Cisco.350-701.v2025-02-21.q424

Exam Code:	350-701
Exam Name:	Implementing and Operating Cisco Security Core Technologies
Certification Provider:	Cisco
Free Question Number:	424
Version:	v2025-02-21
# of views:	634
# of Questions views:	4240
https://www.freeqas.com/qa/Cisco/350-701/Cisco.350-701.v2025-02-21.q424.html	

NEW QUESTION: 1
A network engineer is configuring NetFlow top talkers on a Cisco router Drag and drop the steps in the process from the left into the sequence on the right

Answer:

NEW QUESTION: 2
Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)
A. It must include the current date.
B. It must reside in the trusted store of the WSA.
C. It must reside in the trusted store of the endpoint.
D. It must have been signed by an internal CA.
E. it must contain a SAN.
Answer: (SHOW ANSWER)
The WSA uses a root certificate and a private key to decrypt HTTPS traffic. The root certificate must reside in the trusted store of the WSA, and it must be able to sign server certificates on the fly. The server certificates that the WSA generates must contain a SAN (Subject Alternative Name) field, which specifies the hostnames or IP addresses that the certificate is valid for. The SAN field is required by modern browsers and applications to verify the identity of the server. If the WSA does not include a SAN field in the server certificate, the browser or application may reject the connection or display a warning message.
The other options are not correct because:
* A. The current date is not a criterion for the WSA to use a certificate to decrypt application traffic. The WSA checks the validity period of the certificate, which includes the start date and the end date. The current date must be within the validity period, but it does not have to be the same as the start date or the end date.
* C. The root certificate that the WSA uses to decrypt HTTPS traffic does not have to reside in the trusted store of the endpoint. However, the endpoint must trust the root certificate in order to accept the server certificate that the WSA generates. This can be achieved by manually installing the root certificate on the endpoint, or by using a group policy or a certificate management system to distribute the root certificate to the endpoints.
* D. The root certificate that the WSA uses to decrypt HTTPS traffic does not have to be signed by an internal CA. The WSA can generate its own self-signed root certificate, or it can use a root certificate that is signed by an external CA. However, the root certificate must be trusted by the endpoints, as explained in option C.
References := : WSA Certificate Usage for HTTPS Decryption : [User Guide for AsyncOS 12.0 for Cisco Web Security Appliances - GD (General Deployment) - Create Decryption Policies to Control HTTPS Traffic]

NEW QUESTION: 3
Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'
```

What function does the API key perform while working with https://api.amp.cisco.com/v1/computers?
A. plays dent ID
B. HTTP authentication
C. HTTP authorization

D. imports requests

Answer: (SHOW ANSWER)

NEW QUESTION: 4

Refer to the exhibit.

```
SwitchA (config)# interface gigabitethernet1/0/1
SwitchA (config-if)# dot1x host-mode multi-host
SwitchA (config-if)# dot1x timeout quiet-period 3
SwitchA (config-if)# dot1x timeout tx-period 15
SwitchA (config-if)# authentication port-control auto
SwitchA (config-if)# switchport mode access
SwitchA (config-if)# switchpoint access vlan 12
```

An engineer configured wired 802.1x on the network and is unable to get a laptop to authenticate. Which port configuration is missing?

A. authentication open

B. dot1x pae authenticator

C. dotlx reauthentication

D. cisp enable

Answer: (SHOW ANSWER)

NEW QUESTION: 5

What is the difference between EPP and EDR?

A. EPP focuses primarily on threats that have evaded front-line defenses that entered the environment.

B. Having an EPP solution allows an engineer to detect, investigate, and remediate modern threats.

C. Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior.

D. EDR focuses solely on prevention at the perimeter.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 6

An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation. What must be un solution?

A. L2TP is an IP packet encapsulation protocol, and GRE over IPsec is a tunneling protocol.

B. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701.

C. GRE over IPsec adds its own header, and L2TP does not.

D. GRE over IPsec cannot be used as a standalone protocol, and L2TP can.

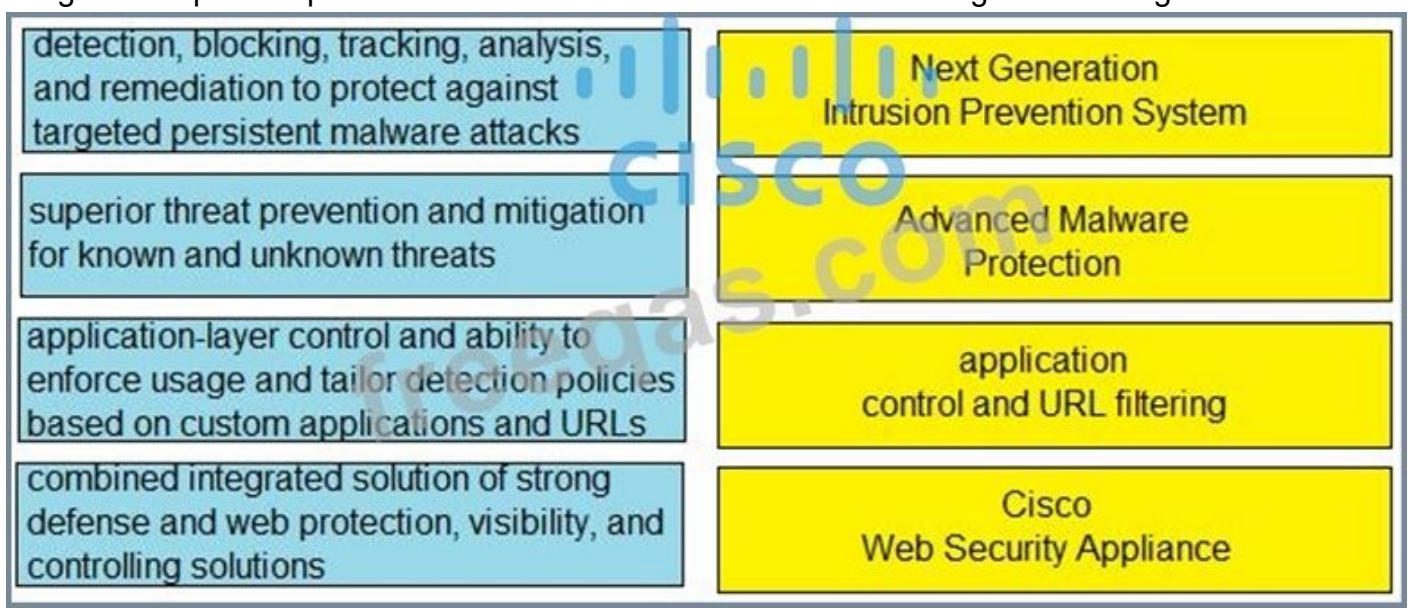
Answer: (SHOW ANSWER)

L2TP and GRE are both tunneling protocols that can be used to create site-to-site VPNs. However, they have some differences in how they encapsulate and transport data. L2TP is a layer 2 protocol that uses IP packet encapsulation to carry PPP frames over an IP network. L2TP does not add any additional header to the IP packet, but relies on IPsec to provide encryption and authentication. GRE is a layer 3 protocol that adds its own header to the IP packet, which contains information such as the protocol type, checksum, and key. GRE can be used to carry any type of payload over an IP network, not just PPP frames. GRE also requires IPsec to provide security for the tunnel. Therefore, the correct answer is C, because GRE over IPsec adds its own header, and L2TP does not1234 References := 1: Implementing and Operating

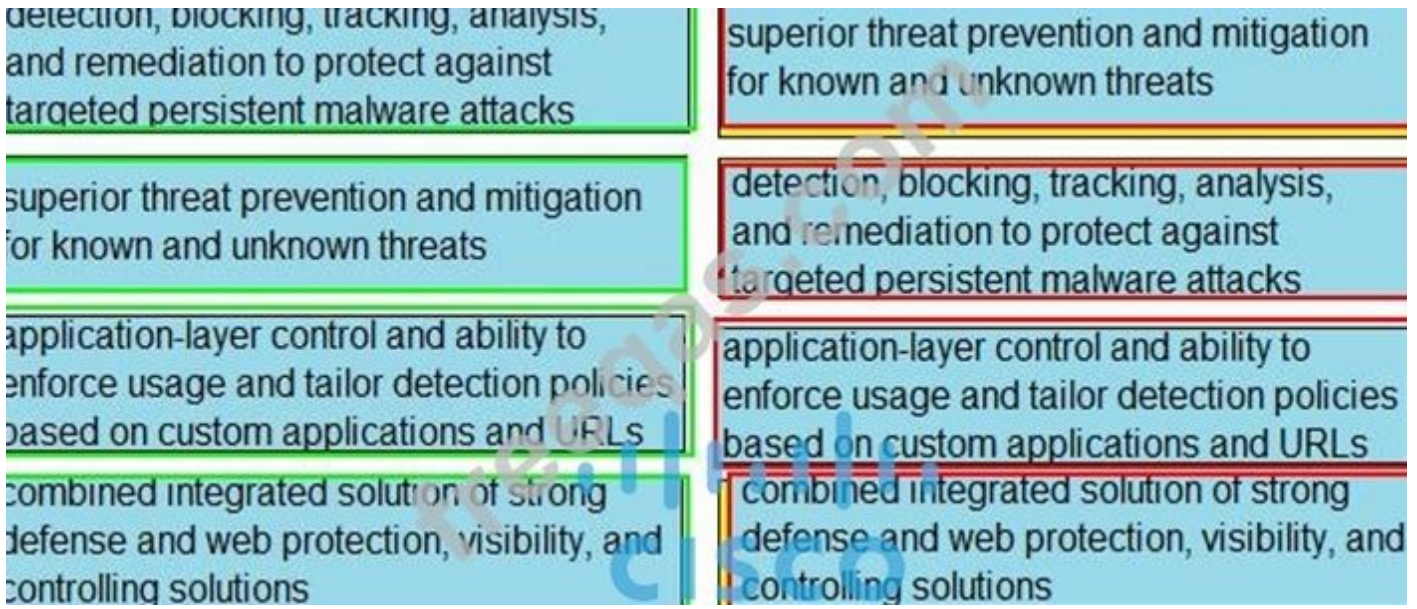
Cisco Security Core Technologies (SCOR) v1.0 - Module 5: Secure Connectivity 2: What is the difference between L2TP vs GRE 3: GRE over IPSec vs L2TP over IPSEC 4: difference between L2TP/GRE/MPLS

NEW QUESTION: 7
Which Cisco platform onboards the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing the endpoint to gain network access?
A. Cisco ISE
B. Cisco NAC
C. Cisco TACACS+
D. Cisco WSA
Answer: A (LEAVE A REPLY)
Cisco ISE is a platform that can onboard the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing the endpoint to gain network access. Cisco ISE has an internal CA service that can validate and sign certificate requests from endpoints, generate and store keys and certificates, and provide an OCSP responder to check the validity of certificates. Cisco ISE also supports Enrollment over Secure Transport (EST), which is a protocol that allows endpoints to securely enroll with a CA and obtain certificates. Cisco ISE can use EST to provision certificates to endpoints and configure their network settings to use EAP-TLS authentication. Cisco ISE can also use BYOD workflows to onboard endpoints and issue certificates to them.
References:
* Understand ISE Internal Certificate Authority Services
* Endpoint On-boarding using Internal ISE CA
* Cisco ISE BYOD Prescriptive Deployment Guide

NEW QUESTION: 8
Drag and drop the capabilities from the left onto the correct technologies on the right.



Answer:



NEW QUESTION: 9
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. 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
D. 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
Answer: D (LEAVE A REPLY)

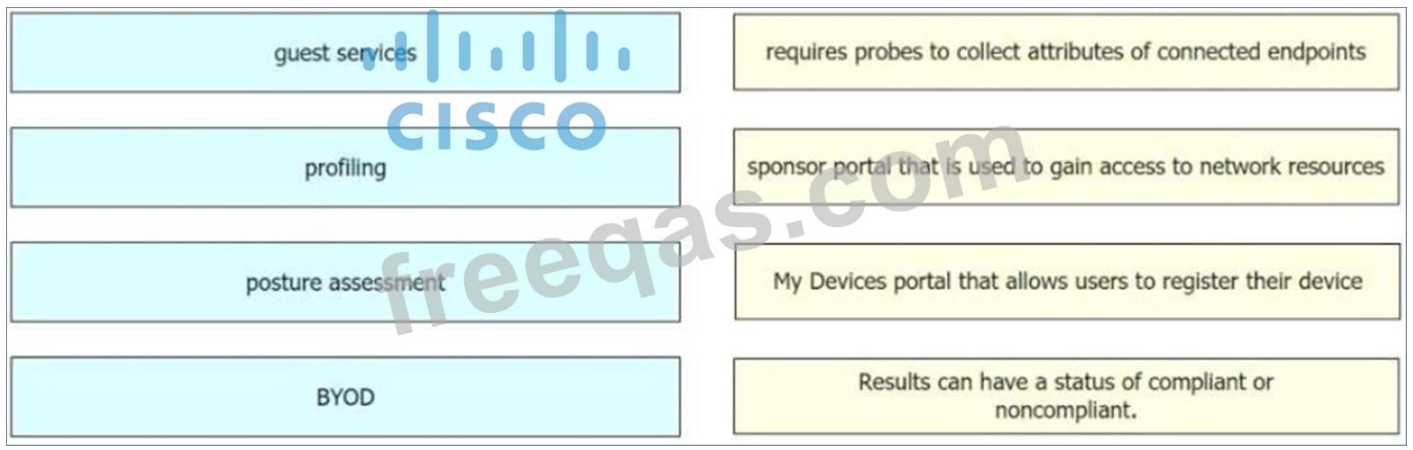
NEW QUESTION: 10
What is provided by the Secure Hash Algorithm in a VPN?
A. integrity
B. key exchange
C. encryption
D. authentication
Answer: (SHOW ANSWER)
Explanation The HMAC-SHA-1-96 (also known as HMAC-SHA-1) encryption technique is used by IPSec to ensure that a message has not been altered. (-> 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.
Explanation 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: 11
Which type of protection encrypts RSA keys when they are exported and imported?
A. passphrase
B. file
C. NGE
D. nonexportable
Answer: A (LEAVE A REPLY)

NEW QUESTION: 12
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. Configure the port using the ip ssh port 22 command.
B. Enable the SSH server using the ip ssh server command.
C. Disable telnet using the no ip telnet command.
D. Generate the RSA key using the crypto key generate rsa command.
Answer: D (LEAVE A REPLY)
Reference:
https://learningnetwork.cisco.com/s/question/0D53i00000KsrhK/rsa-key

NEW QUESTION: 13
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: B (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_client_posture_policies.html#:~:text=Policy%20Requirement%20Types-,Mandatory%20Requirements,the%20requirements%20within%20the%20time%20specified%20in%20the%20remediation%20timer%20settings.,-For%20example%2C%20you 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

NEW QUESTION: 14
Drag and drop the concepts from the left onto the correct descriptions on the right



Answer:

NEW QUESTION: 15
Which two capabilities does an MDM provide? (Choose two.)
A. delivery of network malware reports to an inbox in a schedule
B. unified management of mobile devices, Macs, and PCs from a centralized dashboard
C. enforcement of device security policies from a centralized dashboard
D. manual identification and classification of client devices
E. unified management of Android and Apple devices from a centralized dashboard
Answer: B,C (LEAVE A REPLY)
Mobile device management (MDM) is a toolset that provides a workforce with mobile productivity tools and applications while keeping corporate data secure1. One of the essential capabilities of an MDM solution is the unified management of mobile devices, Macs, and PCs from a centralized dashboard2. This allows IT and security departments to manage all of a company's devices, regardless of their operating system, and perform tasks such as provisioning, configuration, update, lock, wipe, and troubleshoot2. Another important capability of an MDM solution is the enforcement of device security policies from a centralized dashboard3. This enables IT and security departments to protect the device's applications, data, and content, and ensure compliance with organizational and regulatory standards3. For example, an MDM solution can set minimum password strength, encrypt data, restrict access, and detect threats3.
References: 1: What is Mobile Device Management (MDM)? | IBM 2: 5 Essential Capabilities of an MDM Solution | Macworld 3: What is device management? | Microsoft Learn

NEW QUESTION: 16
Which solution for remote workers enables protection, detection, and response on the endpoint against known and unknown threats?
A. Cisco AnyConnect

B. Cisco Duo
C. Cisco AMP for Endpoints
D. Cisco Umbrella
Answer: C (LEAVE A REPLY)

NEW QUESTION: 17
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)
ExplanationThe Southbound API is used to communicate between Controllers and network devices

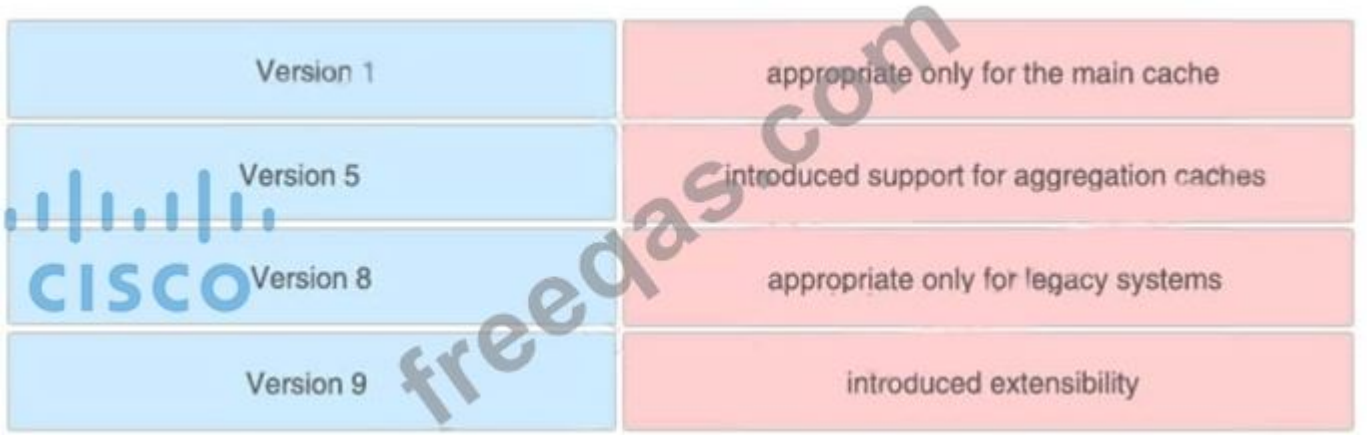
NEW QUESTION: 18
Why should organizations migrate to a multifactor authentication strategy?
A. Multifactor authentication methods of authentication are never compromised
B. Single methods of authentication can be compromised more easily than multifactor authentication
C. Biometrics authentication leads to the need for multifactor authentication due to its ability to be hacked easily
D. Multifactor authentication does not require any piece of evidence for an authentication mechanism
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
What is the function of the crypto is a kmp key cisc406397954 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel?
A. It defines what data is going to be encrypted via the VPN
B. It configures the pre-shared authentication key
C. It prevents all IP addresses from connecting to the VPN server.
D. It configures the local address for the VPN server.
Answer: (SHOW ANSWER)
The function of the crypto is a kmp key cisc406397954 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel is to configure the pre-shared authentication key. This command specifies the key that will be used to authenticate the Internet Key Exchange (IKE) phase 1 negotiation between the IPsec peers. The key is associated with the address 0.0.0.0 0.0.0.0, which means that it will apply to any peer that initiates or responds to the IKE negotiation. This is a common configuration for dynamic IPsec VPN scenarios, such as Dynamic Multipoint VPN (DMVPN) or Easy VPN, where the IP addresses of the peers are not known in advance. However, this is also a less secure

configuration, as it exposes the VPN server to potential brute-force attacks from any source. A more secure configuration would be to specify the exact IP address or subnet of the peer, or to use certificates instead of pre-shared keys.
References:
* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Securing the Cloud, Lesson 2: Site-to-Site VPNs, Topic: IPsec VPN Configuration
* Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4 - Configuring Internet Key Exchange for IPsec VPNs [Support] - Cisco, Configuring IKE Policies, Step 3: crypto isakmp key keystring [address | hostname] [mask | no-xauth] [netmask mask]

NEW QUESTION: 20
Which technology must be used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?
A. DMVPN
B. FlexVPN
C. IPsec DVTI
D. GET VPN
Answer: D (LEAVE A REPLY)
Explanation: 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: 21
Drag and drop the NetFlow export formats from the left onto the descriptions on the right.



Answer:

Explanation: The Version 1 format was the initially released version. Do not use the Version 1 format unless you are using a legacy collection system that requires it. Use Version 9 or Version 5 export format. Version 5 export format is suitable only for the main cache; it cannot be expanded to support new features. Version 8 export format is available only for aggregation caches; it cannot be expanded to support new features. Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgnflow-data-expt.html

NEW QUESTION: 22

Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'

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']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
            mac = network_interface.get('mac')
            ip = network_interface.get('ip')
            ipv6 = network_interface.get('ipv6')
            print(mac, ip, ipv6)
```

What does the API do when connected to a Cisco security appliance?

A. get the process and PID information from the computers in the network

B. create an SNMP pull mechanism for managing AMP

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

NEW QUESTION: 23
What is the difference between a vulnerability and an exploit?
A. A vulnerability is a weakness that can be exploited by an attacker
B. An exploit is a hypothetical event that causes a vulnerability in the network
C. A vulnerability is a hypothetical event for an attacker to exploit
D. An exploit is a weakness that can cause a vulnerability in the network
Answer: A (LEAVE A REPLY)

NEW QUESTION: 24
Which direction do attackers encode data in DNS requests during exfiltration using DNS tunneling?
A. inbound
B. outbound
C. east-west
D. north-south
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Cisco SensorBase gaihers threat information from a variety of Cisco products and services and performs analytics to find patterns on threats
Which term describes this process?
A. sharing
B. consumption
C. authoring
D. deployment
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Refer to the exhibit.

```
Info: New SMTP ICID 30 interface Management (192.168.0.100)
   address 10.128.128.200 reverse dns host unknown verified no
Info: ICID 30 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS None
Info: ICID 30 TLS success protocol TLSv1 cipher
   DHE-RSA-AES256-SHA
Info: SMTP Auth: (ICID 30) succeeded for user: cisco using
   AUTH mechanism: LOGIN with profile: ldap_smtp
Info: MID 80 matched all recipients for per-recipient policy
   DEFAULT in the outbound table
```

Which type of authentication is in use?

A. LDAP authentication for Microsoft Outlook

B. POP3 authentication

C. SMTP relay server authentication

D. external user and relay mail authentication

Answer: D (LEAVE A REPLY)

The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.

The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.

Reference:

The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.

The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

NEW QUESTION: 27

When a transparent authentication fails on the Web Security Appliance, which type of access does the end user get?

A. limited Internet

B. full Internet

C. blocked

D. guest

Answer: C (LEAVE A REPLY)

NEW QUESTION: 28

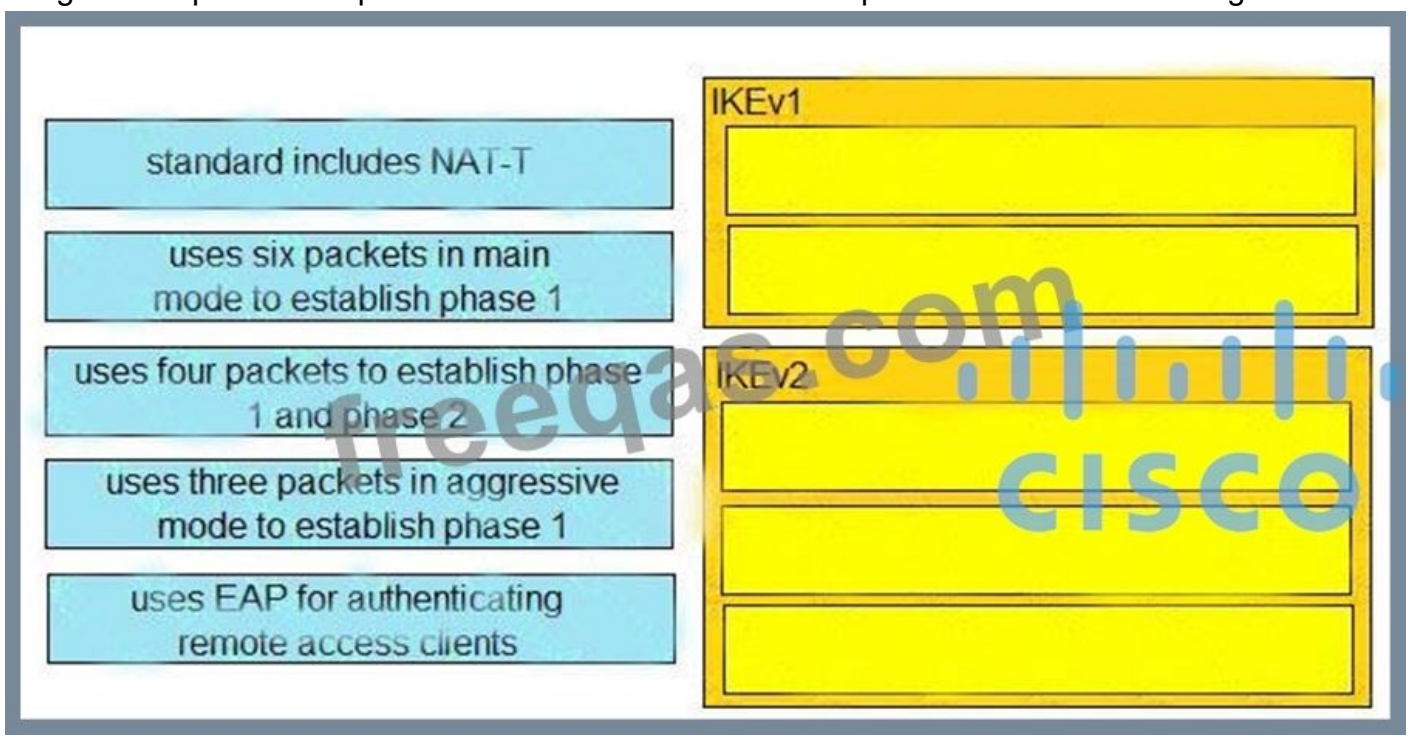
What are two DDoS attack categories? (Choose two)

A. sequential

B. protocol

C. database
D. volume-based
E. screen-based
Answer: B,D (LEAVE A REPLY)
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: 29
Drag and drop the descriptions from the left onto the correct protocol versions on the right.



Answer:

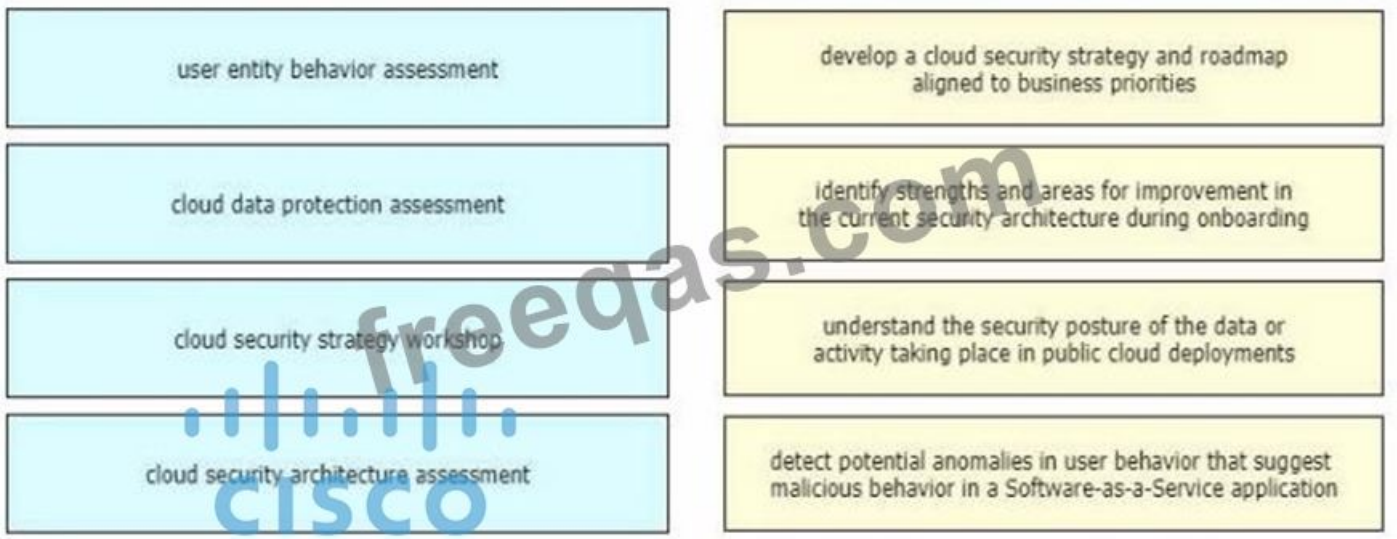
NEW QUESTION: 30
Which form of attack is launched using botnets?
A. EIDDOS
B. virus
C. DDOS
D. TCP flood
Answer: C (LEAVE A REPLY)
Explanation
A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them.
Cyber criminals use botnets to instigate botnet attacks, which include malicious activities such as credentials leaks, unauthorized access, data theft and DDoS attacks.

NEW QUESTION: 31
Which two parameters are used to prevent a data breach in the cloud? (Choose two.)
A. DLP solutions
B. strong user authentication
C. complex cloud-based web proxies
D. encryption
E. antispoofing programs
Answer: A,B (LEAVE A REPLY)

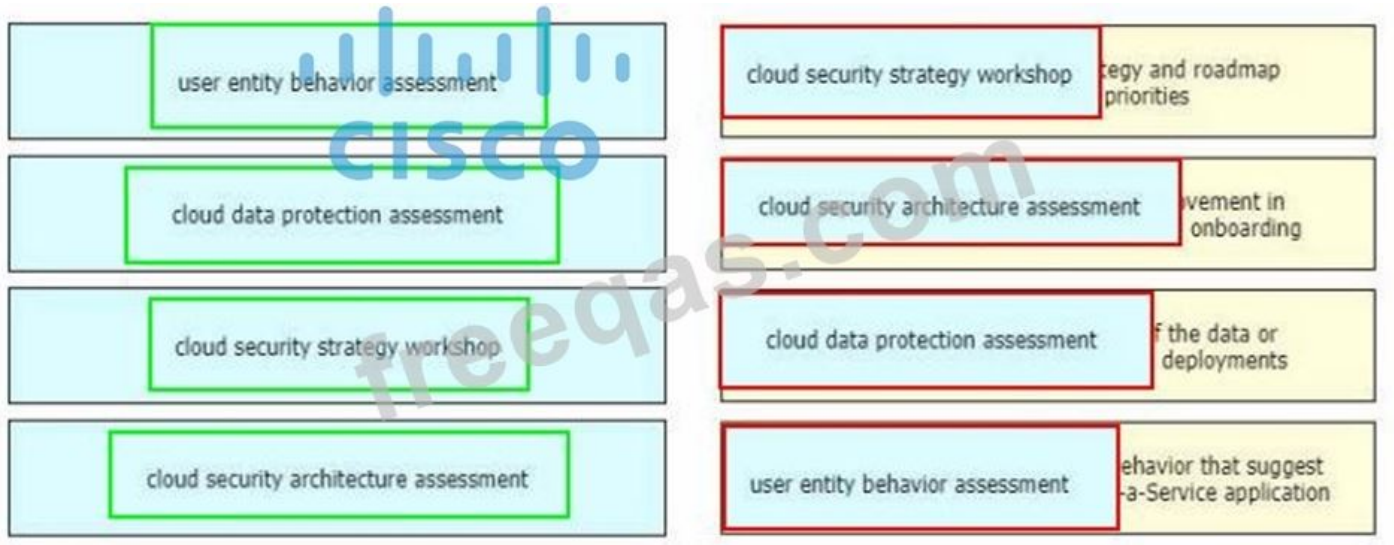
NEW QUESTION: 32
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two.)
A. virtualization
B. middleware
C. operating systems
D. applications
E. data
Answer: D,E (LEAVE A REPLY)
https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/

NEW QUESTION: 33
An engineer adds a custom detection policy to a Cisco AMP deployment and encounters issues with the configuration. The simple detection mechanism is configured, but the dashboard indicates that the hash is not
64 characters and is non-zero. What is the issue?
A. The hash being uploaded is part of a set in an incorrect format
B. The engineer is attempting to upload a file instead of a hash
C. The engineer is attempting to upload a hash created using MD5 instead of SHA-256
D. The file being uploaded is incompatible with simple detections and must use advanced detections
Answer: (SHOW ANSWER)

NEW QUESTION: 34
Drag and drop the cloud security assessment components from the left onto the definitions on the right.



Answer:



NEW QUESTION: 35

What are two things to consider when using PAC files with the Cisco WSA? (Choose two.)

A. By default, they direct traffic through a proxy when the PC and the host are on the same subnet.

B. The WSA hosts PAC files on port 9001 by default.

C. If the WSA host port is changed, the default port redirects web traffic to the correct port automatically.

D. PAC files use if-else statements to determine whether to use a proxy or a direct connection for traffic between the PC and the host.

E. The WSA hosts PAC files on port 6001 by default.

Answer: (SHOW ANSWER)

NEW QUESTION: 36

What is a prerequisite when integrating a Cisco ISE server and an AD domain?

A. Place the Cisco ISE server and the AD server in the same subnet

B. Configure a common administrator account

C. Configure a common DNS server

D. Synchronize the clocks of the Cisco ISE server and the AD server

Answer: D (LEAVE A REPLY)

The following are the prerequisites to integrate Active Directory with Cisco ISE. + Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI. + If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation. + You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F

+ Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI.

+ If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation.

+ You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE. Reference:

The following are the prerequisites to integrate Active Directory with Cisco ISE. + Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI. + If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation. + You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F

NEW QUESTION: 37

Which CLI command is used to register a Cisco FirePower sensor to Firepower Management Center?

A. configure system add <host><key>

B. configure manager <key> add host

C. configure manager delete

D. configure manager add <host><key

Answer: (SHOW ANSWER)

a Cisco FirePower sensor to Firepower Management Center is configure manager add <host><key>. This command establishes a secure connection between the sensor and the FMC using a registration key.

The <host> parameter can be either the IP address or the hostname of the FMC. The <key> parameter can be any alphanumeric string that matches the one configured on the FMC. This command is executed on the sensor's CLI in the privileged EXEC mode12. References: 1: Implementing and Operating Cisco Security Core Technologies (SCOR) course, Module 2: Network Security, Lesson 2: Deploying Cisco Firepower Next-Generation Firewall, Topic: Registering the Cisco Firepower NGFW to the FMC2: Firepower Management Center Configuration Guide, Version 6.6 - Device Management Basics [Cisco Secure Firewall Management Center] - Cisco.

NEW QUESTION: 38

An organization is trying to implement micro-segmentation on the network and wants to be able to gain visibility on the applications within the network. The solution must be able to maintain and force compliance. Which product should be used to meet these requirements?

A. Cisco Umbrella

B. Cisco AMP

C. Cisco Stealthwatch

D. Cisco Tetration

Answer: (SHOW ANSWER)

Micro-segmentation secures applications by expressly allowing particular application traffic and, by default, denying all other traffic. Micro-segmentation is the foundation for implementing a zero-trust security model for application workloads in the data center and cloud. Cisco Tetration is an application workload security platform designed to secure your compute instances across any infrastructure and any cloud. To achieve this, it uses behavior and attribute-driven microsegmentation policy generation and enforcement. It enables trusted access through automated, exhaustive context from various systems to automatically adapt security policies. To generate accurate microsegmentation policy, Cisco Tetration performs application dependency mapping to discover the relationships between different application tiers and infrastructure services. In addition, the platform supports "what-if" policy analysis using real-time data or historical data to assist in the validation and risk assessment of policy application pre-enforcement to ensure ongoing application availability. The normalized microsegmentation policy can be enforced through the application workload itself for a consistent approach to workload microsegmentation across any environment, including virtualized, bare-metal, and container workloads running in any public cloud or any data center. Once the microsegmentation policy is enforced, Cisco Tetration continues to monitor for compliance deviations, ensuring the segmentation policy is up to date as the application behavior change. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf denying all other traffic. Micro-segmentation is the foundation for implementing a zero-trust security model for application workloads in the data center and cloud.

Cisco Tetration is an application workload security platform designed to secure your compute instances across any infrastructure and any cloud. To achieve this, it uses behavior and attribute-driven microsegmentation policy generation and enforcement. It enables trusted access through automated, exhaustive context from various systems to automatically adapt security policies.

To generate accurate microsegmentation policy, Cisco Tetration performs application dependency mapping to discover the relationships between different application tiers and infrastructure services. In addition, the platform supports "what-if" policy analysis using real-time data or historical data to assist in the validation and risk assessment of policy application pre-enforcement to ensure ongoing application availability. The normalized microsegmentation policy can be enforced through the application workload itself for a consistent approach to workload microsegmentation across any environment, including virtualized, bare-metal, and container workloads running in any public cloud or any data center. Once the microsegmentation policy is enforced, Cisco Tetration continues to monitor for compliance deviations, ensuring the segmentation policy is up to date as the application behavior change.

Micro-segmentation secures applications by expressly allowing particular application traffic and, by default, denying all other traffic. Micro-segmentation is the foundation for implementing a zero-trust security model for application workloads in the data center and cloud. Cisco Tetration is an application workload security platform designed to secure your compute instances across any infrastructure and any cloud. To achieve this, it uses behavior and attribute-driven microsegmentation policy generation and enforcement. It enables trusted access through automated, exhaustive context from various systems to automatically adapt security policies. To generate accurate microsegmentation policy, Cisco Tetration performs application dependency mapping to discover the relationships between different application tiers and infrastructure services. In addition, the platform supports "what-if" policy analysis using real-time data or historical data to assist in the validation and risk assessment of policy application pre-enforcement to ensure ongoing application availability. The normalized microsegmentation policy can be enforced through the application workload itself for a consistent approach to workload microsegmentation across any environment, including virtualized, bare-metal, and container workloads running in any public cloud or any data center. Once the microsegmentation policy is

enforced, Cisco Tetration continues to monitor for compliance deviations, ensuring the segmentation policy is up to date as the application behavior change. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf

NEW QUESTION: 39
Which two protocols must be configured to authenticate end users to the Cisco WSA? (Choose two.)
A. CHAP
B. RADIUS
C. TACACS+
D. NTLMSSP
E. Kerberos
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 40
Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?
A. transparent
B. redirection
C. forward
D. proxy gateway
Answer: A (LEAVE A REPLY)
Explanation There are two possible methods to accomplish the redirection of traffic to Cisco WSA: transparent proxy mode and explicit proxy mode. In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to Cisco WSA, without any configuration on the client. The transparent proxy deployment is used in this design, and the Cisco ASA firewall is used to redirect traffic to the appliance because all of the outbound web traffic passes through the device and is generally managed by the same operations staff who manage Cisco WSA. Reference:
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesignGuide-AUG13.pdf There are two possible methods to accomplish the redirection of traffic to Cisco WSA: transparent proxy mode and explicit proxy mode.
In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to Cisco WSA, without any configuration on the client. The transparent proxy deployment is used in this design, and the Cisco ASA firewall is used to redirect traffic to the appliance because all of the outbound web traffic passes through the device and is generally managed by the same operations staff who manage Cisco WSA.
Explanation There are two possible methods to accomplish the redirection of traffic to Cisco WSA: transparent proxy mode and explicit proxy mode. In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to Cisco WSA, without any configuration on the client. The transparent proxy deployment is used in this design, and the Cisco ASA firewall is used to redirect traffic to the appliance because all of the outbound web traffic passes through the device and is generally managed by the same operations staff who manage Cisco WSA. Reference:
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesignGuide-AUG13.pdf

NEW QUESTION: 41
Which CoA response code is sent if an authorization state is changed successfully on a Cisco IOS device?
A. CoA-NCL

B. CoA-NAK
C. -
D. CoA-ACK
Answer: D (LEAVE A REPLY)
CoA-ACK is the CoA response code that is sent if an authorization state is changed successfully on a Cisco IOS device. CoA-ACK stands for CoA acknowledgment, which indicates that the device has received and processed the CoA request from the server and applied the new authorization settings to the session. The attributes returned within a CoA-ACK can vary based on the CoA request, such as session reauthentication, session termination, or session modification. The other options are not correct because they are not valid CoA response codes. CoA-NCL, CoA-NAK, and CoA-MAV are not defined in RFC 5176, which specifies the CoA protocol. CoA-NAK is the closest option, but it stands for CoA non-acknowledgment, which indicates that the device has rejected the CoA request from the server due to some error or inconsistency. References := Some possible references are:
* RADIUS Change of Authorization - Cisco
* Security and VPN Configuration Guide, Cisco IOS XE 17.x
* RFC 5176 - Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

NEW QUESTION: 42
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 converge multiple accounting technologies into one accounting mechanism
C. They provide monitoring of a wider range of IP packet information from Layer 2 to 4.
D. They provide attack prevention by dropping the traffic.
E. They provide accounting and billing enhancements
Answer: (SHOW ANSWER)

NEW QUESTION: 43
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: D (LEAVE A REPLY)

The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across your organization that Advanced Malware Protection (AMP) sees Reference: https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1 organization that Advanced Malware Protection (AMP) sees Reference:
The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across your organization that Advanced Malware Protection (AMP) sees Reference: https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1

NEW QUESTION: 44
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. Intelligent proxy and SSL decryption is disabled in the policy.
D. Client computers do not have an SSL certificate deployed from an internal CA server.
Answer: (SHOW ANSWER)
https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-Intelligent-Proxy

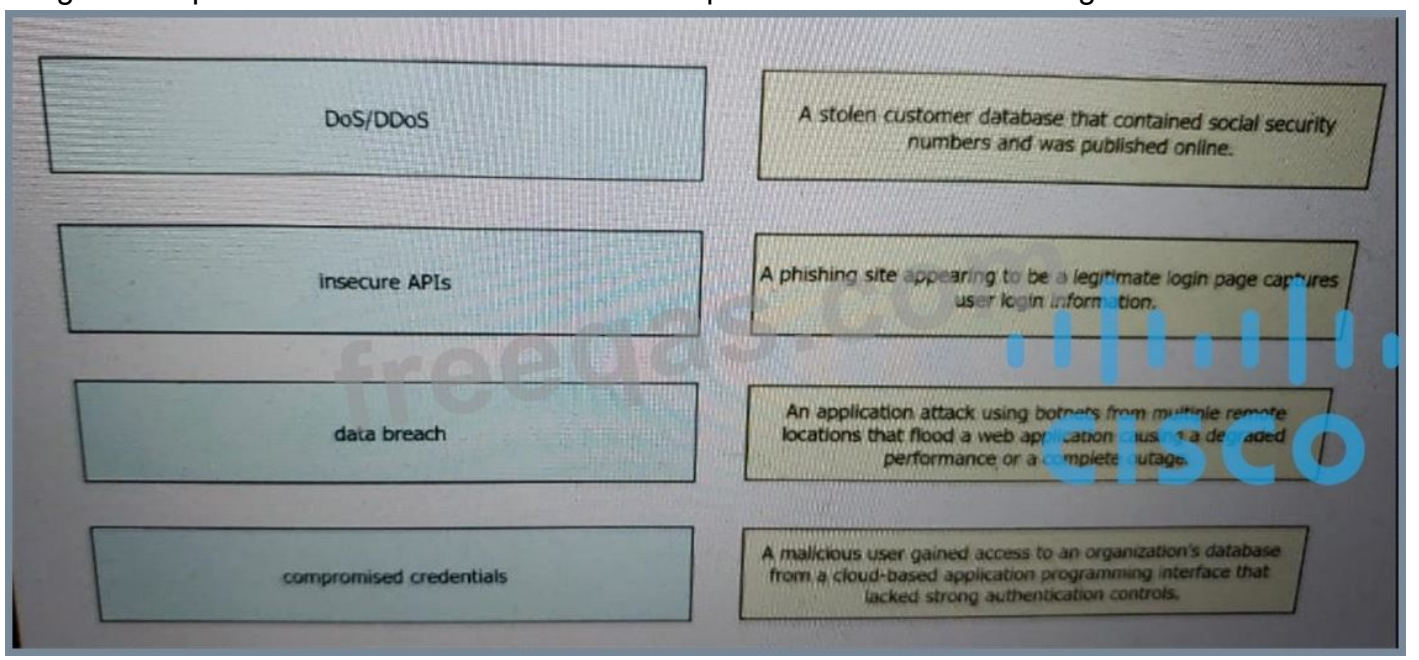
NEW QUESTION: 45
Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two.)
A. packet decoder
B. modbus
C. SSL
D. SIP
E. inline normalization
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 46
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 uses machine learning and real-time behavior analytics.
D. It utilizes sensors that send messages securely.
Answer: C (LEAVE A REPLY)
Reference:
- Determines which identities the recipient perceives is sending the message

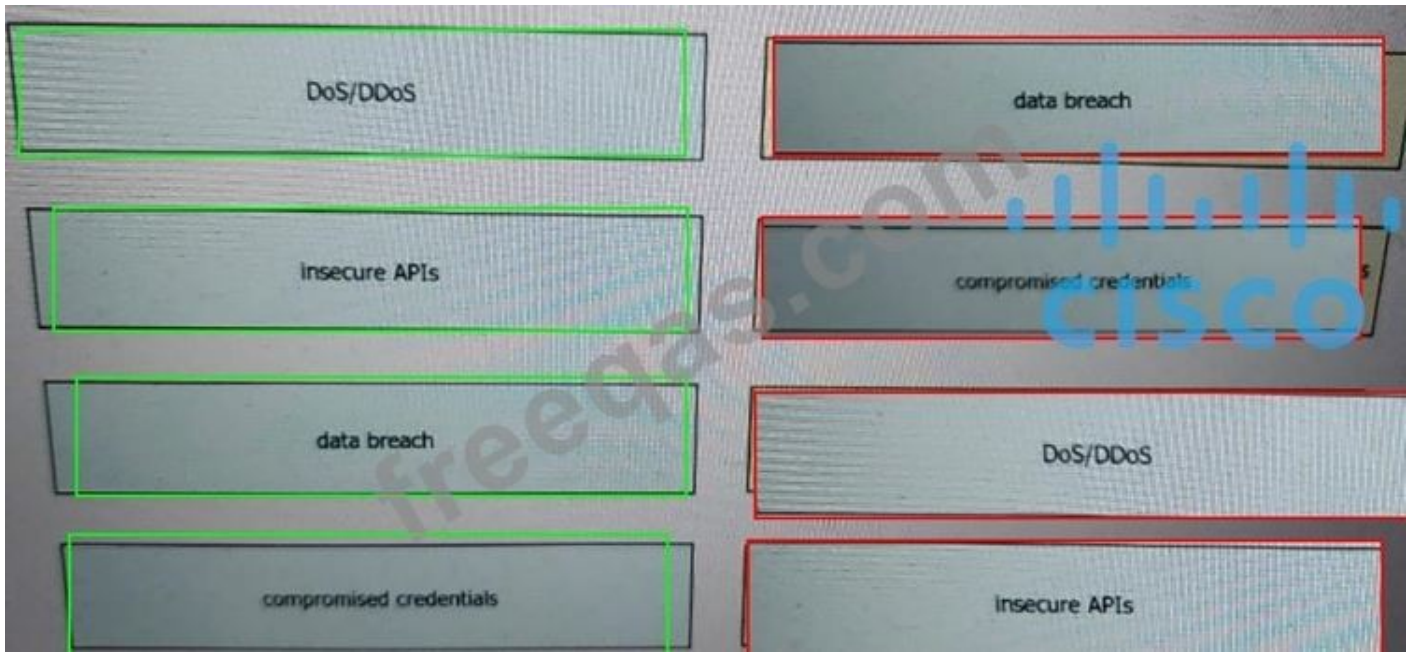
https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740894.pdf

NEW QUESTION: 47
What is a benefit of conducting device compliance checks?
A. It scans endpoints to determine if malicious activity is taking place.
B. It indicates what type of operating system is connecting to the network.
C. It validates if anti-virus software is installed.
D. It detects email phishing attacks.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
Drag and drop the threats from the left onto examples of that threat on the right



Answer:



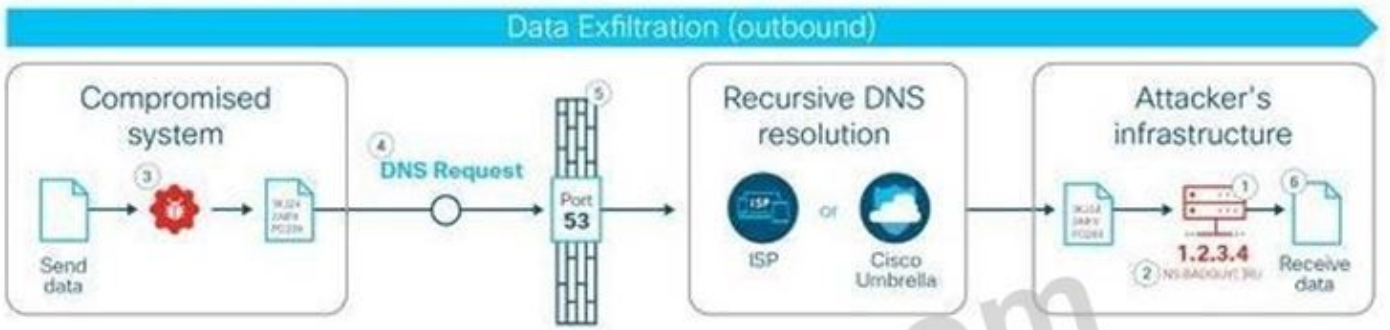
NEW QUESTION: 49
Which two cryptographic algorithms are used with IPsec? (Choose two)
A. AES-BAC
B. AES-ABC
C. HMAC-SHA1/SHA2
D. Triple AMC-CBC
E. AES-CBC
Answer: C,E (LEAVE A REPLY)
Explanation
Explanation
Cryptographic algorithms defined for use with IPsec include:
+ HMAC-SHA1/SHA2 for integrity protection and authenticity.
+ TripleDES-CBC for confidentiality
+ AES-CBC and AES-CTR for confidentiality.
+ AES-GCM and ChaCha20-Poly1305 providing confidentiality and authentication together efficiently.

NEW QUESTION: 50
Which type of attack is social engineering?
A. trojan
B. phishing
C. malware
D. MITM
Answer: B (LEAVE A REPLY)
Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem.

NEW QUESTION: 51
An organization wants to provide visibility and to identify active threats in its network using a VM. The organization wants to extract metadata from network packet flow while ensuring that payloads are not retained or transferred outside the network. Which solution meets these requirements?
A. Cisco Umbrella Cloud
B. Cisco Stealthwatch Cloud PNM
C. Cisco Stealthwatch Cloud PCM
D. Cisco Umbrella On-Premises
Answer: B (LEAVE A REPLY)
Private Network Monitoring (PNM) provides visibility and threat detection for the on-premises network, delivered from the cloud as a SaaS solution. It is the perfect solution for organizations who prefer SaaS products and desire better awareness and security in their on-premises environments while reducing capital expenditure and operational overhead. It works by deploying lightweight software in a virtual machine or server that can consume a variety of native sources of telemetry or extract metadata from network packet flow. It encrypts this metadata and sends it to the Stealthwatch Cloud analytics platform for analysis. Stealthwatch Cloud consumes metadata only. The packet payloads are never retained or transferred outside the network.
This lab focuses on how to configure a Stealthwatch Cloud Private Network Monitoring (PNM) Sensor, in order to provide visibility and effectively identify active threats, and monitors user and device behavior within onpremises networks.
The Stealthwatch Cloud PNM Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.

