW QUESTION: 129
In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?
A. Smurf
B. distributed denial of service
C. cross-site scripting
D. rootkit exploit
Answer: C (LEAVE A REPLY)

Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.
Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on.
For example the code below is written in hex: <a
href=javascript:alert&#
x28'XSS')>Click Here
is equivalent to:
Click Here
Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form.

NEW QUESTION: 130
Which two statements about a Cisco WSA configured in Transparent mode are true? (Choose two.)
A. It requires a PAC file for the client web browser.
B. It requires a proxy for the client web browser.
C. Layer 4 switches can automatically redirect traffic destined to port 80.
D. It can handle explicit HTTP requests.
E. WCCP v2-enabled devices can automatically redirect traffic destined to port 80.
Answer: C,E (LEAVE A REPLY)

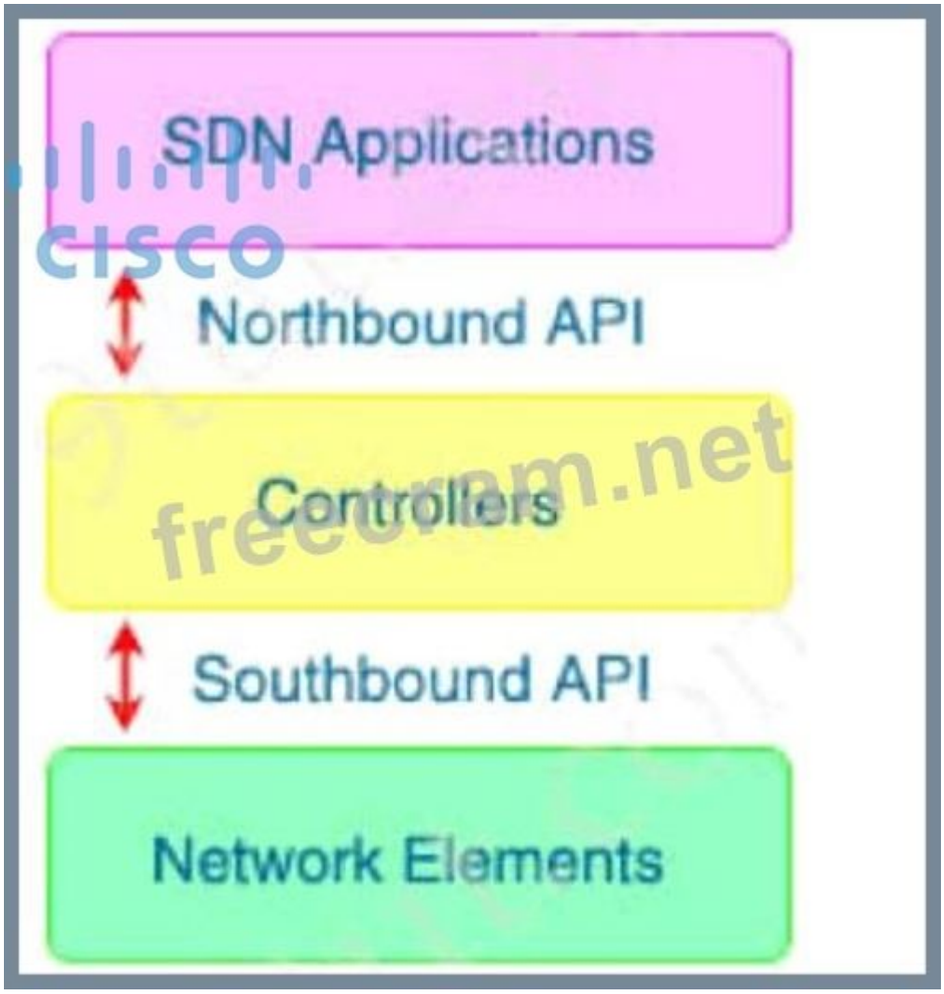
NEW QUESTION: 131
Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats?
A. PSIRT
B. Talos
C. CSIRT
D. DEVNET
Answer: (SHOW ANSWER)
Talos Threat Source is a regular intelligence update from Cisco Talos, highlighting the biggest threats each week and other security news. Reference: https://talosintelligence.com/newsletters Talos Threat Source is a regular intelligence update from Cisco Talos, highlighting the biggest threats each week and other security news. Reference: https://talosintelligence.com/newsletters

NEW QUESTION: 132
What is a benefit of conducting device compliance checks?
A. It indicates what type of operating system is connecting to the network.
B. It scans endpoints to determine if malicious activity is taking place.
C. It detects email phishing attacks.
D. It validates if anti-virus software is installed.