NEW QUESTION: 52
How does DNS Tunneling exfiltrate data?
A. An attacker registers a domain that a client connects to based on DNS records and sends malware through that connection.
B. An attacker opens a reverse DNS shell to get into the client's system and install malware on it.
C. An attacker uses a non-standard DNS port to gain access to the organization's DNS servers in order to poison the resolutions.
D. An attacker sends an email to the target with hidden DNS resolvers in it to redirect them to a malicious domain.
Answer: (SHOW ANSWER)
Explanation

Figure 1. **Data Exfiltration**



1. The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNS nameserver (NS) and malicious payload.
2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. BADGUY[.]RU) is registered or reused. The registrar informs the top-level domain (.RU) nameservers to refer requests for BADGUY[.]RU to NS.BADGUY[.]RU, which has a DNS record mapped to 1.2.3.4.
3. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, PO28X977W, ...).
4. The payload initiates thousands of unique DNS record requests to the attacker's domain with each string as a part of the domain name (e.g. 3KJ242AIE9.BADGUY[.]RU). Depending on the attacker's patience and stealth, requests can be spaced out over days or months to avoid suspicious network activity.
5. The requests are forwarded to a recursive DNS resolver. During resolution, the requests are sent to the attacker's authoritative DNS nameserver.
6. The tunneling kit parses the encoded strings and rebuilds the exfiltrated data.

NEW QUESTION: 53
Refer to the exhibit. When creating an access rule for URL filtering, a network engineer adds certain categories and individual URLs to block. What is the result of the configuration?
A. Only URLs for botnets with reputation scores of 3-5 will be blocked.
B. Only URLs for botnets with a reputation score of 3 will be blocked.
C. Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked.
D. Only URLs for botnets with reputation scores of 1-3 will be blocked.
Answer: D (LEAVE A REPLY)

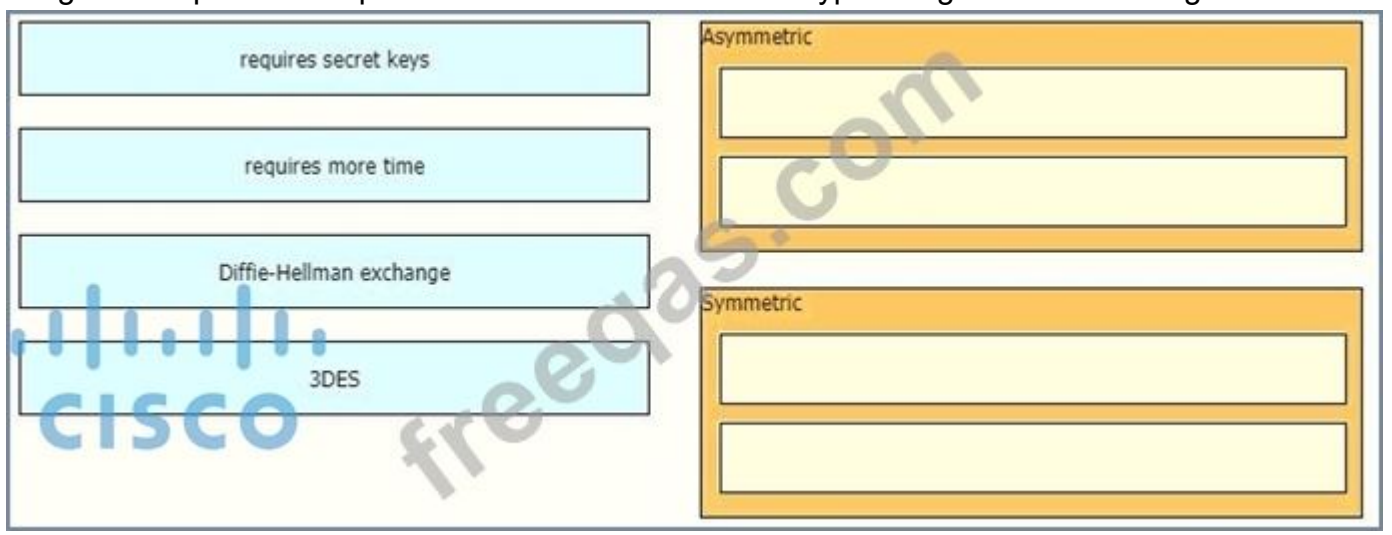
NEW QUESTION: 54
An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?
A. Cisco Umbrella
B. Cisco Cloud Email Security
C. Cisco NGFW
D. Cisco Cloudlock
Answer: D (LEAVE A REPLY)
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

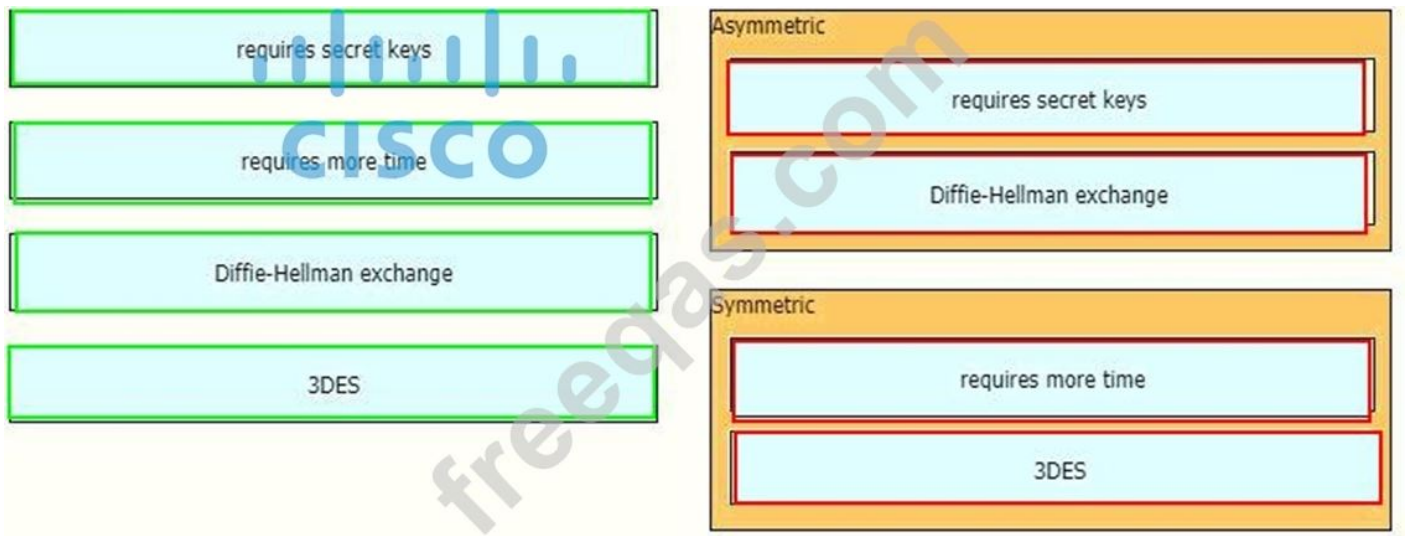
NEW QUESTION: 55
Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?
A. SDLC
B. Docker
C. Lambda
D. Contiv
Answer: (SHOW ANSWER)

NEW QUESTION: 56
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 GET HTTP method to obtain a token to be used for authentication.
C. It uses the POST 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: C (LEAVE A REPLY)

NEW QUESTION: 57
Drag and drop the descriptions from the left onto the encryption algorithms on the right.



Answer:



NEW QUESTION: 58
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 protects endpoint systems through application control and real-time scanning.
D. It enables behavioral analysis to be used for the endpoints.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/at-a-glance-c45-731874.html

NEW QUESTION: 59
Using Cisco Firepower's Security Intelligence policies, upon which two criteria is Firepower block based? (Choose two.)
A. protocol IDs
B. URLs
C. IP addresses
D. port numbers
E. MAC addresses
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 60
Which information is required when adding a device to Firepower Management Center?
A. username and password
B. encryption method
C. device serial number
D. registration key

Answer: D (LEAVE A REPLY)
Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html#ID-2242-0000069d

NEW QUESTION: 61
Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?
A. interpacket variation
B. software package variation
C. flow insight variation
D. process details variation
Answer: A (LEAVE A REPLY)
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.
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:
cisco_nexus_9300_ex_platform_switches_white_paper_uki.pdf
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.
cisco_nexus_9300_ex_platform_switches_white_paper_uki.pdf

NEW QUESTION: 62
Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?
A. Encrypted Traffic Analytics
B. Threat Intelligence Director
C. Cognitive Threat Analytics
D. Cisco Talos Intelligence
Answer: (SHOW ANSWER)
Explanation
As shown in the image, on the FMC you have to configure sources from where you would like to download threat intelligence information. The FMC then pushes that information (observables) to sensors. When the traffic matches the observables, the incidents appear in the FMC user interface (GUI).
https://www.cisco.com/c/en/us/support/docs/storage-networking/security/214859-configure-and-troubleshoot-cis

NEW QUESTION: 63
Why would a user choose an on-premises ESA versus the CES solution?
A. Sensitive data must remain onsite.
B. Demand is unpredictable.
C. The server team wants to outsource this service.
D. ESA is deployed inline.
Answer: A (LEAVE A REPLY)
One of the main reasons why a user would choose an on-premises ESA versus the CES solution is to have more control over the sensitive data that flows through the email system. With an on-premises ESA, the user can ensure that the data is stored and processed within their own network and data center, and that they comply with any regulatory or organizational requirements for data security and privacy. With a CES solution, the user would have to trust Cisco to handle the data in their cloud infrastructure, and to adhere to the service level agreements and security policies that are agreed upon. Some users may not be comfortable with this level of outsourcing, especially if they have strict data governance or compliance needs12. References: 1: Physical ESA vs Cloud ESA - Cisco Community 2: Cisco Email Security Appliance - Data Sheet

NEW QUESTION: 64
A mall provides security services to customers with a shared appliance. The mall wants separation of management on the shared appliance. Which ASA deployment mode meets these needs?
A. transparent mode
B. routed mode
C. multiple context mode
D. multiple zone mode
Answer: C (LEAVE A REPLY)