Answer: (SHOW ANSWER)

NEW QUESTION: 133
Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?
A. user input validation in a web page or web application
B. Linux and Windows operating systems
C. database
D. web page images
Answer: (SHOW ANSWER)
SQL injection usually occurs when you ask a user for input, like their username/userid, but the user gives ("injects") you an SQL statement that you will unknowingly run on your database. For example:
Look at the following example, which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
If user enter something like this: "100 OR 1=1" then the SzQL statement will look like this:
SELECT * FROM Users WHERE UserId = 100 OR 1=1;
The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE. A hacker might get access to all the user names and passwords in this database.

NEW QUESTION: 134
What is the function of SDN southbound API protocols?
A. to allow for the dynamic configuration of control plane applications
B. to enable the controller to make changes
C. to enable the controller to use REST
D. to allow for the static configuration of control plane applications
Answer: (SHOW ANSWER)
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs. Reference: https://www.ciscopress.com/articles/article.asp?p=3004581&seqNum=2
scalability needs.
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs. Reference: https://www.ciscopress.com/articles/article.asp?p=3004581&seqNum=2



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

NEW QUESTION: 135
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: (SHOW ANSWER)
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: 136
Refer to the exhibit.

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

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

A. adds authentication to a switch

B. adds a switch to Cisco DNA Center

C. receives information about a switch

Answer: (SHOW ANSWER)

NEW QUESTION: 137
An organization is implementing URL blocking using Cisco Umbrell
a. The users are able to go to some sites
but other sites are not accessible due to an error. Why is the error occurring?
A. Client computers do not have the Cisco Umbrella Root CA certificate installed.
B. IP-Layer Enforcement is not configured.
C. Client computers do not have an SSL certificate deployed from an internal CA server.
D. Intelligent proxy and SSL decryption is disabled in the policy
Answer: (SHOW ANSWER)
Other features are dependent on SSL Decryption functionality, which requires the Cisco Umbrella root certificate. Having the SSL Decryption feature improves: Custom URL Blocking-Required to block the HTTPS version of a URL. ... Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed. Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you may wish to prevent it from appearing. To avoid these error pages, install the Cisco Umbrella root certificate into your browser or the browsers of your users-if you're a network admin. Reference: https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information certificate. Having the SSL Decryption feature improves:
Custom URL Blocking-Required to block the HTTPS version of a URL.
...
Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed. Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you may wish to prevent it from appearing.
To avoid these error pages, install the Cisco Umbrella root certificate into your browser or the browsers of your users-if you're a network admin.
Other features are dependent on SSL Decryption functionality, which requires the Cisco Umbrella root certificate. Having the SSL Decryption feature improves: Custom URL Blocking-Required to block the HTTPS version of a URL. ... Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed. Typical errors include "The security certificate presented by this website was not issued by

a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you may wish to prevent it from appearing. To avoid these error pages, install the Cisco Umbrella root certificate into your browser or the browsers of your users-if you're a network admin. Reference: https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information

NEW QUESTION: 138
What is the intent of a basic SYN flood attack?
A. to solicit DNS responses
B. to flush the register stack to re-initiate the buffers
C. to exceed the threshold limit of the connection queue
D. to cause the buffer to overflow
Answer: C (LEAVE A REPLY)

NEW QUESTION: 139
An engineer needs behavioral analysis to detect malicious activity on the hosts, and is configuring the organization's public cloud to send telemetry using the cloud provider's mechanisms to a security device. Which mechanism should the engineer configure to accomplish this goal?
A. VPC flow logs
B. Flow
C. mirror port
D. NetFlow
Answer: (SHOW ANSWER)

NEW QUESTION: 140
Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two)

A. packet decoder
B. SIP
C. modbus
D. inline normalization
E. SSL
Answer: (SHOW ANSWER)
Application layer protocols can represent the same data in a variety of ways. The Firepower System provides application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results. Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-

guidev60/Application_Layer_Preprocessors.html#ID-2244-0000080c FirePower uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.
application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results.
Reference:
Application layer protocols can represent the same data in a variety of ways. The Firepower System provides application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results. Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Application_Layer_Preprocessors.html#ID-2244-0000080c FirePower uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

NEW QUESTION: 141
What is the role of Cisco Umbrella Roaming when it is installed on an endpoint?
A. To protect the endpoint against malicious file transfers
B. To ensure that assets are secure from malicious links on and off the corporate network
C. To establish secure VPN connectivity to the corporate network
D. To enforce posture compliance and mandatory software
Answer: (SHOW ANSWER)
Umbrella Roaming is a cloud-delivered security service for Cisco's next-generation firewall. It protects your employees even when they are off the VPN.