NEW QUESTION: 65
Refer to the exhibit.

```
Sysauthcontrol                  Enabled
Dot1x Protocol Version          3

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

Which command was used to display this output?

A. show dot1x all summary

B. show dot1x interface gi1/0/12

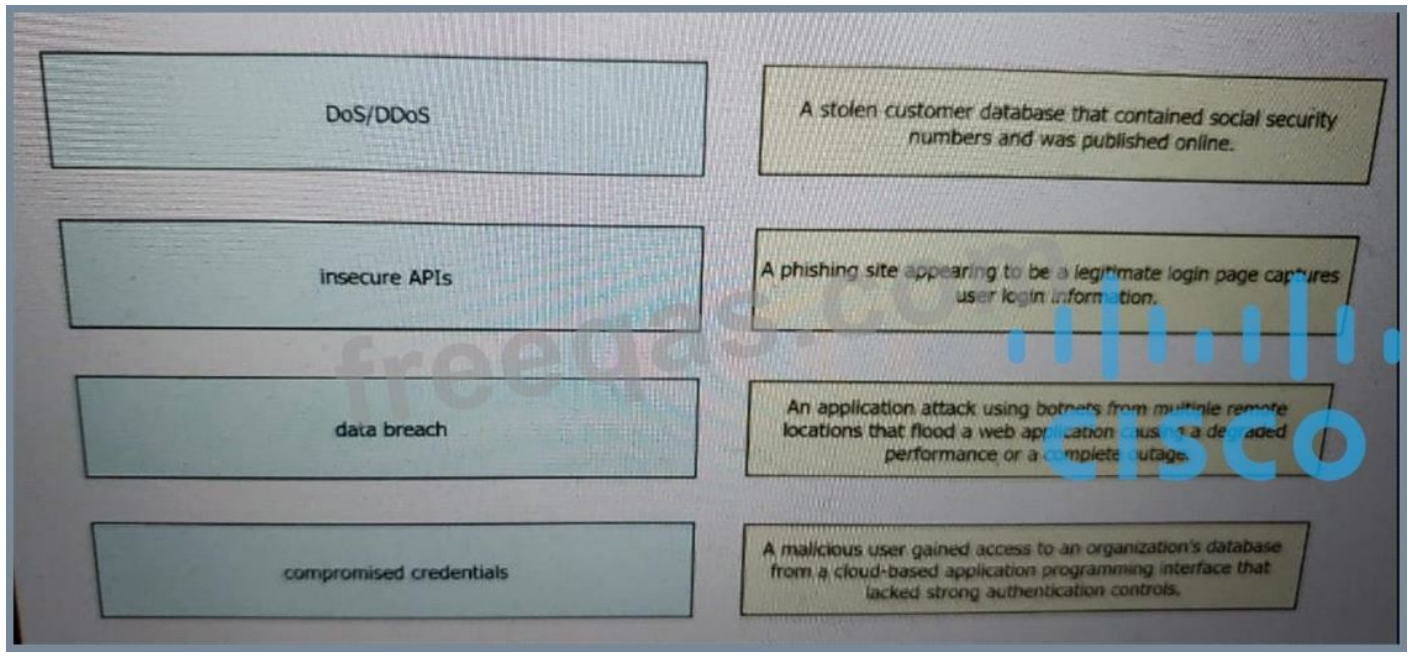
C. show dot1x all

D. show dot1x

Answer: (SHOW ANSWER)

NEW QUESTION: 66

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



Answer:

NEW QUESTION: 67
How does a WCCP-configured router identify if the Cisco WSA is functional?
A. The WSA sends a Here-I-Am message every 10 seconds, and the router acknowledges with an ISee-You message.
B. The router sends a Here-I-Am message every 10 seconds, and the WSA acknowledges with an ISee-You message.
C. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the router.
D. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the WSA.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 68
Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine?
(Choose two.)
A. TACACS+
B. SMTP
C. RADIUS
D. DHCP
E. sFlow
Answer: (SHOW ANSWER)

NEW QUESTION: 69
Which statement describes a serverless application?
A. The application runs from an ephemeral, event-triggered, and stateless container that is fully managed by a cloud provider.
B. The application is installed on network equipment and not on physical servers.
C. The application delivery controller in front of the server farm designates on which server the application runs each time.
D. The application runs from a containerized environment that is managed by Kubernetes or Docker Swarm.
Answer: (SHOW ANSWER)

NEW QUESTION: 70

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

A. Multiple NetFlow collectors are supported.

B. Advanced NetFlow v9 templates and legacy v5 formatting are supported.

C. Flow-create events are delayed.

D. Secure NetFlow connections are optimized for Cisco Prime Infrastructure

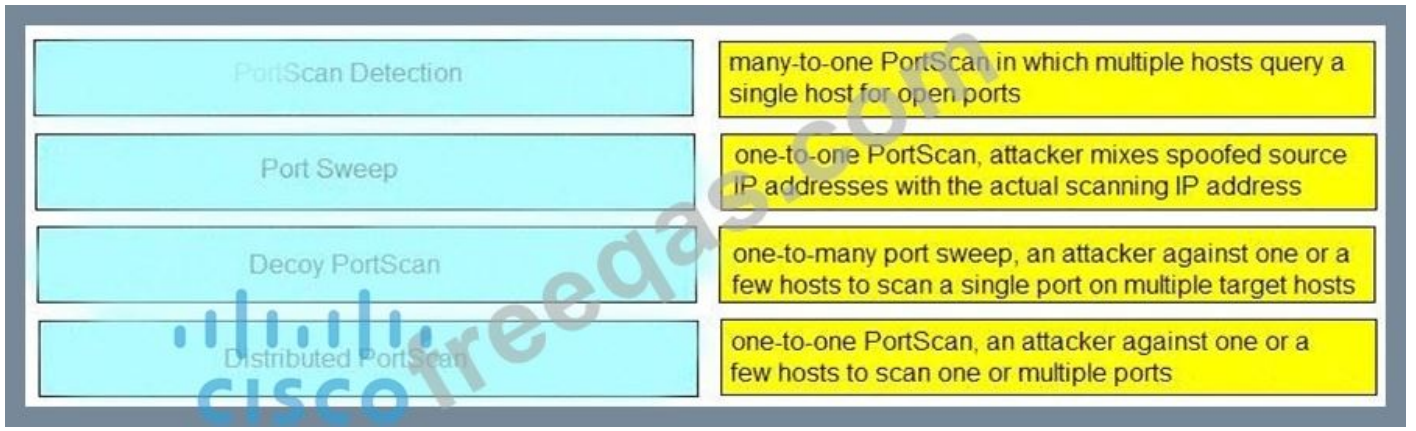
Answer: C (LEAVE A REPLY)

Reference:

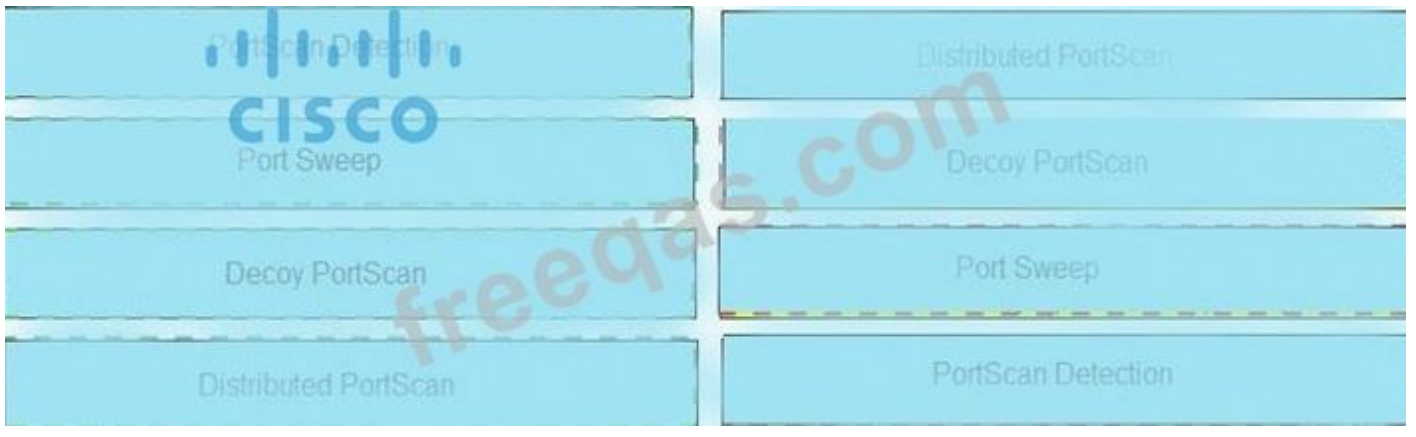
Each NSEL data record has the event time field (NF_F_EVENT_TIME_MSEC), which is the time that the event occurred in milliseconds. The NetFlow packet may consist of multiple events; however, the time that the packet is sent does not represent the time that the event occurred, because the NetFlow service waits for multiple events to pack the NetFlow packet.

NEW QUESTION: 71

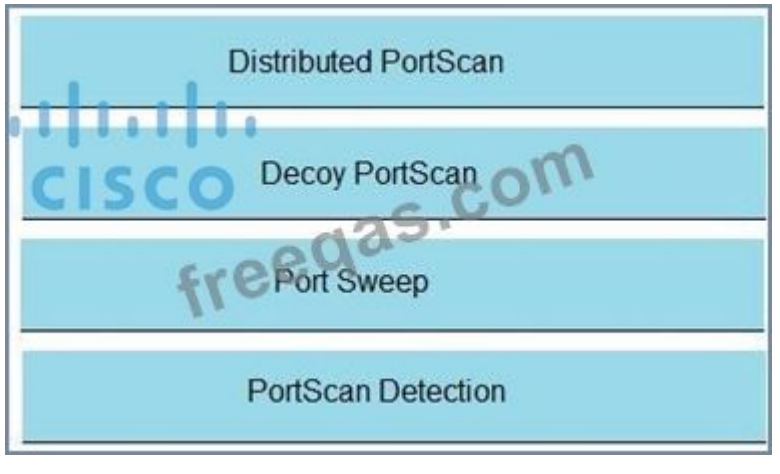
Drag and drop the Firepower Next Generation Intrustion Prevention System detectors from the left onto the correct definitions on the right.



Answer:

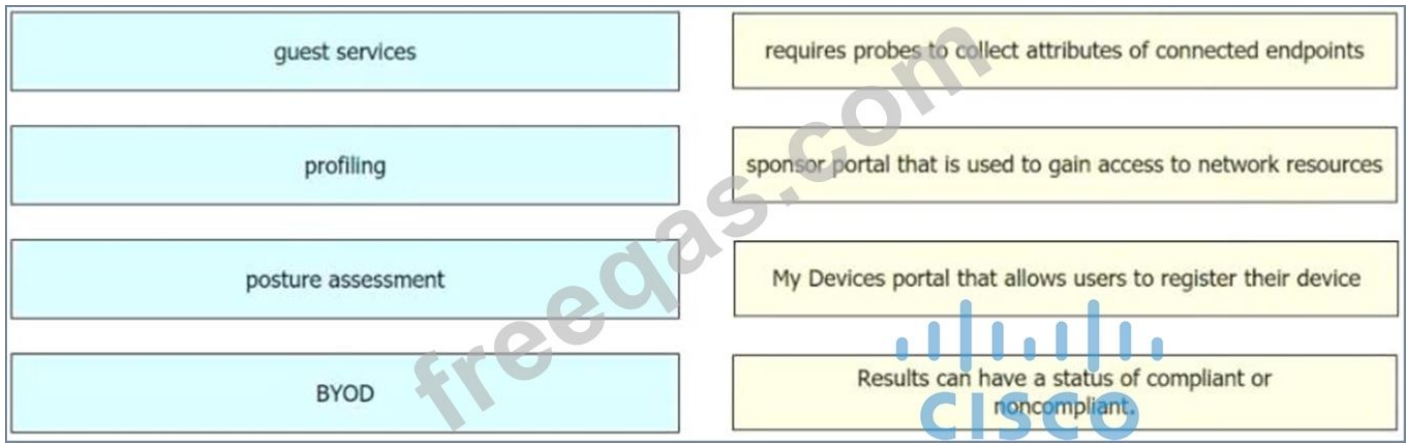


Explanation

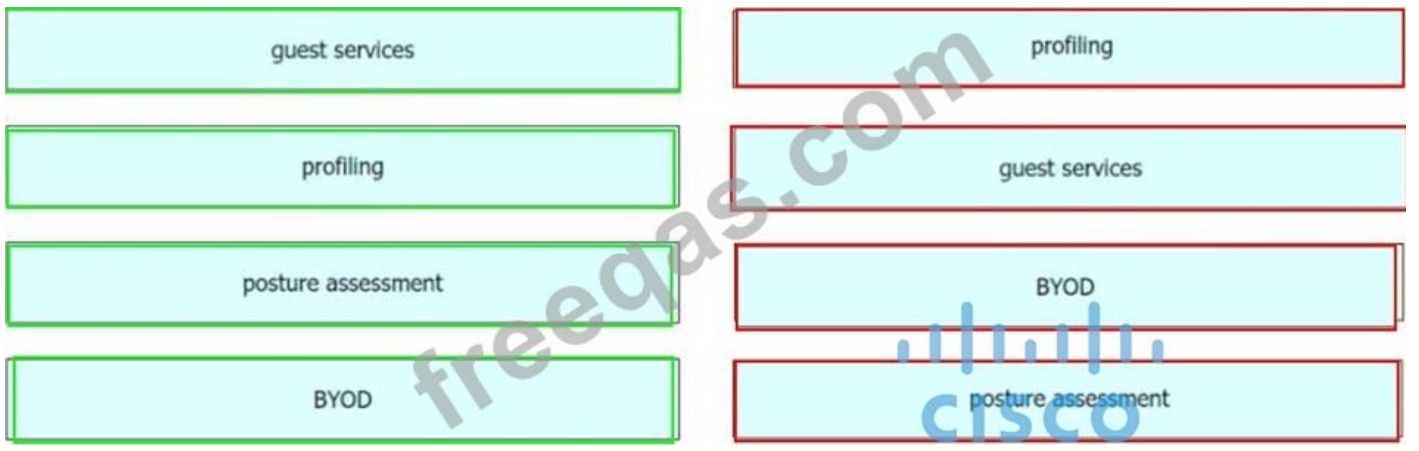


Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/detecti

NEW QUESTION: 72
Drag and drop the concepts from the left onto the correct descriptions on the right



Answer:



NEW QUESTION: 73
What features does Cisco FTDv provide over ASAv?
A. Cisco FTDv runs on VMWare while ASAv does not
B. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not
C. Cisco FTDv runs on AWS while ASAv does not
D. Cisco FTDv supports URL filtering while ASAv does not
Answer: D (LEAVE A REPLY)
Cisco FTDv is a virtual appliance that combines the features of Cisco ASA and Cisco Firepower NGIPS. It provides stateful firewall, IPS, URL filtering, malware protection, and other advanced security functions.
Cisco ASAv is a virtual appliance that only provides stateful firewall and VPN features. It does not support URL filtering or other Firepower functions. Therefore, Cisco FTDv provides more features than ASAv, especially for next-generation firewall capabilities. References :=
* Cisco Firewall in AWS - Should i use ASAv or FTDv/FMCv?
* Difference between Cisco ASAv, NGIPSv and FTDv...?
* Are there any differences in features between Cisco ASA hardware ...

NEW QUESTION: 74

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: 75

Which IETF attribute is supported for the RADIUS CoA feature?

A. 24 State

B. 30 Calling-Station-ID

C. 42 Acct-Session-ID

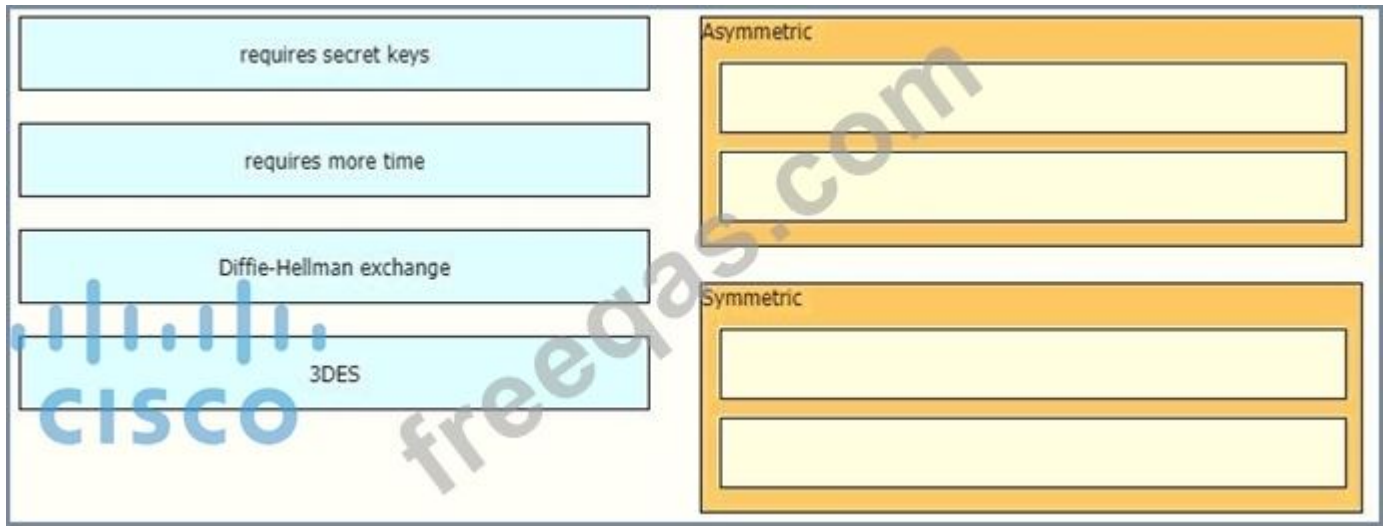
D. 81 Message-Authenticator

Answer: A (LEAVE A REPLY)

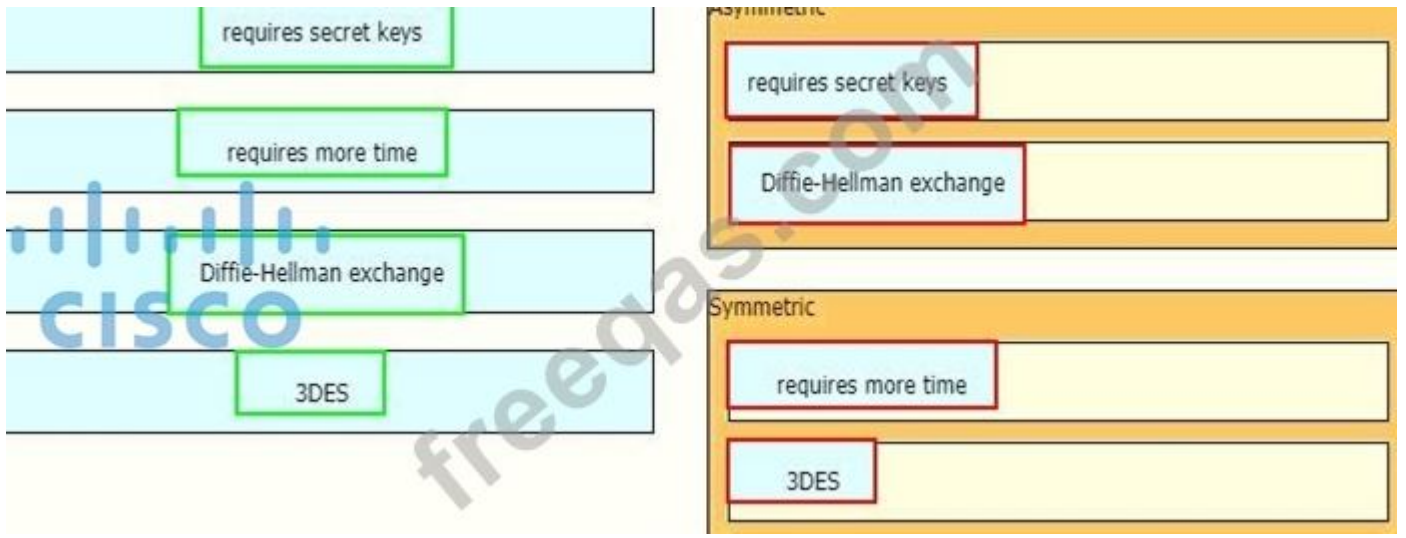
The RADIUS CoA feature supports the IETF attribute 24 State, which is used to identify the session for which the CoA request is intended. The State attribute is sent by the device in the Access-Accept message and must be echoed back by the RADIUS server in the CoA-Request message. The other attributes are not supported for the RADIUS CoA feature.
To understand the concept of RADIUS CoA and the supported attributes, you can refer to the following sections of the source book:
* Section 1.1.2: Describe the concepts of network security
* Section 1.1.2.6: Describe the concepts of RADIUS CoA
* Section 1.1.2.7: Describe the concepts of supported IETF attributes
References:
* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0
* RADIUS Change of Authorization - Cisco
* RADIUS attribute for change of authorization - Ruckus Networks

NEW QUESTION: 76
An organization has two systems in their DMZ that have an unencrypted link between them for communication. The organization does not have a defined password policy and uses several default accounts on the systems. The application used on those systems also have not gone through stringent code reviews.
Which vulnerability would help an attacker brute force their way into the systems?
A. missing encryption
B. weak passwords
C. lack of input validation
D. lack of file permission
Answer: A (LEAVE A REPLY)

NEW QUESTION: 77
Drag and drop the descriptions from the left onto the encryption algorithms on the right.



Answer:

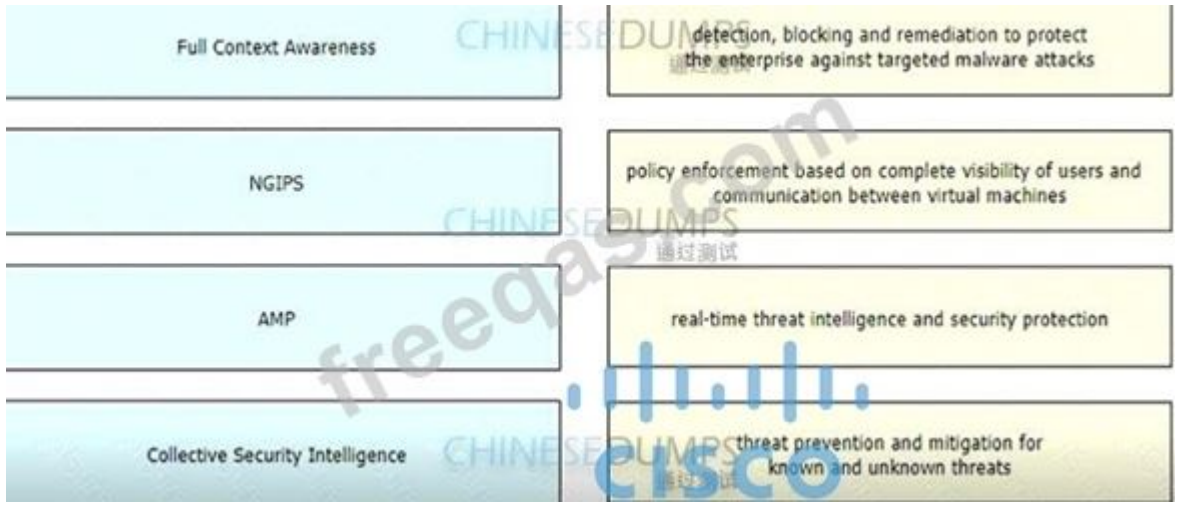


NEW QUESTION: 78
Which capability is exclusive to a Cisco AMP public cloud instance as compared to a private cloud instance?
A. RBAC
B. SPERO detection engine
C. TETRA detection engine
D. ETHOS detection engine
Answer: D (LEAVE A REPLY)

NEW QUESTION: 79
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. Upload the organization root CA to Cisco Umbrella.
C. Modify the user's browser settings to suppress errors from Cisco Umbrella.
D. Install the Cisco Umbrella root CA onto the user's device.
Answer: (SHOW ANSWER)

NEW QUESTION: 80

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



Answer:

Explanation:

Full Context Awareness - policy enforcement

NGIPS - threat prevention

AMP - real-time

Collective Sec Intel - Detection, blocking an remediation

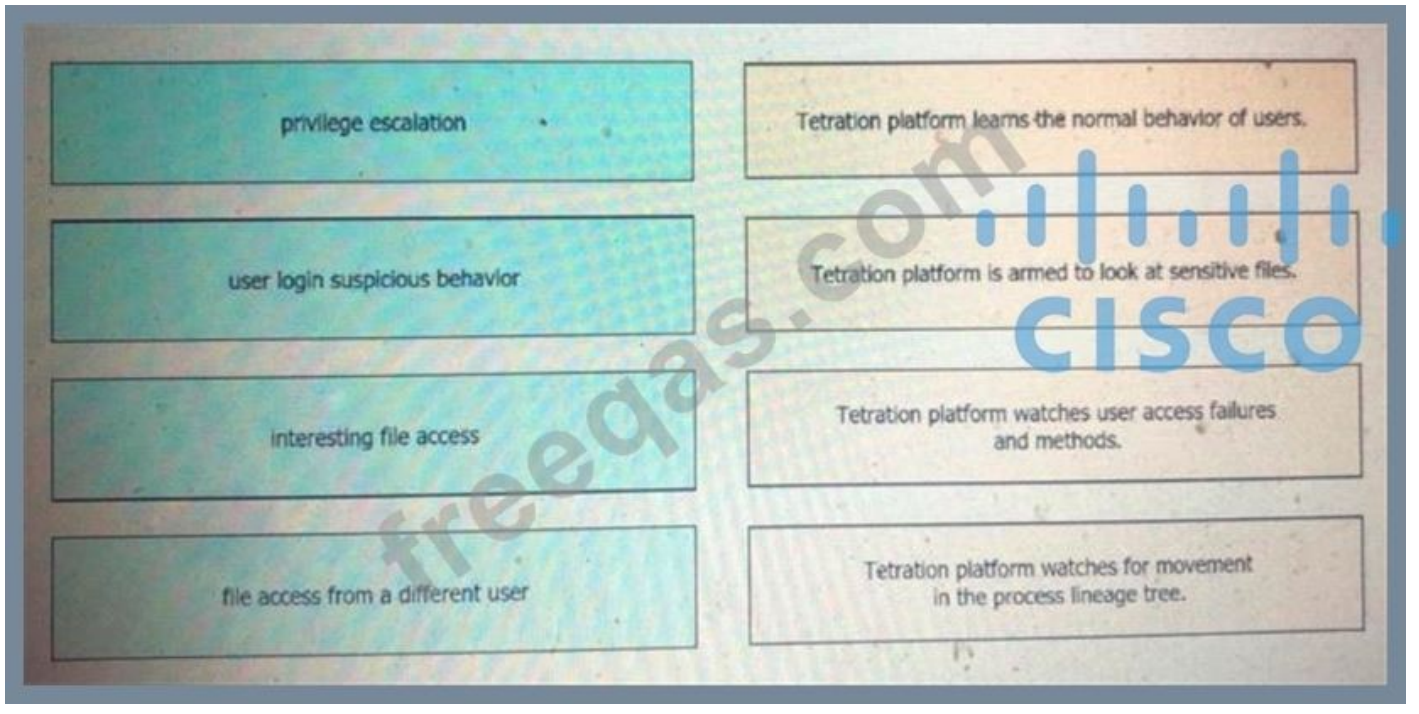
NEW QUESTION: 81

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

Answer:

NEW QUESTION: 82

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



Answer:

NEW QUESTION: 83
An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?
A. TCP 6514
B. UDP 1700
C. TCP 49
D. UDP 1812
Answer: (SHOW ANSWER)
Explanation CoA Messages are sent on two different udp ports depending on the platform. Cisco standardizes on UDP port1700, while the actual RFC calls out using UDP port 3799.

NEW QUESTION: 84
An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?
A. TCP 6514
B. UDP 1700
C. TCP 49
D. UDP 1812
Answer: (SHOW ANSWER)
- RADIUS Change of Authorization (CoA) Send: UDP/1700
- RADIUS Change of Authorization (CoA) Listen/Relay: UDP/1700, 3799

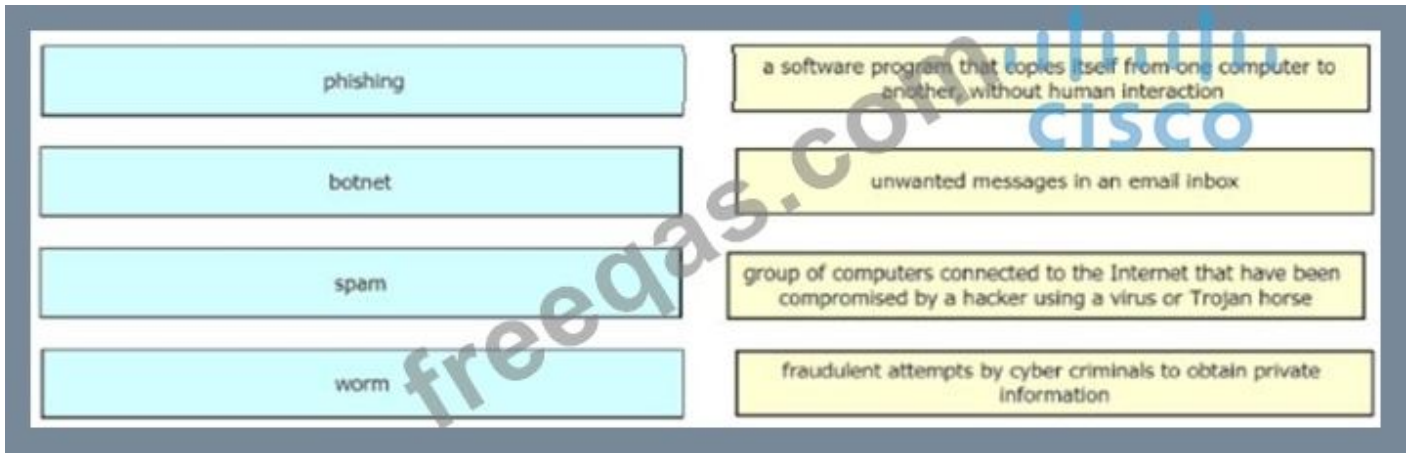
NEW QUESTION: 85
Which Cisco cloud security software centrally manages policies on multiple platforms such as Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS?
A. Cisco Defense Orchestrator
B. Cisco Configuration Professional
C. Cisco Secureworks
D. Cisco DNAC
Answer: A (LEAVE A REPLY)
Cisco Defense Orchestrator (CDO) 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. CDO centrally manages elements of policy and configuration across Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS1. CDO also provides visibility, automation, and orchestration capabilities to simplify and unify security operations2. The other options are not cloud security software that can centrally manage policies on multiple platforms. Cisco Configuration Professional is a device management tool for Cisco routers and switches. Cisco Secureworks is a security services provider that offers threat intelligence and incident response. Cisco DNAC is a network controller that automates and assures services across campus, branch, and edge networks. References :=
* Cisco Defense Orchestrator Data Sheet
* Cisco Defense Orchestrator

NEW QUESTION: 86
Refer to the exhibit.

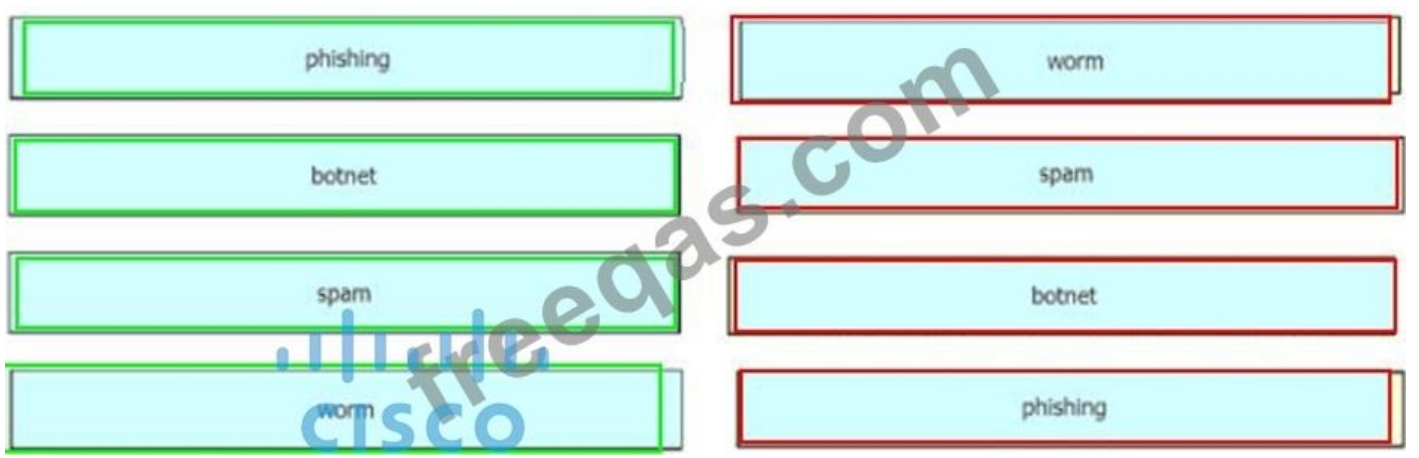
```
snmp-server group SNMP v3 auth access
15
```

What does the number 15 represent in this configuration?
A. privilege level for an authorized user to this router
B. access list that identifies the SNMP devices that can access the router
C. interval in seconds between SNMPv3 authentication attempts
D. number of possible failed attempts until the SNMPv3 user is locked out
Answer: B (LEAVE A REPLY)
The syntax of this command is shown below:
snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]}] [read read-view] [write write-view] [notify notify-view] [access access-list]
The command above restricts which IP source addresses are allowed to access SNMP functions on the router. You could restrict SNMP access by simply applying an interface ACL to block incoming SNMP packets that don't come from trusted servers. However, this would not be as effective as using the global SNMP commands shown in this recipe. Because you can apply this method once for the whole router, it is much simpler than applying ACLs to block SNMP on all interfaces separately. Also, using interface ACLs would block not only SNMP packets intended for this router, but also may stop SNMP packets that just happened to be passing through on their way to some other destination device.

NEW QUESTION: 87
Drag and drop the common security threats from the left onto the definitions on the right.



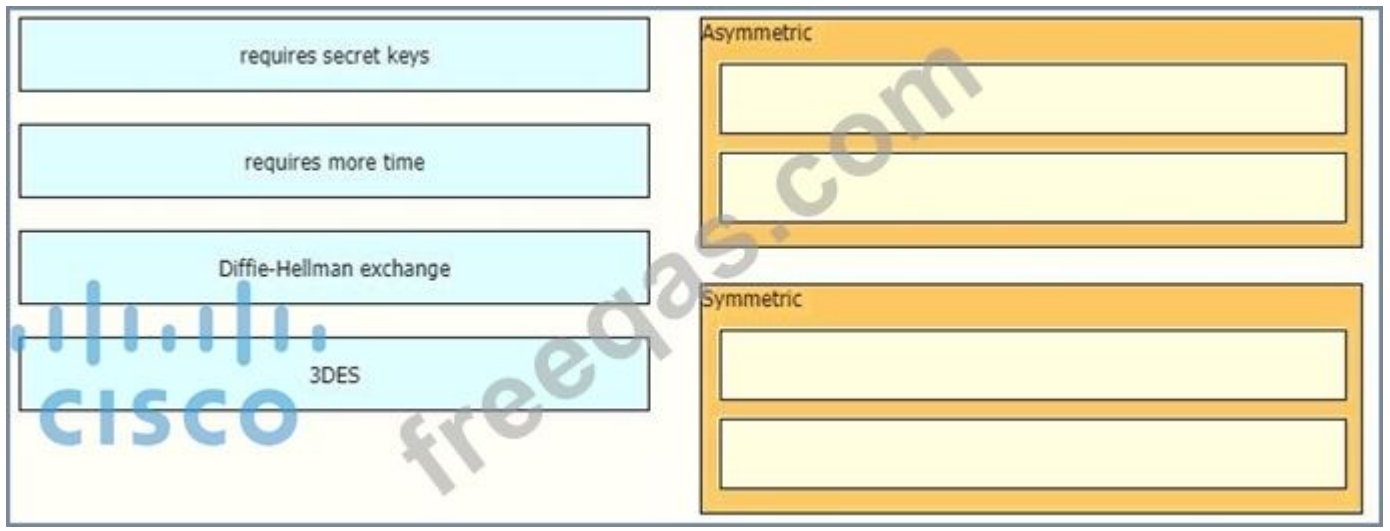
Answer:



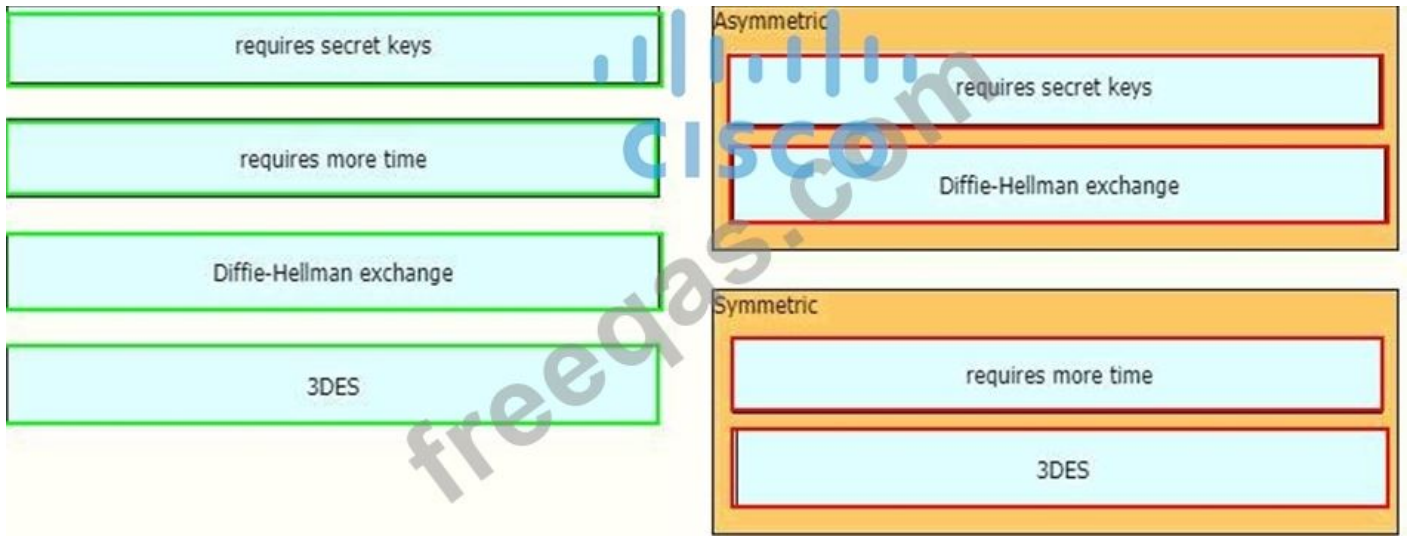
NEW QUESTION: 88
A network engineer must monitor user and device behavior within the on-premises network. This data must be sent to the Cisco Stealthwatch Cloud analytics platform for analysis. What must be done to meet this requirement using the Ubuntu-based VM appliance deployed in a VMware-based hypervisor?
A. Configure a Cisco FMC to send syslogs to Cisco Stealthwatch Cloud
B. Deploy the Cisco Stealthwatch Cloud PNM sensor that sends data to Cisco Stealthwatch Cloud
C. Deploy a Cisco FTD sensor to send network events to Cisco Stealthwatch Cloud
D. Configure a Cisco FMC to send NetFlow to Cisco Stealthwatch Cloud
Answer: B (LEAVE A REPLY)
Explanation The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.
Explanation The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf

NEW QUESTION: 89
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two.)
A. virtualization
B. middleware
C. operating systems
D. applications
E. data
Answer: D,E (LEAVE A REPLY)
Reference:
https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/

NEW QUESTION: 90
Drag and drop the descriptions from the left onto the encryption algorithms on the right.

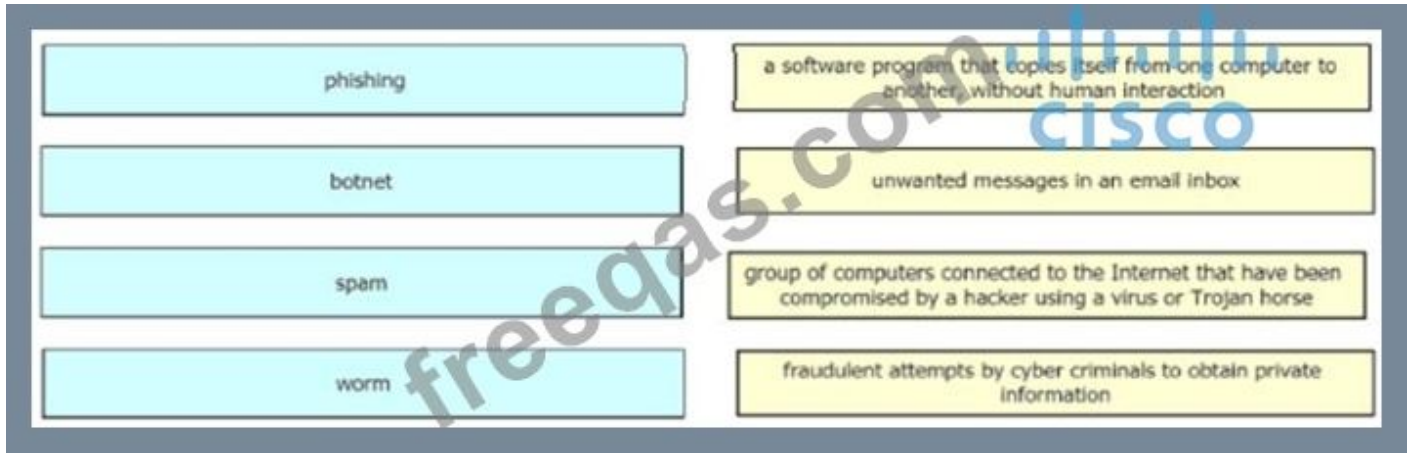


Answer:

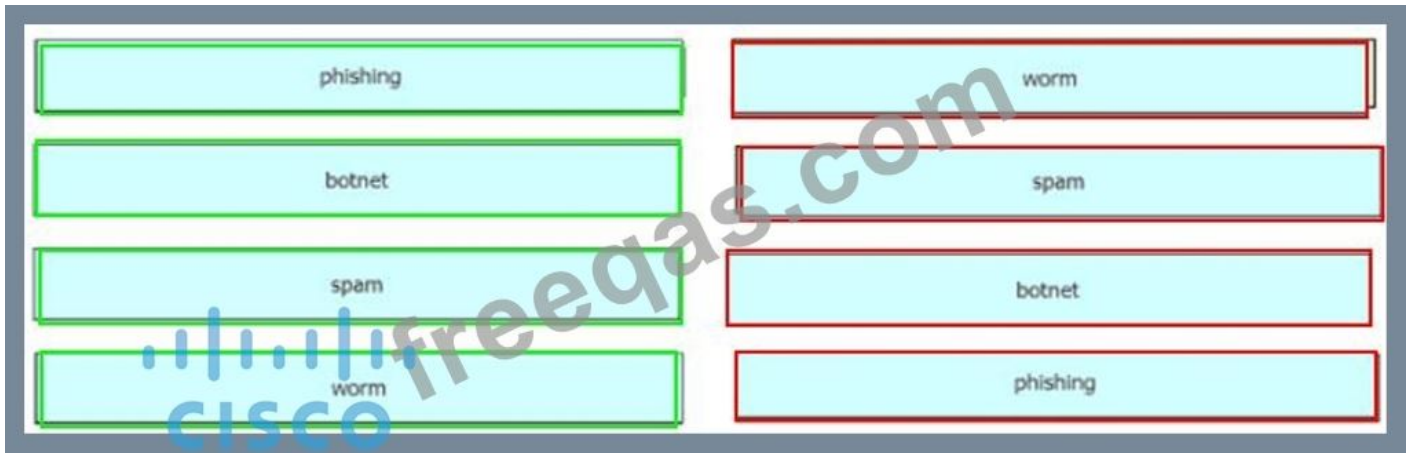


NEW QUESTION: 91

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



Answer:

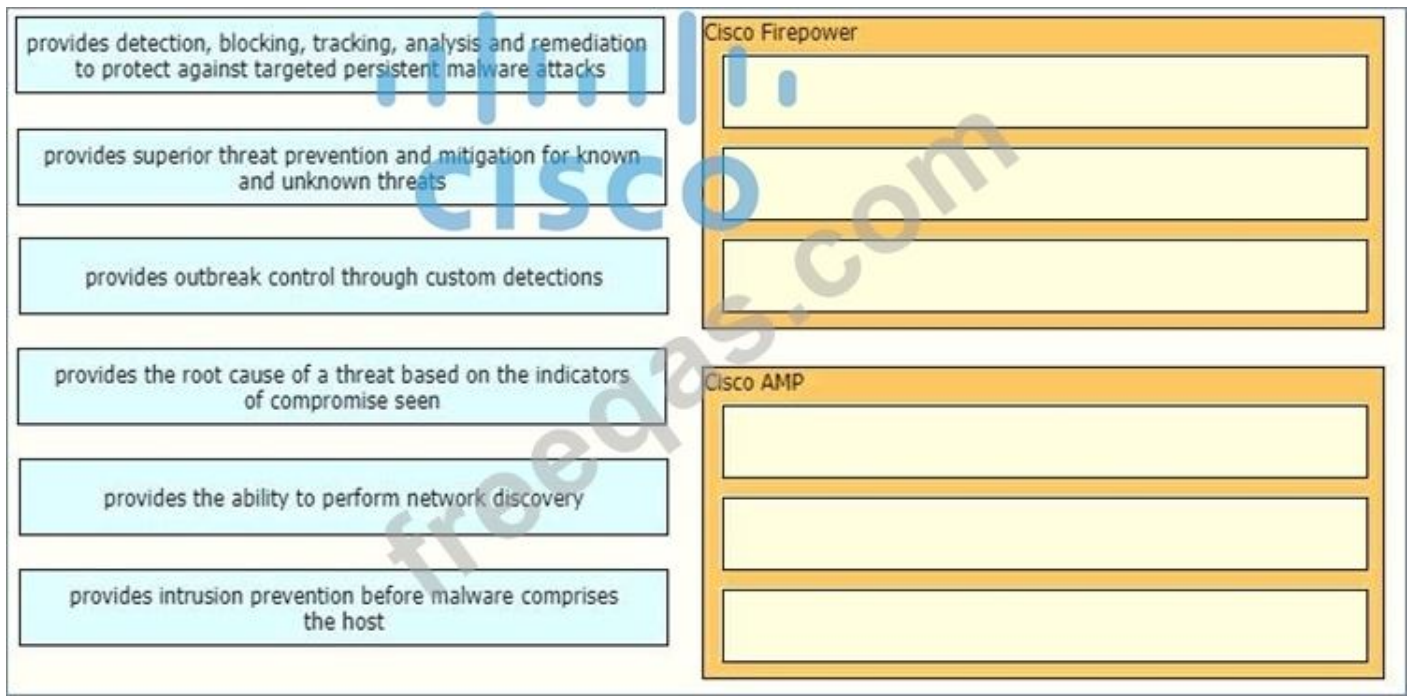


NEW QUESTION: 92
Refer to the exhibit.

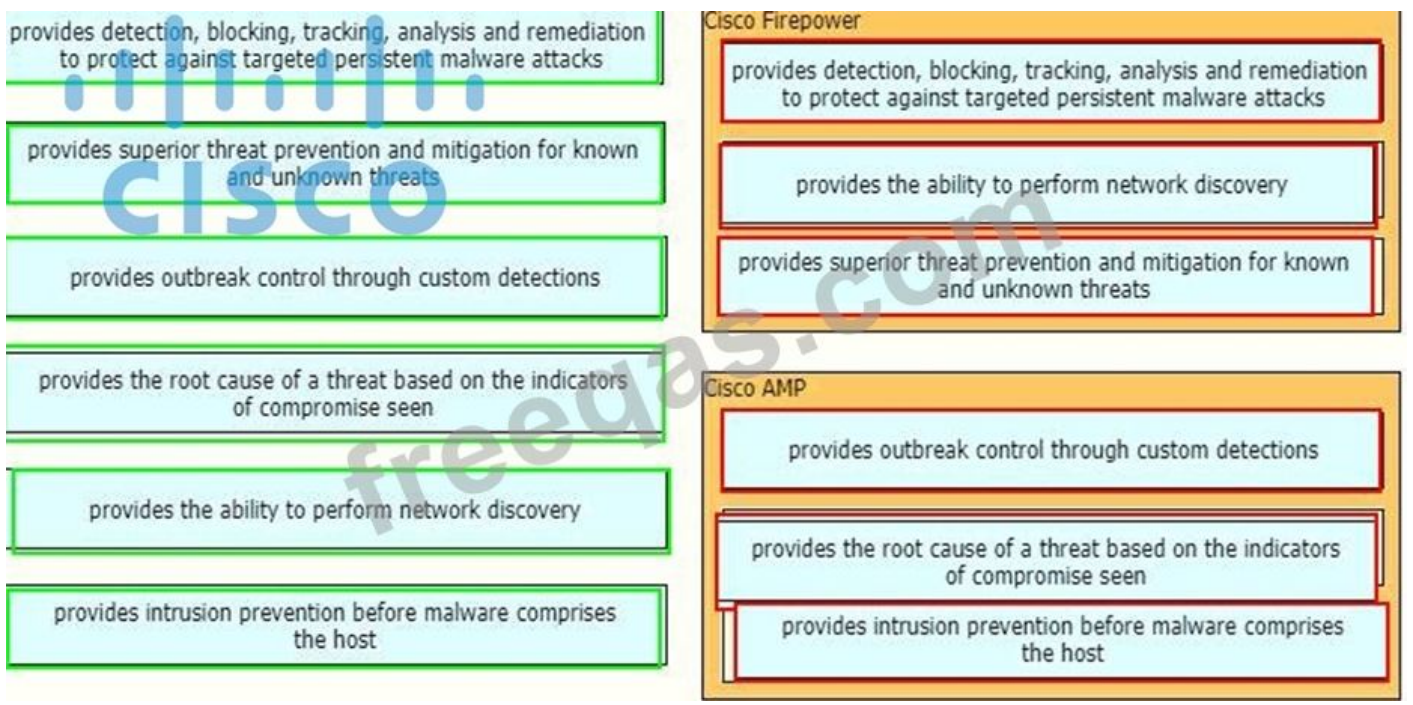
```
aaa new-model
radius-server host 10.0.0.12 key
secret12
```

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

NEW QUESTION: 93
Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.



Answer:



NEW QUESTION: 94

Which parameter is required when configuring a Netflow exporter on a Cisco Router?

A. DSCP value

B. Source interface

C. Exporter name

D. Exporter description

Answer: C (LEAVE A REPLY)

ExplanationAn example of configuring a NetFlow exporter is shown below:flow exporter Exporterdestination 192.168.100.22transport udp 2055

NEW QUESTION: 95
An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically. What must be configured to accomplish this?
A. Configure the Cisco WSA to modify policies based on the traffic seen.
B. Configure the Cisco ESA to receive real-time updates from Talos
C. Configure the Cisco WSA to receive real-time updates from Talos.
D. Configure the Cisco ESA to modify policies based on the traffic seen.
Answer: D (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/esa/esa120/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_01100.html

NEW QUESTION: 96
In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?
A. cross-site scripting
B. man-in-the-middle
C. LDAP injection
D. insecure API
Answer: B (LEAVE A REPLY)

NEW QUESTION: 97
Which command is used to log all events to a destination colector 209.165.201.107?
A. CiscoASA(config-cmap)#flow-export event-type flow-update destination 209.165.201.10
B. CiscoASA(config-pmap-c)#flow-export event-type flow-update destination 209.165.201.10
C. CiscoASA(config-cmap)# flow-export event-type all destination 209.165.201.
D. CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.10
Answer: (SHOW ANSWER)

NEW QUESTION: 98
What are two list types within AMP for Endpoints Outbreak Control? (Choose two)
A. blocked ports
B. simple custom detections
C. command and control
D. allowed applications
E. URL
Answer: B,D (LEAVE A REPLY)
Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists.
A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine.
Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf

NEW QUESTION: 99
Which CLI command is used to register a Cisco FirePower sensor to Firepower Management Center?
A. configure manager <key> add host
B. configure manager delete
C. configure manager add <host><key
D. configure system add <host><key>
Answer: C (LEAVE A REPLY)

NEW QUESTION: 100
An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?
A. TCP 6514
B. UDP 1700
C. TCP 49
D. UDP 1812
Answer: B (LEAVE A REPLY)
Explanation
Explanation
CoA Messages are sent on two different udp ports depending on the platform. Cisco standardizes on UDP port 1700, while the actual RFC calls out using UDP port 3799.

NEW QUESTION: 101
A switch with Dynamic ARP Inspection enabled has received a spoofed ARP response on a trusted interface.
How does the switch behave in this situation?
A. It forwards the packet after validation by using the MAC Binding Table.
B. It drops the packet after validation by using the IP & MAC Binding Table.
C. It forwards the packet without validation.
D. It drops the packet without validation.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 102
Why should organizations migrate to an MFA strategy for authentication?
A. MFA does not require any piece of evidence for an authentication mechanism.
B. Biometrics authentication leads to the need for MFA due to its ability to be hacked easily.
C. MFA methods of authentication are never compromised.
D. Single methods of authentication can be compromised more easily than MFA.
Answer: D (LEAVE A REPLY)

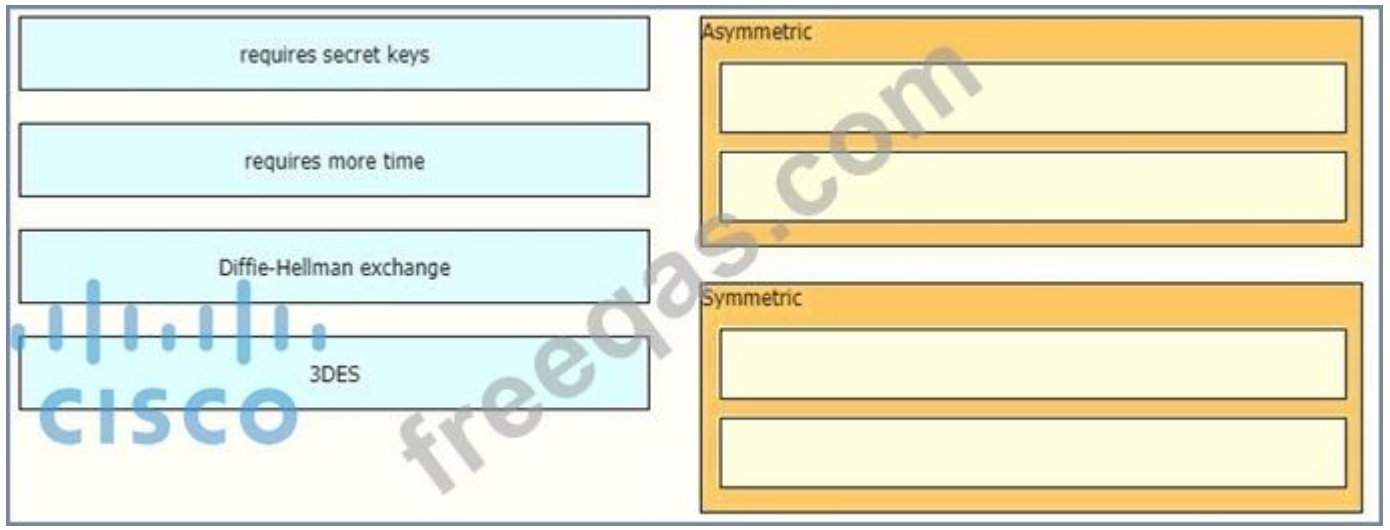
NEW QUESTION: 103

An organization is implementing URL blocking using Cisco Umbrella. 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: A (LEAVE A REPLY)
Reference: https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information

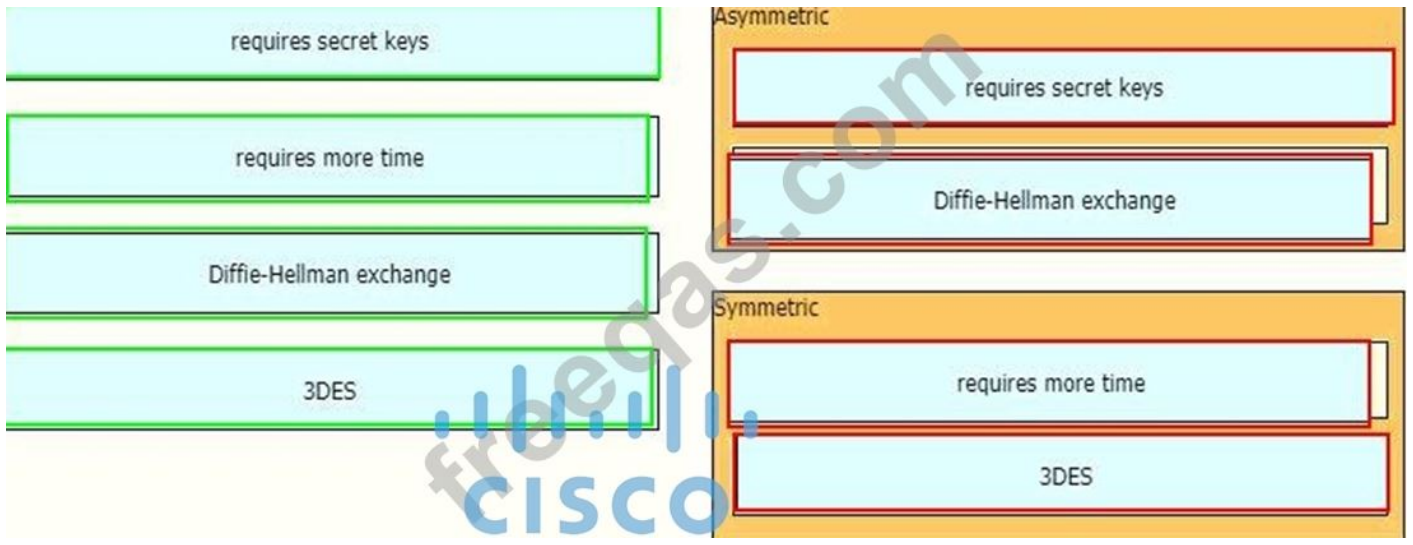
NEW QUESTION: 104
Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?
A. transparent
B. redirection
C. forward
D. proxy gateway
Answer: A (LEAVE A REPLY)
Reference:
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesign

NEW QUESTION: 105
An attacker needs to perform reconnaissance on a target system to help gain access to it. The system has weak passwords, no encryption on the VPN links, and software bugs on the system's applications. Which vulnerability allows the attacker to see the passwords being transmitted in clear text?
A. weak passwords for authentication
B. improper file security
C. software bugs on applications
D. unencrypted links for traffic
Answer: D (LEAVE A REPLY)
Explanation
https://www.cisco.com/ELearning/bulk/public/celc/CRS/media/targets/resources_mod07/7_3_5_improving_secu

NEW QUESTION: 106
Drag and drop the descriptions from the left onto the encryption algorithms on the right.



Answer:



NEW QUESTION: 107
Which technology provides the benefit of Layer 3 through Layer 7 innovative deep packet inspection, enabling the platform to identify and output various applications within the network traffic flows?
A. Cisco NBAR2
B. Account on Resolution
C. Cisco Prime Infrastructure
D. Cisco ASAV
Answer: (SHOW ANSWER)

NEW QUESTION: 108

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: B (LEAVE A REPLY)

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: 109

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

A. It allows the endpoint to authenticate with 802.1x or MAB.

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

C. It adds endpoints to identity groups dynamically.

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

Answer: D (LEAVE A REPLY)

Posture is a service in Cisco ISE that checks the compliance of endpoints with corporate security policies before allowing them to connect to the network. Posture policies define the requirements that endpoints must meet to be compliant, such as having antivirus software installed and updated, or having a specific registry key value. If an endpoint is compliant, Cisco ISE can apply a Change of Authorization (CoA) to grant it access to the network resources. CoA is a mechanism that allows Cisco ISE to dynamically change the authorization attributes of an existing session, such as VLAN, dACL, or SGT, without requiring the user to reauthenticate.

CoA can be triggered by various events, such as posture assessment results, profiling changes, or manual actions by the administrator. CoA can also be used to quarantine or disconnect non-compliant endpoints.

Therefore, ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE provides the benefit of allowing CoA to be applied if the endpoint status is compliant. References :=

* Cisco Identity Services Engine Administrator Guide, Release 2.2 - Configure Client Posture Policies
* Cisco Identity Services Engine Administrator Guide, Release 2.2 - Change of Authorization

NEW QUESTION: 110

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

A. TLSv1.2

B. TLSv1.1

C. BJTLSv1

D. DTLSv1

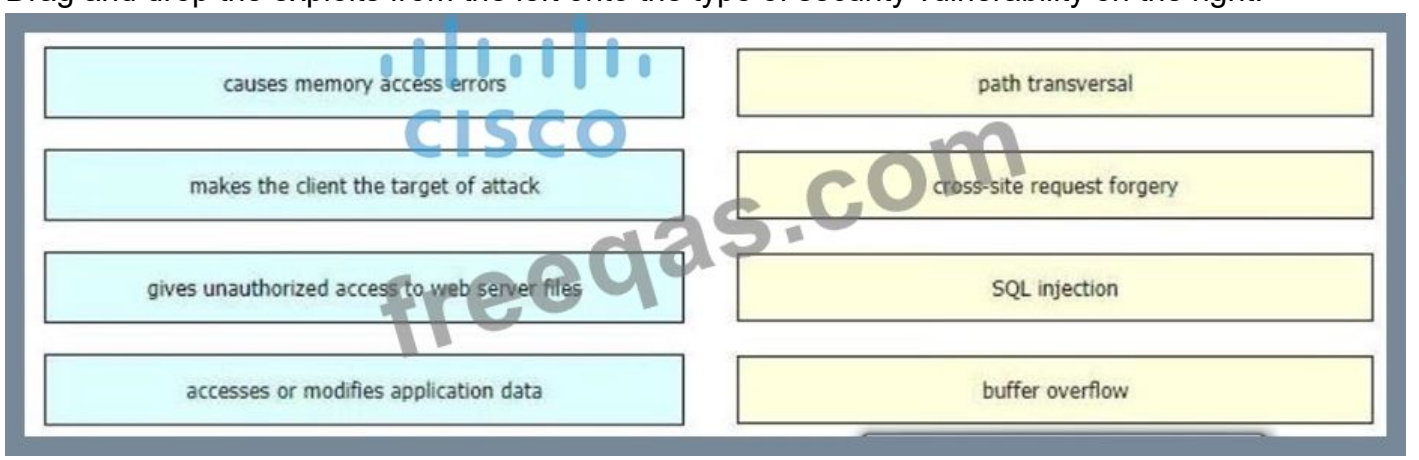
Answer: (SHOW ANSWER)
ExplanationDTLS is used for delay sensitive applications (voice and video) as its UDP based while TLS is TCP based.Therefore DTLS offers strongest throughput performance. The throughput of DTLS at the time of AnyConnect connection can be expected to have processing performance close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

NEW QUESTION: 111
A company has 5000 Windows users on its campus. Which two precautions should IT take to prevent WannaCry ransomware from spreading to all clients? (Choose two.)
A. Segment different departments to different IP blocks and enable Dynamic ARp inspection on all VLANs
B. Perform a posture check to allow only network access to (hose Windows devices that are already patched.
C. Put all company users in the trusted segment of NGFW and put all servers to the DMZ segment of the Cisco NGFW. ni
D. Ensure that noncompliant endpoints are segmented off to contain any potential damage.
E. Ensure that a user cannot enter the network of another department.
Answer: B,D (LEAVE A REPLY)

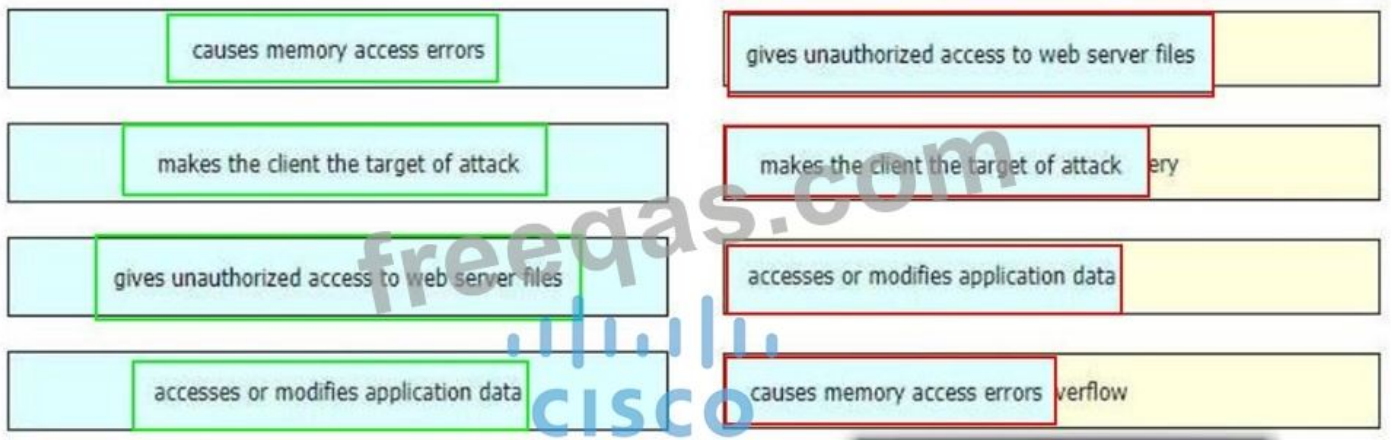
NEW QUESTION: 112
Refer to the exhibit. What is the function of the Python script code snippet for the Cisco ASA REST API?
A. changes the hostname of the Cisco ASA
B. adds a global rule into policies
C. deletes a global rule from policies
D. obtains the saved configuration of the Cisco ASA firewall
Answer: B (LEAVE A REPLY)

NEW QUESTION: 113
Refer to the exhibit. What does this Python script accomplish?
A. It authenticates to a Cisco ISE with an SSH connection.
B. It authenticates to a Cisco ISE server using the username of ersad
C. It allows authentication with TLSv1 SSL protocol
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
Drag and drop the exploits from the left onto the type of security vulnerability on the right.

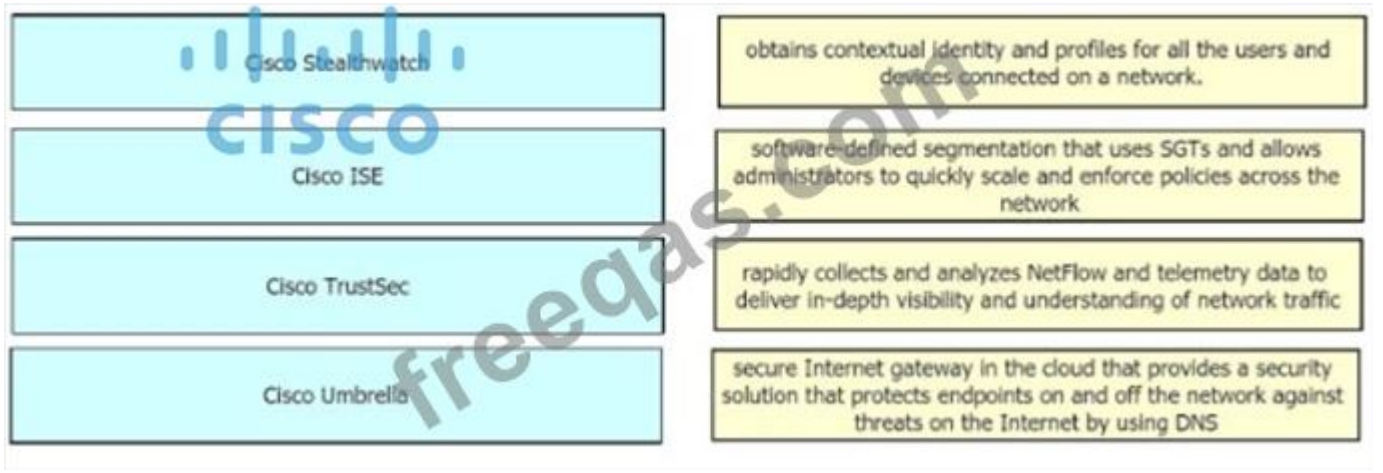


Answer:



NEW QUESTION: 115

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



Answer:

NEW QUESTION: 116

What are the two most commonly used authentication factors in multifactor authentication? (Choose two.)

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

A. encryption factor

B. confidentiality factor
C. time factor
D. biometric factor
E. knowledge factor
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 117
An organization deploys multiple Cisco FTD appliances and wants to manage them using one centralized solution The organization does not have a local VM but does have existing Cisco ASAs that must migrate over to Cisco FTDs Which solution meets the needs of the organization?
A. Cisco FMC
B. Cisco FDM
C. CSM
D. CDO
Answer: C (LEAVE A REPLY)

NEW QUESTION: 118
Which two conditions are prerequisites for stateful failover for IPsec? (Choose two)
A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically
B. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.
C. The IPsec configuration that is set up on the active device must be duplicated on the standby device
D. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically.
E. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device
Answer: (SHOW ANSWER)
ExplanationStateful failover for IP Security (IPsec) enables a router to continue processing and forwarding IPsec packetsafter a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automaticallytakes over the tasks of the active (primary) router if the active router loses connectivity for any reason. Thisfailover process is transparent to users and does not require adjustment or reconfiguration of any remote peer.Stateful failover for IPsec requires that your network contains two identical routers that are available to be eitherthe primary or secondary device. Both routers should be the same type of device, have the same CPU andmemory, and have either no encryption accelerator or identical encryption accelerators.Prerequisites for Stateful Failover for IPsec Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpnavailability-15- the prerequisites only stated that "Both routers should be the same type of device" but in the"Restrictions for Stateful Failover for IPsec" section of the link above, it requires "Both the active and standby devices must run the identical version of the Cisco IOS software" so answer E is better than answer B.

NEW QUESTION: 119
Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)
A. Cisco ISE
B. Cisco DNA Center
C. Cisco Umbrella

D. Cisco Duo Security
E. Cisco TrustSec
Answer: (SHOW ANSWER)

NEW QUESTION: 120
What is a benefit of using Cisco FMC over Cisco ASDM?
A. Cisco FMC uses Java while Cisco ASDM uses HTML5.
B. Cisco FMC provides centralized management while Cisco ASDM does not.
C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.
D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices
Answer: B (LEAVE A REPLY)
Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system "You cannot use an FMC to manage ASA firewall functions." Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management. Reference: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheetc78-736775.html the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Reference:
Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system
"You cannot use an FMC to manage ASA firewall functions."
The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management.
Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system "You cannot use an FMC to manage ASA firewall functions." Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management. Reference: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheetc78-736775.html

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

NEW QUESTION: 122
What must be used to share data between multiple security products?
A. Cisco Rapid Threat Containment
B. Cisco Platform Exchange Grid
C. Cisco Advanced Malware Protection
D. Cisco Stealthwatch Cloud
Answer: B (LEAVE A REPLY)
To share data between multiple security products, you must use Cisco Platform Exchange Grid (pxGrid).
pxGrid is an open and scalable framework that allows for bi-directional any-to-any partner platform integrations. pxGrid uses REST and WebSocket interfaces to exchange intelligence and obtain contextual information from Cisco Identity Services Engine (ISE) and other security products. pxGrid can also direct ISE to contain threats by setting network policies. pxGrid enables cross-platform network system collaboration across your IT infrastructure and helps you monitor security, detect threats, and manage assets, configuration, identity, and access.
References: Introduction to the Cisco Platform Exchange Grid (pxGrid) in ISE, Cisco Identity Services Engine Administrator Guide, Release 3.3

NEW QUESTION: 123
Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?
A. cloud web services
B. network AMP
C. private cloud
D. public cloud
Answer: C (LEAVE A REPLY)
Cisco Advanced Malware Protection (AMP) for Endpoints is a cloud-based solution that provides endpoint protection against malware and advanced threats. It can be deployed in different architectures depending on the customer's needs and preferences. One of the deployment options is the private cloud, which is designed to keep data within a network perimeter. In this option, the customer hosts the AMP for Endpoints console and the AMP cloud on their own infrastructure, and the endpoints connect to the private cloud for analysis and policy enforcement. This option provides more control and privacy over the data, but also requires more resources and maintenance from the customer. The other deployment options are the public cloud, which uses the Cisco-hosted AMP cloud and console, and the hybrid cloud, which uses a combination of the public and private clouds123 References: 1: Protecting Against Malware Threats with Cisco AMP for Endpoints (SSFAMP) course overview 2: Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco 3: Cisco Advanced Malware Protection for Endpoints - Zones

NEW QUESTION: 124

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

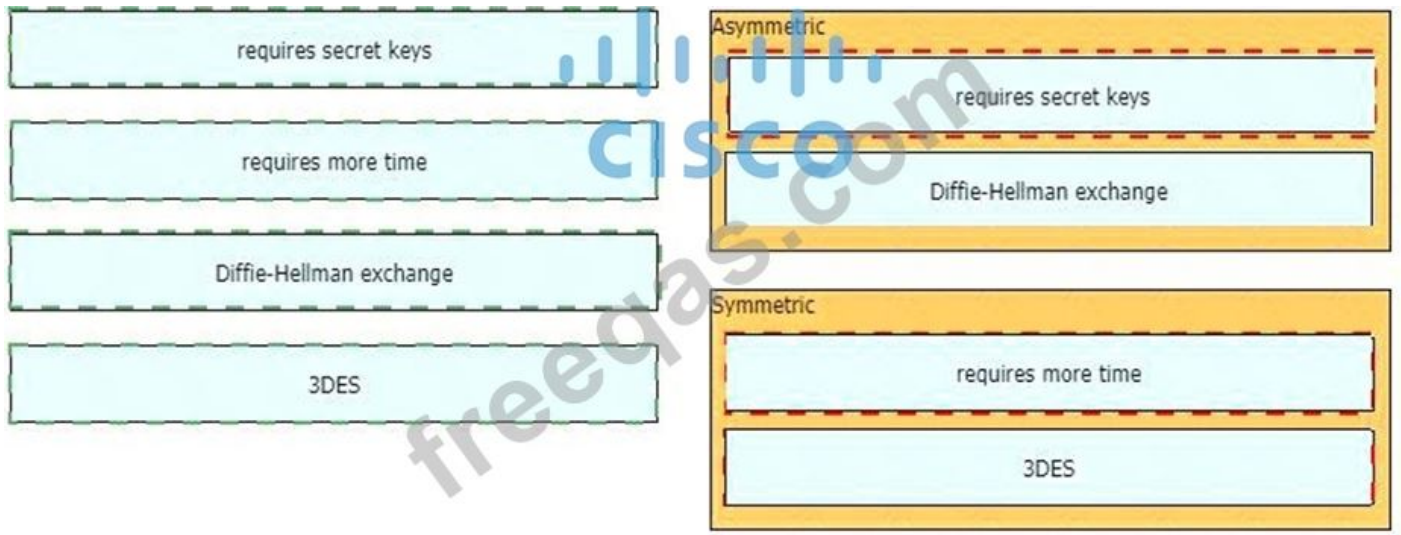
A. weak passwords for authentication
B. improper file security
C. software bugs on applications
D. unencrypted links for traffic
Answer: D (LEAVE A REPLY)
https://www.cisco.com/ELearning/bulk/public/celc/CRS/media/targets/resources_mod07/7_3_5_improving_security.pdf

NEW QUESTION: 125
In a PaaS model, which layer is the tenant responsible for maintaining and patching?

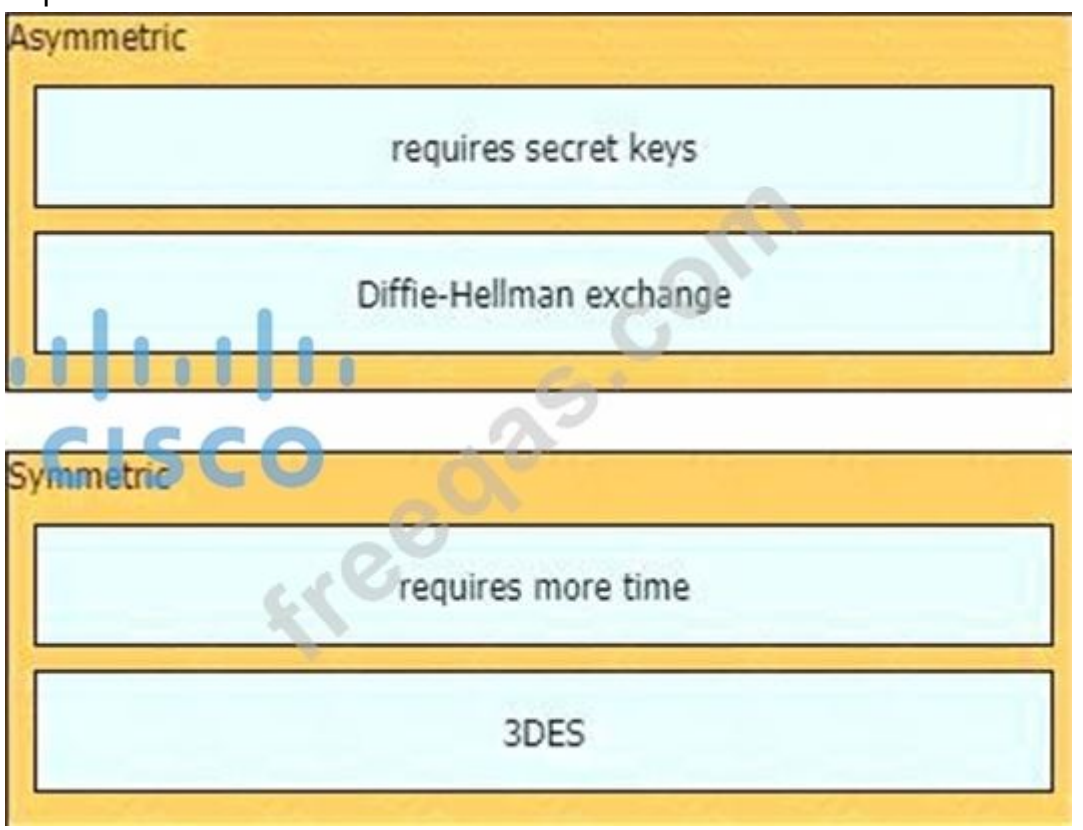
A. hypervisor
B. virtual machine
C. network
D. application
Answer: D (LEAVE A REPLY)
Explanation
Explanation/Reference: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

NEW QUESTION: 126
Drag and drop the descriptions from the left onto the encryption algorithms on the right.

Answer:



Explanation:



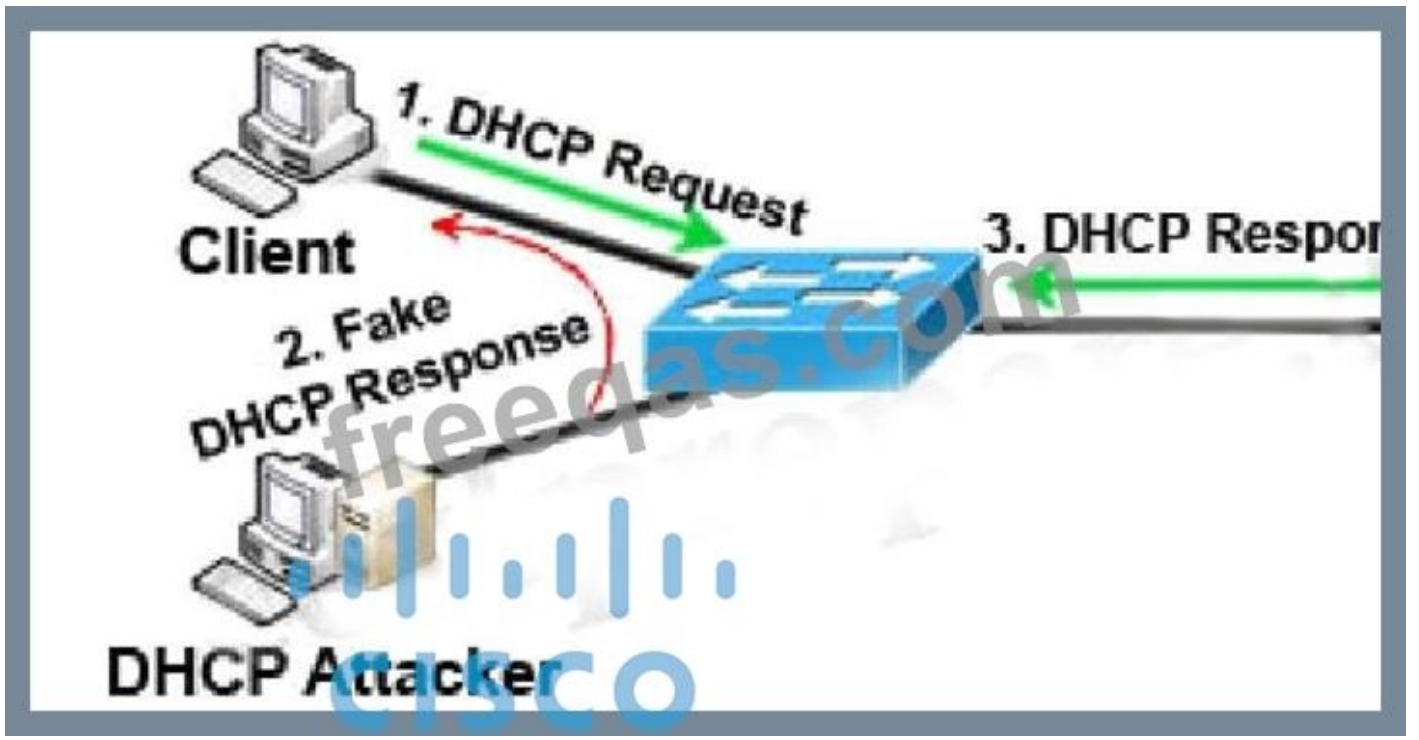
ExplanationSymmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetric encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.Asymmetric encryption takes relatively more time than the symmetric encryption.Diffie Hellman algorithm is an asymmetric algorithm used to establish a shared secret for a symmetric keyalgorithm. Nowadays most of the people uses hybrid crypto system i.e, combination of symmetric andasymmetric encryption. Asymmetric Encryption is used as a technique in key exchange mechanism to share secret key and after the key is shared between sender and receiver, the communication will take place using symmetric encryption. The shared secret key will be used to encrypt the communication.Triple DES (3DES), a symmetric-key algorithm for the encryption of electronic data, is the successor of DES (Data Encryption Standard) and provides more secure encryption then DES.Note: Although
"requires secret keys" option in this question is a bit unclear but it can only be assigned toSymmetric algorithm.

NEW QUESTION: 127
What is the purpose of the Trusted Automated exchange cyber threat intelligence industry standard?

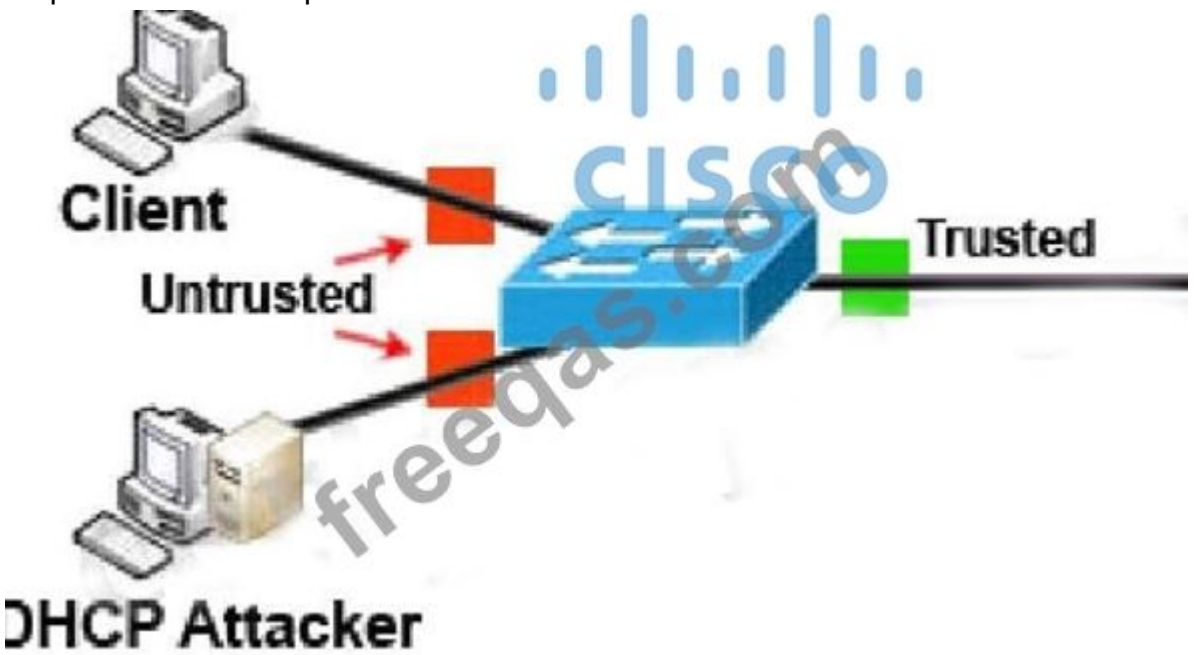
A. public collection of threat intelligence feeds
B. threat intelligence sharing organization
C. language used to represent security information
D. service used to exchange security information
Answer: D (LEAVE A REPLY)
Trusted Automated eXchange of Intelligence Information (TAXII) is a collection of services and message exchanges that enable the sharing of cyber threat intelligence across product, service, and organizational boundaries. It is designed to support the exchange of CTI represented in STIX, but is not limited to STIX.
TAXII defines an API that aligns with common sharing models, such as hub-and-spoke, peer-to-peer, and subscribe/publish. TAXII is not a public collection of threat intelligence feeds, a threat intelligence sharing organization, or a language used to represent security information. Those are possible descriptions of STIX, which is a complementary standard to TAXII. References: STIX and TAXII Approved as OASIS Standards to Enable Automated Exchange of Cyber Threat Intelligence, STIX V2.1 and TAXII V2.1 OASIS Standards are published, What is STIX/TAXII? | Cloudflare, What is STIX / TAXII? Learn about the industry standards for Cyber ..., What are STIX/TAXII Standards I Resources I Anomali

NEW QUESTION: 128
What is the most common type of data exfiltration that organizations currently experience?
A. HTTPS file upload site
B. Microsoft Windows network shares
C. SQL database injections
D. encrypted SMTP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 129
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: 130
Refer to the exhibit.

An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained. Which command should be configured on the switch interface in order to provide the user with network connectivity?

A. ip dhcp snooping verify mac-address

B. ip dhcp snooping limit 41

C. ip dhcp snooping vlan 41

D. ip dhcp snooping trust

Answer: D (LEAVE A REPLY)

Explanation

Explanation

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: 131

What is an attribute of the DevSecOps process?

A. isolated security team

B. security scanning and theoretical vulnerabilities

C. development security

D. mandated security controls and check lists

Answer: C (LEAVE A REPLY)

NEW QUESTION: 132

An engineer adds a custom detection policy to a Cisco AMP deployment and encounters issues with the configuration The simple detection mechanism is configured, but the dashboard indicates that the hash is not 64 characters and is non-zero What is the issue?

A. The file being uploaded is incompatible with simple detections and must use advanced detections

B. The engineer is attempting to upload a file instead of a hash
C. The hash being uploaded is part of a set in an incorrect format
D. The engineer is attempting to upload a hash created using MD5 instead of SHA-256
Answer: D (LEAVE A REPLY)

NEW QUESTION: 133
An engineer is configuring AMP for endpoints and wants to block certain files from executing.
Which outbreak control method is used to accomplish this task?
A. device flow correlation
B. advanced custom detections
C. application blocking list
D. simple detections
Answer: C (LEAVE A REPLY)

NEW QUESTION: 134
An engineer recently completed the system setup on a Cisco WSA Which URL information does the system send to SensorBase Network servers?
A. Summarized server-name information and MD5-hashed path information
B. complete URL,without obfuscating the path segments
C. URL information collected from clients that connect to the Cisco WSA using Cisco AnyConnect
D. none because SensorBase Network Participation is disabled by default
Answer: A (LEAVE A REPLY)
The Cisco WSA can participate in the Cisco SensorBase Network, which is a threat management database that collects and shares data from Cisco security products. By participating in the SensorBase Network, the WSA can receive web reputation scores and URL categories for the requested web content, and also contribute data to improve the accuracy and efficacy of the service. The data that the WSA sends to the SensorBase Network servers includes information about request attributes and how the appliance handles requests. However, to protect the privacy and confidentiality of the users and the organization, the WSA does not send the complete URL, but only the summarized server-name information and the MD5-hashed path information. The MD5 hash is a one-way encryption algorithm that converts the path information into a fixed-length string that cannot be reversed. This way, the SensorBase Network can identify the URL without revealing the actual content or parameters of the request. The WSA also does not send any personal or confidential information such as usernames and passwords, or any information about HTTPS transactions, except for the IP address, web reputation score, and URL category of the server name in the certificate. The SensorBase Network Participation is enabled by default, but it can be disabled by the administrator if desired123. References: 3:
Web Base Network Participation (WBNP) and Sender Base Network Participation (SBNP) - Cisco 2: User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance - GD (General Deployment) - Introduction 1: User Guide for AsyncOS 12.0 for Cisco Web Security Appliances - GD (General Deployment) - Introduction

NEW QUESTION: 135
An engineer is implementing NTP authentication within their network and has configured both the client and server devices with the command ntp authentication-key 1 md5 Cisc392368270. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however it is unable to do so. Which command is required to enable the client to accept the server's authentication key?

A. ntp peer 1.1.1.1 key 1
B. ntp server 1.1.1.1 key 1
C. ntp server 1.1.1.2 key 1
D. ntp peer 1.1.1.2 key 1
Answer: B (LEAVE A REPLY)
Explanation
To configure an NTP enabled router to require authentication when other devices connect to it, use the following commands:
NTP_Server(config)#ntp authentication-key 2 md5 securitytut
NTP_Server(config)#ntp authenticate
NTP_Server(config)#ntp trusted-key 2
Then you must configure the same authentication-key on the client router:
NTP_Client(config)#ntp authentication-key 2 md5 securitytut
NTP_Client(config)#ntp authenticate
NTP_Client(config)#ntp trusted-key 2
NTP_Client(config)#ntp server 10.10.10.1 key 2
Note: To configure a Cisco device as a NTP client, use the command ntp server <IP address>. For example:
Router(config)#ntp server 10.10.10.1. This command will instruct the router to query 10.10.10.1 for the time.

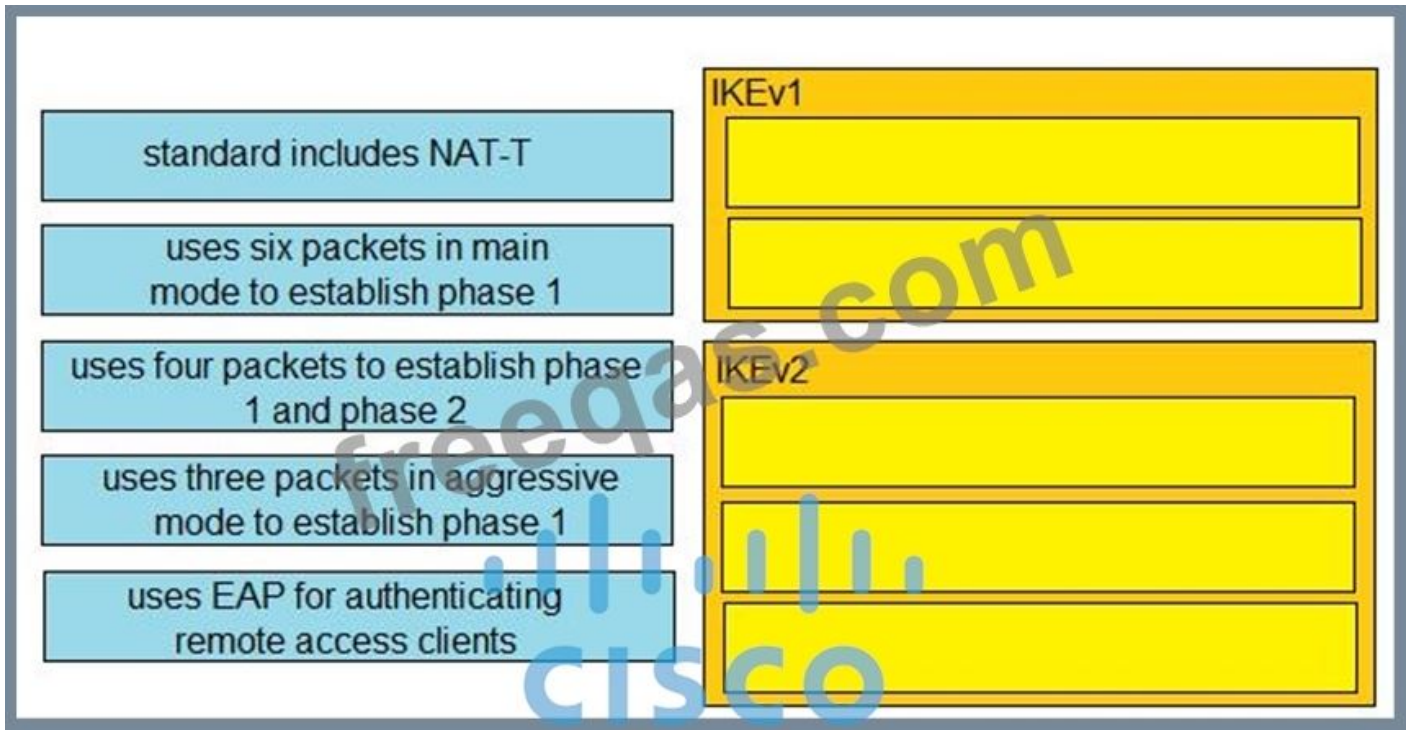
NEW QUESTION: 136
Which component of Cisco umbrella architecture increases reliability of the service?
A. Anycast IP
B. AMP Threat grid
C. Cisco Talos
D. BGP route reflector
Answer: A (LEAVE A REPLY)
Anycast IP is a component of Cisco umbrella architecture that increases reliability of the service by allowing the same IP address to exist on multiple servers around the world. This way, the user's request is automatically routed to the nearest and fastest data center, and failover is seamless in case of an outage. Anycast IP also reduces latency and improves performance by using BGP to select the shortest path to the destination12. References := 1: Why Cisco Umbrella uses anycast routing - Cisco Umbrella 2: Cisco Umbrella At a Glance

NEW QUESTION: 137
What is the purpose of a NetFlow version 9 template record?
A. It serves as a unique identification number to distinguish individual data records
B. It specifies the data format of NetFlow processes.

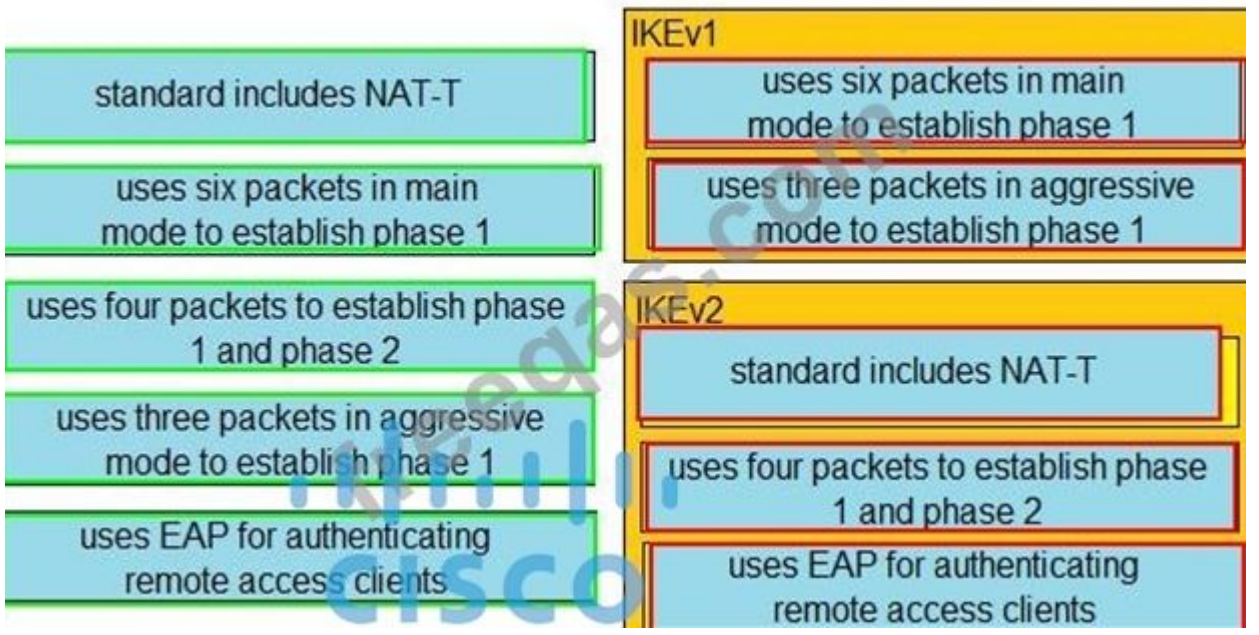
C. It defines the format of data records.
D. It provides a standardized set of information about an IP flow.
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Which Cisco security solution gives the most complete view of the relationships and evolution of Internet domains IPs, and flies, and helps to pinpoint attackers' infrastructures and predict future threat?
A. Cisco Secure Network Analytics
B. Cisco Secure Cloud Analytics
C. Cisco Umbrella Investigate
D. Cisco pxGrid
Answer: C (LEAVE A REPLY)
Cisco Umbrella Investigate is a cloud-based service that provides interactive threat intelligence on domains, IPs, and files. It helps security analysts to uncover the attacker's infrastructure and predict future threats by analyzing the relationships and evolution of internet domains, IPs, and files. It also integrates with other Cisco security solutions, such as Cisco Secure Network Analytics, Cisco Secure Cloud Analytics, and Cisco pxGrid, to provide a holistic view of the network and cloud security posture. Cisco Umbrella Investigate is based on the data collected by Cisco Umbrella, which processes more than 620 billion DNS requests per day from over
190 countries. Cisco Umbrella Investigate uses statistical and machine learning models to automatically score and classify the data, and provides a risk score for each domain, IP, and file, along with the contributing factors and historical context. Cisco Umbrella Investigate also allows security analysts to query the data using a web-based console or an API, and to visualize the results using graphs, tables, and maps. Cisco Umbrella Investigate is the most complete and interactive threat intelligence solution that helps to prevent cyber attacks before they happen. References := Some possible references are:
* Cisco Umbrella Investigate
* Cyber Attack Prevention - Cisco Umbrella
* Cisco Umbrella Investigate - Cisco Umbrella

NEW QUESTION: 139
Drag and drop the descriptions from the left onto the correct protocol versions on the right.



Answer:



NEW QUESTION: 140

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

A. NetFlow

B. Packet Tracer

C. Network Discovery

D. Access Control

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 141
Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?
A. file access from a different user
B. interesting file access
C. user login suspicious behavior
D. privilege escalation
Answer: C (LEAVE A REPLY)
Explanation Explanation The various suspicious patterns for which the Cisco Tetration platform looks in the current release are: + Shell code execution: Looks for the patterns used by shell code. + Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree. + Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these, it can detect Meltdown, Spectre, and other cache-timing attacks. + Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping). + User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods. + Interesting file access: Cisco Tetration platform can be armed to look at sensitive files. + File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user. + Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html Explanation The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:
+ Shell code execution: Looks for the patterns used by shell code.
+ Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.
+ Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts.
Using these, it can detect Meltdown, Spectre, and other cache-timing attacks.
+ Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping).
+ User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods.
+ Interesting file access: Cisco Tetration platform can be armed to look at sensitive files.
+ File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user.
+ Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time.
Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform.
Explanation Explanation The various suspicious patterns for which the Cisco Tetration platform looks in the current release are: + Shell code execution: Looks for the patterns used by shell code. + Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree. + Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these, it can detect Meltdown, Spectre, and other cache-timing attacks. + Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping). + User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods. + Interesting file access: Cisco Tetration platform can be armed to look at sensitive files. + File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user. + Unseen command: Cisco Tetration platform learns the

behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html

NEW QUESTION: 142
An engineer must modify an existing remote access VPN using a Cisco AnyConnect Secure Mobility client solution and a Cisco Secure Firewall. Currently, all the traffic generate by the user Is sent to the VPN tunnel and the engineer must now exclude some servers and access them directly instead. Which element must be modified to achieve this goat?
A. NAT exemption
B. encryption domain
C. routing table
D. group policy
Answer: D (LEAVE A REPLY)
To achieve the goal of excluding some servers from the VPN tunnel and accessing them directly, the engineer must modify the group policy that is applied to the remote access VPN users. The group policy contains the settings for split tunneling, which is a feature that allows the VPN client to route some traffic through the VPN tunnel and some traffic directly to the internet. Split tunneling can be configured based on the destination IP address, the application, or the domain name of the traffic. By modifying the group policy, the engineer can specify which servers or networks should be excluded from the VPN tunnel and accessed directly by the VPN client. This can improve the performance and efficiency of the VPN connection, as well as reduce the load on the VPN gateway and the corporate network. However, split tunneling also introduces some security risks, such as exposing the VPN client to internet threats, bypassing the corporate firewall and security policies, and leaking sensitive data. Therefore, the engineer must carefully evaluate the trade-offs and best practices of using split tunneling for remote access VPNs. References :=
* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Secure Connectivity, Lesson 3.1: Implementing and Troubleshooting Remote Access VPN, Topic 3.1.4:
Configure and Verify Remote Access VPN, Subtopic 3.1.4.2: Configure and Verify Split Tunneling
* VPN Split Tunneling: What It Is & Pros and Cons
* Cisco ASA - Enable Split Tunnel for Remote VPN Clients

NEW QUESTION: 143
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 The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across your organization that Advanced Malware Protection (AMP) sees Reference: 2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1 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 2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1

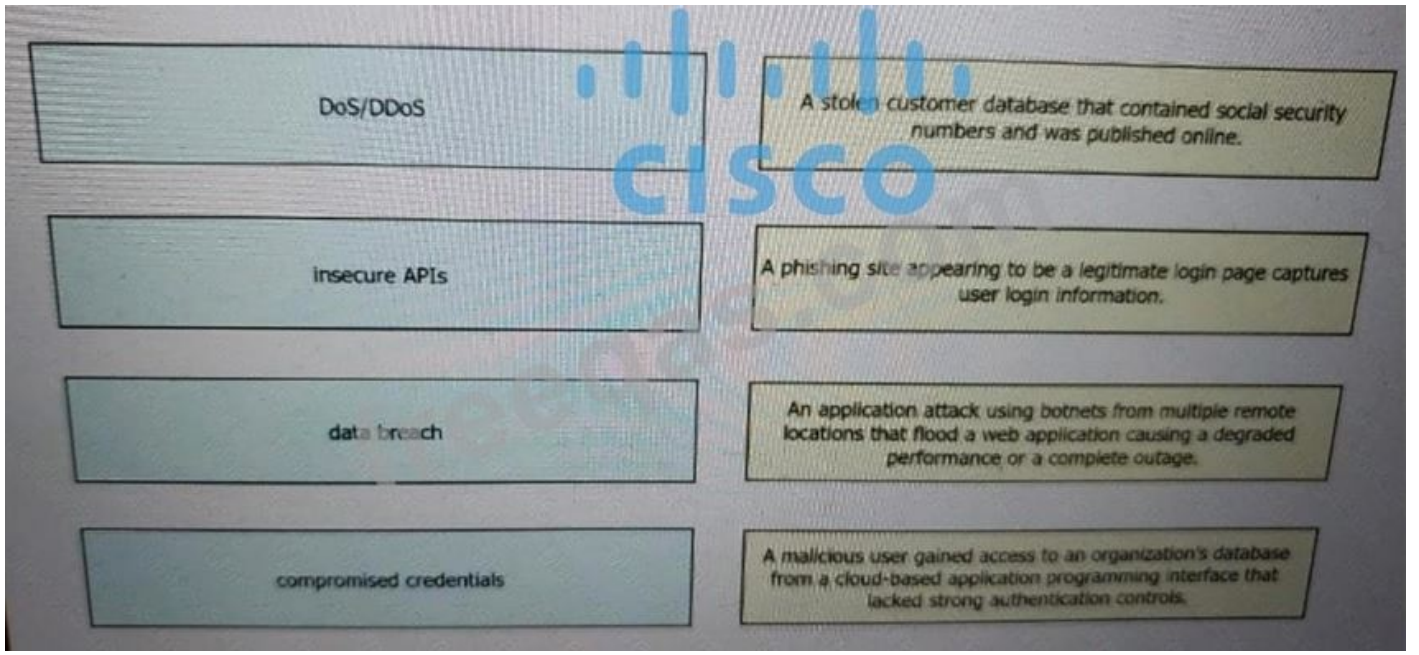
NEW QUESTION: 144
An engineer wants to automatically assign endpoints that have a specific OUI into a new endpoint group. Which probe must be enabled for this type of profiling to work?
A. NMAP
B. NetFlow
C. DHCP
D. SNMP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 145
Which two deployment modes does the Cisco ASA FirePower module support? (Choose two)
A. transparent mode
B. routed mode
C. inline mode
D. active mode
E. passive monitor-only mode
Answer: C,D (LEAVE A REPLY)
You can configure your ASA FirePOWER module using one of the following deployment models: You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/firewall/asa-firewall-asdm/ modules-sfr.html You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment.
Reference:
You can configure your ASA FirePOWER module using one of the following deployment models: You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/firewall/asa-firewall-asdm/ modules-sfr.html

NEW QUESTION: 146
On which part of the IT environment does DevSecOps focus?
A. wireless network

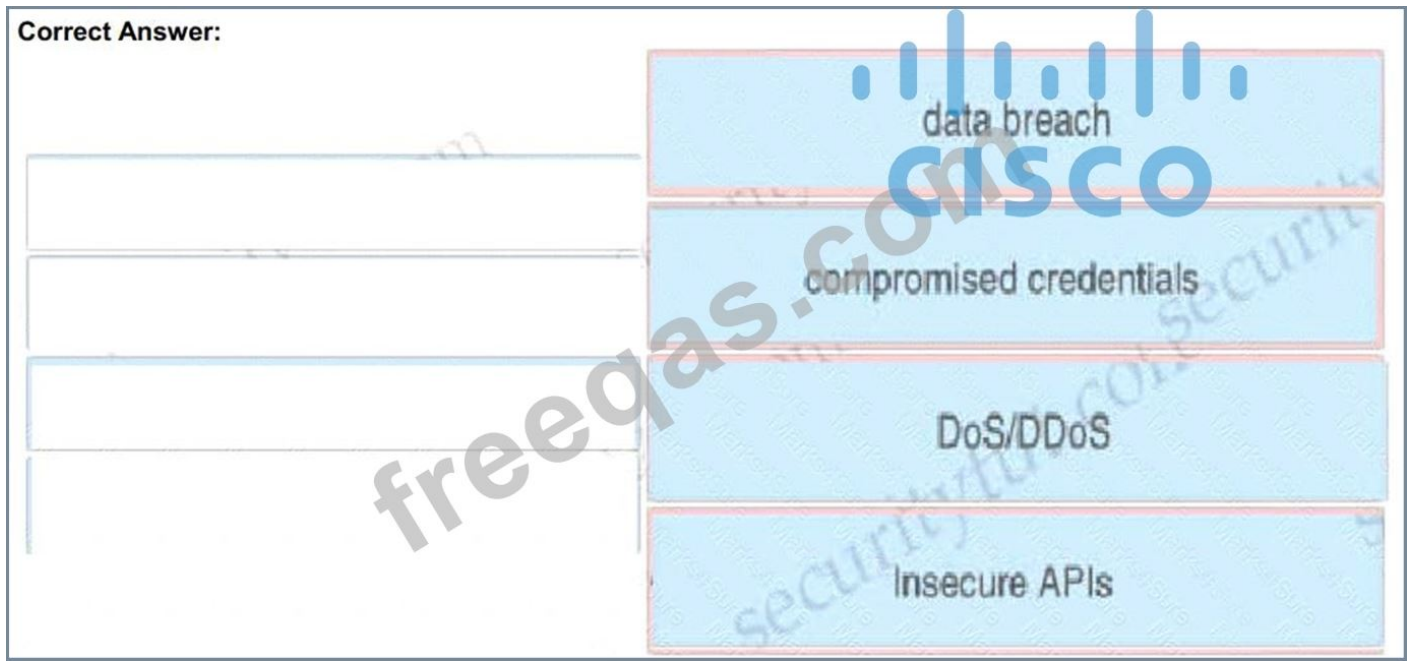
B. data center
C. application development
D. perimeter network
Answer: C (LEAVE A REPLY)

NEW QUESTION: 147
Drag and drop the threats from the left onto examples of that threat on the right



Answer:

Explanation:



ExplanationA data breach is the intentional or unintentional release of secure or private/confidential information to anuntrusted environment.When your credentials have been compromised, it means someone other than you may be in possession of your account information, such as your username and/or password.

NEW QUESTION: 148

Which attribute has the ability to change during the RADIUS CoA?

A. NTP

B. Authorization

C. Accessibility

D. Membership

Answer: B (LEAVE A REPLY)

Explanation The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15- sy-book/sec-rad-coa.html The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. Reference:

Explanation The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15- sy-book/sec-rad-coa.html

NEW QUESTION: 149

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

A. Configure the Cisco ESA to drop the malicious emails.

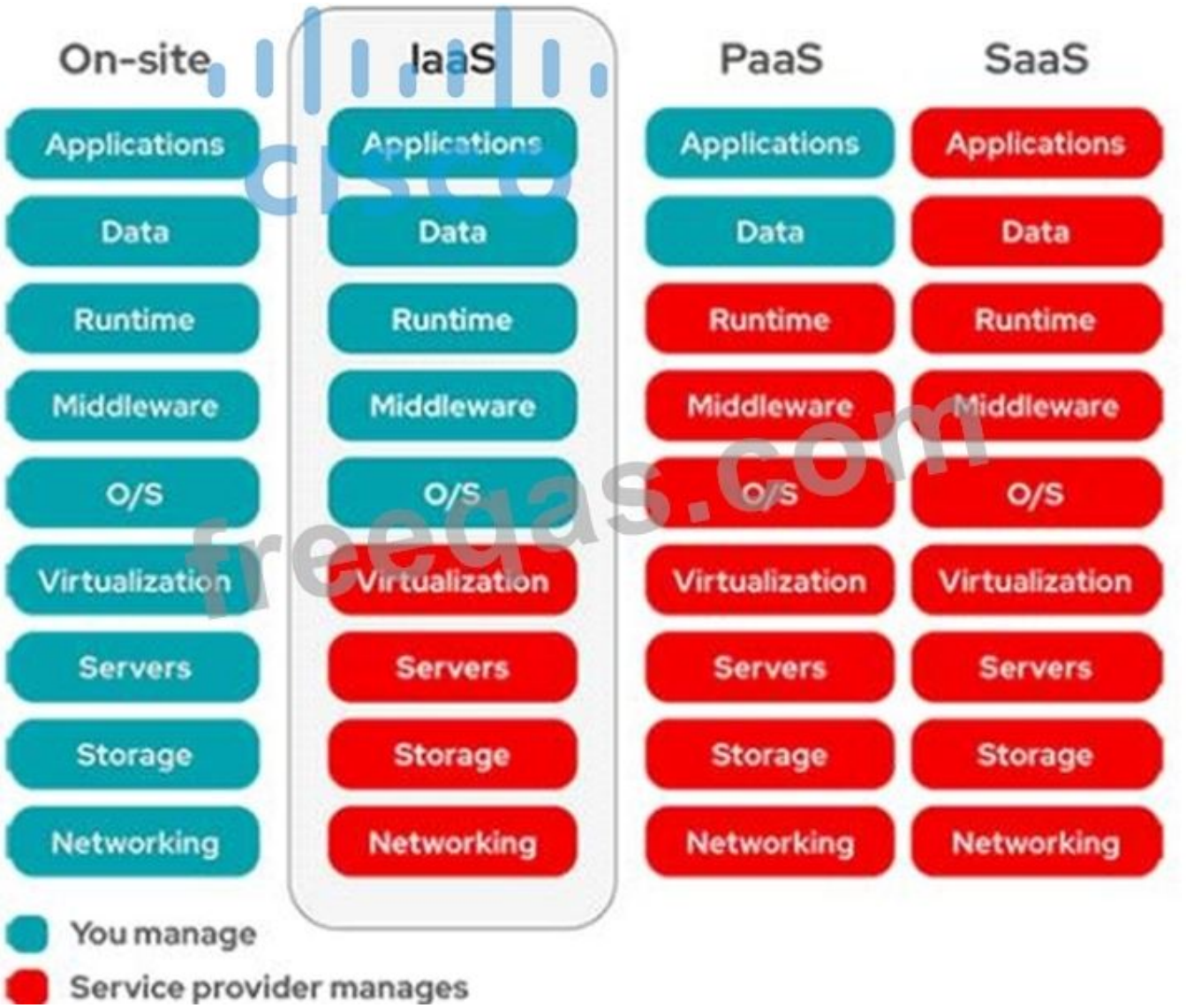
B. Configure policies to quarantine malicious emails.

C. Configure policies to stop and reject communication

D. Configure the Cisco ESA to reset the TCP connection.

Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118219-configure-esa-00.html

NEW QUESTION: 150
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)
Explanation
Explanation
Customers must manage applications and data in PaaS.



NEW QUESTION: 151
Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two)

A. DDoS
B. antispam
C. antivirus
D. encryption
E. DLP
Answer: (SHOW ANSWER)
Cisco Hybrid Email Security is a unique service offering that combines a cloud-based email security deployment with an appliance-based email security deployment (on premises) to provide maximum choice and control for your organization. The cloud-based infrastructure is typically used for inbound email cleansing, while the onpremises appliances provide granular control - protecting sensitive information with data loss prevention (DLP) and encryption technologies.
Reference:
Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

NEW QUESTION: 152
Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application traffic?
A. Cisco Security Intelligence
B. Cisco Application Visibility and Control
C. Cisco Model Driven Telemetry
D. Cisco DNA Center
Answer: (SHOW ANSWER)
The Cisco Application Visibility and Control (AVC) solution leverages multiple technologies to recognize, analyze, and control over 1000 applications, including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. AVC combines several Cisco IOS/IOS XE components, as well as communicating with external tools, to integrate the following functions into a powerful solution...
Reference:
avc_tech_overview.html

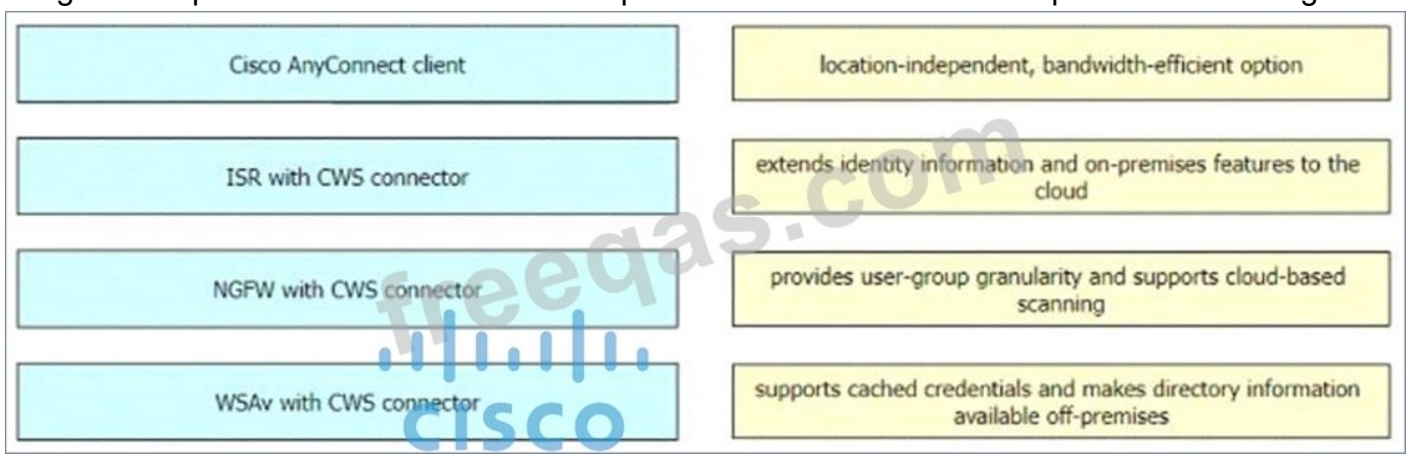
NEW QUESTION: 153
An organization wants to secure data in a cloud environment Its security model requires that all users be authenticated and authorized Security configuration and posture must be continuously validated before access is granted or maintained to applications and data There is also a need to allow certain application traffic and deny all other traffic by default Which technology must be used to implement these requirements?
A. microsegmentation
B. access control policy

C. virtual LAN
D. virtual routing and forwarding
Answer: B (LEAVE A REPLY)

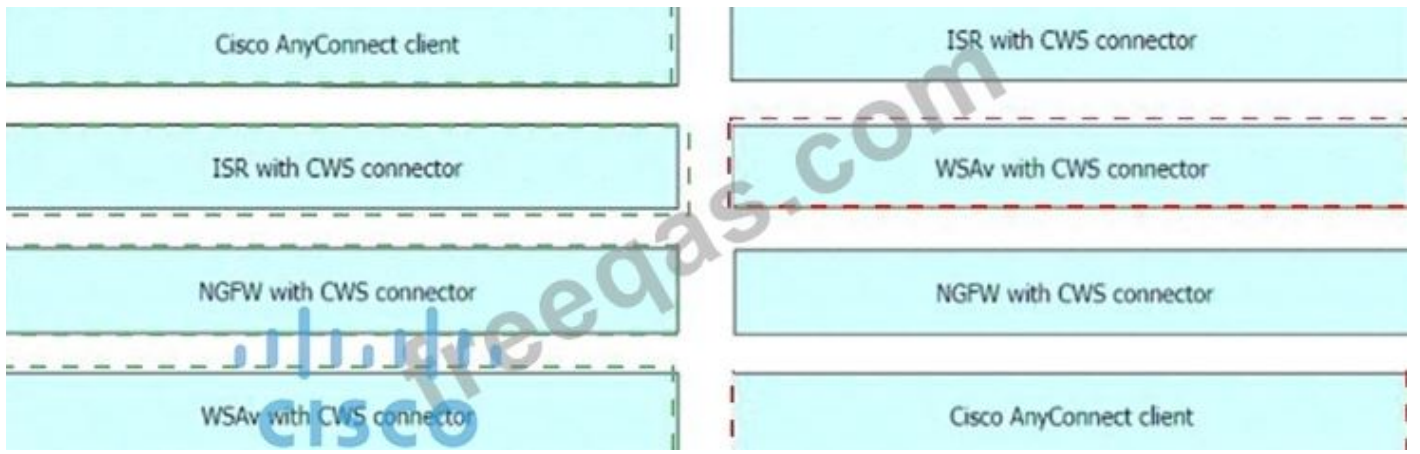
NEW QUESTION: 154
Which algorithm is an NGE hash function?
A. MD5
B. SHA-2
C. HMAC
D. SHA-1
Answer: (SHOW ANSWER)

NEW QUESTION: 155
What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?
A. trusted automated exchange
B. Indicators of Compromise
C. The Exploit Database
D. threat intelligence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 156
Drag and drop the Cisco CWS redirection options from the left onto the capabilities on the right.



Answer:



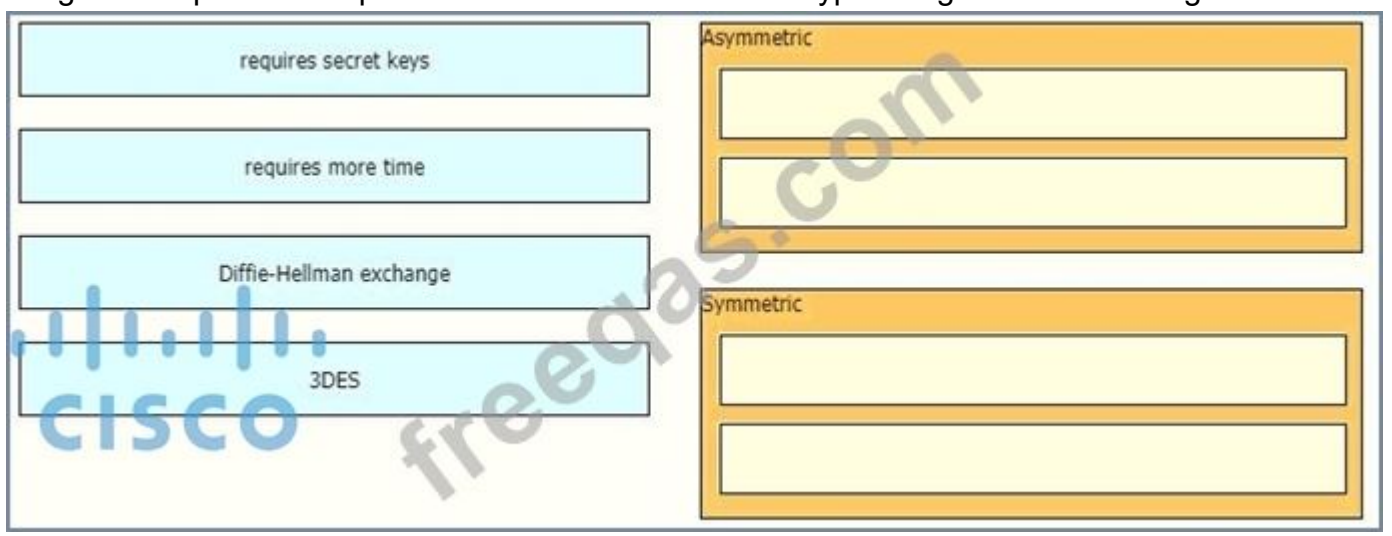
Explanation:

Reference:

https://www.westconcomstor.com/medias/CWS-data-sheet-c78-729637-1-.pdf?context=bWFzdGVyfHJvb3R8M

NEW QUESTION: 157

Drag and drop the descriptions from the left onto the encryption algorithms on the right.



Answer:

NEW QUESTION: 158
An MDM provides which two advantages to an organization with regards to device management? (Choose two)
A. asset inventory management
B. allowed application management
C. Active Directory group policy management
D. network device management
E. critical device management
Answer: A,B (LEAVE A REPLY)
Mobile Device Management (MDM) is a solution that allows an organization to manage, monitor, and secure mobile devices such as smartphones, tablets, and laptops. MDM provides two main advantages to an organization with regards to device management:
* Asset inventory management: MDM helps an organization keep track of all the mobile devices that are connected to its network, including their location, status, configuration, and usage. MDM also enables an organization to remotely wipe or lock devices that are lost, stolen, or compromised, preventing data loss and unauthorized access. Asset inventory management helps an organization optimize its resources, reduce costs, and comply with regulations12.
* Allowed application management: MDM allows an organization to control what applications can be installed and run on the mobile devices, as well as how they can access and share data. MDM can also push updates and patches to the devices, ensuring that they are always running the latest and most secure
* versions of the applications. Allowed application management helps an organization enhance security, productivity, and performance of the mobile devices34.
References: 1: 7 Advantages and Disadvantages of Mobile Device Management [2024] 2: 5 Benefits of Mobile Device Management - ESET 3: Top 10 Benefits of Mobile Device Management (MDM) - TechFunnel 4: Benefits of Mobile Device Management (MDM) for Businesses

NEW QUESTION: 159
In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?
A. LDAP injection
B. man-in-the-middle
C. cross-site scripting
D. insecure API
Answer: B (LEAVE A REPLY)

In a man-in-the-middle (MITM) attack, the attacker inserts their machine between two hosts that are communicating with each other, and secretly relays and possibly alters the messages between them. The attacker can intercept, modify, or spoof the data, and the hosts are unaware that their communication is compromised. A MITM attack can target any communication channel that uses weak or no encryption, such as email, web, or wireless networks. A MITM attack can break the confidentiality, integrity, and authenticity of the communication, and can have various goals, such as eavesdropping, stealing credentials, impersonating a legitimate party, or redirecting traffic. A MITM attack can be prevented by using strong encryption protocols, such as TLS, IPSec, or SSH, and verifying the identity of the communication endpoints using certificates or other means. References: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Man-in-the-middle attack - Wikipedia, Man-in-the-Middle Attack: Types and Examples - Fortinet

NEW QUESTION: 160
A network administrator is using the Cisco ESA with AMP to upload files to the cloud for analysis. The network is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?
A. AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.
B. The file is queued for upload when connectivity is restored.
C. The file upload is abandoned.
D. The ESA immediately makes another attempt to upload the file.
Answer: D (LEAVE A REPLY)
Explanation

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html

NEW QUESTION: 161
Which threat involves software being used to gain unauthorized access to a computer system?
A. virus
B. NTP amplification
C. ping of death
D. HTTP flood
Answer: (SHOW ANSWER)
A virus is a type of malware that infects a computer system by attaching itself to another program or file. Once executed, the virus can replicate itself and spread to other files or systems. A virus can be used to gain unauthorized access to a computer system by exploiting software vulnerabilities, stealing credentials, or installing backdoors. A virus can also cause damage to the system by deleting, modifying, or encrypting data, or consuming system resources. According to the Implementing and Operating Cisco Security Core Technologies (SCOR) course, viruses are one of the most common forms of malware and can be classified into different types based on their behavior, such as boot sector viruses, file infectors, macro viruses, or polymorphic viruses1. References: 1: Implementing and Operating Cisco Security Core Technologies (SCOR) course, Module 1: Malware Analysis, Lesson 1: Malware Types and Characteristics, Topic: Virus.

NEW QUESTION: 162
Drag and drop the capabilities from the left onto the correct technologies on the right.

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

Answer:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	superior threat prevention and mitigation for known and unknown threats
superior threat prevention and mitigation for known and unknown threats	detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	combined integrated solution of strong defense and web protection, visibility, and controlling solutions

NEW QUESTION: 163

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: D (LEAVE A REPLY)
Explanation Explanation 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 Explanation 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:
Explanation Explanation 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

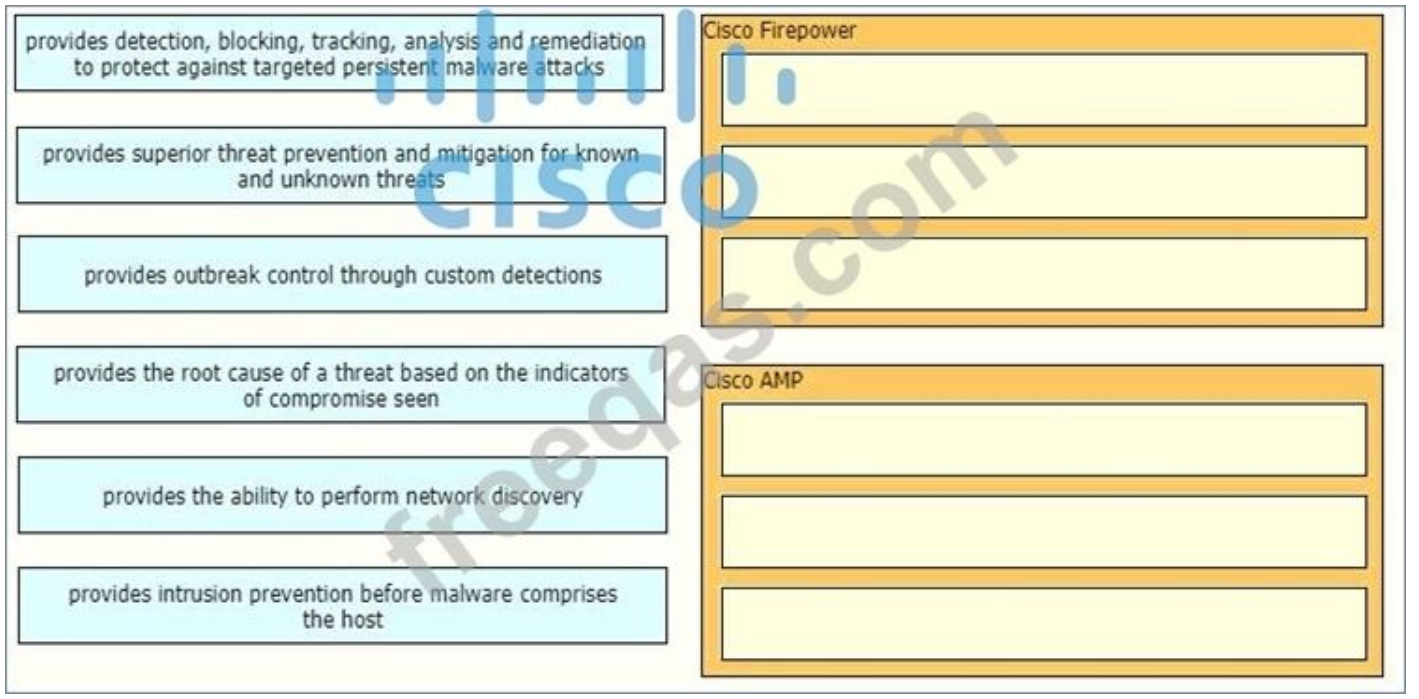
NEW QUESTION: 164
Refer to the exhibit.

```
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
```

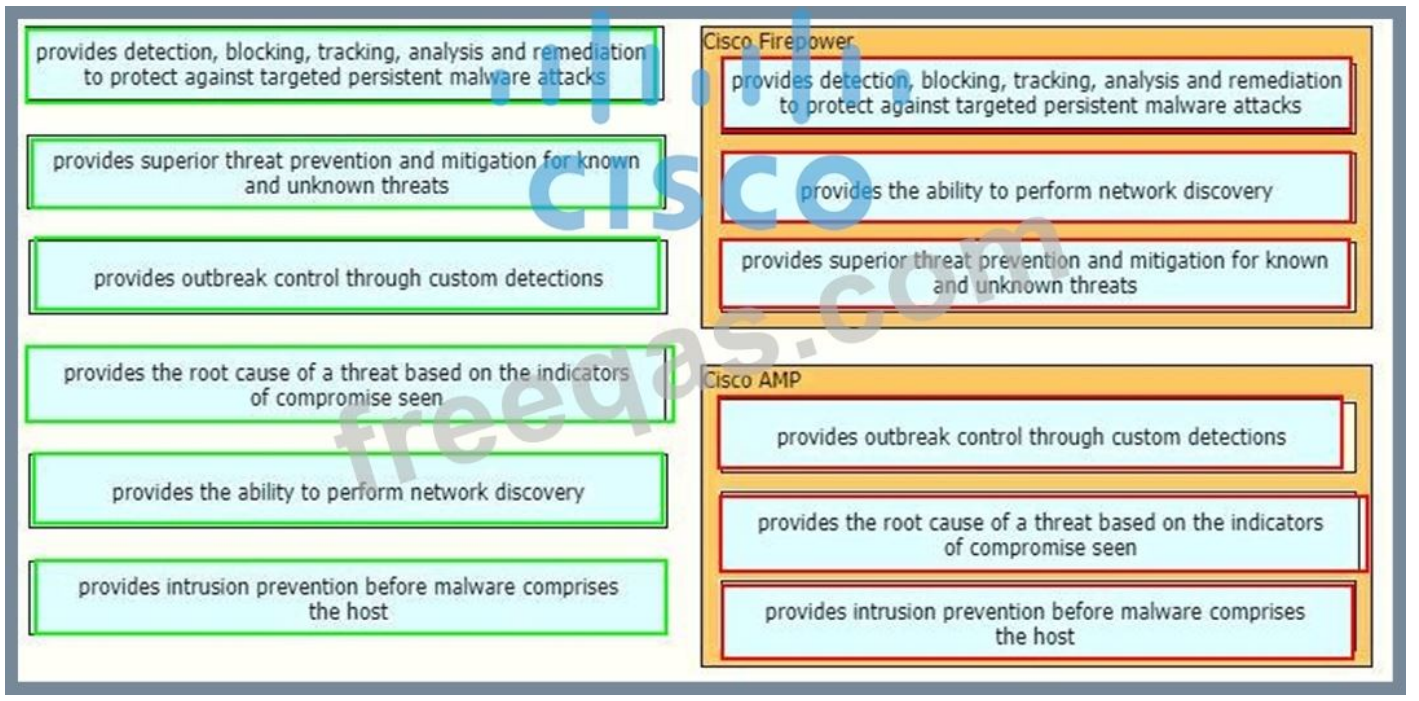
An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained. Which command should be configured on the switch interface in order to provide the user with network connectivity?
A. ip dhcp snooping verify mac-address
B. ip dhcp snooping limit 41
C. ip dhcp snooping vlan 41
D. ip dhcp snooping trust
Answer: D (LEAVE A REPLY)
Explanation 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 thatdetermines 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: 165

Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.

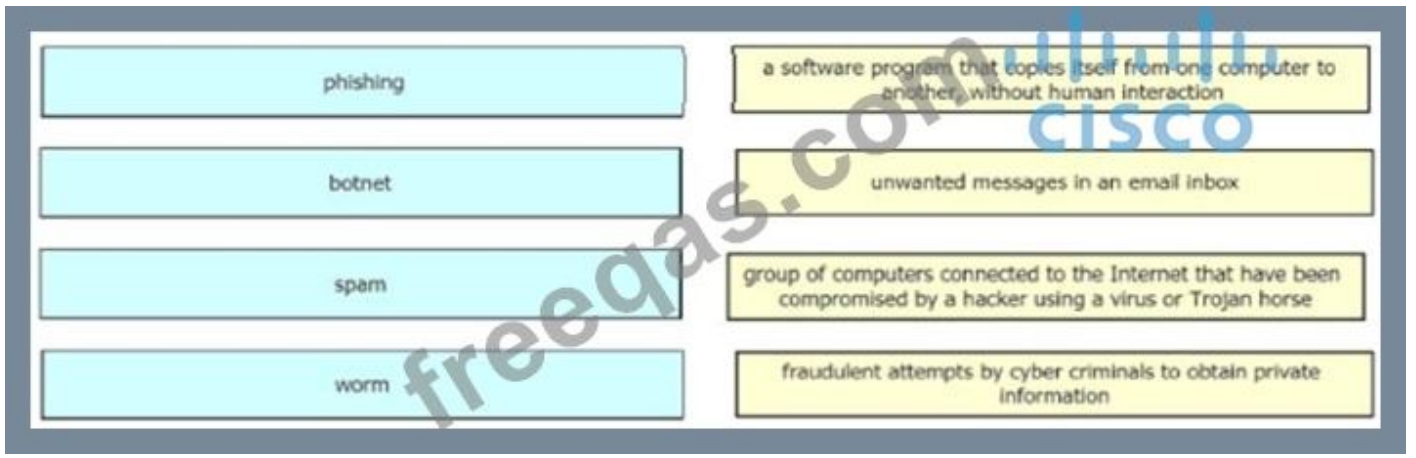


Answer:

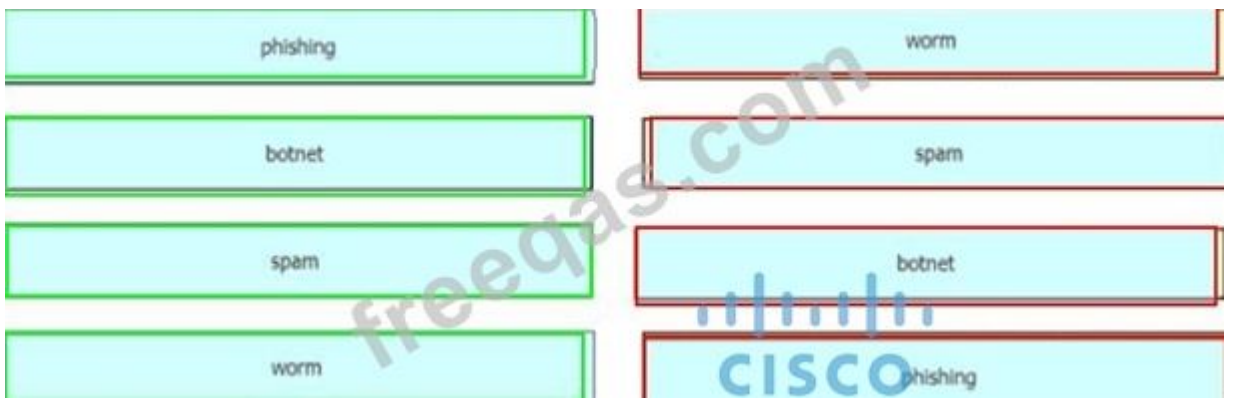


NEW QUESTION: 166

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



Answer:



NEW QUESTION: 167

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

A. Automatically deploy new virtual routers

B. Upgrade software on switches and routers

C. Application monitors for power utilization of devices and IoT sensors

D. Connect to Information Technology Service Management Platforms

E. Create new SSIDs on a wireless LAN controller

Answer: C,D (LEAVE A REPLY)

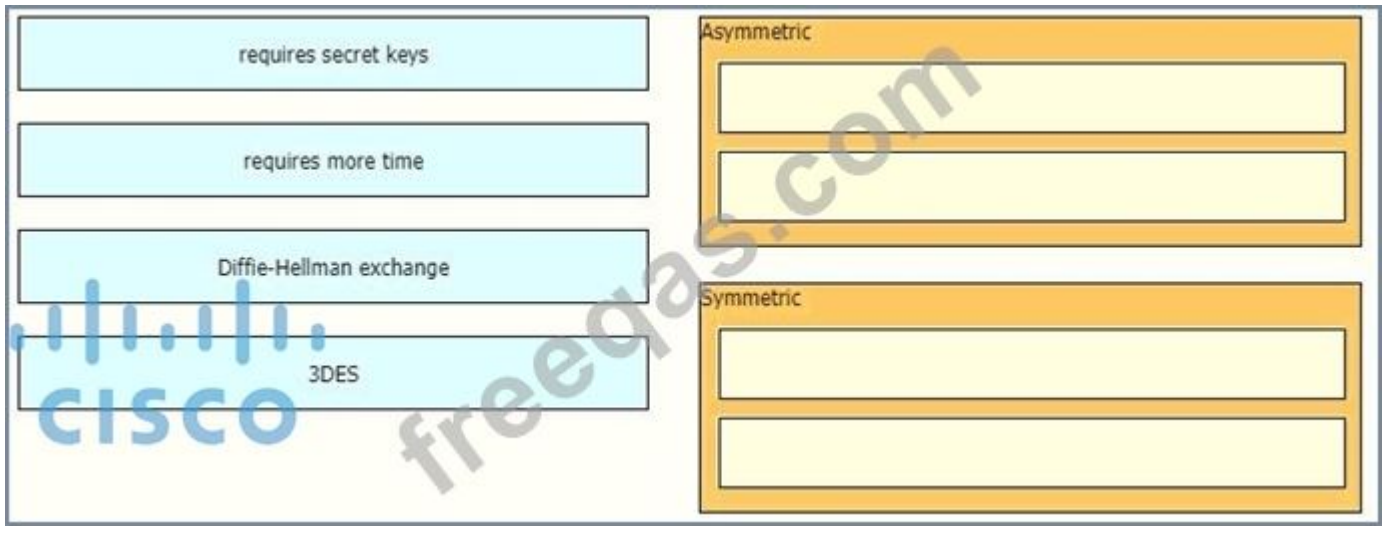
Explanation Integration API (Westbound) Integration capabilities are part of Westbound interfaces. To meet the need to scale and accelerate operations in modern data centers, IT operators require intelligent, end-to-end work flows built with open APIs. The Cisco DNA Center platform provides mechanisms for integrating Cisco DNA Assurance workflows and data with thirdparty IT Service Management (ITSM) solutions. Reference: https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/events-andnotifications-eastbound -> Therefore answer D is correct. Westbound-Integration APIs Cisco DNA Center platform can power end-to-end IT processes across the value chain by integrating various domains such as ITSM, IPAM, and reporting. By leveraging the REST-based Integration Adapter APIs,

bidirectional interfaces can be built to allow the exchange of contextual information between Cisco DNA Center and the external, third-party IT systems. The westbound APIs provide the capability to publish the network data, events and notifications to the external systems and consume information in Cisco DNA Center from the connected systems. Reference: https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitiveadvantage Therefore the most suitable choice is Integration APIs can monitor for power utilization of devices and IoT sensors -> Answer C is correct.
Integration API (Westbound)
Integration capabilities are part of Westbound interfaces. To meet the need to scale and accelerate operations in modern data centers, IT operators require intelligent, end-to-end work flows built with open APIs. The Cisco DNA Center platform provides mechanisms for integrating Cisco DNA Assurance workflows and data with thirdparty IT Service Management (ITSM) solutions.
Reference:
-> Therefore answer D is correct.
Westbound-Integration APIs
Cisco DNA Center platform can power end-to-end IT processes across the value chain by integrating various domains such as ITSM, IPAM, and reporting. By leveraging the REST-based Integration Adapter APIs, bidirectional interfaces can be built to allow the exchange of contextual information between Cisco DNA Center and the external, third-party IT systems. The westbound APIs provide the capability to publish the network data, events and notifications to the external systems and consume information in Cisco DNA Center from the connected systems.
Therefore the most suitable choice is Integration APIs can monitor for power utilization of devices and IoT Explanation Integration API (Westbound) Integration capabilities are part of Westbound interfaces. To meet the need to scale and accelerate operations in modern data centers, IT operators require intelligent, end-to-end work flows built with open APIs. The Cisco DNA Center platform provides mechanisms for integrating Cisco DNA Assurance workflows and data with thirdparty IT Service Management (ITSM) solutions. Reference: https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/events-andnotifications-eastbound -> Therefore answer D is correct. Westbound-Integration APIs Cisco DNA Center platform can power end-to-end IT processes across the value chain by integrating various domains such as ITSM, IPAM, and reporting. By leveraging the REST-based Integration Adapter APIs, bidirectional interfaces can be built to allow the exchange of contextual information between Cisco DNA Center and the external, third-party IT systems. The westbound APIs provide the capability to publish the network data, events and notifications to the external systems and consume information in Cisco DNA Center from the connected systems. Reference: https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitiveadvantage Therefore the most suitable choice is Integration APIs can monitor for power utilization of devices and IoT sensors -> Answer C is correct.

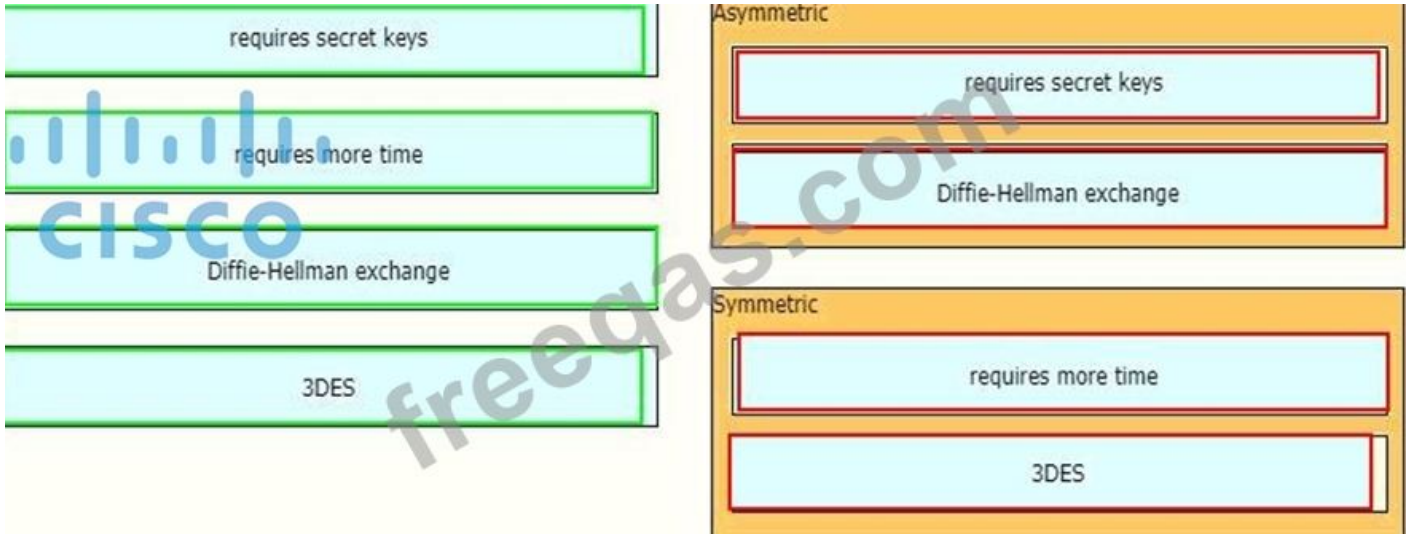
NEW QUESTION: 168
Which threat intelligence standard contains malware hashes?
A. structured threat information expression
B. advanced persistent threat
C. trusted automated exchange or indicator information
D. open command and control
Answer: C (LEAVE A REPLY)
Trusted Automated Exchange of Indicator Information (TAXII) is a standard that defines how to exchange cyber threat intelligence (CTI) over HTTPS. CTI includes indicators of compromise (IOCs), such as malware hashes, IP addresses, URLs, and domains, that can be used to detect and respond to cyberattacks. TAXII enables the sharing of CTI in a secure, automated, and interoperable way among different organizations and tools. Structured Threat Information Expression (STIX) is a standard that defines how to represent and structure CTI in a

common language. STIX and TAXII are often used together to facilitate the exchange of CTI. Advanced Persistent Threat (APT) is not a standard, but a term used to describe a sophisticated and stealthy cyberattack that persists over a long period of time, often targeting specific organizations or sectors.
Open Command and Control (OpenC2) is a standard that defines how to communicate and execute cyber defense actions across different technologies and domains. OpenC2 enables the orchestration and automation of cyber defense actions, such as blocking, isolating, or redirecting malicious traffic or devices. References := Some possible references are:
* [Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 4: Content Security, Lesson 4.3: Cisco Umbrella, Topic 4.3.1: Cisco Umbrella Investigate
* 350-701 SCOR - Cisco, Exam Topics, 4.0 Content Security, 4.3 Describe the components, capabilities,
* and benefits of Cisco Umbrella, 4.3.a Investigate
* TAXII - OASIS Cyber Threat Intelligence Technical Committee, Overview, Introduction
* STIX - OASIS Cyber Threat Intelligence Technical Committee, Overview, Introduction
* OpenC2 - OASIS Open Command and Control Technical Committee, Overview, Introduction
* What is an Advanced Persistent Threat (APT)? | Fortinet, Definition, What is an APT?

NEW QUESTION: 169
Drag and drop the descriptions from the left onto the encryption algorithms on the right.

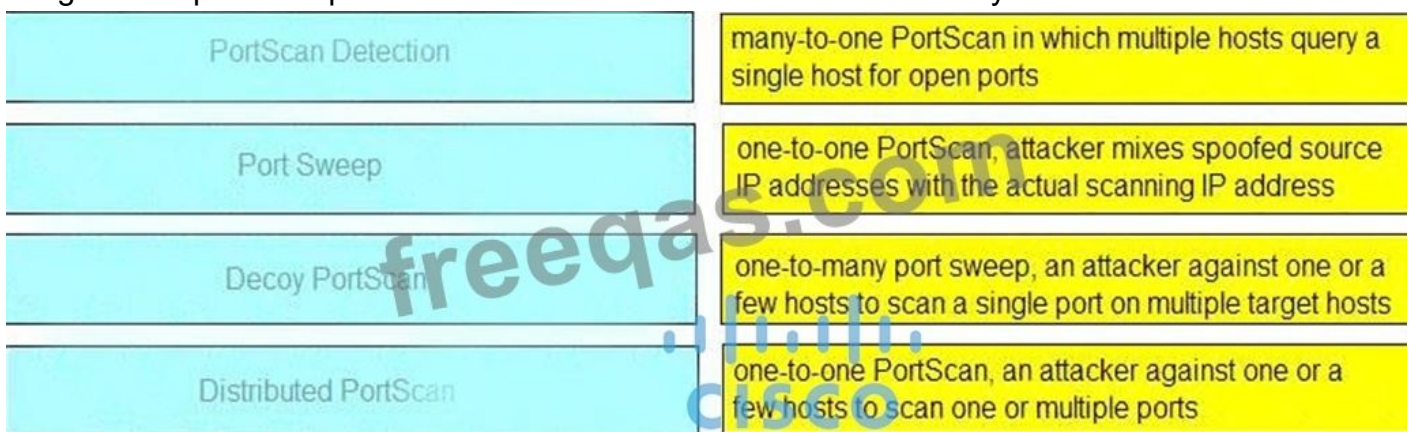


Answer:



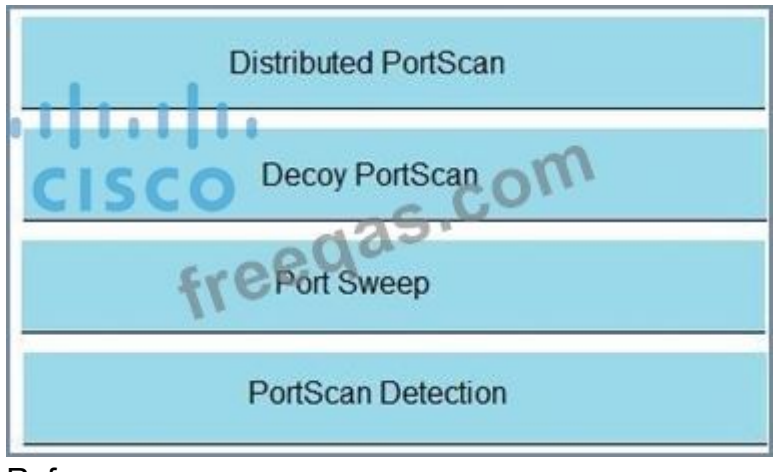
NEW QUESTION: 170

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



Answer:

Explanation



Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/detecti

NEW QUESTION: 171

Which Cisco AMP feature allows an engineer to look back to trace past activities, such as file and process activity on an endpoint?

A. retrospective security

B. advanced search

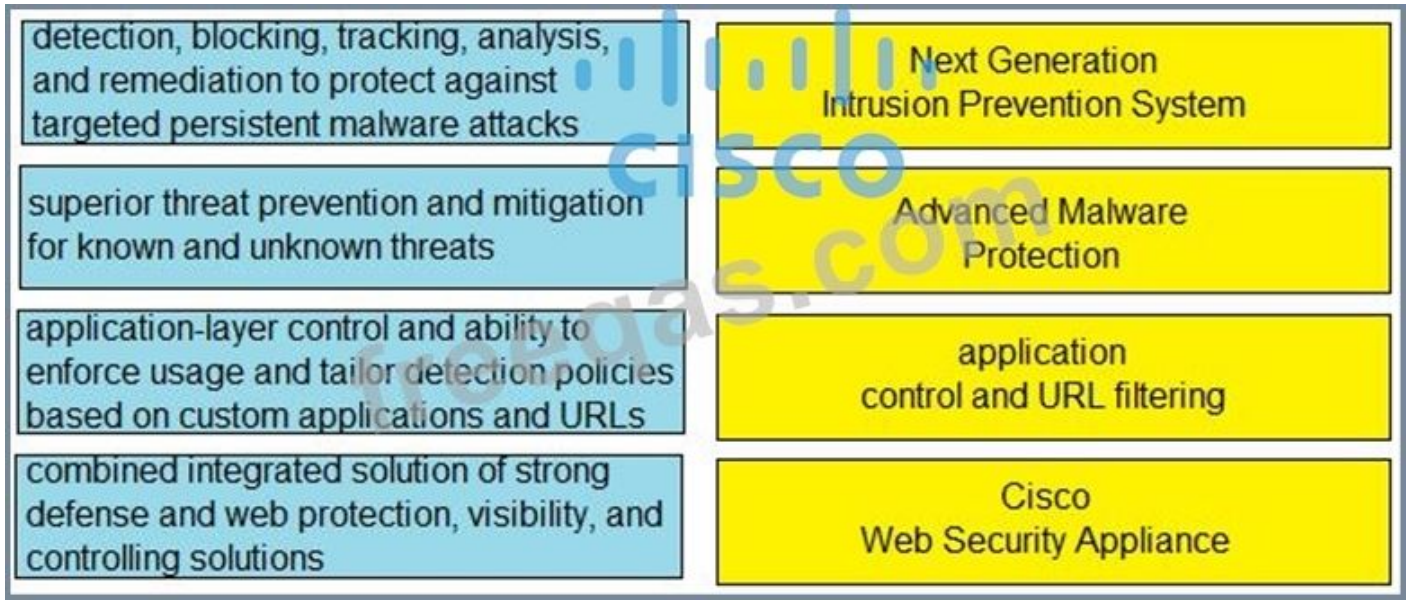
C. advanced investigation

D. endpoint isolation

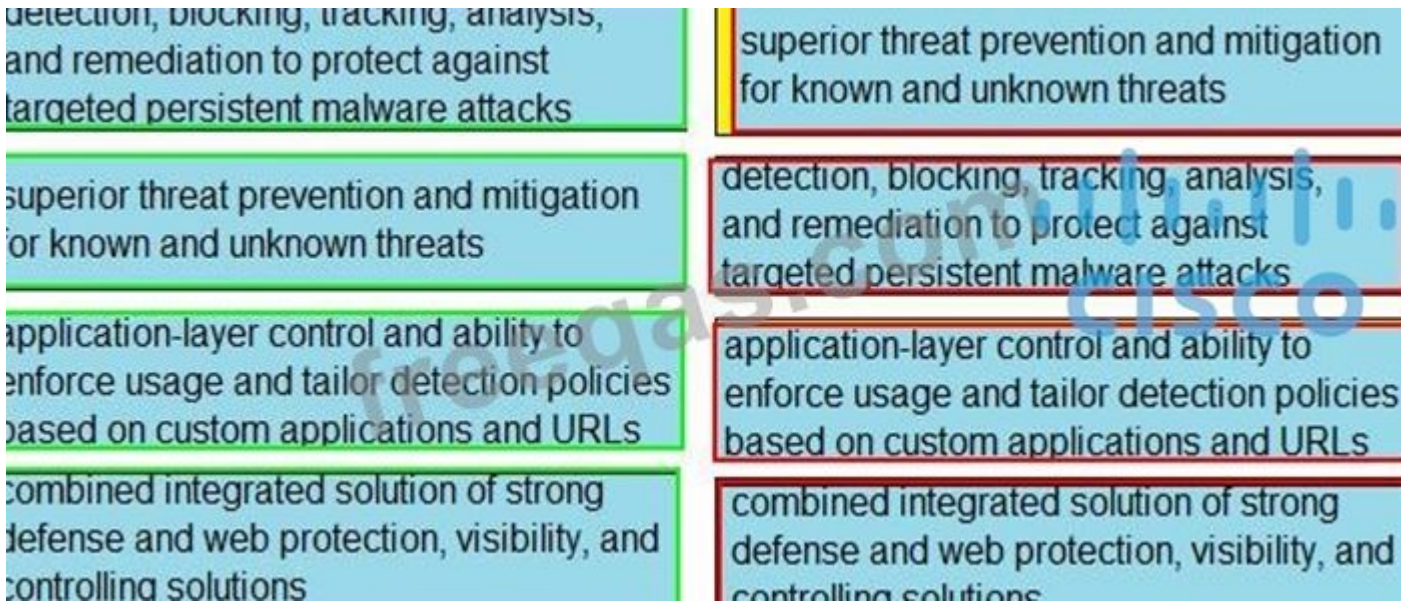
Answer: A (LEAVE A REPLY)

NEW QUESTION: 172
An engineer is configuring AMP for endpoints and wants to block certain files from executing. Which outbreak control method is used to accomplish this task?
A. device flow correlation
B. simple detections
C. application blocking list
D. advanced custom detections
Answer: C (LEAVE A REPLY)
The application blocking list is an outbreak control method that allows the administrator to block certain files from executing on the endpoints based on their SHA values. This can prevent malware from running on the endpoints and causing damage. The other options are not outbreak control methods, but rather different features of AMP for endpoints. Device flow correlation is a network analysis feature that monitors connections and detects malicious activity. Simple detections and advanced custom detections are custom rules that can be created by the administrator to detect and block files based on signatures or other criteria. References:
* Configure Windows Policy in AMP for Endpoints - Cisco
* Prevent, Detect and Respond with Cisco AMP for Endpoints

NEW QUESTION: 173
Drag and drop the capabilities from the left onto the correct technologies on the right.



Answer:



NEW QUESTION: 174

What is a benefit of using Cisco FMC over Cisco ASDM?

A. Cisco FMC uses Java while Cisco ASDM uses HTML5.

B. Cisco FMC provides centralized management while Cisco ASDM does not.

C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.

D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices

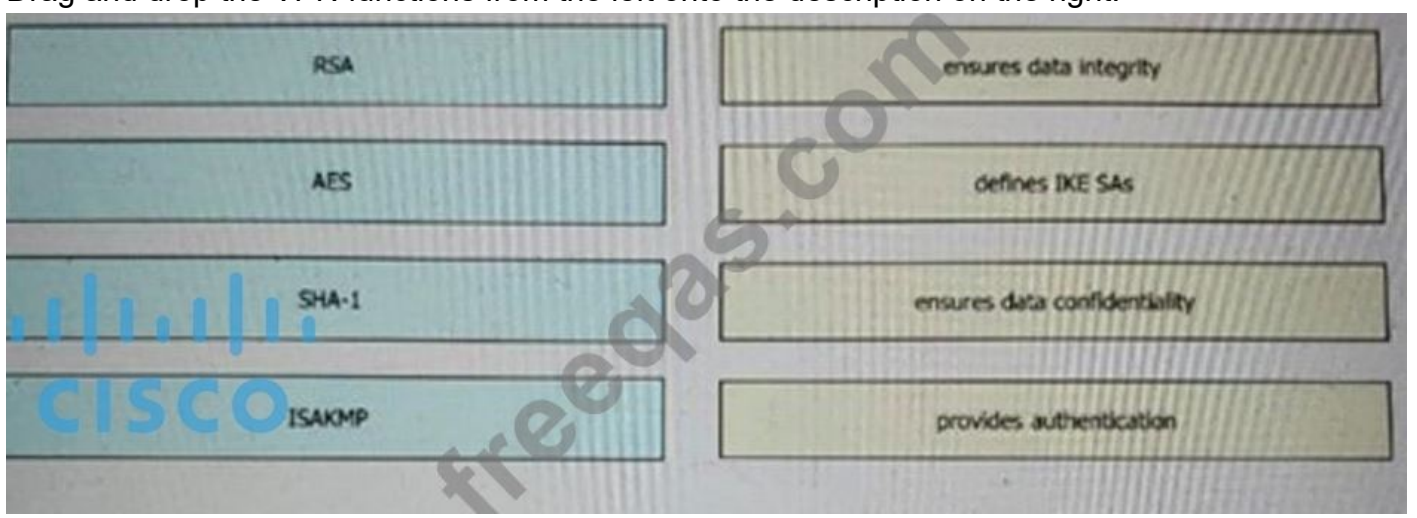
Answer: D (LEAVE A REPLY)

Explanation

https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html

NEW QUESTION: 175

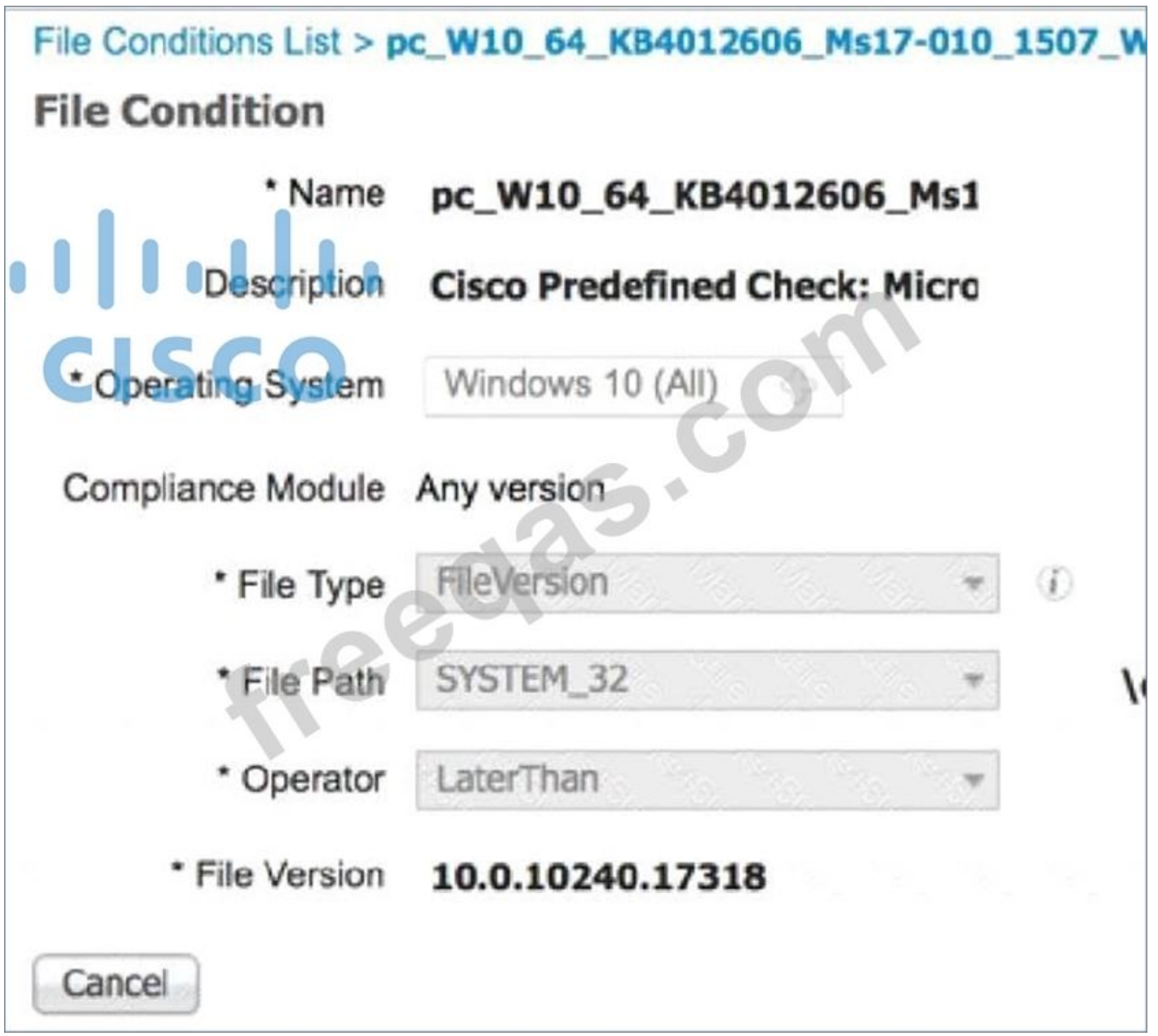
Drag and drop the VPN functions from the left onto the description on the right.



Answer:

NEW QUESTION: 176
An engineer needs to configure an access control policy rule to always send traffic for inspection without using the default action. Which action should be configured for this rule?
A. monitor
B. allow
C. block
D. trust
Answer: B (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/acce the first three access control rules in the policy-Monitor, Trust, and Block-cannot inspect matching traffic. Monitor rules track and log but do not inspect network traffic, so the system continues to match traffic against additional rules to determine whether to permit or deny it
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/acce

NEW QUESTION: 177
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)
ExplanationA 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: 178
What is the function of the Context Directory Agent?
A. accepts user authentication requests on behalf of Web Security Appliance for user identification
B. reads the Active Directory logs to map IP addresses to usernames
C. relays user authentication requests from Web Security Appliance to Active Directory
D. maintains users' group memberships
Answer: B (LEAVE A REPLY)

NEW QUESTION: 179
Refer to the exhibit.

What will occur when this device tries to connect to the port?

A. 802 1X will work and the device will be allowed on the network

B. 802.1X will not work, but MAB will start and allow the device on the network.

C. 802 1X and MAB will both be used and ISE can use policy to determine the access level

D. 802.1X will not work and the device will not be allowed network access

Answer: (SHOW ANSWER)

NEW QUESTION: 180

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: A (LEAVE A REPLY)

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

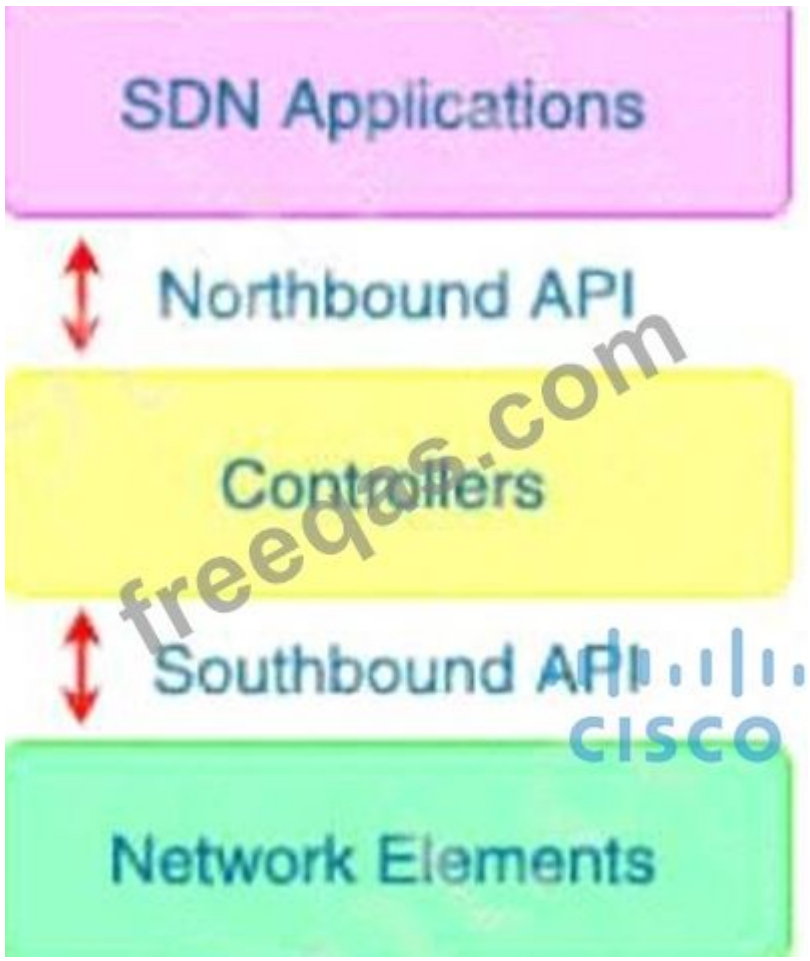
network. Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. If requirements are optional and clients fail these requirements, then the clients have an option to continue during posture evaluation of endpoints. Mandatory Requirements During policy evaluation, 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: 181
What are two benefits of using Cisco Duo as an MFA solution? (Choose two.)
A. provides simple and streamlined login experience for multiple applications and users
B. encrypts data that is stored on endpoints
C. native integration that helps secure applications across multiple cloud platforms or on-premises environments
D. grants administrators a way to remotely wipe a lost or stolen device
E. allows for centralized management of endpoint device applications and configurations
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 182
Which system performs compliance checks and remote wiping?
A. MDM
B. ISE
C. AMP
D. OTP
Answer: A (LEAVE A REPLY)
MDM stands for Mobile Device Management, which is a system that performs compliance checks and remote wiping on mobile devices. MDM allows administrators to enforce security policies, monitor device status, and remotely manage devices in case of loss, theft, or compromise. MDM can also integrate with other Cisco security solutions, such as ISE, AMP, and Umbrella, to provide enhanced protection and visibility for mobile devices. References:
* Mobile Device Management (MDM) - Cisco
* Implementing and Operating Cisco Security Core Technologies (SCOR) - Module 5: Secure Network Access

NEW QUESTION: 183
Which type of API is being used when a controller within a software-defined network architecture dynamically makes configuration changes on switches within the network?

A. westbound AP
B. southbound API
C. northbound API
D. eastbound API
Answer: B (LEAVE A REPLY)
ExplanationExplanationSouthbound APIs enable SDN controllers to dynamically make changes based on real-time demands andscalability needs.



NEW QUESTION: 184
Which two descriptions of AES encryption are true? (Choose two)
A. AES is less secure than 3DES.
B. AES is more secure than 3DES.
C. AES can use a 168-bit key for encryption.
D. AES can use a 256-bit key for encryption.
E. AES encrypts and decrypts a key three times in sequence.
Answer: (SHOW ANSWER)
AES encryption is a symmetric block cipher algorithm that uses a single key to encrypt and decrypt data. It is more secure than 3DES, which is an older and slower algorithm that encrypts and decrypts a key three times in sequence. AES can use different key sizes, such as 128, 192, or 256 bits, depending on the security level required. The longer the key, the more rounds of encryption and decryption are performed, making it harder to break. AES encryption is based on a substitution-permutation network, which consists of a series of operations that transform the input data into the output data using the key. References :=

https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

NEW QUESTION: 185
Which two tasks allow NetFlow on a Cisco ASA 5500 Series firewall? (Choose two.)
A. Create a class map to match interesting traffic.
B. Apply NetFlow Exporter to the outside interface in the inbound direction.
C. Define a NetFlow collector by using the flow-export command.
D. Enable NetFlow Version 9.
E. Create an ACL to allow UDP traffic on port 9996.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 186
What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?
A. Cisco Umbrella
B. External Threat Feeds
C. Cisco Threat Grid
D. Cisco Stealthwatch
Answer: C (LEAVE A REPLY)
Explanation Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically.
Explanation Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector

NEW QUESTION: 187
Which capability is exclusive to a Cisco AMP public cloud instance as compared to a private cloud instance?
A. RBAC
B. ETHOS detection engine
C. SPERO detection engine
D. TETRA detection engine
Answer: B (LEAVE A REPLY)
ETHOS is one of the many detection engines that AMP uses to continuously protect you from malware. It is only available in the public cloud, as it requires a large amount of data and processing power to operate.
ETHOS uses machine learning to analyze the behavior and characteristics of files and determine their maliciousness. It can detect both known and unknown threats, as well as polymorphic and metamorphic malware that can change their appearance or code. ETHOS is part of the AMP cloud's dynamic analysis capabilities, which also include SPERO and Threat Grid12.

The private cloud instance of AMP does not have ETHOS, as it is meant to be an on-premises, self-contained solution that satisfies stringent privacy requirements. The private cloud instance also does not have SPERO or Threat Grid, unless they are deployed separately as additional appliances. The private cloud instance relies on the TETRA detection engine, which is a signature-based engine that can identify known malware. TETRA is updated regularly with new signatures from the AMP cloud, but it cannot detect unknown or zero-day threats as effectively as ETHOS34.
Therefore, the capability that is exclusive to the AMP public cloud instance as compared to the private cloud instance is the ETHOS detection engine. References: 1: Cisco Advanced Malware Protection Private Cloud Appliance Data Sheet 2: What is AMP Private Cloud 3: Deploy Cisco AMP Private Cloud on Cisco HyperFlex Systems 4: AMP Private Cloud vs Public Cloud Dashboard different

NEW QUESTION: 188
How does Cisco Umbrella archive logs to an enterprise owned storage?
A. by using the Application Programming Interface to fetch the logs
B. by sending logs via syslog to an on-premises or cloud-based syslog server
C. by the system administrator downloading the logs from the Cisco Umbrella web portal
D. by being configured to send logs to a self-managed AWS S3 bucket
Answer: D (LEAVE A REPLY)
The Cisco Umbrella Multi-Org console has the ability to upload, store, and archive traffic activity logs from your organizations' Umbrella dashboards to the cloud through Amazon S3. CSV formatted Umbrella logs are compressed (gzip) and uploaded every ten minutes so that there's a minimum of delay between traffic from the organization's Umbrella dashboard being logged and then being available to download from an S3 bucket.
By having your organizations' logs uploaded to an S3 bucket, you can then download logs automatically to keep in perpetuity in backup storage.
The Cisco Umbrella Multi-Org console has the ability to upload, store, and archive traffic activity logs from your organizations' Umbrella dashboards to the cloud through Amazon S3. CSV formatted Umbrella logs are compressed (gzip) and uploaded every ten minutes so that there's a minimum of delay between traffic from the organization's Umbrella dashboard being logged and then being available to download from an S3 bucket.
By having your organizations' logs uploaded to an S3 bucket, you can then download logs automatically to keep in perpetuity in backup storage.
Reference:
The Cisco Umbrella Multi-Org console has the ability to upload, store, and archive traffic activity logs from your organizations' Umbrella dashboards to the cloud through Amazon S3. CSV formatted Umbrella logs are compressed (gzip) and uploaded every ten minutes so that there's a minimum of delay between traffic from the organization's Umbrella dashboard being logged and then being available to download from an S3 bucket.
By having your organizations' logs uploaded to an S3 bucket, you can then download logs automatically to keep in perpetuity in backup storage.

NEW QUESTION: 189
When wired 802.1X authentication is implemented, which two components are required? (Choose two.)
A. authentication server: Cisco Identity Service Engine
B. authenticator: Cisco Catalyst switch
C. supplicant: Cisco AnyConnect ISE Posture module

D. authenticator: Cisco Identity Services Engine
E. authentication server: Cisco Prime Infrastructure
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 190
An engineer is configuring Dropbox integration with Cisco Cloudlock. Which action must be taken before granting API access in the Dropbox admin console?
A. Authorize Dropbox within the Platform settings in the Cisco Cloudlock portal.
B. Add Dropbox to the Cisco Cloudlock Authentication and API section in the Cisco Cloudlock portal.
C. Send an API request to Cisco Cloudlock from Dropbox admin portal.
D. Add Cisco Cloudlock to the Dropbox admin portal.
Answer: B (LEAVE A REPLY)
Cisco AMP for Endpoints provides next-generation protection by leveraging an endpoint protection platform (EPP) and endpoint detection and response (EDR) capabilities. EPP is a set of multifaceted prevention techniques that stop threats from compromising endpoints, such as behavioral analytics, machine learning, and signature-based methods. EDR is a set of powerful features that reduce the attack surface and remediate faster, such as advanced threat hunting, endpoint isolation, and dynamic malware analysis. Cisco AMP for Endpoints also integrates with SecureX, a built-in platform that offers extended detection and response (XDR) capabilities across multiple control points, such as network, cloud, email, and web. By combining EPP, EDR, and XDR, Cisco AMP for Endpoints delivers a comprehensive and resilient endpoint security solution that can detect, respond, and recover from sophisticated attacks. References:
* Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco
* Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco

NEW QUESTION: 191
Which technology provides the benefit of Layer 3 through Layer 7 innovative deep packet inspection, enabling the platform to identify and output various applications within the network traffic flows?
A. Cisco NBAR2
B. Cisco ASAV
C. Account on Resolution
D. Cisco Prime Infrastructure
Answer: (SHOW ANSWER)
Cisco NBAR2 is a classification engine that recognizes and classifies a wide variety of protocols and applications based on their deep packet inspection (DPI) signatures. NBAR2 enables the platform to identify and output various applications within the network traffic flows, such as web, email, voice, video, and so on.
NBAR2 also supports custom protocols and applications, allowing the platform to classify traffic based on user-defined criteria. NBAR2 helps the platform to apply the appropriate quality of service (QoS), security, and policy for each application or protocol. References := Some possible references are:
* Cisco NBAR2
* Classifying Network Traffic Using NBAR
* Next Generation NBAR (NBAR2)

NEW QUESTION: 192
What is the difference between deceptive phishing and spear phishing?
A. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.
B. Deceptive phishing is an attacked aimed at a specific user in the organization who holds a C-level role.
C. Spear phishing is when the attack is aimed at the C-level executives of an organization
D. A spear phishing campaign is aimed at a specific person versus a group of people.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 193
What are two functionalities of northbound and southbound APIs within Cisco SDN architecture? (Choose two.)
A. Northbound APIs utilize RESTful API methods such as GET, POST, and DELETE.
B. Southbound interfaces utilize device configurations such as VLANs and IP addresses.
C. Southbound APIs are used to define how SDN controllers integrate with applications.
D. Northbound interfaces utilize OpenFlow and OpFlex to integrate with network devices.
E. Southbound APIs utilize CLI, SNMP, and RESTCONF.
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 194
An engineer is configuring cloud logging using a company-managed Amazon S3 bucket for Cisco Umbrella logs. What benefit does this configuration provide for accessing log data?
A. No other applications except Cisco Umbrella can write to the S3 bucket
B. Data can be stored offline for 30 days.
C. It can grant third-party SIEM integrations write access to the S3 bucket
D. It is included m the license cost for the multi-org console of Cisco Umbrella
Answer: (SHOW ANSWER)

NEW QUESTION: 195
A network administrator configures Dynamic ARP Inspection on a switch. After Dynamic ARP Inspection is applied, all users on that switch are unable to communicate with any destination. The network administrator checks the interface status of all interfaces, and there is no err-disabled interface. What is causing this problem?
A. DHCP snooping has not been enabled on all VLANs.
B. The ip arp inspection limit command is applied on all interfaces and is blocking the traffic of all users.
C. Dynamic ARP Inspection has not been enabled on all VLANs
D. The no ip arp inspection trust command is applied on all user host interfaces
Answer: D (LEAVE A REPLY)
Explanation
Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. After enabling DAI, all ports become untrusted ports.

NEW QUESTION: 196

Refer to the exhibit.

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

A. set the IP address of an interface

B. complete no configurations

C. complete all configurations

D. add subinterfaces

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 197

Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

A. File Analysis

B. SafeSearch

C. SSL Decryption

D. Destination Lists

Answer: (SHOW ANSWER)

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

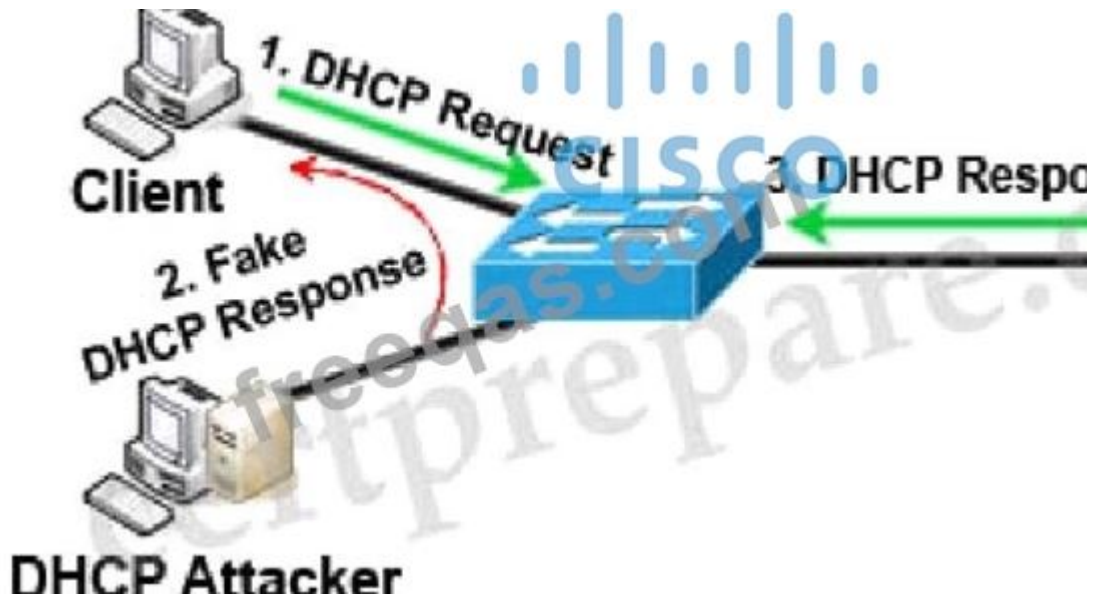
NEW QUESTION: 198

What is the function of the Context Directory Agent?

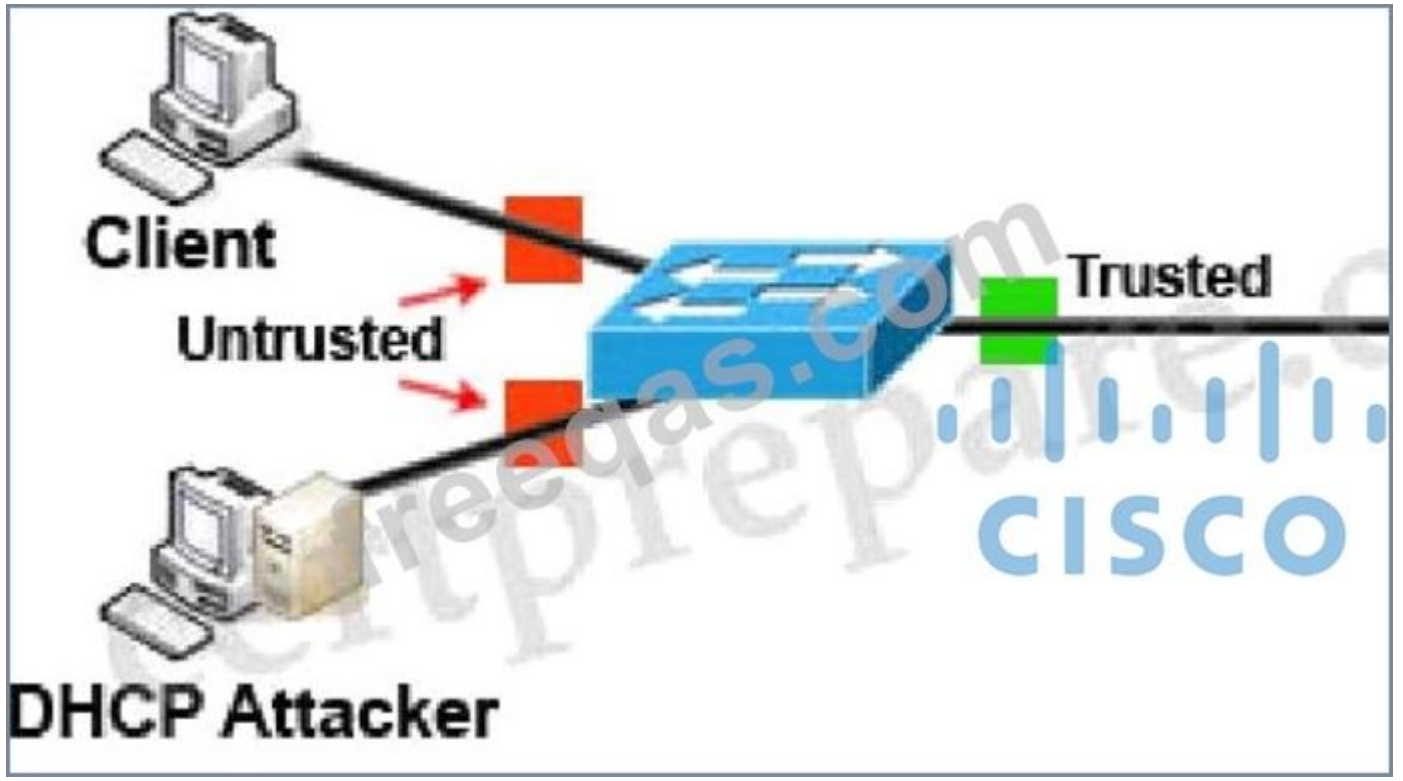
A. maintains users' group memberships

B. relays user authentication requests from Web Security Appliance to Active Directory
C. reads the Active Directory logs to map IP addresses to usernames
D. accepts user authentication requests on behalf of Web Security Appliance for user identification
Answer: C (LEAVE A REPLY)
Explanation Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to). CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices. Reference: https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/ cda_oveviw.html Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to). CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices.
Reference:
Explanation Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to). CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices. Reference: https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/ cda_oveviw.html

NEW QUESTION: 199
An administrator is configuring a DHCP server to better secure their environment. They need to be able to ratelimit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?
A. Set a trusted interface for the DHCP server
B. Set the DHCP snooping bit to 1
C. Add entries in the DHCP snooping database
D. Enable ARP inspection for the required VLAN
Answer: A (LEAVE A REPLY)
To understand DHCP snooping we need to learn about DHCP spoofing attack first.



DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle".
The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.
DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.



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

NEW QUESTION: 200
Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

A. redirection
B. proxy gateway
C. transparent
D. forward
Answer: C (LEAVE A REPLY)

NEW QUESTION: 201
Which RADIUS attribute can you use to filter MAB requests in an 802.1 x deployment?
A. 1
B. 2
C. 6
D. 31
Answer: C (LEAVE A REPLY)
Because MAB uses the MAC address as a username and password, you should make sure that the RADIUS server can differentiate MAB requests from other types of requests for network access. This precaution will prevent other clients from attempting to use a MAC address as a valid credential. Cisco switches uniquely identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB Access-Request message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server.

NEW QUESTION: 202
An engineer must configure Cisco AMP for Endpoints so that it contains a list of files that should not be executed by users. These files must not be quarantined. Which action meets this configuration requirement?
A. Identity the network IPs and place them in a blocked list.
B. Modify the advanced custom detection list to include these files.
C. Create an application control blocked applications list.
D. Add a list for simple custom detection.
Answer: C (LEAVE A REPLY)
create an application control blocked applications list. This option allows you to specify a list of files that you want to prevent from running on the endpoints that have the AMP connector installed. The files are identified by their SHA-256 hashes, and you can upload them individually or in a batch. The files are not quarantined, but they are blocked from execution and reported as events in the AMP console1. This option is different from the simple custom detection list, which is used to detect and quarantine specific files that are considered malicious2. The advanced custom detection list is also used to detect and quarantine files, but it allows you to specify more criteria such as file size, file name, and file path3. The IP block and allow lists are used to control the network traffic to and from the endpoints, not the file execution4.
References: 1: Configure Application Control on the AMP for Endpoints Portal 2: Configure a Simple Custom Detection List on the AMP for Endpoints Portal 3: [Configure an Advanced Custom Detection List on the AMP for Endpoints Portal] 4:
[Configure IP Block and Allow Lists on the AMP for Endpoints Portal]

NEW QUESTION: 203
Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application traffic?
A. Cisco Security Intelligence
B. Cisco Application Visibility and Control

C. Cisco Model Driven Telemetry
D. Cisco DNA Center
Answer: (SHOW ANSWER)
The Cisco Application Visibility and Control (AVC) solution leverages multiple technologies to recognize, analyze, and control over 1000 applications, including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. AVC combines several Cisco IOS/IOS XE components, as well as communicating with external tools, to integrate the following functions into a powerful solution...
Reference: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/guide/avc-user-guide/ avc_tech_overview.html analyze, and control over 1000 applications, including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. AVC combines several Cisco IOS/IOS XE components, as well as communicating with external tools, to integrate the following functions into a powerful solution...
Reference:
The Cisco Application Visibility and Control (AVC) solution leverages multiple technologies to recognize, analyze, and control over 1000 applications, including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. AVC combines several Cisco IOS/IOS XE components, as well as communicating with external tools, to integrate the following functions into a powerful solution...
Reference: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/guide/avc-user-guide/ avc_tech_overview.html

NEW QUESTION: 204
The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the ASA be added on the Cisco UC Manager platform?
A. Certificate Trust List
B. Secured Collaboration Proxy
C. Enterprise Proxy Service
D. Endpoint Trust List
Answer: A (LEAVE A REPLY)

NEW QUESTION: 205
Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or Microsoft vSwitch?
A. inter-EPG isolation
B. intra-EPG isolation
C. inter-VLAN security
D. placement in separate EPGs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 206
An administrator is establishing a new site-to-site VPN connection on a Cisco IOS router. The organization needs to ensure that the ISAKMP key on the hub is used only for terminating traffic from the IP address of
172.19.20.24. Which command on the hub will allow the administrator to accomplish this?
A. crypto ca identity 172.19.20.24
B. crypto isakmp key Cisco0123456789 172.19.20.24
C. crypto enrollment peer address 172.19.20.24

D. crypto isakmp identity address 172.19.20.24

Answer: (SHOW ANSWER)

The command "crypto isakmp identity address 172.19.20.24" is not valid. We can only use "crypto isakmp identity {address | hostname}. The following example uses preshared keys at two peers and sets both their ISAKMP identities to the IP address.

At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified:

crypto isakmp identity address

crypto isakmp key sharedkeystring address 192.168.1.33

At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified:

crypto isakmp identity address

crypto isakmp key sharedkeystring address 10.0.0.1

The command "crypto isakmp identity address 172.19.20.24" is not valid. We can only use "crypto isakmp identity {address | hostname}. The following example uses preshared keys at two peers and sets both their ISAKMP identities to the IP address.

At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified:

crypto isakmp identity address

crypto isakmp key sharedkeystring address 192.168.1.33

At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified:

crypto isakmp identity address

crypto isakmp key sharedkeystring address 10.0.0.1

Reference:

The command "crypto enrollment peer address" is not valid either.

The command "crypto ca identity ..." is only used to declare a trusted CA for the router and puts you in the caidentity configuration mode. Also it should be followed by a name, not an IP address. For example: "crypto ca identity CA-Server" -> Answer A is not correct.

Only answer B is the best choice left.

The command "crypto isakmp identity address 172.19.20.24" is not valid. We can only use "crypto isakmp identity {address | hostname}. The following example uses preshared keys at two peers and sets both their ISAKMP identities to the IP address.

At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified:

crypto isakmp identity address

crypto isakmp key sharedkeystring address 192.168.1.33

At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified:

crypto isakmp identity address

crypto isakmp key sharedkeystring address 10.0.0.1

The command "crypto enrollment peer address" is not valid either.

The command "crypto ca identity ..." is only used to declare a trusted CA for the router and puts you in the caidentity configuration mode. Also it should be followed by a name, not an IP address. For example: "crypto ca identity CA-Server" -> Answer A is not correct.

The command "crypto enrollment peer address" is not valid either.

The command "crypto ca identity ..." is only used to declare a trusted CA for the router and puts you in the caidentity configuration mode. Also it should be followed by a name, not an IP address. For example: "crypto ca identity CA-Server" -> Answer A is not correct.

Only answer B is the best choice left.

NEW QUESTION: 207

Which two key and block sizes are valid for AES? (Choose two.)

A. 64-bit block size, 112-bit key length
B. 64-bit block size, 168-bit key length
C. 128-bit block size, 192-bit key length
D. 128-bit block size, 256-bit key length
E. 192-bit block size, 256-bit key length
Answer: C,D (LEAVE A REPLY)
Explanation/Reference: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

NEW QUESTION: 208
Which technology limits communication between nodes on the same network segment to individual applications?
A. serverless infrastructure
B. microsegmentation
C. SaaS deployment
D. machine-to-machine firewalling
Answer: B (LEAVE A REPLY)
Microsegmentation is a technology that limits communication between nodes on the same network segment to individual applications by creating secure zones across cloud and data center environments. Microsegmentation isolates application workloads from one another and secures them individually with granular firewall policies based on a zero-trust security approach1. Microsegmentation can reduce the attack surface, prevent the lateral movement of threats, and strengthen regulatory compliance1.
Serverless infrastructure is a technology that allows developers to run code without provisioning or managing servers2. Serverless infrastructure does not limit communication between nodes on the same network segment to individual applications, but rather abstracts away the underlying infrastructure from the application logic.
SaaS deployment is a technology that delivers software applications over the internet as a service3. SaaS deployment does not limit communication between nodes on the same network segment to individual applications, but rather provides access to software applications from any device and location.
Machine-to-machine firewalling is a technology that controls the communication between machines or devices on a network. Machine-to-machine firewalling does not limit communication between nodes on the same network segment to individual applications, but rather applies rules to the traffic between machines or devices based on their IP addresses, ports, protocols, or other criteria.
References :=
* What Is Micro-Segmentation? - Cisco
* What is serverless?
* What is SaaS?
* [Machine-to-Machine Firewalling]

NEW QUESTION: 209
What does Cisco ISE use to collect endpoint attributes that are used in profiling?
A. probes
B. posture assessment
C. Cisco AnyConnect Secure Mobility Client
D. Cisco pxGrid
Answer: (SHOW ANSWER)

Cisco ISE uses probes to collect endpoint attributes that are used in profiling. Probes are software modules that run on the ISE Policy Service Nodes (PSNs) and gather information about the endpoints connected to the network. Probes can use various protocols and methods to collect endpoint attributes, such as RADIUS, DHCP, SNMP, HTTP, DNS, NetFlow, NMAP, Active Directory, and Cisco pxGrid. The collected attributes are then matched to predefined or custom conditions that define the endpoint profiles. Endpoint profiling enables ISE to identify and classify the endpoints and apply the appropriate policies based on their identity, role, and context12. References: 1: Cisco ISE 2.4 Endpoint Profiling - Cisco 2: How To Create an Endpoint Profile - Cisco Community Reference: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/2-6/admin_guide

NEW QUESTION: 210
For Cisco IOS PKI, which two types of Servers are used as a distribution point for CRLs? (Choose two)
A. SDP
B. LDAP
C. subordinate CA
D. SCP
E. HTTP
Answer: (SHOW ANSWER)
Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI.
A PKI is composed of the following entities: ...
- A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs)

NEW QUESTION: 211
Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'
```