NEW QUESTION: 142
A network engineer must migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vMotion. What is a requirement for both physical hosts?
A. The hosts must have access to the same defined network.
B. The hosts must run Cisco AsyncOS 10.0 or greater.
C. The hosts must run different versions of Cisco AsyncOS.
D. The hosts must use a different datastore than the virtual appliance.
Answer: (SHOW ANSWER)

NEW QUESTION: 143
An engineer needs a solution for TACACS+ authentication and authorization for device administration.
The engineer also wants to enhance wired and wireless network security by requiring users and endpoints to use 802.1X, MAB, or WebAuth. Which product meets all of these requirements?
A. Cisco AMP for Endpoints
B. Cisco Stealthwatch

C. Cisco Identity Services Engine
D. Cisco Prime Infrastructure
Answer: (SHOW ANSWER)

NEW QUESTION: 144
Refer to the exhibit.

```
import requests
url = https://api.amp.cisco.com/v1/computers
headers = {
   'accept' : application/json
   'content-type' : application/json
   'authorization' : Basic API Credentials
   'cache-control' : "no cache"
}
response = requests.request ("GET", url, headers = headers)
print (response.txt)
```

What will happen when this Python script is run?
A. The compromised computers and malware trajectories will be received from Cisco AMP
B. The list of computers and their current vulnerabilities will be received from Cisco AMP
C. The compromised computers and what compromised them will be received from Cisco AMP
D. The list of computers, policies, and connector statuses will be received from Cisco AMP
Answer: (SHOW ANSWER)
The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across your organization that Advanced Malware Protection (AMP) sees Reference: 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: 145
Which role is a default guest type in Cisco ISE?
A. Contractor
B. Full-Time
C. Monthly
D. Yearly
Answer: (SHOW ANSWER)

NEW QUESTION: 146
What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?

A. Enable Intelligent Proxy
B. Activate SSL decryption
C. Activate the Advanced Malware Protection license
D. Enable IP Layer enforcement
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Which license is required for Cisco Security Intelligence to work on the Cisco Next Generation Intrusion Prevention System?
A. URL filtering
B. malware
C. control
D. protect
Answer: (SHOW ANSWER)

NEW QUESTION: 148
An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?
A. HAT
B. SAT
C. RAT
D. BAT
Answer: (SHOW ANSWER)

NEW QUESTION: 149
Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?
A. ip device-tracking
B. aaa server radius dynamic-author
C. auth-type all
D. aaa new-model
Answer: (SHOW ANSWER)

NEW QUESTION: 150
Where are individual sites specified to be blacklisted in Cisco Umbrella?
A. application settings
B. content categories
C. security settings
D. destination lists
Answer: (SHOW ANSWER)

A destination list is a list of internet destinations that can be blocked or allowed based on the administrative preferences for the policies applied to the identities within your organization. A destination is an IP address (IPv4), URL, or fully qualified domain name. You can add a destination list to Umbrella at any time; however, a destination list does not come into use until it is added to a policy. Reference: https://docs.umbrella.com/deployment-umbrella/docs/working-with-destination-lists preferences for the policies applied to the identities within your organization. A destination is an IP address (IPv4), URL, or fully qualified domain name. You can add a destination list to Umbrella at any time; however, a destination list does not come into use until it is added to a policy.
A destination list is a list of internet destinations that can be blocked or allowed based on the administrative preferences for the policies applied to the identities within your organization. A destination is an IP address (IPv4), URL, or fully qualified domain name. You can add a destination list to Umbrella at any time; however, a destination list does not come into use until it is added to a policy. Reference: https://docs.umbrella.com/deployment-umbrella/docs/working-with-destination-lists

NEW QUESTION: 151
Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?
A. Correlation
B. Intrusion
C. Access Control
D. Network Discovery
Answer: (SHOW ANSWER)
The Firepower System uses network discovery and identity policies to collect host, application, and user data for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible. You can configure your network discovery policy to perform host and application detection. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.html for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible.
You can configure your network discovery policy to perform host and application detection.
The Firepower System uses network discovery and identity policies to collect host, application, and user data for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible. You can configure your network discovery policy to perform host and application detection. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introduction_to_network_discovery_and_identity.html

NEW QUESTION: 152

Which Cisco platform ensures that machines that connect to organizational networks have the recommended antivirus definitions and patches to help prevent an organizational malware outbreak?

A. Cisco WiSM

B. Cisco ESA

C. Cisco ISE

D. Cisco Prime Infrastructure

Answer: C (LEAVE A REPLY)

A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. We can configure ISE to check for the Windows patch at Work Centers > Posture > Posture Elements > Conditions > File.

In this example, we are going to use the predefined file check to ensure that our Windows 10 clients have the critical security patch installed to prevent the Wanna Cry malware; and we can also configure ISE to update the client with this patch.