What does the API key do while working with https://api.amp.cisco.com/v1/computers?
A. displays client ID
B. HTTP authorization
C. Imports requests
D. HTTP authentication
Answer: D (LEAVE A REPLY)
The API key is used for HTTP authentication when working with APIs, including

https://api.amp.cisco.com/v1/computers. It ensures that the user or system making the API request is authenticated and authorized to access the resources requested. The image you sent shows a Python code snippet that imports the requests module, assigns a client ID and an API key to variables, and uses them to make an API call. The API key is passed as a header parameter in the requests.get() function, which is a common way of implementing HTTP authentication. The other options are not correct because they do not describe the role of the API key. The client ID is a different parameter that identifies the user or system making the request, but it does not authenticate them. HTTP authorization is a process of granting or denying access to resources based on the user's identity and permissions, but it is not the same as authentication.
Importing requests is a Python statement that loads the requests module, which is a library for making HTTP requests, but it has nothing to do with the API key. References := Some possible references are:
* Cisco AMP for Endpoints API
* requests - HTTP for Humans
* HTTP authentication - MDN Web Docs

NEW QUESTION: 212
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. Deploy an encryption appliance.
B. Enable flagged message handling
C. Map sender !P addresses to a host interface.
D. Provision the email appliance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 213
Email security has become a high priority task for a security engineer at a large multi-national organization due to ongoing phishing campaigns. To help control this, the engineer has deployed an Incoming Content Filter with a URL reputation of (-10 00 to -6 00) on the Cisco ESA Which action will the system perform to disable any links in messages that match the filter?
A. Defang
B. Quarantine
C. FilterAction
D. ScreenAction
Answer: (SHOW ANSWER)
Defanging is the process of modifying a URL in a message to prevent it from being clickable. This can help protect users from malicious links that have a low URL reputation score. Defanging is one of the actions that can be configured in the Incoming Content Filter on the Cisco ESA. The other actions are Quarantine, FilterAction, and ScreenAction. Quarantine sends the message to a quarantine area for further inspection.