NEW QUESTION: 153
Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps.
Which two actions must be taken to ensure that interfaces are put back into service? (Choose two)
A. Have Cisco Prime Infrastructure issue an SNMP set command to re-enable the ports after the pre configured interval.
B. Use EEM to have the ports return to service automatically in less than 300 seconds.
C. Enter the shutdown and no shutdown commands on the interfaces.
D. Enable the snmp-server enable traps command and wait 300 seconds
E. Ensure that interfaces are configured with the error-disable detection and recovery feature
Answer: (SHOW ANSWER)
You can also bring up the port by using these commands:

+ The "shutdown" interface configuration command followed by the "no shutdown" interface configuration command restarts the disabled port.
+ The "errdisable recovery cause ..." global configuration command enables the timer to automatically recover error-disabled state, and the "errdisable recovery interval interval" global configuration command specifies the time to recover error-disabled state.

NEW QUESTION: 154
What are two Trojan malware attacks? (Choose two)
A. sync
B. backdoor
C. frontdoor
D. rootkit
E. smurf
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 155
An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users. Which action accomplishes this goal?
A. Restrict access to only websites with trusted third-party signed certificates.
B. Modify the user's browser settings to suppress errors from Cisco Umbrella.
C. Upload the organization root CA to Cisco Umbrella.
D. Install the Cisco Umbrella root CA onto the user's device.
Answer: (SHOW ANSWER)

NEW QUESTION: 156
How does Cisco Advanced Phishing Protection protect users?
A. It validates the sender by using DKIM.
B. It determines which identities are perceived by the sender
C. It utilizes sensors that send messages securely.
D. It uses machine learning and real-time behavior analytics.
Answer: D (LEAVE A REPLY)
Cisco Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to protect against identity deception-based threats. Reference: https://docs.ces.cisco.com/docs/advanced-phishing-protection Cisco Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to protect against identity deception-based threats. Reference: https://docs.ces.cisco.com/docs/advanced-phishing-protection

NEW QUESTION: 157
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: 158
What is an advantage of the Cisco Umbrella roaming client?
A. the ability to dynamically categorize traffic to previously uncategorized sites
B. visibility into traffic that is destined to sites within the office environment
C. visibility into IP-based threats by tunneling suspicious IP connections
D. the ability to see all traffic without requiring TLS decryption
Answer: (SHOW ANSWER)

NEW QUESTION: 159
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: (SHOW ANSWER)
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: 160
Which posture assessment requirement provides options to the client for remediation and requires the remediation within a certain timeframe?

A. Audit
B. Mandatory
C. Optional

D. Visibility

Answer: (SHOW ANSWER)

A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role and an operating system. All the clients connecting to your network must meet mandatory requirements during posture evaluation to become compliant on the network. Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. If requirements are optional and clients fail these requirements, then the clients have an option to continue during posture evaluation of endpoints. Mandatory Requirements During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings. For example, you have specified a mandatory requirement with a user-defined condition to check the existence of C:\temp\text.file in the absolute path. If the file does not exist, the mandatory requirement fails and the user will be moved to Non-Compliant state. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_010111.html Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. If requirements are optional and clients fail these requirements, then the clients have an option to continue during posture evaluation of endpoints.

Mandatory Requirements

During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings.

For example, you have specified a mandatory requirement with a user-defined condition to check the existence of C:\temp\text.file in the absolute path. If the file does not exist, the mandatory requirement fails and the user will be moved to Non-Compliant state.

Reference:

A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role and an operating system. All the clients connecting to your network must meet mandatory requirements during posture evaluation to become compliant on the network. Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. If requirements are optional and clients fail these requirements, then the clients have an option to continue during posture evaluation of endpoints. Mandatory Requirements During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings. For example, you have specified a mandatory requirement with a user-defined condition to check the existence of C:\temp\text.file in the absolute path. If the file does not exist, the mandatory requirement fails and the user will be moved to Non-Compliant state. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_010111.html

NEW QUESTION: 161

An engineer is trying to securely connect to a router and wants to prevent insecure algorithms from being used.

However, the connection is failing. Which action should be taken to accomplish this goal?

A. Disable telnet using the no ip telnet command.
B. Enable the SSH server using the ip ssh server command.
C. Configure the port using the ip ssh port 22 command.
D. Generate the RSA key using the crypto key generate rsa command.
Answer: (SHOW ANSWER)
In this question, the engineer was trying to secure the connection so maybe he was trying to allow SSH to the device. But maybe something went wrong so the connection was failing (the connection used to be good). So maybe he was missing the "crypto key generate rsa" command.

NEW QUESTION: 162
Which benefit does endpoint security provide the overall security posture of an organization?
A. It streamlines the incident response process to automatically perform digital forensics on the endpoint
B. It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.
C. It allows the organization to detect and respond to threats at the edge of the network
D. It allows the organization to mitigate web-based attacks as long as the user is active in the domain
Answer: (SHOW ANSWER)