FilterAction applies a predefined action such as drop, bounce, or deliver. ScreenAction displays a warning message to the user before allowing them to access the URL. Defanging is the only action that disables the links in the message without affecting the delivery or visibility of the message12. References: 1: URL Filtering on the Cisco IronPort ESA - Mikail's Blog 2: Configure URL Filtering for Secure Email Gateway and Cloud Gateway - Cisco Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/esa-content-filters.pdf

NEW QUESTION: 214
Which attribute has the ability to change during the RADIUS CoA?
A. NTP
B. Authorization
C. Accessibility
D. Membership
Answer: B (LEAVE A REPLY)
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-

NEW QUESTION: 215
A company is experiencing exfiltration of credit card numbers that are not being stored on-premise. The company needs to be able to protect sensitive data throughout the full environment Which tool should be used to accomplish this goal?
A. Security Manager
B. Cloudlock
C. Web Security Appliance
D. Cisco ISE
Answer: B (LEAVE A REPLY)
https://www.cisco.com/c/dam/en/us/products/collateral/security/cloudlock/cisco-cloudlock-cloud-data-securitydatasheet.pdf

NEW QUESTION: 216
Which license is required for Cisco Security Intelligence to work on the Cisco Next Generation Intrusion Prevention System?
A. control
B. malware
C. URL filtering
D. protect
Answer: D (LEAVE A REPLY)
Cisco Security Intelligence is a feature that allows you to block or monitor traffic based on IP addresses or domain names that are known to be malicious or suspicious. Cisco Security Intelligence requires a Protect license on the Cisco Next Generation Intrusion Prevention System (NGIPS), which is part of the Firepower Threat Defense (FTD) software. A Protect license allows you to perform intrusion detection and prevention, file control, and Security Intelligence filtering1. The other license options (control, malware, and URL filtering) do not enable Cisco Security Intelligence on the NGIPS. References:
* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, section "Security Intelligence"
* Firepower Management Center Configuration Guide, Version 6.0, section "Licensing the Firepower System"

NEW QUESTION: 217

What is a characteristic of a bridge group in ASA Firewall transparent mode"

A. It allows ARP traffic with a single access rule.

B. It is a Layer 3 segment and includes one port and customizable access rules.

C. It includes multiple interfaces and access rules between interfaces are customizable

D. It has an IP address on its BVI interface and is used for management traffic.

Answer: (SHOW ANSWER)

Explanation

A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place.

NEW QUESTION: 218

What is the primary benefit of deploying an ESA in hybrid mode?

A. You can fine-tune its settings to provide the optimum balance between security and performance for your environment

B. It provides the lowest total cost of ownership by reducing the need for physical appliances

C. It provides maximum protection and control of outbound messages

D. It provides email security while supporting the transition to the cloud

Answer: (SHOW ANSWER)

ExplanationCisco Hybrid Email Security is a unique service offering that facilitates the deployment of your email securityinfrastructure both on premises and in the cloud. You can change the number of on-premises versus cloudusers at any time throughout the term of your contract, assuming the total number of users does not change.This allows for deployment flexibility as your organization's needs change.

NEW QUESTION: 219

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

A. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).

B. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.

C. It allows multiple security products to share information and work together to enhance security posture in the network.

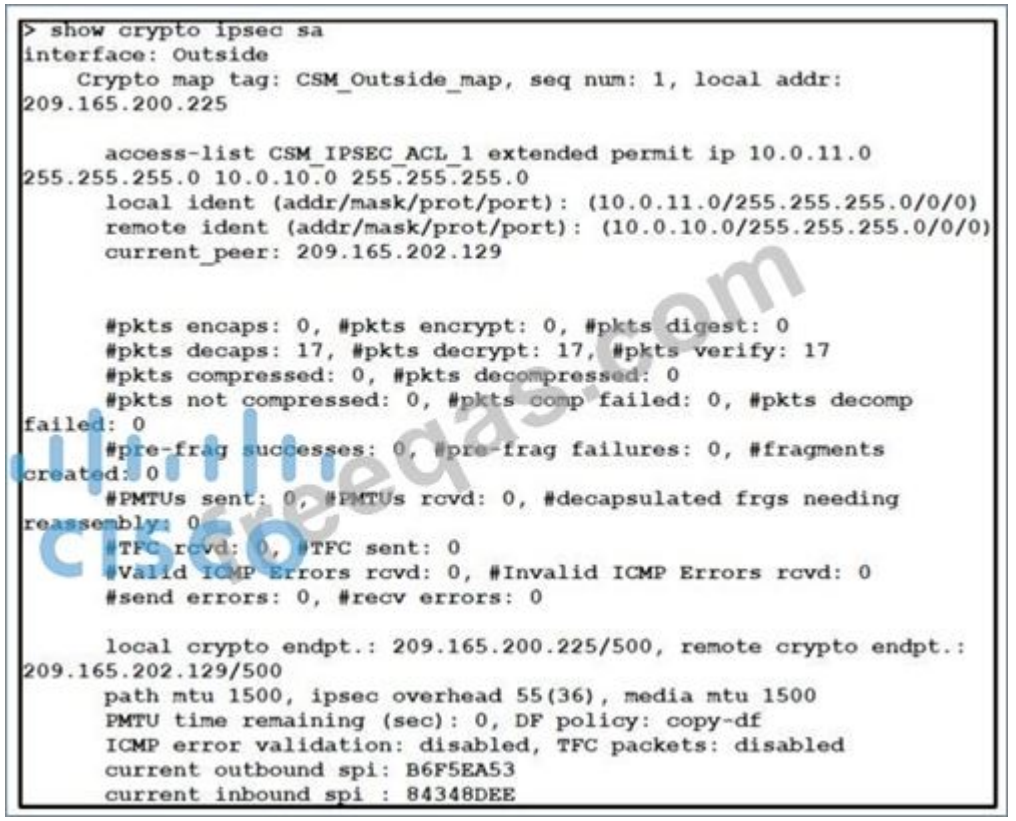
D. It integrates with third-party products to provide better visibility throughout the network.

E. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 220

Refer to the exhibit.



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

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

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

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

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

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 221

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

A. rootkit exploit

B. distributed denial of service

C. smurf

D. cross-site scripting

Answer: (SHOW ANSWER)

NEW QUESTION: 222

What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two.)

A. data exfiltration

B. command and control communication

C. intelligent proxy

D. snort

E. URL categorization

Answer: A,B (LEAVE A REPLY)

Explanation/Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a- glance-c45-736555.pdf

NEW QUESTION: 223

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

A. Encrypted Traffic Analytics

B. Threat Intelligence Director

C. Cognitive Threat Analytics

D. Cisco Talos Intelligence

Answer: (SHOW ANSWER)

Reference:

As shown in the image, on the FMC you have to configure sources from where you would like to download threat intelligence information. The FMC then pushes that information (observables) to sensors. When the traffic matches the observables, the incidents appear in the FMC user interface (GUI).

https://www.cisco.com/c/en/us/support/docs/storage-networking/security/214859-configure-and-troubleshoot-cisco-threat.html

NEW QUESTION: 224

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

A. virtualization

B. middleware

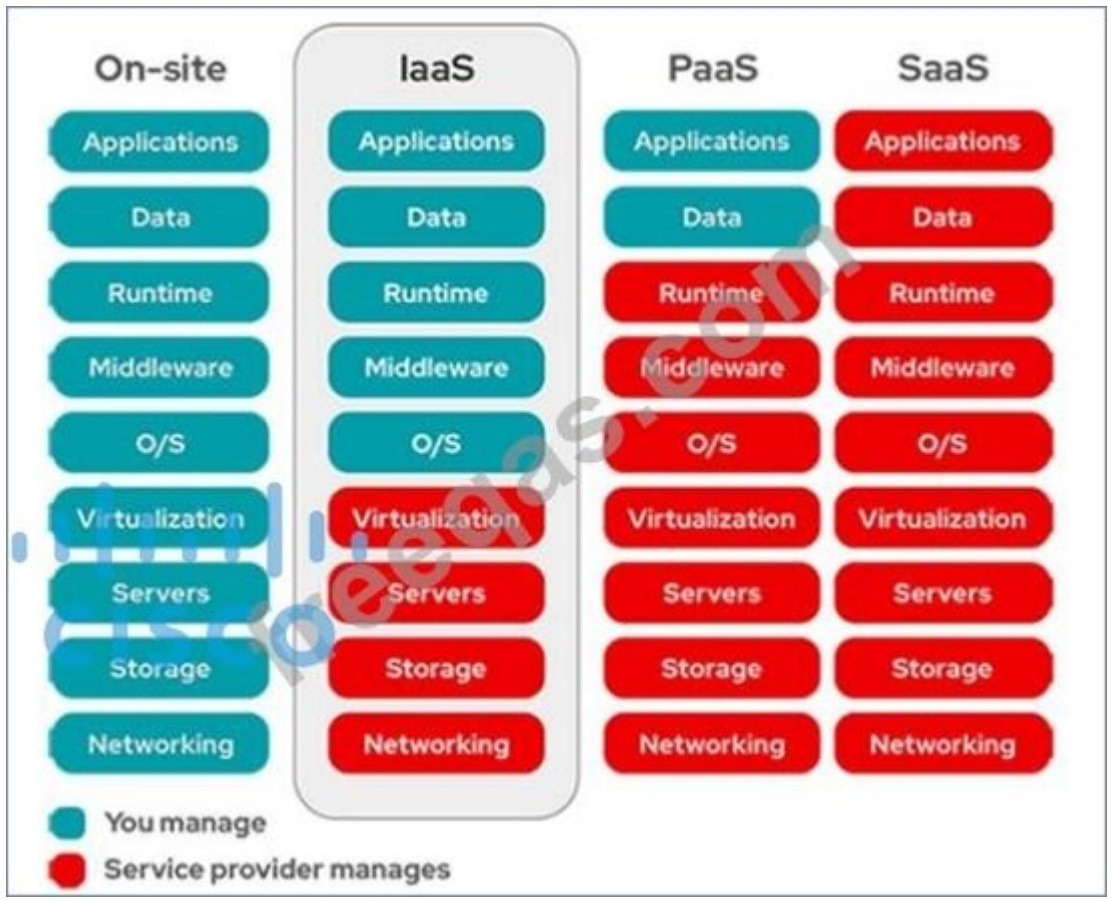
C. operating systems

D. applications

E. data

Answer: (SHOW ANSWER)

Customers must manage applications and data in PaaS.

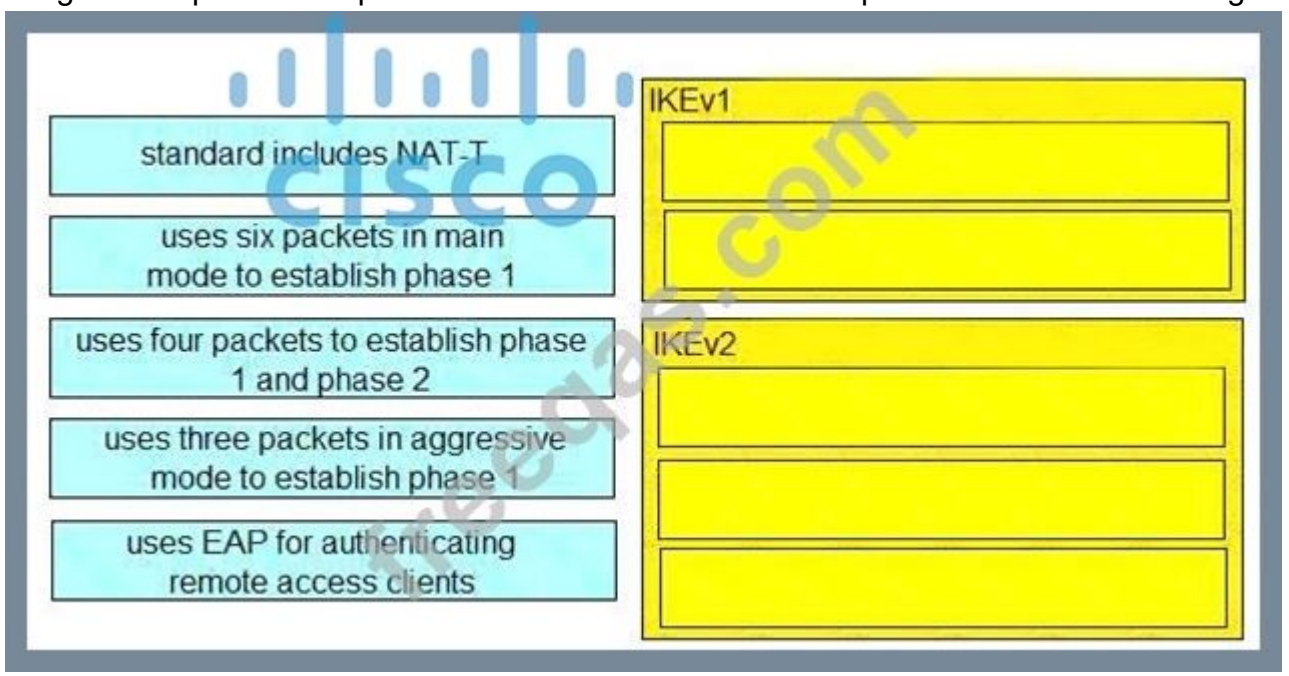


NEW QUESTION: 225
How many interfaces per bridge group does an ASA bridge group deployment support?
A. up to 4
B. up to 16
C. up to 8
D. up to 2
Answer: (SHOW ANSWER)

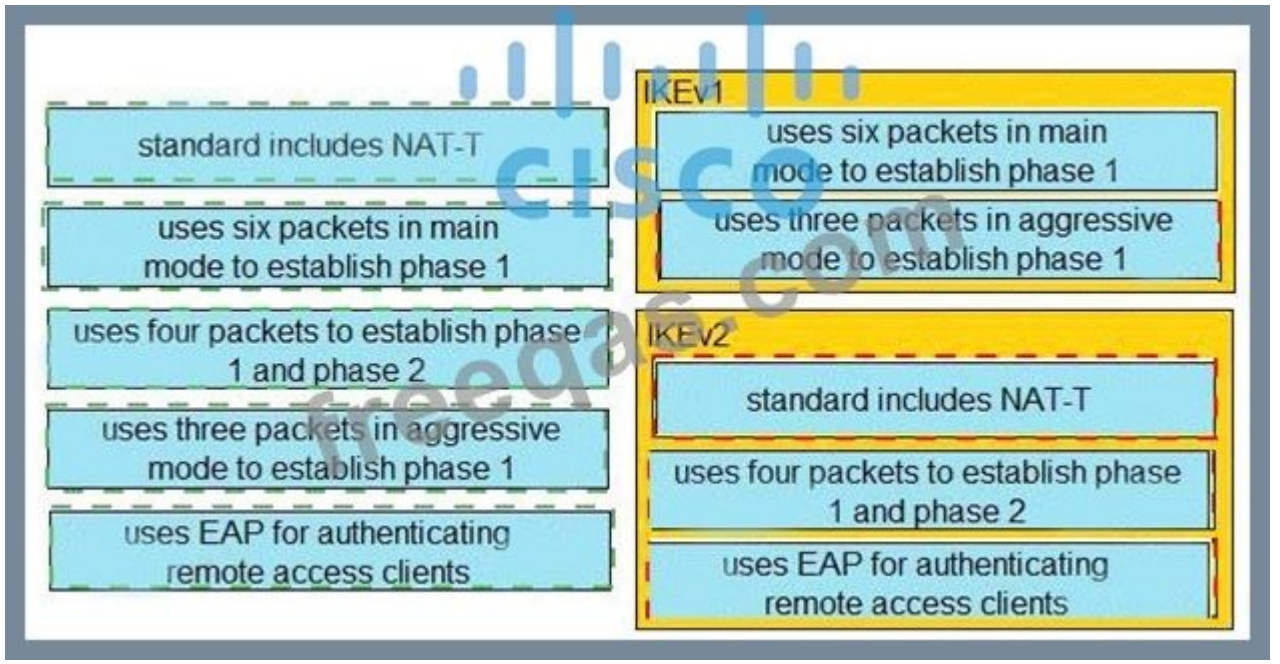
NEW QUESTION: 226
What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.) The eDirectory client must be installed on each client workstation.
A. Deploy a separate eDirectory server: the client IP address is recorded in this server
B. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.
C. Create NTLM or Kerberos authentication realm and enable transparent user identification
D. Create an LDAP authentication realm and disable transparent user identification.
Answer: (SHOW ANSWER)

NEW QUESTION: 227
What is managed by Cisco Security Manager?
A. access point
B. WSA
C. ASA
D. ESA
Answer: C (LEAVE A REPLY)
Cisco Security Manager provides a comprehensive management solution for:
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco intrusion prevention systems 4200 and 4500 Series Sensors
- Cisco AnyConnect Secure Mobility Client
Cisco Security Manager provides a comprehensive management solution for:
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco intrusion prevention systems 4200 and 4500 Series Sensors
- Cisco AnyConnect Secure Mobility Client
Cisco Security Manager provides a comprehensive management solution for:
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco intrusion prevention systems 4200 and 4500 Series Sensors
- Cisco AnyConnect Secure Mobility Client

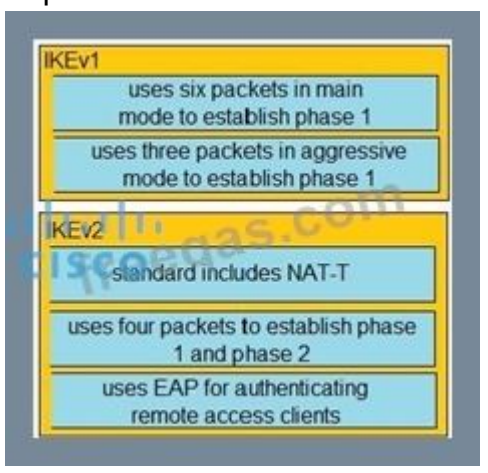
NEW QUESTION: 228
Drag and drop the descriptions from the left onto the correct protocol versions on the right.



Answer:



Explanation



NEW QUESTION: 229

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

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

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

C. The file upload is abandoned.

D. The ESA immediately makes another attempt to upload the file.

Answer: A (LEAVE A REPLY)

Explanation

- The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html

NEW QUESTION: 230

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

A. 3DES

B. RSA

C. DES
D. AES
Answer: B (LEAVE A REPLY)
Explanation
Compared to RSA, the prevalent public-key cryptography of the Internet today, Elliptic Curve Cryptography (ECC) offers smaller key sizes, faster computation,as well as memory, energy and bandwidth savings and is thus better suited forsmall devices.

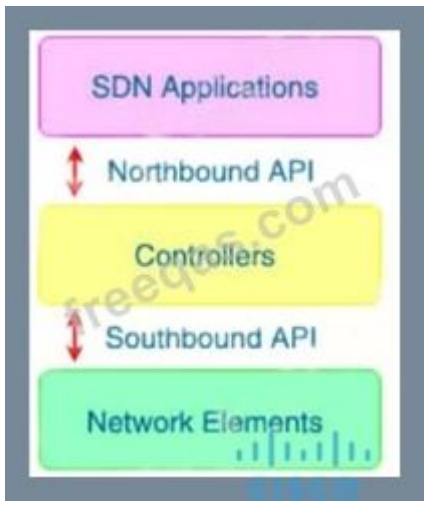
NEW QUESTION: 231
Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?
A. Nexus
B. Stealthwatch
C. Firepower
D. Tetration
Answer: D (LEAVE A REPLY)
Tetration is the solution that protects hybrid cloud deployment workloads with application visibility and segmentation. Tetration enables a zero-trust model using segmentation, which allows you to identify security incidents faster, contain lateral movement, and reduce your attack surface. Tetration supports both on-premises and public cloud workloads and provides real-time telemetry data, behavior analysis, software inventory, and policy enforcement. Tetration is part of the Cisco Zero Trust portfolio, which also includes solutions for securing the workforce and workplace. References:
* Cisco Tetration Platform - Cisco, Topic: Cisco Tetration offers holistic workload protection for multicloud data centers by enabling a zero-trust model using segmentation.
* [Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 5: Securing the Cloud, Lesson 5.3: Cloud Workload Security, Topic 5.3.1: Tetration
* Cisco Zero Trust Tetration, Topic: Tetration provides zero-trust security for workloads as part of the Cisco Zero Trust portfolio.

NEW QUESTION: 232
What does endpoint isolation in Cisco AMP for Endpoints security protect from?
A. an infection spreading across the network E
B. a malware spreading across the user device
C. an infection spreading across the LDAP or Active Directory domain from a user account
D. a malware spreading across the LDAP or Active Directory domain from a user account
Answer: (SHOW ANSWER)
https://community.cisco.com/t5/endpoint-security/amp-endpoint-isolation/td-p/4086674#:~:text=Isolating%20an

NEW QUESTION: 233
Which type of API is being used when a controller within a software-defined network architecture dynamically makes configuration changes on switches within the network?
A. westbound AP
B. southbound API
C. northbound API
D. eastbound API

Answer: B (LEAVE A REPLY)

Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs.



NEW QUESTION: 234

Which feature enables a Cisco ISR to use the default bypass list automatically for web filtering?

A. filters

B. group key

C. company key

D. connector

Answer: D (LEAVE A REPLY)

A connector is a feature that enables a Cisco ISR to use the default bypass list automatically for web filtering.

A connector is a software component that runs on the ISR and communicates with the Cloud Web Security service. The connector intercepts the web traffic from the branch users and redirects it to the Cloud Web Security service for scanning and policy enforcement. The connector also maintains a default bypass list, which contains the domains and URLs that are not redirected to the Cloud Web Security service. The default bypass list is updated automatically by the Cloud Web Security service and can be customized by the administrator. The default bypass list helps to improve the performance and reliability of the web filtering solution by avoiding unnecessary redirections of trusted or sensitive web traffic12. References: 1: Security Configuration Guide: Cloud Web Security, Cisco IOS Release 15M&T - Cisco Integrated Services Routers Generation 2 with Cisco Cloud Web Security Solution [Support] - Cisco 2: Security Configuration Guide:
Cloud Web Security, Cisco IOS Release 15M&T - Configuring Cloud Web Security on Integrated Services Routers Generation 2 [Support] - Cisco

NEW QUESTION: 235

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

A. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.

B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.

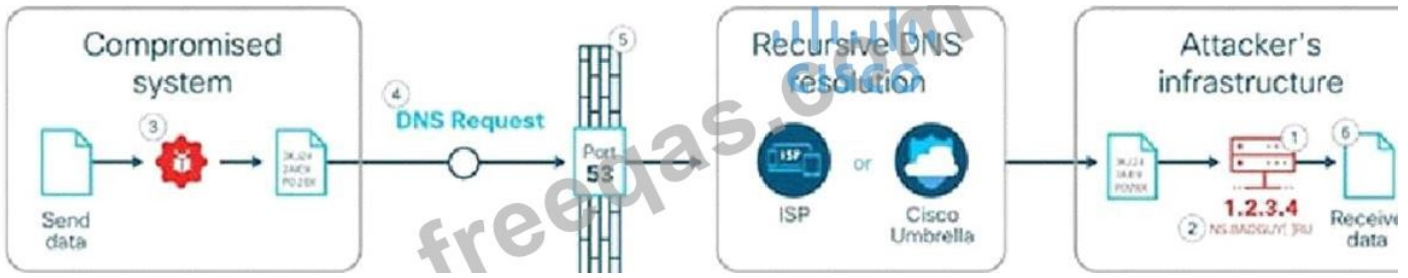
C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network.

D. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.

Answer: B (LEAVE A REPLY)

ExplanationDomain name system (DNS) is the protocol that translates human-friendly URLs, such as securitytut.com, into IP addresses, such as 183.33.24.13. Because DNS messages are only used as the beginning of each communication and they are not intended for data transfer,

many organizations do not monitor their DNS traffic for malicious activity. As a result, DNS-based attacks can be effective if launched against their networks. DNS tunneling is one such attack.An example of DNS Tunneling is shown below:

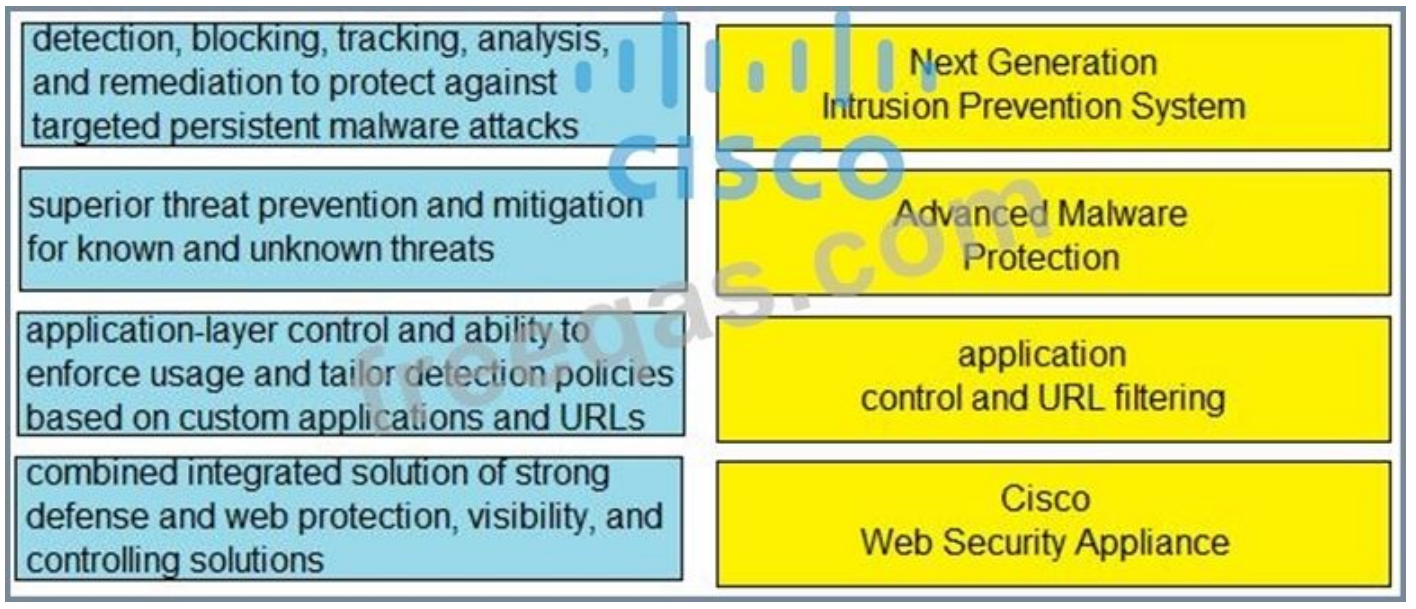


* The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNSnameserver (NS) and malicious payload.2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. attackerdomain.com) is registered or reused. The registrar informs the top-level domain (.com) nameservers to refer requests for attackerdomain.com to ns.attackerdomain.com, which has a DNS record mapped to 1.2.3.43. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a

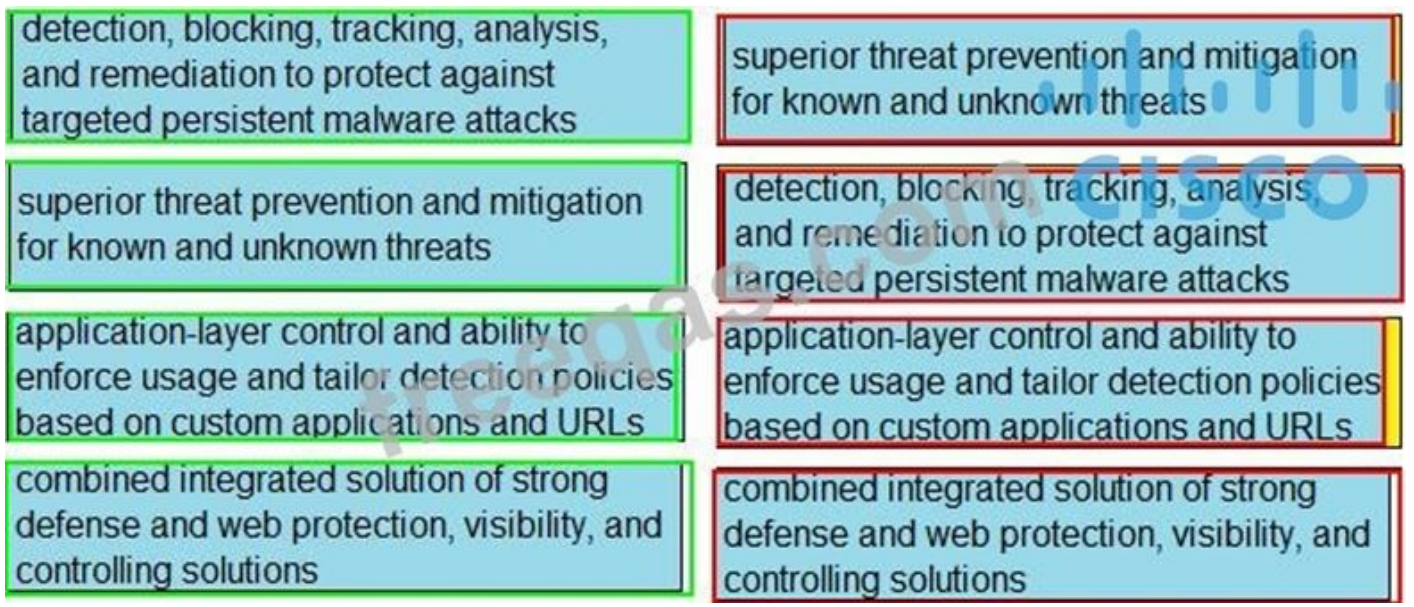
* series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, P028X977W,...).4. The payload initiates thousands of unique DNS record requests to the attacker's domain with each string as Reference: https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0

NEW QUESTION: 236

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



Answer:



NEW QUESTION: 237

What is a feature of container orchestration?

A. ability to deploy Kubernetes clusters in air-gapped sites

B. ability to deploy Amazon ECS clusters by using the Cisco Container Platform data plane

C. ability to deploy Amazon EKS clusters by using the Cisco Container Platform data plane

D. automated daily updates

Answer: (SHOW ANSWER)

NEW QUESTION: 238

Refer to the exhibit When configuring this access control rule in Cisco FMC, what happens with the traffic destined to the DMZjnside zone once the configuration is deployed?

A. No traffic will be allowed through to the DMZ_inside zone regardless of if it's trusted or not

B. All traffic from any zone to the DMZ_inside zone will be permitted with no further inspection

C. All traffic from any zone will be allowed to the DMZ_inside zone only after inspection

D. No traffic will be allowed through to the DMZ_inside zone unless it's already trusted

Answer: (SHOW ANSWER)

NEW QUESTION: 239

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

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

B. Set the tunnel to go through the Cisco FTD

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

D. Set the tunnel port to 8305

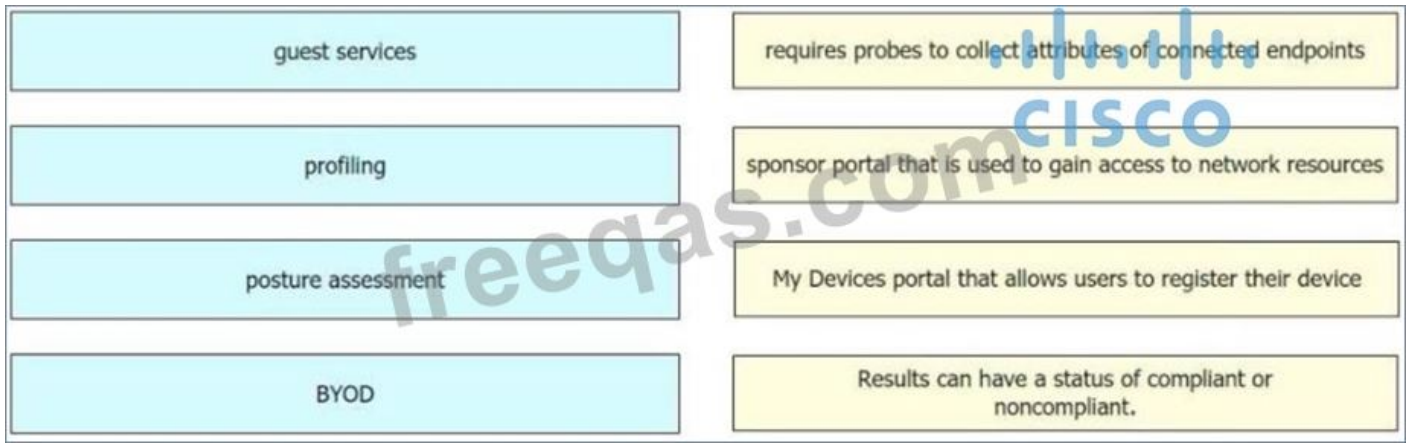
The FMC and managed devices communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305.

Answer: (SHOW ANSWER)

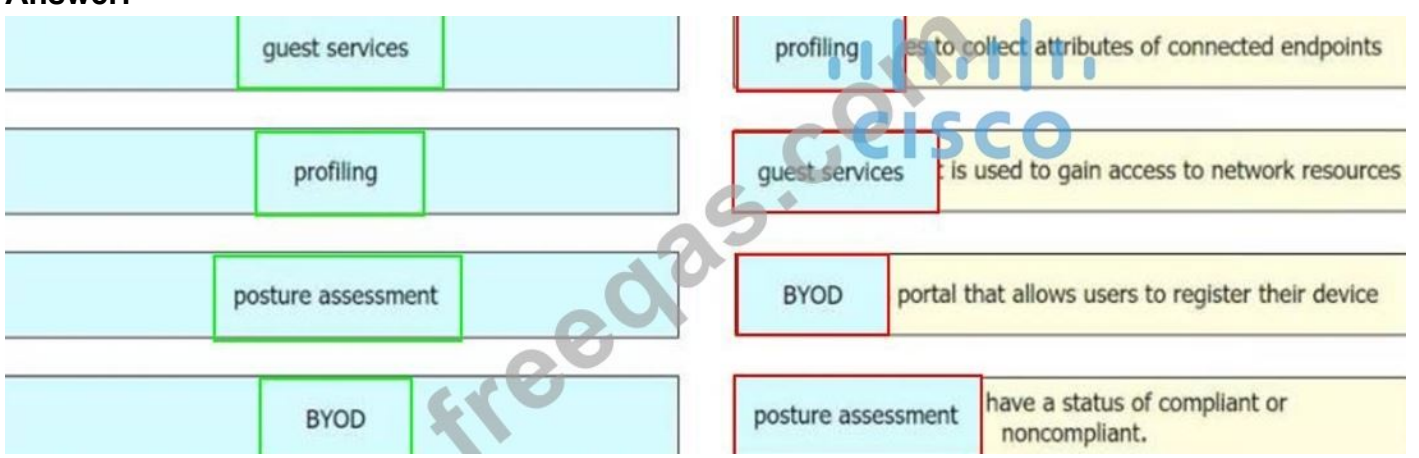
Cisco strongly recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate with each other.

NEW QUESTION: 240
When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, which name is used?
A. Common Vulnerabilities and Exposures
B. Common Exploits and Vulnerabilities
C. Common Security Exploits
D. Common Vulnerabilities, Exploits and Threats
Answer: A (LEAVE A REPLY)
Explanation
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cve/174/cve-addressed-1741.html

NEW QUESTION: 241
Drag and drop the concepts from the left onto the correct descriptions on the right

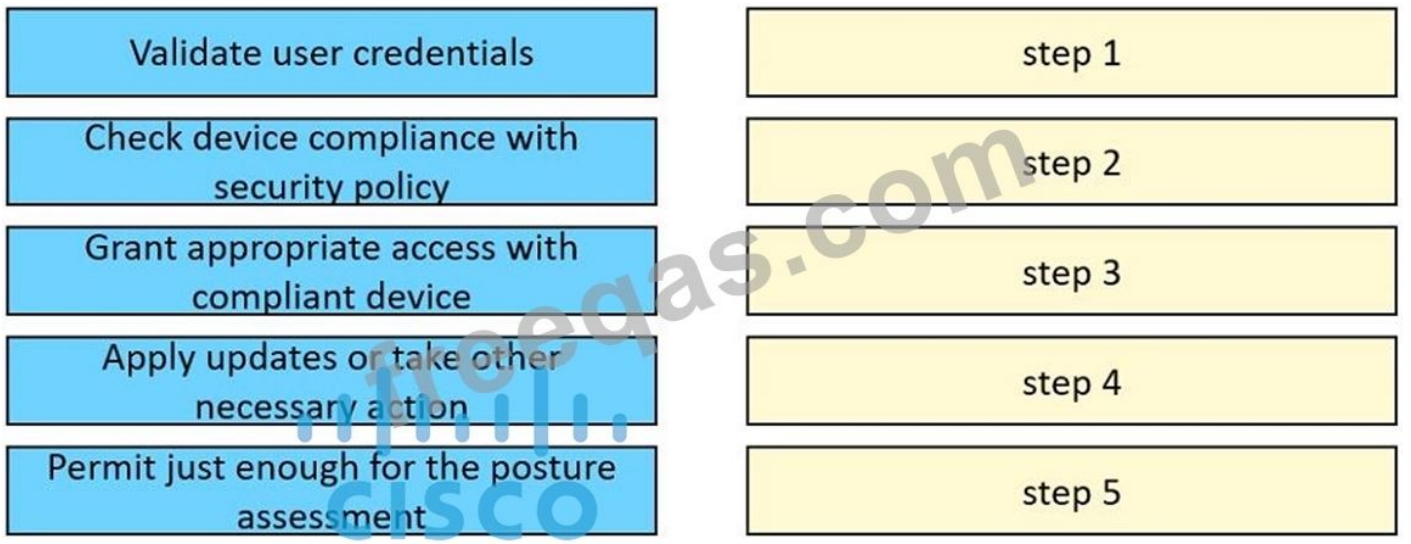


Answer:

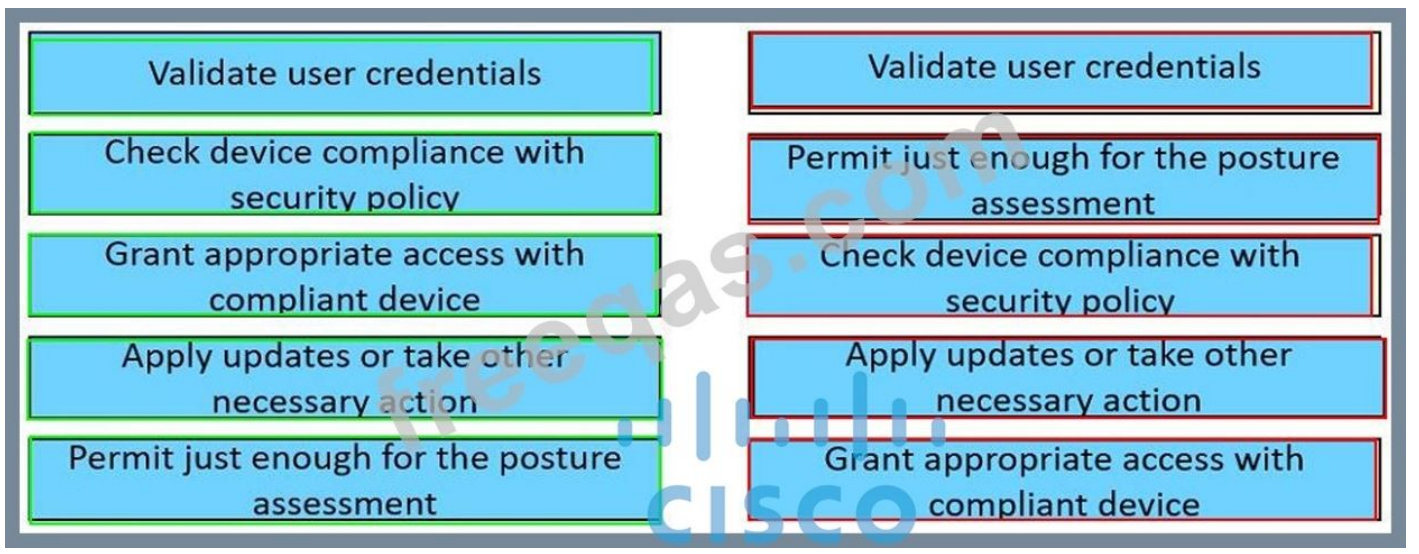


NEW QUESTION: 242

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



Answer:



NEW QUESTION: 243

Which two key and block sizes are valid for AES? (Choose two)

A. 64-bit block size, 112-bit key length

B. 64-bit block size, 168-bit key length

C. 128-bit block size, 192-bit key length

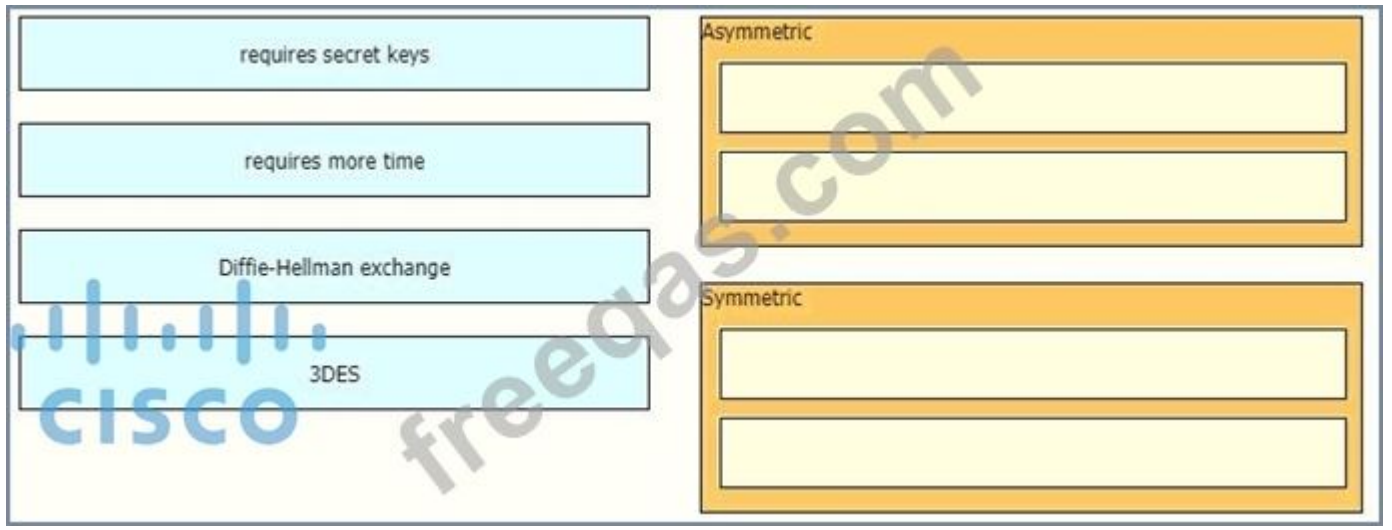
D. 128-bit block size, 256-bit key length

E. 192-bit block size, 256-bit key length

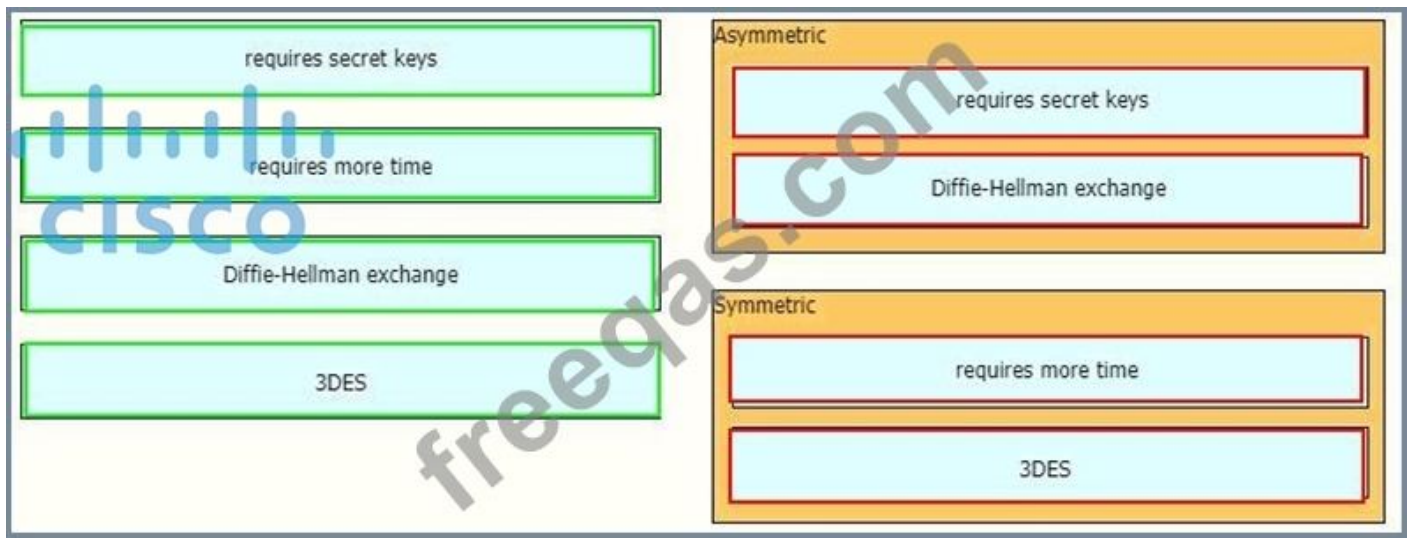
Answer: C,D (LEAVE A REPLY)

ExplanationThe AES encryption algorithm encrypts and decrypts data in blocks of 128 bits (block size). It can do this using 128-bit, 192-bit, or 256-bit keys

NEW QUESTION: 244
Drag and drop the descriptions from the left onto the encryption algorithms on the right.



Answer:



NEW QUESTION: 245
An engineer configured a new network identity in Cisco Umbrella but must verify that traffic is being routed through the Cisco Umbrella network.
Which action tests the routing?
A. Ensure that the client computers are pointing to the on-premises DNS servers.
B. Enable the Intelligent Proxy to validate that traffic is being routed correctly.
C. Add the public IP address that the client computers are behind to a Core Identity.
D. Browse to http://welcome.umbrella.com/ to validate that the new identity is working.
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 246
What are two DDoS attack categories? (Choose two.)
A. protocol
B. volume-based

C. sequential
D. source-based
E. database
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 247
What is the concept of CI/CD pipelining?
A. The project is split into several phases where one phase cannot start before the previous phase finishes successfully.
B. The project code is centrally maintained and each code change should trigger an automated build and test sequence
C. The project is split into time-limited cycles and focuses on pair programming for continuous code review
D. Each project phase is independent from other phases to maintain adaptiveness and continual improvement
Answer: B (LEAVE A REPLY)
CI/CD pipelining is a method of software development that aims to deliver software faster and more reliably by automating the process of integrating, testing, and deploying code changes. CI stands for continuous integration, which means that every code change is merged into a shared repository and verified by automated tests. CD stands for continuous delivery, which means that the code is always in a deployable state and can be released to production environments with minimal human intervention. CI/CD pipelining enables developers to collaborate more effectively, detect and fix errors earlier, and deliver value to customers more frequently.
CI/CD pipelining is a key practice of DevOps, a culture and set of processes that bridge the gap between development and operations teams.
References:
https://www.redhat.com/en/topics/devops/what-cicd-pipeline
https://about.gitlab.com/topics/ci-cd/cicd-pipeline/

NEW QUESTION: 248
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)
A. Patch for cross-site scripting.
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.
D. Install a spam and virus email filter.
E. Protect systems with an up-to-date antimalware program
Answer: D,E (LEAVE A REPLY)
Explanation
Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

NEW QUESTION: 249
Which portion of the network do EPP solutions solely focus on and EDR solutions do not?
A. server farm
B. perimeter
C. core
D. East-West gateways
Answer: B (LEAVE A REPLY)

EPP solutions solely focus on the perimeter of the network, which is the boundary between the internal and external networks. The perimeter is where most of the endpoints, such as laptops, desktops, mobile devices, and IoT devices, are located and connected to the network. EPP solutions aim to prevent, detect, and remediate security threats on these endpoints by using technologies such as antivirus, data encryption, and data loss prevention. EPP solutions rely on signatures and other indicators of intrusion by known threats to block malicious activity and malware on the endpoints12.
EDR solutions do not focus on the perimeter, but rather on the entire network, including the core and the East-West gateways. The core is the central part of the network that connects different segments and provides high-speed data transmission. The East-West gateways are the points of communication between different segments within the network, such as between different data centers or cloud environments. EDR solutions provide continuous and comprehensive visibility into endpoint activities across the network by using threat hunting tools for behavior-based endpoint threat detection. EDR solutions monitor and record endpoint data, detect anomalies and malicious behavior, and respond to threats that EPP and other security tools did not catch. EDR solutions also enable security teams to proactively investigate and contain incidents by using incident data search, alert triage, threat validation, and malicious activity blocking134.
References := 1: EPP vs. EDR: Why You Need Both - CrowdStrike 2: Comparing endpoint security: EPP vs.
EDR vs. XDR | Infosec 3: EDR vs EPP: What is the Difference? - Exabeam 4: EDR vs EPP: Key Features, Differences, and How They Work Together

NEW QUESTION: 250
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: A,E (LEAVE A REPLY)
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.
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.
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:
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.
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
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: 251
What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?
A. trusted automated exchange
B. Indicators of Compromise
C. The Exploit Database
D. threat intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 252
An engineer is implementing NTP authentication within their network and has configured both the client and server devices with the command ntp authentication-key 1 md5 Cisc392368270. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however it is unable to do so. Which command is required to enable the client to accept the server's authentication key?
A. ntp peer 1.1.1.1 key 1
B. ntp server 1.1.1.1 key 1
C. ntp server 1.1.1.2 key 1
D. ntp peer 1.1.1.2 key 1
Answer: B (LEAVE A REPLY)
To configure an NTP enabled router to require authentication when other devices connect to it, use the following commands:
NTP_Server(config)#ntp authentication-key 2 md5 securitytut

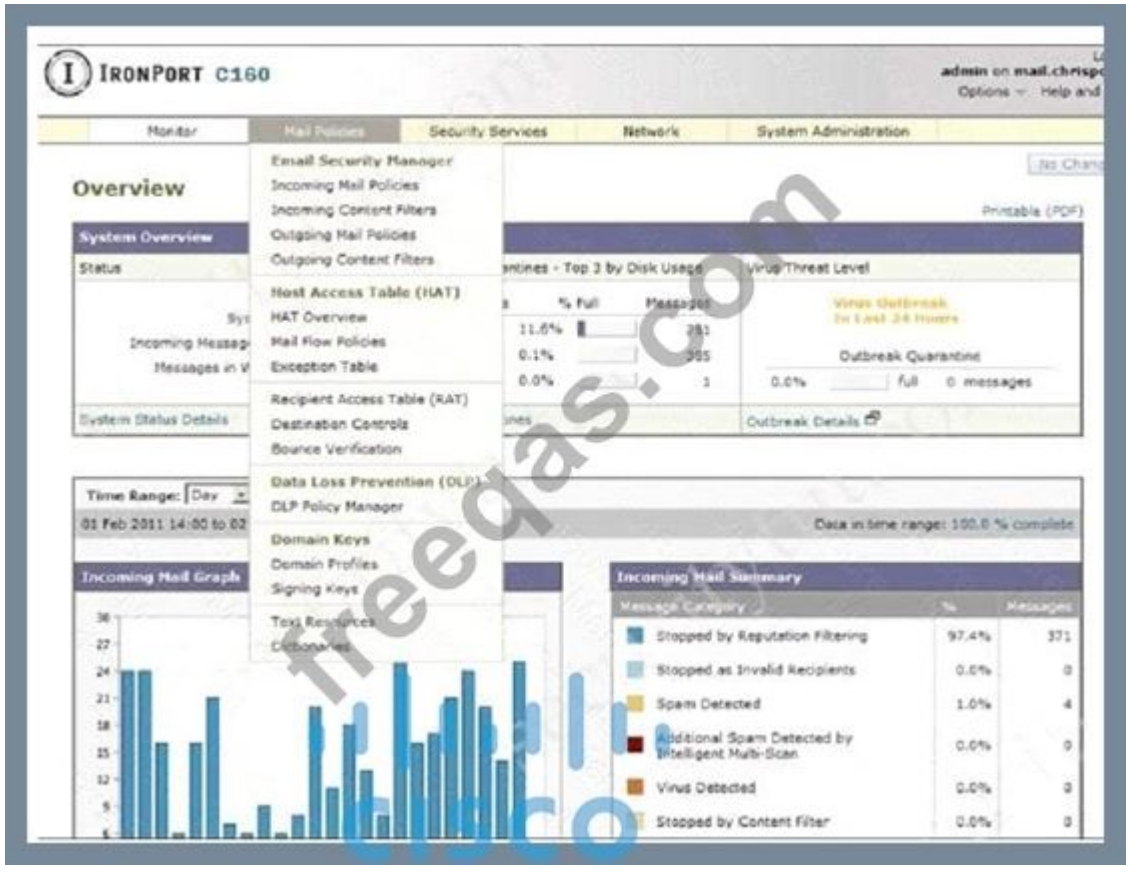
NTP_Server(config)#ntp authenticate
NTP_Server(config)#ntp trusted-key 2
Then you must configure the same authentication-key on the client router:
NTP_Client(config)#ntp authentication-key 2 md5 securitytut
NTP_Client(config)#ntp authenticate
NTP_Client(config)#ntp trusted-key 2
NTP_Client(config)#ntp server 10.10.10.1 key 2
Note: To configure a Cisco device as a NTP client, use the command ntp server <IP address>. For example:
Router(config)#ntp server 10.10.10.1. This command will instruct the router to query 10.10.10.1 for the time.

NEW QUESTION: 253
Refer to the exhibit.

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

A network administrator configures command authorization for the admm5 user. What is the admin5 user able to do on HQ_Router after this configuration?
A. add subinterfaces
B. complete all configurations
C. complete no configurations
D. set the IP address of an interface
Answer: C (LEAVE A REPLY)

NEW QUESTION: 254
An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically.
What must be configured to accomplish this?
A. Configure the Cisco WSA to modify policies based on the traffic seen
B. Configure the Cisco ESA to receive real-time updates from Talos
C. Configure the Cisco WSA to receive real-time updates from Talos
D. Configure the Cisco ESA to modify policies based on the traffic seen
Answer: (SHOW ANSWER)
ExplanationExplanationThe Mail Policies menu is where almost all of the controls related to email filtering happens. All the security and content filtering policies are set here, so it's likely that, as an ESA administrator, the pages on this menu are where you are likely to spend most of your time.



NEW QUESTION: 255
An organization has a Cisco ESA set up with policies and would like to customize the action assigned for violations. The organization wants a copy of the message to be delivered with a message added to flag it as a DLP violation. Which actions must be performed in order to provide this capability?
A. deliver and add disclaimer text
B. deliver and send copies to other recipients
C. quarantine and alter the subject header with a DLP violation
D. quarantine and send a DLP violation notification
Answer: C (LEAVE A REPLY)

NEW QUESTION: 256
Which two features of Cisco Email Security can protect your organization against email threats? (Choose two)
A. Time-based one-time passwords
B. Data loss prevention
C. Heuristic-based filtering
D. Geolocation-based filtering
E. NetFlow
Answer: B,D (LEAVE A REPLY)
Explanation : Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution. Cisco Email Security appliance can now handle incoming mail connections and incoming messages from specific geolocations and perform appropriate actions on them, for example: - Prevent email threats coming from specific geographic regions. - Allow or disallow emails coming from specific geographic regions. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/

b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_00.html Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution.
Cisco Email Security appliance can now handle incoming mail connections and incoming messages from specific geolocations and perform appropriate actions on them, for example:
- Prevent email threats coming from specific geographic regions.
- Allow or disallow emails coming from specific geographic regions.
Reference:
Explanation : Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution. Cisco Email Security appliance can now handle incoming mail connections and incoming messages from specific geolocations and perform appropriate actions on them, for example: - Prevent email threats coming from specific geographic regions. - Allow or disallow emails coming from specific geographic regions. Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_00.html

NEW QUESTION: 257
What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?
A. trusted automated exchange
B. Indicators of Compromise
C. The Exploit Database
D. threat intelligence
Answer: D (LEAVE A REPLY)
Threat intelligence is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems. Threat intelligence is the result of collecting, analyzing, and contextualizing data from various sources, such as network traffic, logs, feeds, reports, etc. Threat intelligence provides insights into the tactics, techniques, and procedures (TTPs) of adversaries, as well as their motivations, intentions, and capabilities. Threat intelligence can help organizations to detect, prevent, and respond to cyberattacks, as well as to improve their security posture and resilience12.
The other options are not correct, because they are not terms for having information about threats and threat actors. Trusted automated exchange is a concept that refers to the sharing of threat intelligence among trusted entities in a timely and secure manner3. Indicators of Compromise (IoCs) are pieces of forensic data, such as IP addresses, domains, hashes, etc., that indicate a potential intrusion or compromise of a system or network.
The Exploit Database is a public repository of exploits and vulnerable software, maintained by Offensive Security. References:
* 1: What is Cyber Threat Intelligence? - Cisco
* 2: Cisco Talos Intelligence Group - Comprehensive Threat Intelligence
* 3: Trusted Automated Exchange of Intelligence Information (TAXII) Version 2.0

* [4]: What Are Indicators of Compromise (IOCs)? - Cisco
* [5]: The Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers

NEW QUESTION: 258
Which two capabilities of Integration APIs are utilized with Cisco DNA center? (Choose two)
A. Upgrade software on switches and routers
B. Automatically deploy new virtual routers
C. Create new SSIDs on a wireless LAN controller
D. Third party reporting
E. Connect to ITSM platforms
Answer: (SHOW ANSWER)

NEW QUESTION: 259
What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?
A. It deletes any application that does not belong in the network
B. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously
C. It discovers and controls cloud apps that are connected to a company's corporate environment
D. It sends the application information to an administrator to act on
Answer: C (LEAVE A REPLY)

NEW QUESTION: 260
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: D (LEAVE A REPLY)

NEW QUESTION: 261
What is the most commonly used protocol for network telemetry?
A. NctFlow
B. TFTP
C. SNMP
D. SMTP
Answer: (SHOW ANSWER)

NEW QUESTION: 262
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. SAML server
C. Method
D. AAA server group
Answer: C (LEAVE A REPLY)

NEW QUESTION: 263

Interface	MAC Address	Method	Domain	Status	Fg Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth	0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth	0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth	0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth	0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth	0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth	0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth	0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth	0A02198200000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth	0A02198200001
Gi10/29	0026.0b5e.52a8	dot1x	VOICE	Auth	0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth	0A02198200000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth	0A02198200000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth	0A02198200000
Gi7/4	54ee.75db.d766	dot1x	DATA	Auth	0A02198200001
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth	0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth	0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth	0A02198200000

Refer to the exhibit. Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?
A. show dot1x all
B. show authentication method
C. show authentication sessions
D. show authentication registrations
Answer: B (LEAVE A REPLY)

NEW QUESTION: 264
Which component of Cisco umbrella architecture increases reliability of the service?
A. Anycast IP
B. Cisco Talos
C. BGP route reflector
D. AMP Threat grid
Answer: B (LEAVE A REPLY)

NEW QUESTION: 265
Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two)
A. Block SQL code execution in the web application database login.
B. Check integer, float, or Boolean string parameters to ensure accurate values.
C. Write SQL code instead of using object-relational mapping libraries.
D. Use prepared statements and parameterized queries.

E. Secure the connection between the web and the app tier.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 266
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: D (LEAVE A REPLY)
Installing the Cisco Umbrella root CA onto the user's device is the action that accomplishes the goal of inspecting traffic without alerting end-users. This is because the root CA allows the user's device to trust the certificates issued by the Cisco Umbrella intelligent proxy, which acts as a man-in-the-middle for SSL sites on Umbrella's grey list. Without the root CA, the user's browser would raise errors when accessing those sites, as it would detect an untrusted certificate. By installing the root CA, the user's browser would accept the certificate and allow the traffic to be proxied and inspected by the intelligent proxy. References:
* Enable SSL Decryption - Umbrella User Guide
* SSL Decryption in the Intelligent Proxy - Cisco Umbrella
* Cisco Umbrella Intelligent Proxy and SSL Decryption
* Intelligent Proxy and SSL Decryption with Cisco Umbrella

NEW QUESTION: 267
How is DNS tunneling used to exfiltrate data out of a corporate network?
A. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.
B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.
C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network.
D. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 268
An organization has a Cisco ESA set up with DLP policies and would like to customize the action assigned for violations. The organization wants a copy of the message to be delivered with a message added to flag it as a DLP violation. Which actions must be performed in order to provide this capability?
A. quarantine and alter the subject header with a DLP violation
B. deliver and add disclaimer text
C. deliver and send copies to other recipients
D. quarantine and send a DLP violation notification
Answer: D (LEAVE A REPLY)

NEW QUESTION: 269

A network administrator is configuring a rule in an access control policy to block certain URLs and selects the "Chat and Instant Messaging" category. Which reputation score should be selected to accomplish this goal?

A. 1

B. 3

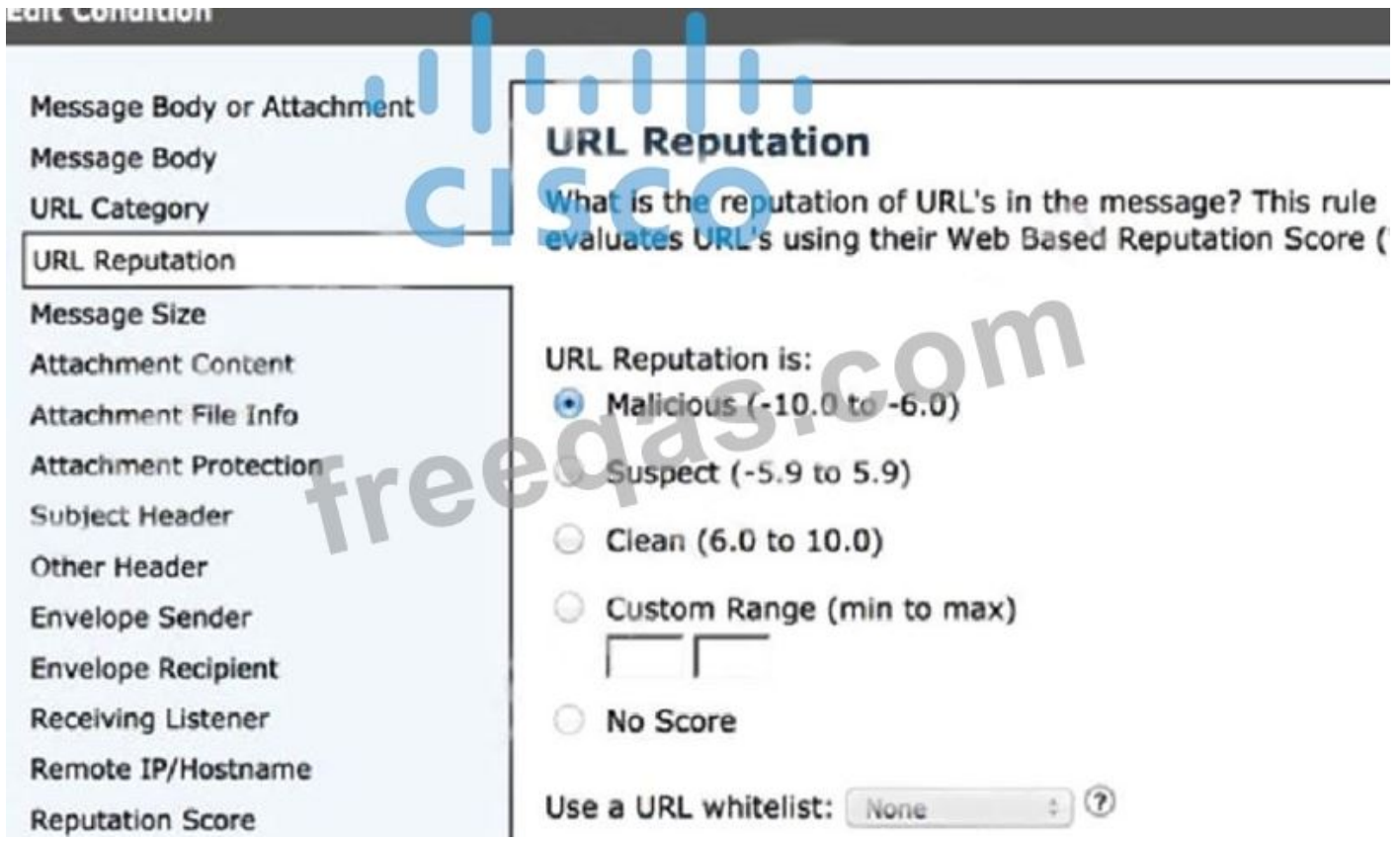
C. 5

D. 10

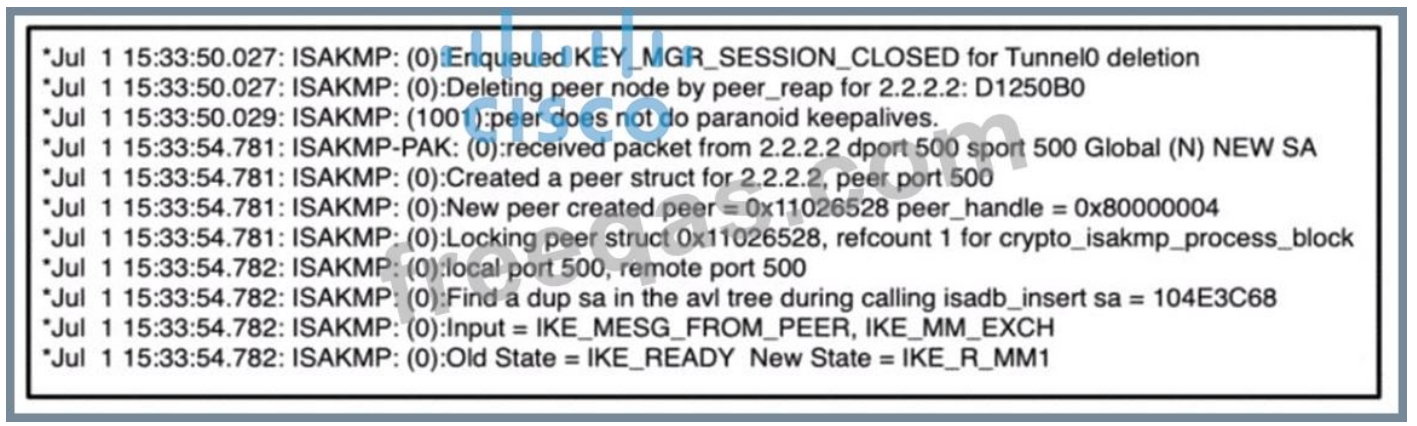
Answer: (SHOW ANSWER)

We choose "Chat and Instant Messaging" category in "URL Category":

To block certain URLs we need to choose URL Reputation from 6 to 10.



NEW QUESTION: 270
Refer to the exhibit,



which command results in these messages when attempting to troubleshoot an iPsec VPN connection?

A. debug crypto isakmp

B. debug crypto ipsec endpoint

C. debug crypto Ipsec

D. debug crypto isakmp connection

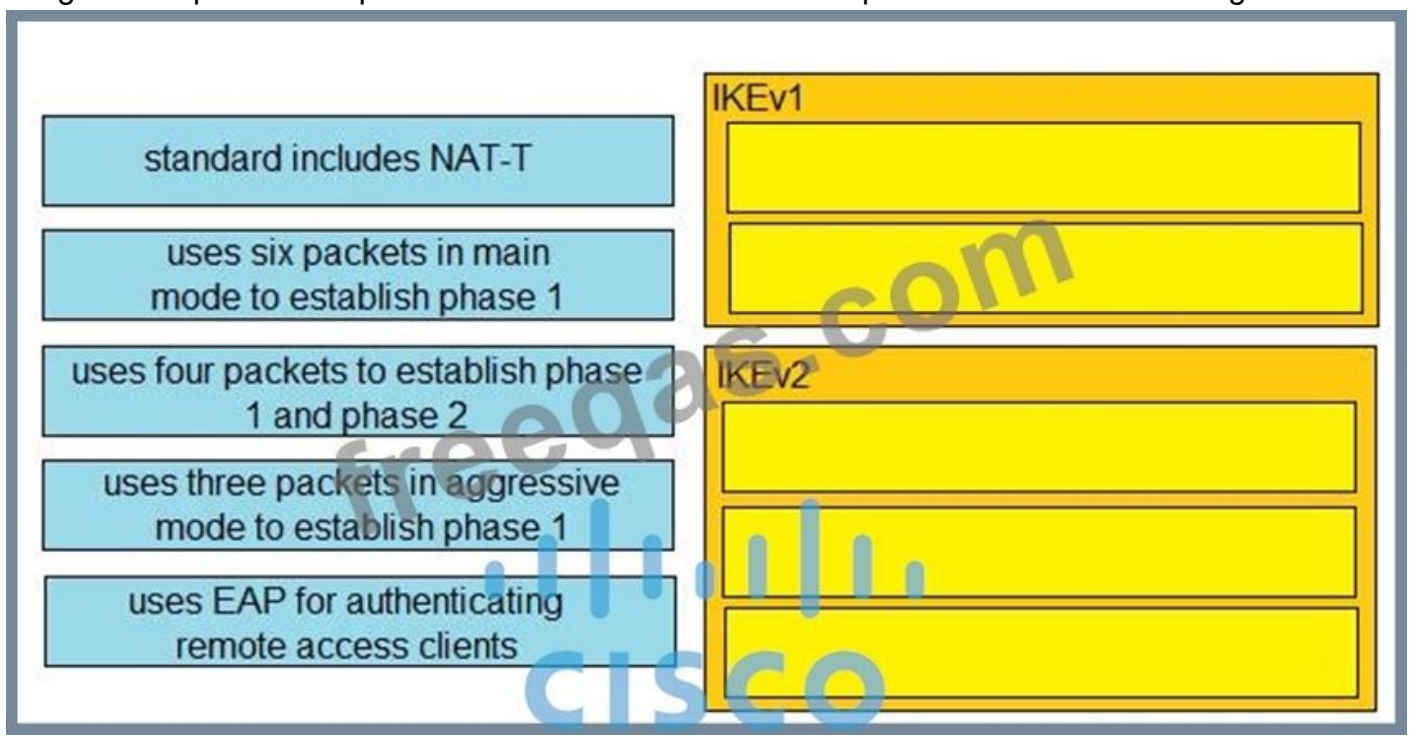
Answer: (SHOW ANSWER)

The command that results in these messages when attempting to troubleshoot an iPsec VPN connection is debug crypto isakmp. This command displays debug information about the Internet Key Exchange (IKE) protocol, which is used to establish security associations (SAs) for IPsec VPNs. The messages in the exhibit show various steps and statuses of the IKE negotiation process, such as creating and deleting peer structures, receiving and sending packets, and checking the compatibility of the security policies and proposals. The other commands are either invalid (debug crypto ipsec endpoint and debug crypto isakmp connection) or display different information (debug crypto ipsec shows the details of the IPsec encryption and decryption operations). References:

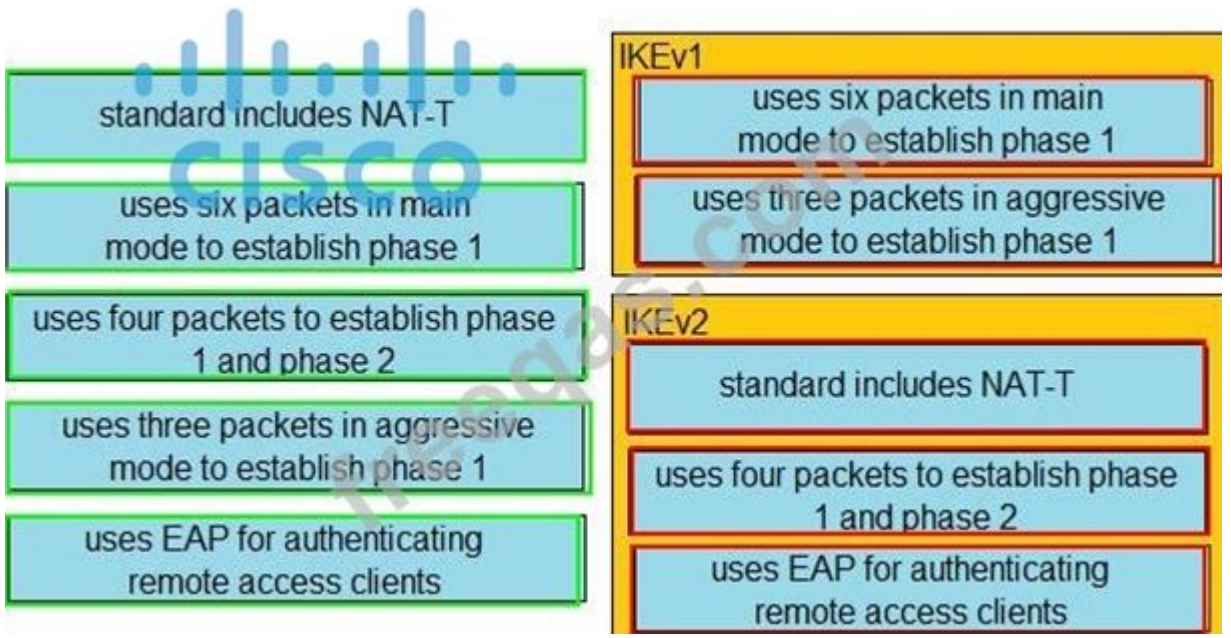
https://www.cisco.com/c/en/us/training-events/training-certifications/training/training-services/courses/implemen
https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.h

NEW QUESTION: 271
What is the benefit of integrating Cisco ISE with a MDM solution?
A. It provides compliance checks for access to the network
B. It provides the ability to update other applications on the mobile device
C. It provides the ability to add applications to the mobile device through Cisco ISE
D. It provides network device administration access
Answer: A (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/ m_ise_interoperability_mdm.html

NEW QUESTION: 272
Drag and drop the descriptions from the left onto the correct protocol versions on the right.



Answer:



NEW QUESTION: 273

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

A. Orchestration

B. CI/CD pipeline

C. Container

D. Security

Answer: B (LEAVE A REPLY)

Unlike the traditional software life cycle, the CI/CD implementation process gives a weekly or daily update instead of monthly or quarterly. The fun part is customers won't even realize the update is in their applications, as they happen on the fly.

Unlike the traditional software life cycle, the CI/CD implementation process gives a weekly or daily update instead of monthly or quarterly. The fun part is customers won't even realize the update is in their applications, as they happen on the fly.

Reference:

Unlike the traditional software life cycle, the CI/CD implementation process gives a weekly or daily update instead of monthly or quarterly. The fun part is customers won't even realize the update is in their applications, as they happen on the fly.

NEW QUESTION: 274

A Cisco Firepower administrator needs to configure a rule to allow a new application that has never been seen on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose two)

A. permit

B. trust

C. reset

D. allow

E. monitor

Answer: B,E (LEAVE A REPLY)

Explanation

Explanation

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: 275
An organization has noticed an increase in malicious content downloads and wants to use Cisco Umbrella to prevent this activity for suspicious domains while allowing normal web traffic. Which action will accomplish this task?
A. Set content settings to High
B. Configure the intelligent proxy.
C. Use destination block lists.
D. Configure application block lists.
Answer: B (LEAVE A REPLY)
Obviously, if you allow all traffic to these risky domains, users might access malicious content, resulting in an infection or data leak. But if you block traffic, you can expect false positives, an increase in support inquiries, and thus, more headaches. By only proxying risky domains, the intelligent proxy delivers more granular visibility and control.
The intelligent proxy bridges the gap by allowing access to most known good sites without being proxied and only proxying those that pose a potential risk. The proxy then filters and blocks against specific URLs hosting malware while allowing access to everything else.
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.
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.

NEW QUESTION: 276
What provides visibility and awareness into what is currently occurring on the network?
A. CMX
B. WMI
C. Prime Infrastructure
D. Telemetry
Answer: D (LEAVE A REPLY)
Telemetry - Information and/or data that provides awareness and visibility into what is occurring on the network at any given time from networking devices, appliances, applications or servers in which the core function of the device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks.
Telemetry - Information and/or data that provides awareness and visibility into what is occurring on the network at any given time from networking devices, appliances, applications or servers in which the core function of the device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks.

Telemetry - Information and/or data that provides awareness and visibility into what is occurring on the network at any given time from networking devices, appliances, applications or servers in which the core function of the device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks.

NEW QUESTION: 277
An organization is receiving SPAM emails from a known malicious domain What must be configured in order to prevent the session during the initial TCP communication?
A. Configure the Cisco ESA to drop the malicious emails.
B. Configure policies to quarantine malicious emails.
C. Configure policies to stop and reject communication
D. Configure the Cisco ESA to reset the TCP connection.
Answer: B (LEAVE A REPLY)
Explanation
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118219-configure-esa-00.html

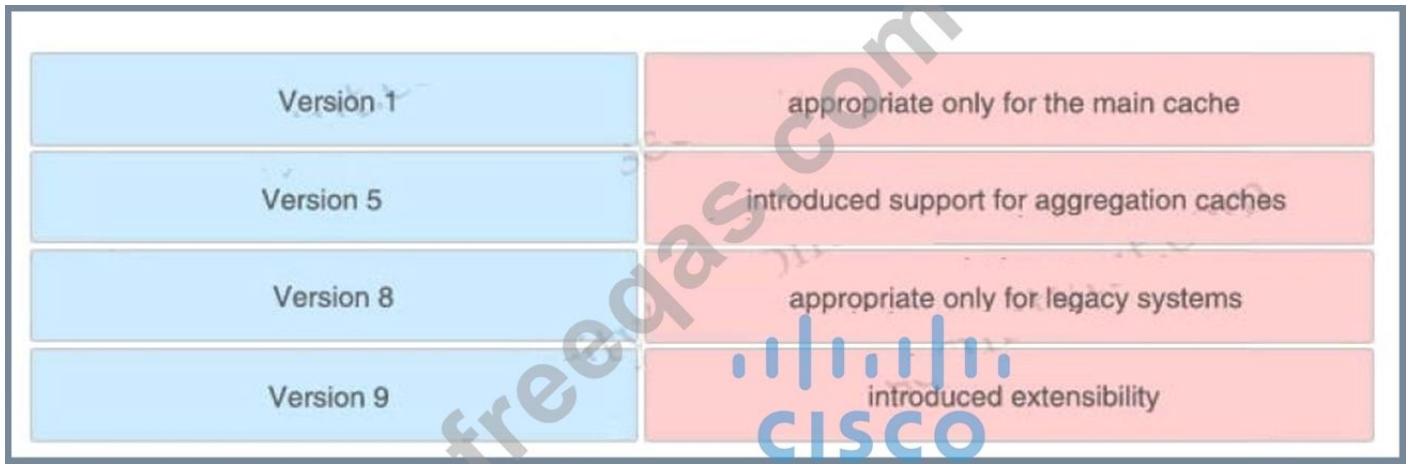
NEW QUESTION: 278
What is a key difference between Cisco Firepower and Cisco ASA?
A. Cisco ASA provides access control while Cisco Firepower does not.
B. Cisco Firepower provides identity-based access control while Cisco ASA does not.
C. Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not.
D. Cisco ASA provides SSL inspection while Cisco Firepower does not.
Answer: (SHOW ANSWER)
Reference:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-firepowerservices/200451-Configure-Intrusion-Policy-and-Signature.html

NEW QUESTION: 279
An email administrator is setting up a new Cisco ESA. The administrator wants to enable the blocking of greymail for the end user. Which feature must the administrator enable first?
A. Intelligent Multi-Scan
B. Anti-Virus Filtering
C. IP Reputation Filtering
D. File Analysis
Answer: A (LEAVE A REPLY)

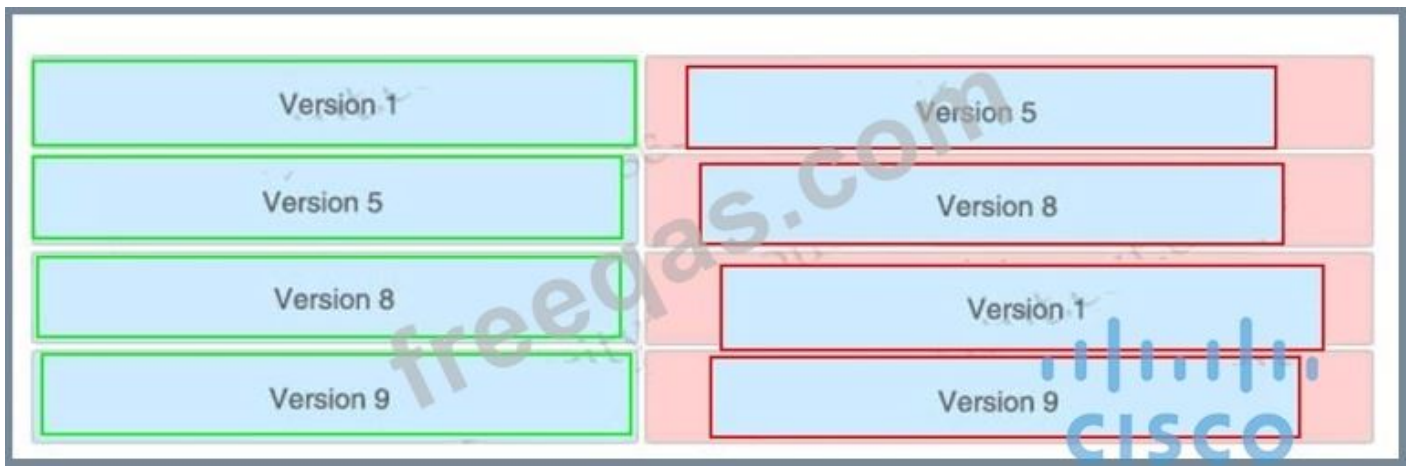
NEW QUESTION: 280
Refer to the exhibit. An administrator is adding a new Cisco FTD device to their network and wants to manage it with Cisco FMC. The Cisco FTD uses a registration key of Cisc392368270 and is not behind a NAT device, Which command is needed to enable this on the Cisco FTD?
A. configure manager add <FMC IP address> <registration key>
B. configure manager add DONTRESOLVE kregistration key>
C. configure manager add DONTRESOLVE <registration key> FTD123
D. configure manager add <FMC IP address> <registration key> 16

Answer: A (LEAVE A REPLY)

NEW QUESTION: 281
Drag and drop the NetFlow export formats from the left onto the descriptions on the right.



Answer:



NEW QUESTION: 282
An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices. The default management port conflicts with other communications on the network and must be changed. What must be done to ensure that all devices can communicate together?
A. Manually change the management port on Cisco FMC and all managed Cisco FTD devices
B. Set the tunnel to go through the Cisco FTD
C. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices
D. Set the tunnel port to 8305
Answer: A (LEAVE A REPLY)
The FMC and managed devices communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305. Cisco strongly recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate with each other.

NEW QUESTION: 283
When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

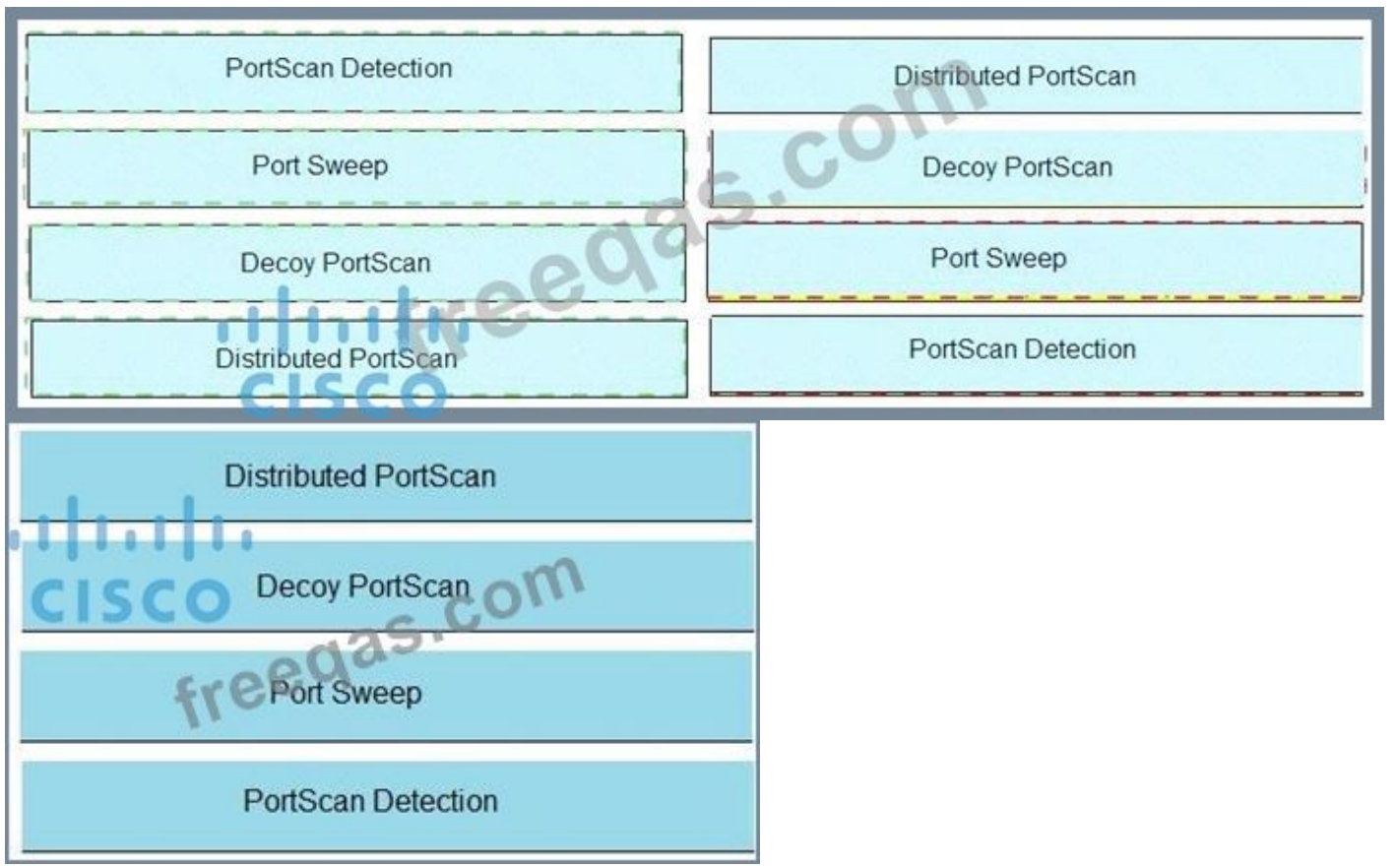
A. File Analysis
B. Content Category Blocking
C. Application Control
D. Security Category Blocking
Answer: D (LEAVE A REPLY)

NEW QUESTION: 284
Using Cisco Cognitive Threat Analytics, which platform automatically blocks risky sites, and test unknown sites for hidden advanced threats before allowing users to click them?
A. Cisco Identity Services Engine (ISE)
B. Cisco Enterprise Security Appliance (ESA)
C. Cisco Web Security Appliance (WSA)
D. Cisco Advanced Stealthwatch Appliance (ASA)
Answer: C (LEAVE A REPLY)
Cisco Web Security Appliance (WSA) is the platform that automatically blocks risky sites, and tests unknown sites for hidden advanced threats before allowing users to click them, using Cisco Cognitive Threat Analytics.
Cisco Cognitive Threat Analytics is a cloud-based solution that reduces the time to discovery of threats operating inside the network by analyzing web traffic and detecting anomalous behavior. Cisco WSA integrates with Cisco Cognitive Threat Analytics to provide enhanced web security and breach detection.
Cisco WSA can also leverage other Cisco security solutions, such as Cisco Umbrella, Cisco Advanced Malware Protection (AMP), and Cisco Talos Intelligence Group, to provide comprehensive web security. References:
* Cisco Web Security Appliance (WSA)
* Cisco Cognitive Threat Analytics At-a-Glance
* Introducing Cisco Cognitive Threat Analytics
* Implementing and Operating Cisco Security Core Technologies (SCOR) - Module 3: Cloud and Content Security

NEW QUESTION: 285
Drag and drop the Firepower Next Generation Intrustion Prevention System detectors from the left onto the correct definitions on the right.

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

Answer:



NEW QUESTION: 286

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.
Talos Threat Source is a regular intelligence update from Cisco Talos, highlighting the biggest threats each week and other security news.
Talos Threat Source is a regular intelligence update from Cisco Talos, highlighting the biggest threats each week and other security news.

NEW QUESTION: 287

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

A. multiple context mode

B. user deployment of Layer 3 networks
C. IPv6
D. clustering
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96-qsg/asav- aws.html

NEW QUESTION: 288
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)
Explanation 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.
Spero analysis examines structural characteristics such as metadata and header information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware.
Reference:
-> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload the whole file. Dynamic analysis sends files to AMP ThreatGrid.
Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco Threat Grid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit.
Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Security Intelligence and Research Group (Talos). Because

local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources. -> Malware analysis does not upload files to anywhere, it only checks the files locally.
There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in a Explanation 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: 289
How does Cisco Workload Optimization portion of the network do EPP solutions solely performance issues?
A. It deploys an AWS Lambda system
B. It automates resource resizing
C. It optimizes a flow path
D. It sets up a workload forensic score
Answer: (SHOW ANSWER)

NEW QUESTION: 290
Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two.)
A. Cisco FTDv configured in routed mode and IPv6 configured
B. Cisco FTDv with one management interface and two traffic interfaces configured
C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises
D. Cisco FTDv with two management interfaces and one traffic interface configured
E. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 291
Which type of API is being used when a security application notifies a controller within a software-defined network architecture about a specific security threat?
A. eastbound API
B. northbound API

C. westbound AP
D. southbound API
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 292
A network administrator is modifying a remote access VPN on an FTD managed by an FMC. The administrator wants to offload traffic to certain trusted domains. The administrator wants this traffic to go out of the client's local internet and send other internet-bound traffic over the VPN Which feature must the administrator configure?
A. dynamic split tunneling
B. local LAN access
C. dynamic access policies
D. reverse route injection
Answer: A (LEAVE A REPLY)
In a remote access VPN configuration, dynamic split tunneling allows traffic to certain trusted domains to bypass the VPN tunnel and exit through the client's local internet gateway. This feature selectively directs only the necessary traffic over the VPN, while allowing direct internet access for specific domains or traffic deemed safe or trusted, optimizing bandwidth and performance for remote users.

NEW QUESTION: 293
When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?
A. Application Control
B. Security Category Blocking
C. Content Category Blocking
D. File Analysis
Answer: (SHOW ANSWER)
Cisco Umbrella groups harmful destinations into categories of security threat, such as Malware, Command Control Callbacks, Phishing Attacks, Dynamic DNS, Potentially Harmful Domains, DNS Tunneling VPN, and Cryptomining1. When web policies are configured in Cisco Umbrella, the security category blocking provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats. By enabling or disabling these categories, the administrator can control the identity access to these destinations and protect the network from malicious traffic2. References: 1: Security Categories - Umbrella User Guide 2: Manage Security Settings - Umbrella User Guide

NEW QUESTION: 294
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. vulnerabilities within protocol
D. intermittent connection to the cloud connectors
Answer: A (LEAVE A REPLY)

NEW QUESTION: 295

An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation. What must be un solution?

A. L2TP is an IP packet encapsulation protocol, and GRE over IPsec is a tunneling protocol.

B. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701.

C. GRE over IPsec adds its own header, and L2TP does not.

D. GRE over IPsec cannot be used as a standalone protocol, and L2TP can.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 296

Which network monitoring solution uses streams and pushes operational data to provide a near real-time view of activity?

A. SNMP

B. SMTP

C. syslog

D. model-driven telemetry

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 297

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.

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:
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.

NEW QUESTION: 298
Which kind of API that is used with Cisco DNA Center provisions SSIDs, QoS policies, and update software versions on switches?
A. Integration
B. Intent
C. Event
D. Multivendor
Answer: (SHOW ANSWER)
The kind of API that is used with Cisco DNA Center to provision SSIDs, QoS policies, and update software versions on switches is the Intent API. The Intent API is a category of APIs that allows users to express their desired network outcomes or intents, such as creating a site, adding a device, or deploying a network profile.
The Intent API then translates these intents into specific network configurations and commands, and applies them to the relevant network devices and services. The Intent API simplifies and automates the network provisioning and management process, and enables users to focus on the business objectives rather than the technical details. Some examples of Intent APIs are:
* Site Management API: This API allows users to create, update, delete, and retrieve sites and buildings in Cisco DNA Center. A site is a logical grouping of network devices and services that share common characteristics, such as location, policies, or functions. A site can have one or more buildings, and a building can have one or more floors. Sites are used to organize and manage the network hierarchy and topology.
* Network Settings API: This API allows users to configure and manage network-wide settings, such as global credentials, network discovery, IP address pools, DHCP and DNS servers, and SNMP settings.

These settings are applied to all network devices and services that are managed by Cisco DNA Center.
* Network Profile API: This API allows users to create, update, delete, and retrieve network profiles in Cisco DNA Center. A network profile is a collection of network settings and policies that define how a network segment or service should operate, such as SSIDs, QoS policies, security policies, and device roles. Network profiles are used to standardize and simplify the network configuration and deployment process, and to ensure consistency and compliance across the network.
* Software Image Management API: This API allows users to manage the software images and versions of network devices that are managed by Cisco DNA Center. Users can import, export, delete, and retrieve software images, as well as assign them to network devices or device groups. Users can also schedule and monitor software image updates, and view the software image compliance status of network devices.
References:
* Cisco DNA Center Platform User Guide, Release 2.3.7.0 and 2.3.7.3, Chapter 1: Introduction to Cisco DNA Center Platform, Topic: Intent APIs
* Introduction to Cisco DNA Center REST APIs, Learning Lab: Cisco DNA Center Platform - Network Devices
* Cisco DNA Center Platform - Cisco DevNet, APIs: Intent APIs

NEW QUESTION: 299
Refer to the exhibit.

```
.mport requests
ırl = https://api.amp.cisco.com/v1/computers
ıeaders = {
   'accept' : application/json
   'content-type' : application/json
   'authorization' : Basic API Credentials
   'cache-control' : "no cache"

:esponse = requests request ("GET", url, headers = headers)
```

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

NEW QUESTION: 300
Which feature is supported when deploying Cisco ASAv within AWS public cloud?
A. IPv6
B. user deployment of Layer 3 networks
C. multiple context mode
D. clustering

Answer: B (LEAVE A REPLY)

NEW QUESTION: 301
Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?
A. multifactor authentication
B. fingerprinting
C. RADIUS-based REAP
D. Dynamic ARP Inspection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 302
R157

```
Info: New SMTP ICID 30 interface Management (192.168.0.100)
   address 10.128.128.200 reverse dns host unknown verified no
Info: ICID 30 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS None
Info: ICID 30 TLS success protocol TLSv1 cipher
   DHE-RSA-AES256-SHA
Info: SMTP Auth: (ICID 30) succeeded for user: cisco using
   AUTH mechanism: LOGIN with profile: ldap_smtp
Info: MID 80 matched all recipients for per-recipient policy
   DEFAULT in the outbound table
```

Which type of authentication is in use?
A. external user and relay mail authentication
B. SMTP relay server authentication
C. LDAP authentication for Microsoft Outlook
D. POP3 authentication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 303
For Cisco IOS PKI, which two types of Servers are used as a distribution point for CRLs? (Choose two)
A. SDP
B. LDAP
C. subordinate CA
D. SCP
E. HTTP
Answer: B,E (LEAVE A REPLY)

Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI.
A PKI is composed of the following entities: ...
- A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs) Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI.
A PKI is composed of the following entities: ...
- A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs) Reference: Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI.
A PKI is composed of the following entities: ...
- A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs)

NEW QUESTION: 304
What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?
A. Multiple NetFlow collectors are supported
B. Advanced NetFlow v9 templates and legacy v5 formatting are supported
C. Secure NetFlow connections are optimized for Cisco Prime Infrastructure
D. Flow-create events are delayed
Answer: D (LEAVE A REPLY)
Explanation Explanation The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions: ... - Delays the export of flow-create events. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.pdf Explanation The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions:
...
- Delays the export of flow-create events.
Explanation Explanation The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions: ... - Delays the export of flow-create events. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.pdf

NEW QUESTION: 305
Refer to the exhibit.

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

A network administrator configures command authorization for the admm5 user. What is the admin5 user able to do on HQ_Router after this configuration?
A. complete no configurations

B. complete all configurations
C. set the IP address of an interface
D. add subinterfaces
Answer: C (LEAVE A REPLY)

NEW QUESTION: 306
Refer to the exhibit.

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

A network administrator configures command authorization for the admin5 user. What is the admin5 user able to do on HQ_Router after this configuration?
A. set the IP address of an interface
B. complete no configurations
C. complete all configurations
D. add subinterfaces
Answer: B (LEAVE A REPLY)
ExplanationThe user "admin5" was configured with privilege level 5. In order to allow configuration (enter globalconfiguration mode), we must type this command:(config)#privilege exec level 5 configure terminalWithout this command, this user cannot do any configuration.Note: Cisco IOS supports privilege levels from 0 to 15, but the privilege levels which are used by default are privilege level 1 (user EXEC) and level privilege 15 (privilege EXEC)

NEW QUESTION: 307
Refer to the exhibit.

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

What is the result of using this authentication protocol in the configuration?
A. The authentication request contains only a password.
B. There are separate authentication and authorization request packets.
C. The authentication and authorization requests are grouped in a single packet.
D. The authentication request contains only a username.
Answer: (SHOW ANSWER)

NEW QUESTION: 308

Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'
```


What does the API key do while working with https://api.amp.cisco.com/v1/computers?

A. displays client ID

B. HTTP authentication

C. Imports requests

D. HTTP authorization

Answer: (SHOW ANSWER)

NEW QUESTION: 309

What is the purpose of CA in a PKI?

A. To issue and revoke digital certificates

B. To validate the authenticity of a digital certificate

C. To create the private key for a digital certificate

D. To certify the ownership of a public key by the named subject

Answer: (SHOW ANSWER)

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

NEW QUESTION: 310

Which capability is provided by application visibility and control?

A. reputation filtering

B. data obfuscation

C. data encryption

D. deep packet inspection

Answer: (SHOW ANSWER)

Application visibility and control (AVC) is a solution that leverages multiple technologies to recognize, analyze, and control over 1000 applications, including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications1. One of the key components of AVC is application recognition, which uses stateful deep packet inspection (DPI) to identify applications within the network traffic flow, using L3 to L7 data2. DPI is a technique that examines the content of packets beyond the header information, and can classify applications based on their signatures, protocols, ports, or other attributes3. DPI enables AVC to monitor and control application performance,

bandwidth usage, quality of service, and security policies4. References := 1: Cisco Application Visibility and Control (AVC) - Cisco 2: Cisco Application Visibility and Control User Guide - Technology Overview 3: What is application visibility and control? | Juniper Networks US 4: Application visibility and control - Secure Internet Access Enterprise

NEW QUESTION: 311
An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1 1 11 using the flow record Stea! thwatch406397954 command Which additional command is required to complete the flow record?
A. match ipv4 ttl
B. cache timeout active 60
C. transport udp 2055
D. destination 1.1.1.1
Answer: (SHOW ANSWER)

NEW QUESTION: 312
Why is it important for the organization to have an endpoint patching strategy?
A. so the latest security fixes are installed on the endpoints
B. so the internal PSIRT organization is aware of the latest bugs
C. so the network administrator is notified when an existing bug is encountered
D. so the organization can identify endpoint vulnerabilities
Answer: C (LEAVE A REPLY)

NEW QUESTION: 313
Which cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group?
A. Hybrid
B. Community
C. Private
D. Public
Answer: (SHOW ANSWER)
Explanation
Community Cloud allows system and services to be accessible by group of organizations. It shares the infrastructure between several organizations from a specific community. It may be managed internally by organizations or by the third-party.

NEW QUESTION: 314
What are two characteristics of the RESTful architecture used within Cisco DNA Center? (Choose two.)
A. REST uses HTTP to send a request to a web service.
B. The POST action replaces existing data at the URL path.
C. REST is a Linux platform-based architecture.
D. REST uses methods such as GET, PUT, POST, and DELETE.
E. REST codes can be compiled with any programming language.
Answer: A,D (LEAVE A REPLY)

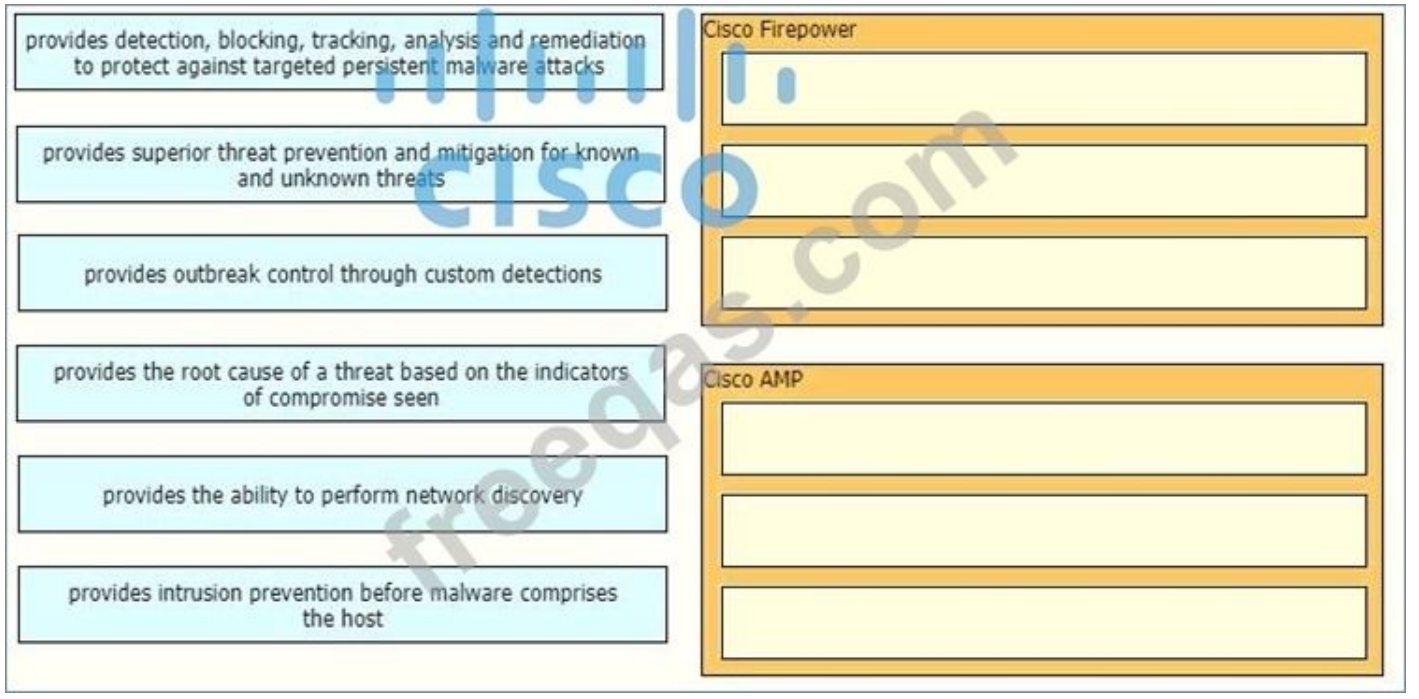
NEW QUESTION: 315
A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an undetermined verdict. What is causing this issue?
A. The policy was created to send a message to quarantine instead of drop
B. The file has a reputation score that is above the threshold
C. The file has a reputation score that is below the threshold
D. The policy was created to disable file analysis
Answer: D (LEAVE A REPLY)
ExplanationMaybe 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: 316
Which two capabilities does TAXII support? (Choose two)
A. Exchange
B. Pull messaging
C. Binding
D. Correlation
E. Mitigating
Answer: A,B (LEAVE A REPLY)
The Trusted Automated eXchangeof Indicator Information (TAXII) specifies mechanisms for exchanging structured cyber threat information between parties over the network.
TAXII exists to provide specific capabilities to those interested in sharing structured cyber threat information.
TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilities that this version of TAXII supports: push messaging, pull messaging, and discovery.
Although there is no "binding" capability in the list but it is the best answer here.

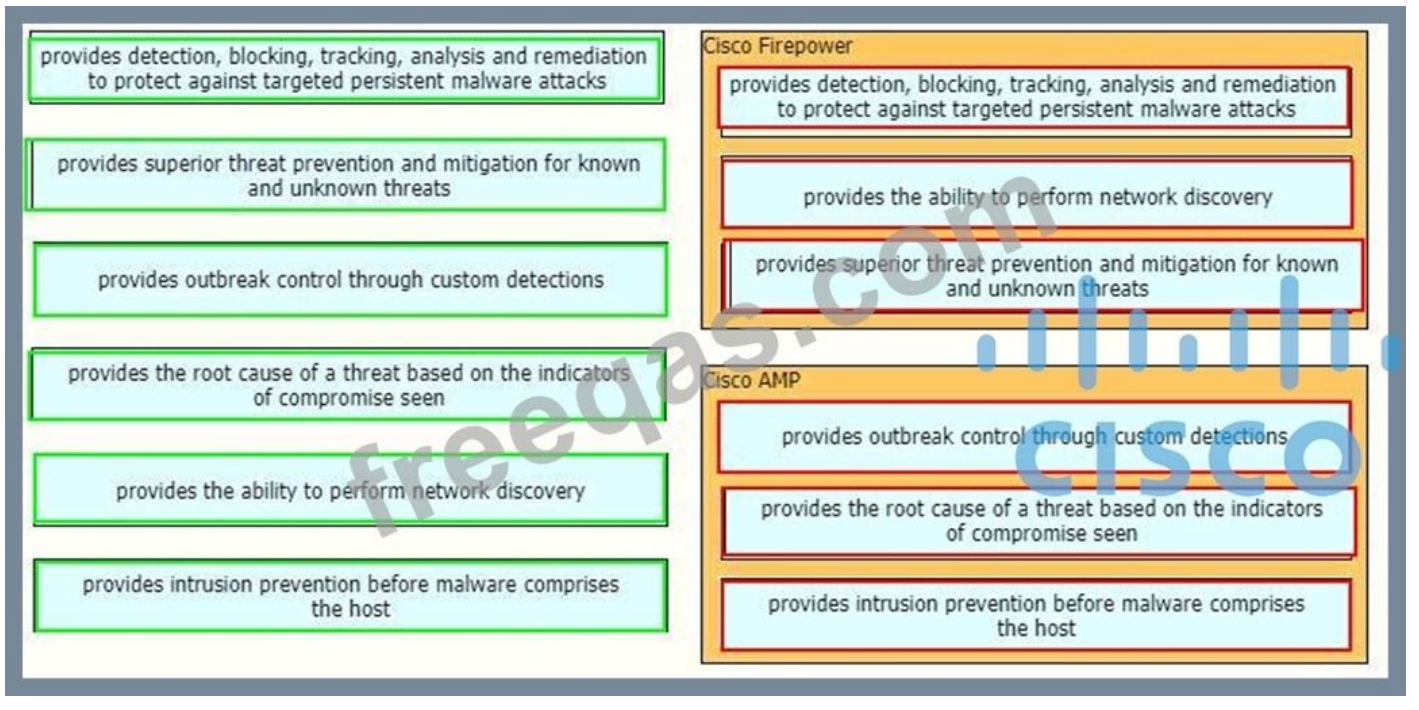
NEW QUESTION: 317
What is the benefit of integrating Cisco ISE with a MDM solution?
A. It provides compliance checks for access to the network

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)
Explanation 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/ Explanation
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: 318
Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.



Answer:



NEW QUESTION: 319
Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two.)
A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS
B. Cisco FTDv with one management interface and two traffic interfaces configured
C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises
D. Cisco FTDv with two management interfaces and one traffic interface configured
E. Cisco FTDv configured in routed mode and IPv6 configured
Answer: A,C (LEAVE A REPLY)
Explanation/Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/ white-paper-c11-740505.html

NEW QUESTION: 320
Where are individual sites specified to be blacklisted in Cisco Umbrella?
A. application settings
B. content categories
C. security settings
D. destination lists
Answer: D (LEAVE A REPLY)
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.
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:
A destination list is a list of internet destinations that can be blocked or allowed based on the administrative preferences for the policies applied to the identities within your organization. A destination is an IP address (IPv4), URL, or fully qualified domain name. You can add a destination list to Umbrella at any time; however, a destination list does not come into use until it is added to a policy.

NEW QUESTION: 321
Which method is used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources?
A. BYOD on boarding
B. Simple Certificate Enrollment Protocol
C. Client provisioning
D. MAC authentication bypass
Answer: A (LEAVE A REPLY)
When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network.
Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal.

Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices.
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.
When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network.
Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal.
Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices.
Reference:
m_ise_devices_byod.html
m_ise_devices_byod.html

NEW QUESTION: 322
What is the purpose of the Cisco Endpoint IoC feature?
A. It provides stealth threat prevention.
B. It is a signature-based engine. W
C. It is an incident response tool 6W
D. It provides precompromise detection.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Secure_Managed_Endpoint.pdf

NEW QUESTION: 323
What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group?
A. posture assessment
B. CoA
C. external identity source
D. SNMP probe
Answer: B (LEAVE A REPLY)
Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.
One of the settings to configure the CoA type is "Reauth". This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.
One of the settings to configure the CoA type is "Reauth". This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.
Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.
One of the settings to configure the CoA type is "Reauth". This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.
Reference:
b_ise_admin_guide_sample_chapter_010101.html
b_ise_admin_guide_sample_chapter_010101.html

NEW QUESTION: 324
An organization is trying to improve their Defense in Depth by blocking malicious destinations prior to a connection being established. The solution must be able to block certain applications from being used within the network. Which product should be used to accomplish this goal?
A. Cisco Firepower
B. Cisco Umbrella
C. ISE
D. AMP
Answer: B (LEAVE A REPLY)
ExplanationExplanationCisco 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.

NEW QUESTION: 325
What does Cisco AMP for Endpoints use to help an organization detect different families of malware?
A. Ethos Engine to perform fuzzy fingerprinting
B. Tetra Engine to detect malware when me endpoint is connected to the cloud
C. Clam AV Engine to perform email scanning
D. Spero Engine with machine learning to perform dynamic analysis
Answer: A (LEAVE A REPLY)
ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected. Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf ETHOS = Fuzzy Fingerprinting using static/passive heuristics a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected.
Reference:
ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected. Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf ETHOS = Fuzzy Fingerprinting using static/passive heuristics

NEW QUESTION: 326

Which Cisco Firewall solution requires zone definition?

A. CBAC

B. Cisco AMP

C. ZBFW

D. Cisco ASA

Answer: C (LEAVE A REPLY)

ZBFW stands for Zone-Based Firewall, which is a feature that allows unidirectional application of IOS firewall policies between groups of interfaces known as zones. Interfaces are assigned to zones, and firewall rules are applied to specific types of traffic moving in one direction between the zones. ZBFW enforces a secure inter-zone policy by default, meaning traffic cannot pass between security zones until an explicit policy allowing that traffic is defined. The zone itself is an abstraction of multiple interfaces with the same or similar security requirements that can be logically grouped together. ZBFW is CBAC's replacement and offers intuitive policies for multiple-interface routers, increased granularity of firewall policy application, and a default deny-all policy that prohibits traffic between firewall security zones until an explicit policy is applied to allow desirable traffic. ZBFW is supported on IOS devices running 12.4(6)T or later, and ASR devices running 12.2(33) or later.

References:

* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Securing the Cloud, Lesson 4.1: Introducing Cisco Cloud Services Router 1000V Series, Topic 4.1.2: Zone-Based Firewall
* Understand the Zone-Based Policy Firewall Design
* Managing Zone-based Firewall Rules
* Zone Based Firewall Overview
* CBAC vs. Zone-based firewall

NEW QUESTION: 327

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

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

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

C. Browse

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

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 328

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 SQL 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: 329
What is a characteristic of traffic storm control behavior?
A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
B. Traffic storm control cannot determine if the packet is unicast or broadcast.
C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.
Answer: (SHOW ANSWER)
Traffic storm control is a feature that prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces. Traffic storm control monitors the level of each traffic type for which it is enabled in 1-second intervals and compares it with the configured threshold, which is a percentage of the total available bandwidth of the port. When the ingress traffic reaches the threshold, traffic storm control drops the traffic until the end of the interval. Traffic storm control uses the Individual/Group bit in the packet destination address to determine if the packet is unicast or broadcast. This bit is set to 0 for unicast addresses and 1 for multicast or broadcast addresses. Traffic storm control does not use the source address to classify the traffic type. References := Configuring Traffic Storm Control - Cisco, Understanding Cisco Traffic Storm Control - NetCraftsmen

NEW QUESTION: 330
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 a switch to Cisco DNA Center

B. adds authentication to a switch

C. receives information about a switch

Answer: A (LEAVE A REPLY)

NEW QUESTION: 331

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

A. white list

B. Sophos engine

C. RAT

D. outbreak filters

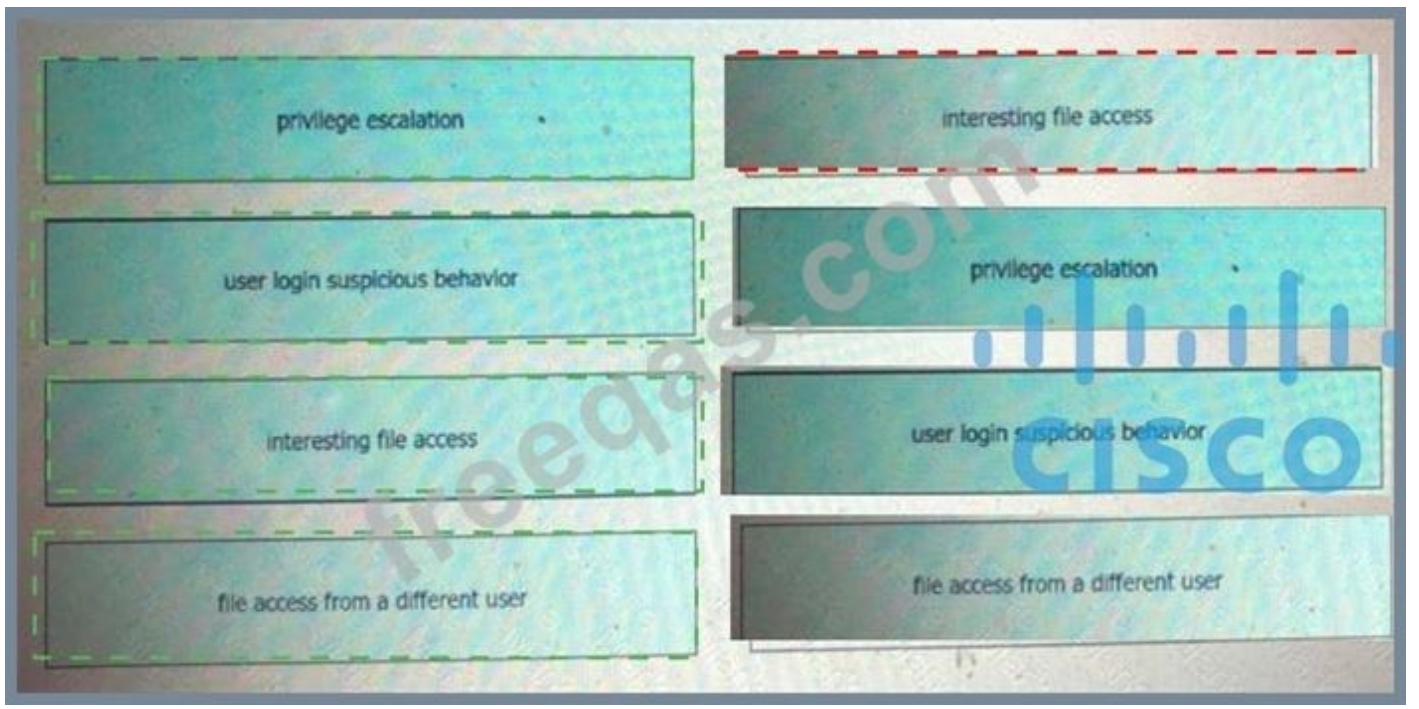
E. DLP

Answer: B,D (LEAVE A REPLY)

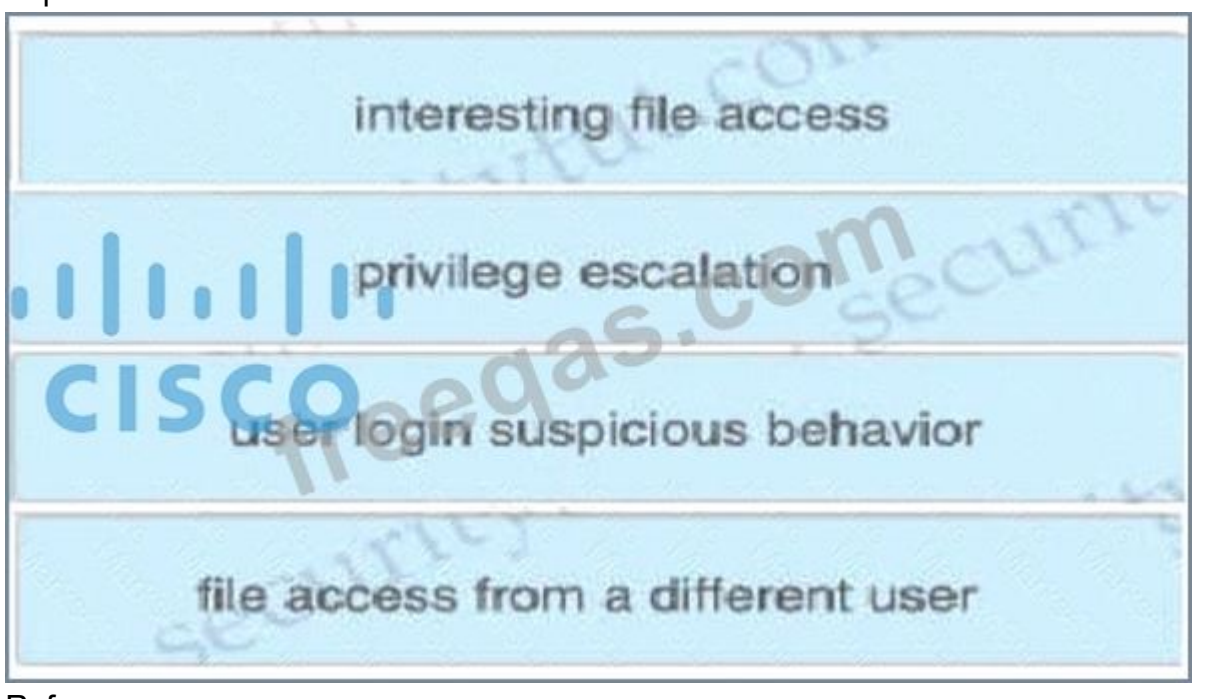
NEW QUESTION: 332
Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?
A. File Analysis
B. SafeSearch
C. SSL Decryption
D. Destination Lists
Answer: (SHOW ANSWER)
Reference:
https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-IntelligentProxy

NEW QUESTION: 333
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.

Answer:

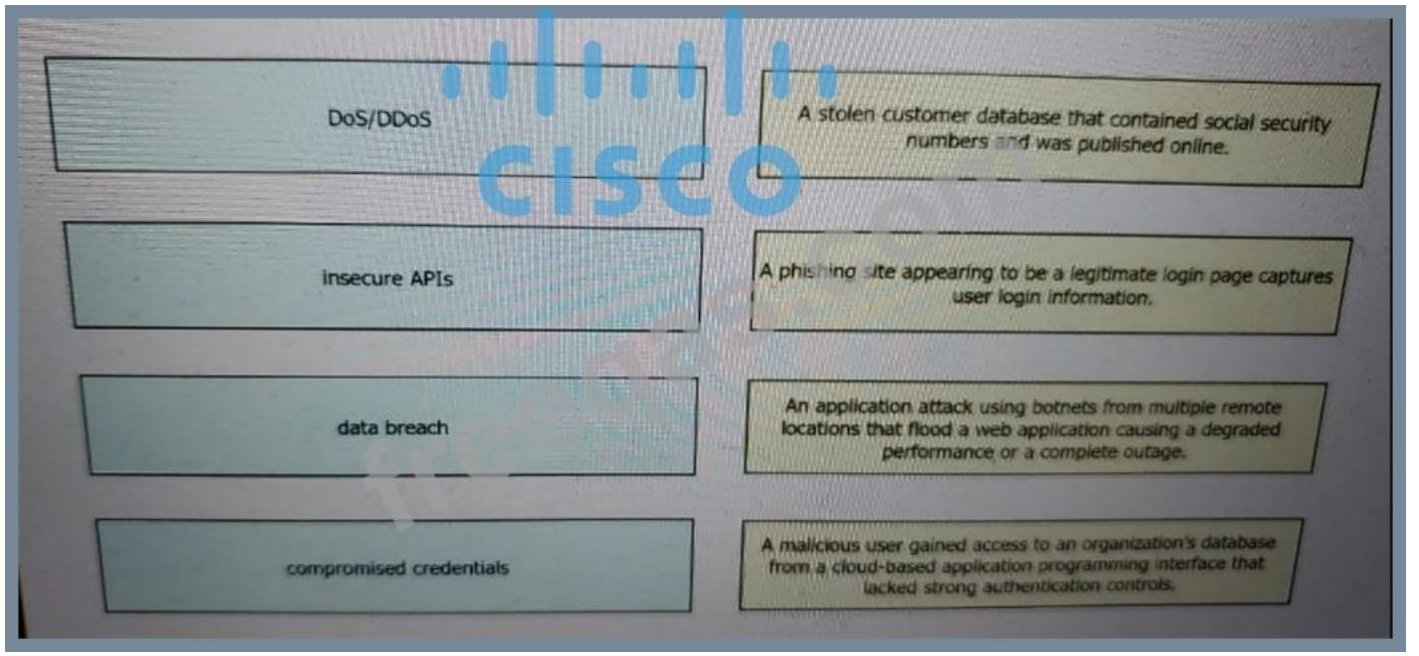


Explanation:

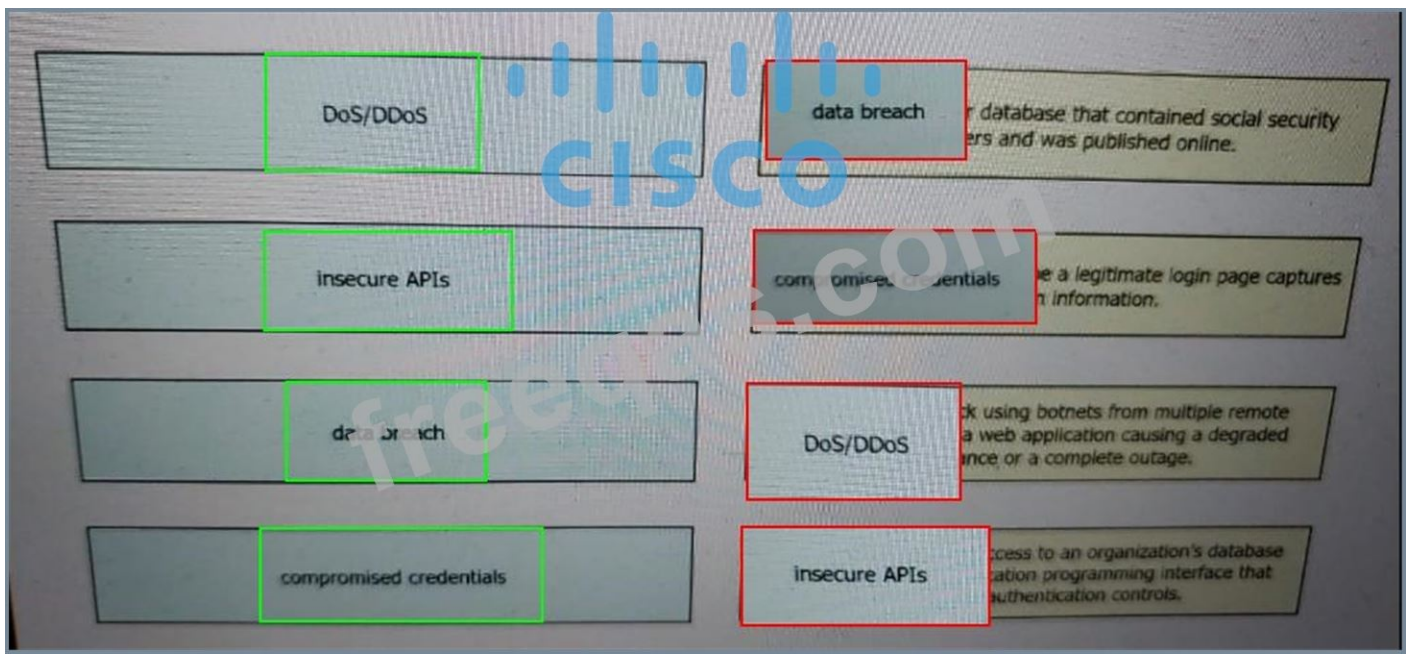


Reference:
https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-74038

NEW QUESTION: 334
Drag and drop the threats from the left onto examples of that threat on the right



Answer:



NEW QUESTION: 335
Which type of data does the Cisco Stealthwatch system collect and analyze from routers, switches, and firewalls?
A. NTP
B. syslog
C. SNMP
D. NetFlow
Answer: D (LEAVE A REPLY)
The Cisco Stealthwatch system collects and analyzes network telemetry such as flow (NetFlow, sFlow, JFlow, IPFIX, etc.) from routers, switches, and firewalls to monitor network and user behavior. The system conducts sophisticated, proprietary analytics on network data to automatically detect abnormal behaviors that may signify an attack1. NetFlow is a protocol that provides information about network traffic flows, such as source and destination IP addresses, ports, protocols, bytes, packets, and timestamps. NetFlow data can be used to identify network anomalies, bandwidth usage, application performance, and security incidents2. References := Some possible references are:

1: Cisco Stealthwatch Improves Threat Defense with Network Visibility and Security Analytics, Zones, 3 2: What is NetFlow? Definition and Benefits, Cisco, 7

NEW QUESTION: 336

Refer to the exhibit. What function does the API key perform while working with https://api.amp.cisco.com/v1/computers?

A. HTTP authorization

B. HTTP authentication

C. plays dent ID

D. imports requests

Answer: B (LEAVE A REPLY)

NEW QUESTION: 337

Refer to the exhibit.

Consider that any feature of DNS requests, such as the length off the domain name and the number of subdomains, can be used to construct models of expected behavior to which observed values can be compared. Which type of malicious attack are these values associated with?

A. Heartbleed SSL Bug

B. W32/AutoRun worm

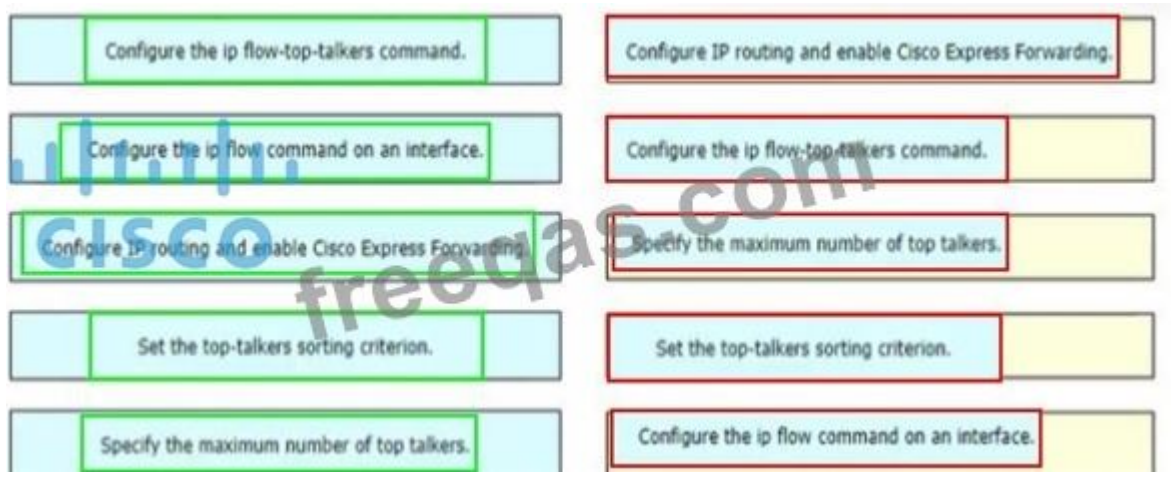
C. Spectre Worm

D. Eternal Blue Windows

Answer: B (LEAVE A REPLY)

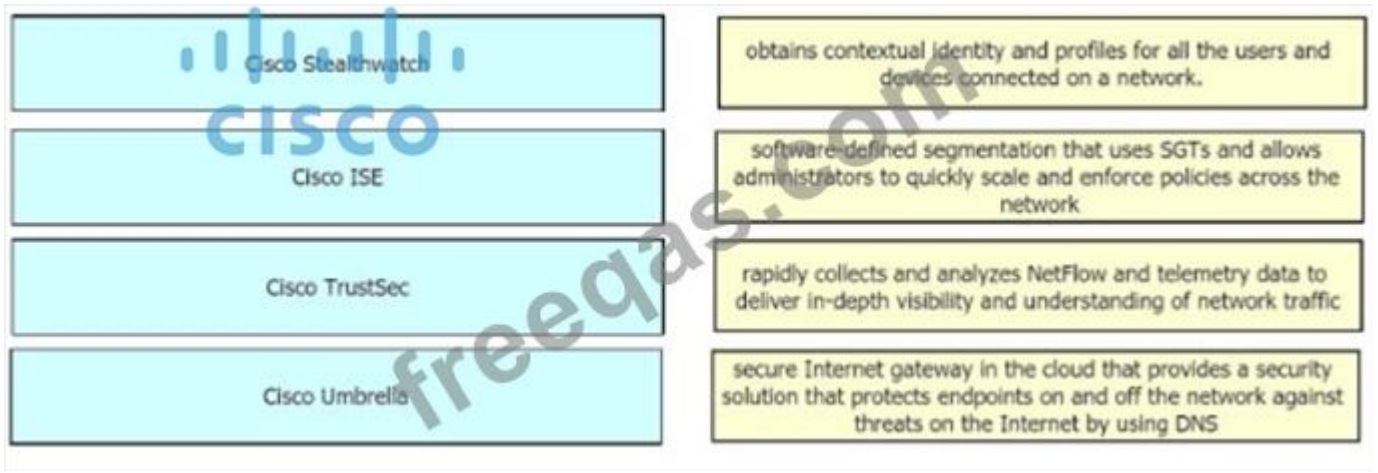
NEW QUESTION: 338
A network engineer is configuring NetFlow top talkers on a Cisco router Drag and drop the steps in the process from the left into the sequence on the right

Answer:



NEW QUESTION: 339
An email administrator is setting up a new Cisco ESA.
The administrator wants to enable the blocking of greymail for the end user. Which feature must the administrator enable first?
A. File Analysis
B. Intelligent Multi-Scan
C. IP Reputation Filtering
D. Anti-Virus Filtering
Answer: (SHOW ANSWER)

NEW QUESTION: 340
Drag and drop the solutions from the left onto the solution's benefits on the right.



Answer:

NEW QUESTION: 341
Which term describes when the Cisco Firepower downloads threat intelligence updates from Cisco Talos?
A. consumption
B. authoring
C. analysis
D. sharing
Answer: (SHOW ANSWER)

NEW QUESTION: 342
Why is it important to have logical security controls on endpoints even though the users are trained to spot security threats and the network devices already help prevent them?
A. because human error or insider threats will still exist
B. to expose the endpoint to more threats
C. because defense-in-depth stops at the network
D. to prevent theft of the endpoints
Answer: (SHOW ANSWER)

NEW QUESTION: 343

An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically.
What must be configured to accomplish this?
A. Configure the Cisco WSA to modify policies based on the traffic seen.
B. Configure the Cisco ESA to receive real-time updates from Talos
C. Configure the Cisco WSA to receive real-time updates from Talos.
D. Configure the Cisco ESA to modify policies based on the traffic seen.
Answer: D (LEAVE A REPLY)
Explanation
https://www.cisco.com/c/en/us/td/docs/security/esa/esa120/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Adm

NEW QUESTION: 344
Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'

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']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
        mac = network_interface.get('mac')
        ip = network_interface.get('ip')
        ipv6 = network_interface.get('ipv6')
        print(mac, ip, ipv6)
```

What does the API do when connected to a Cisco security appliance?
A. get the process and PID information from the computers in the network
B. create an SNMP pull mechanism for managing AMP
C. gather network telemetry information from AMP for endpoints
D. gather the network interface information about the computers AMP sees
Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 345
Why should organizations migrate to an MFA strategy for authentication?
A. Single methods of authentication can be compromised more easily than MFA.
B. Biometrics authentication leads to the need for MFA due to its ability to be hacked easily.
C. MFA methods of authentication are never compromised.
D. MFA does not require any piece of evidence for an authentication mechanism.
Answer: A (LEAVE A REPLY)
single methods of authentication can be compromised more easily than MFA. MFA, or multi-factor authentication, is a security process that requires users to provide two or more factors to verify their identity and access resources. MFA reduces the risk of unauthorized access by making it harder for attackers to compromise all the factors needed, especially if they are different in nature, such as something you know (password), something you have (token), and something you are (biometric).
To understand the concept of MFA and why it is important for authentication security, you can refer to the following sections of the source book:
* Section 1.1.1: Describe the concepts of identity and access management
* Section 1.1.1.1: Describe the concepts of identity principles
* Section 1.1.1.2: Describe the concepts of authentication
* Section 1.1.1.3: Describe the concepts of authorization
* Section 1.1.1.4: Describe the concepts of accounting
* Section 1.1.1.5: Describe the concepts of identity stores
* Section 1.1.1.6: Describe the concepts of MFA
References:
* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0
* What is Multi-Factor Authentication? | IBM
* How to implement Multi-Factor Authentication (MFA) | Microsoft Security Blog

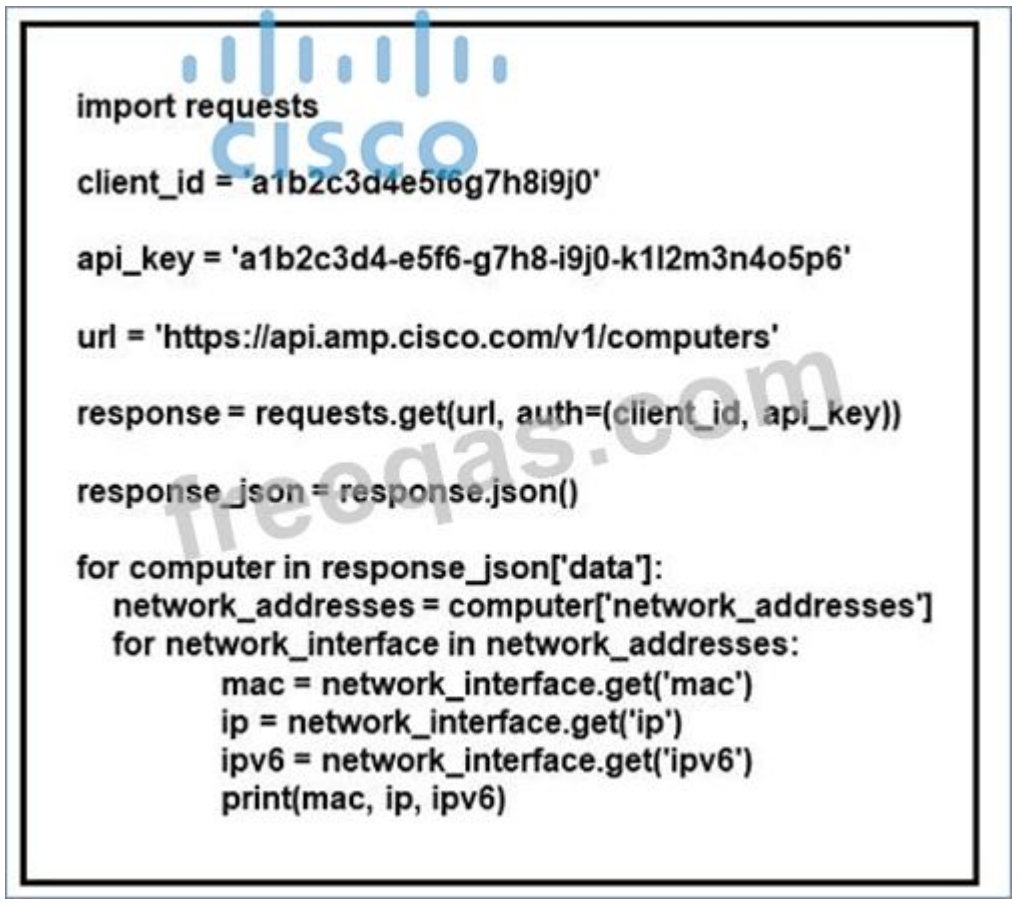
NEW QUESTION: 346
The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the ASA be added on the Cisco UC Manager platform?
A. Certificate Trust List
B. Endpoint Trust List
C. Enterprise Proxy Service
D. Secured Collaboration Proxy
Answer: (SHOW ANSWER)
The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. This means that the ASA acts as a proxy between the Cisco IP Phone and the Cisco Unified Communications Manager (UCM), decrypting, inspecting, and re-encrypting the voice signaling traffic. To do this, the ASA needs to have the certificates of the devices that the phone trusts, such as the UCM servers and the TFTP servers. These certificates are stored in a Certificate Trust List (CTL) file that the phone downloads from the UCM before registration. Therefore, the ASA must be added to the CTL file on the UCM platform, so that the phone can verify the identity of the ASA as a proxy. The

other options are not relevant for this scenario. The Endpoint Trust List is a list of certificates that the UCM trusts for encrypted endpoints. The Enterprise Proxy Service is a feature that allows the UCM to route calls to and from the public switched telephone network (PSTN) through a SIP proxy server. The Secured Collaboration Proxy is a feature that allows the UCM to encrypt the media streams between endpoints using Secure Real-Time Transport Protocol (SRTP). References :=

* Cisco Secure Firewall ASA Unified Communications Guide - TLS Proxy for Encrypted Voice Inspection
* TLS Proxy for Encrypted Voice Inspection - Cisco
* Where must the ASA be added on the Cisco UC Manager platform?

NEW QUESTION: 347

Refer to the exhibit.



What does the API do when connected to a Cisco security appliance?

A. gather the network interface information about the computers AMP sees

B. create an SNMP pull mechanism for managing AMP

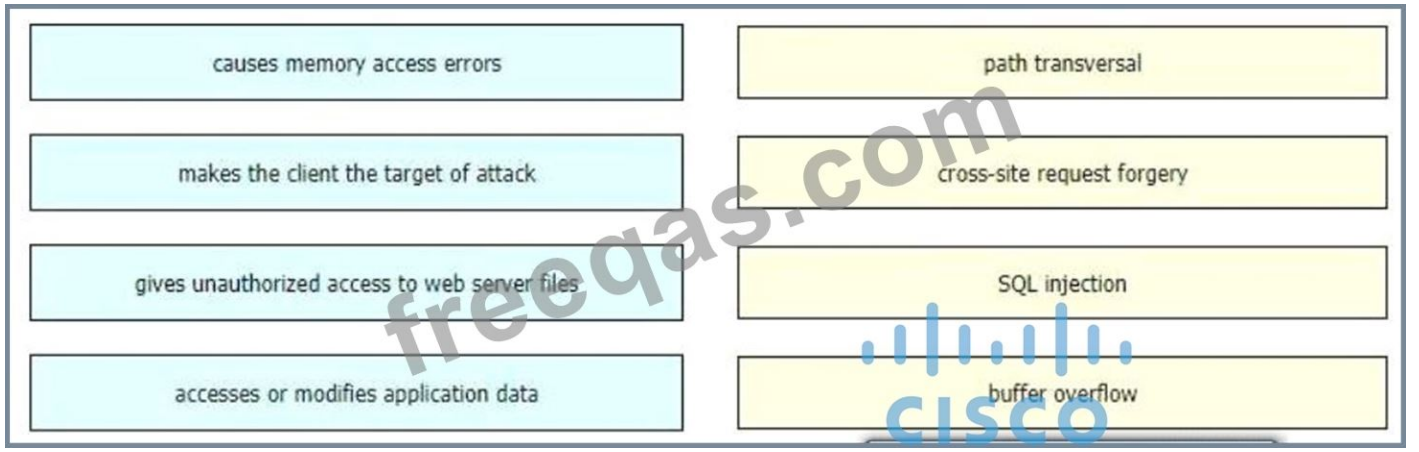
C. gather network telemetry information from AMP for endpoints

D. get the process and PID information from the computers in the network

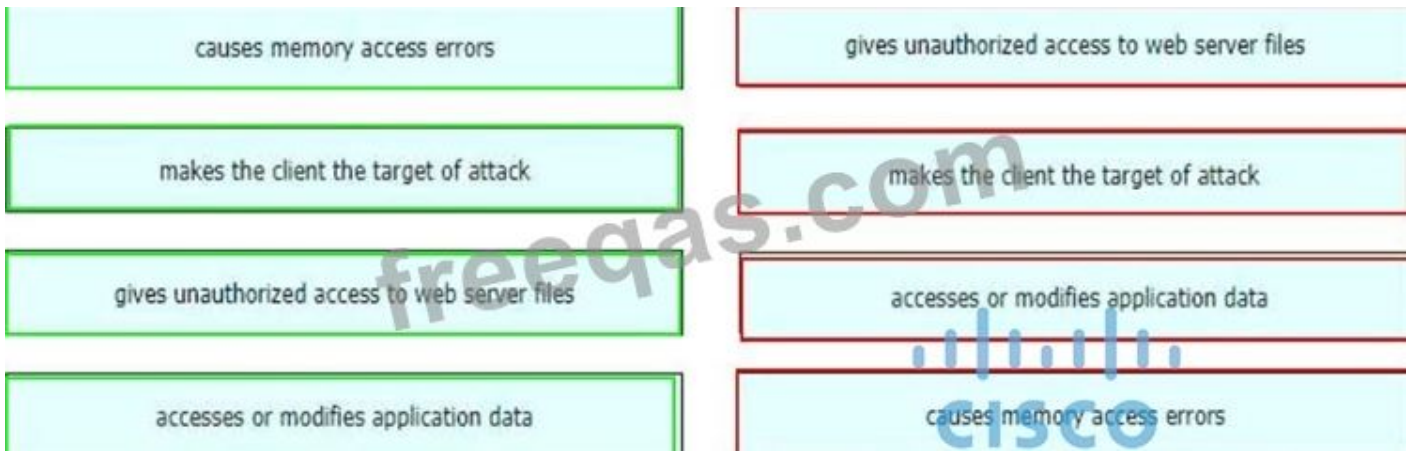
Answer: A (LEAVE A REPLY)

NEW QUESTION: 348
How does the Cisco WSA enforce bandwidth restrictions for web applications?
A. It dynamically creates a scavenger class QoS policy and applies it to each client that connects through the WSA.
B. It sends commands to the uplink router to apply traffic policing to the application traffic.
C. It implements a policy route to redirect application traffic to a lower-bandwidth link.
D. It simulates a slower link by introducing latency into application traffic.
Answer: (SHOW ANSWER)

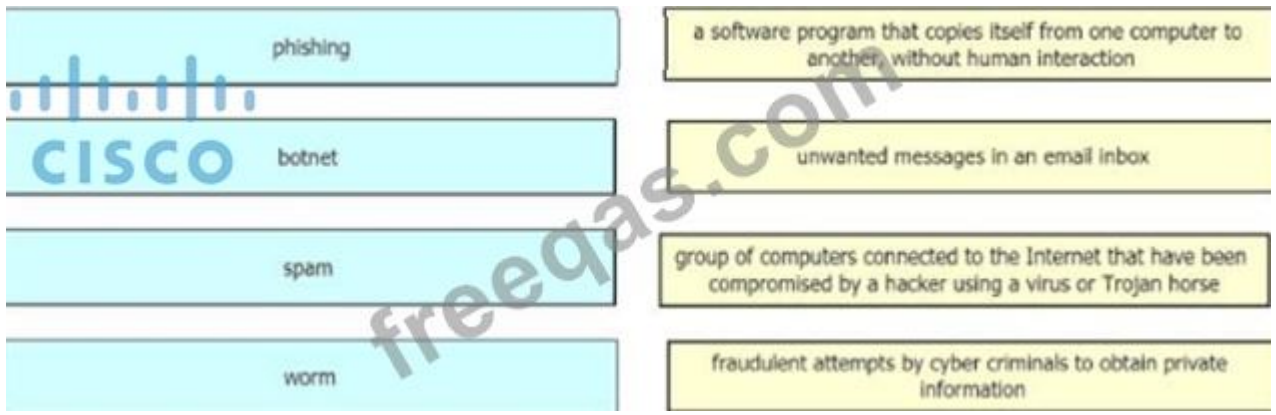
NEW QUESTION: 349
Drag and drop the exploits from the left onto the type of security vulnerability on the right.



Answer:



NEW QUESTION: 350
Drag and drop the common security threats from the left onto the definitions on the right.



Answer:

NEW QUESTION: 351

Which Cisco security solution secures public, private, hybrid, and community clouds?

A. Cisco ISE

B. Cisco ASAv

C. Cisco Cloudlock

D. Cisco pxGrid

Answer: C (LEAVE A REPLY)

Cisco Cloudlock is a cloud-native security solution that secures public, private, hybrid, and community clouds. It provides visibility, compliance, threat protection, and data security for cloud applications and environments. Cisco Cloudlock integrates with various cloud platforms and services, such as AWS, Azure, Google Cloud, Office 365, Salesforce, Dropbox, and more. Cisco Cloudlock monitors user activities, configurations, and sensitive data across the cloud, and alerts or blocks any violations of policies or regulations. Cisco Cloudlock also leverages user and entity behavior analytics (UEBA) to detect and respond to anomalous or malicious behaviors in the cloud. Cisco Cloudlock helps organizations protect their cloud assets and data, while enabling them to embrace the benefits of cloud computing. References :=

* Cloud and Application Security - Cisco
* Cloud Security Products and Solutions - Cisco
* What Is Cloud Security? - Cisco
* [Cisco Cloudlock: Cloud-Native CASB and Cloud Cybersecurity Platform]

NEW QUESTION: 352

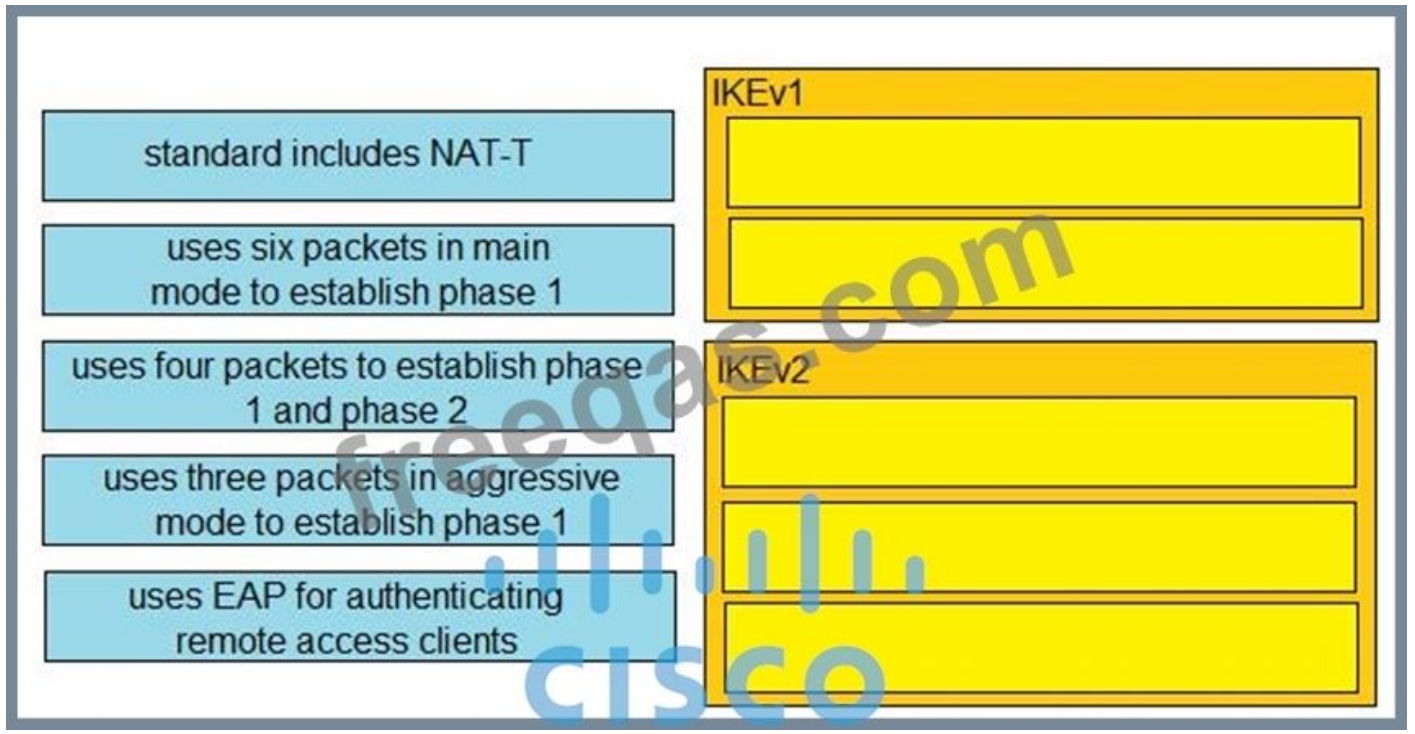
An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems. Why should the organization select either Platform as a Service or Infrastructure as a Service for this environment?

A. Platform as a Service because the customer manages the operating system
B. Infrastructure as a Service because the customer manages the operating system
C. Platform as a Service because the service provider manages the operating system
D. Infrastructure as a Service because the service provider manages the operating system
Answer: (SHOW ANSWER)
Platform as a Service (PaaS) is a cloud service model that delivers and manages all the hardware and software resources to develop applications through the cloud. The service provider is responsible for the infrastructure, middleware, runtime, and operating system, while the customer only has to focus on the application and data. PaaS enables the customer to avoid the hassle of patching, updating, or maintaining the operating system, as well as the underlying hardware and network12. Infrastructure as a Service (IaaS) is a cloud service model that delivers on-demand infrastructure resources, such as compute, storage, networking, and virtualization, to the customer via the cloud. The service provider hosts and manages the infrastructure, but the customer is responsible for the operating system, middleware, virtual machines, and any apps or data. IaaS requires the customer to handle the patch management of the operating system, as well as the security and configuration of the virtual machines34. References := 1: Use platform as a service (PaaS) options - Azure Architecture Center 2: What is Platform-as-a-Service (PaaS)? - Cloudflare 3: PaaS vs IaaS vs SaaS: What's the difference? | Google Cloud 4: SaaS vs PaaS vs IaaS: What's The Difference & How To Choose - BMC Software | Blogs

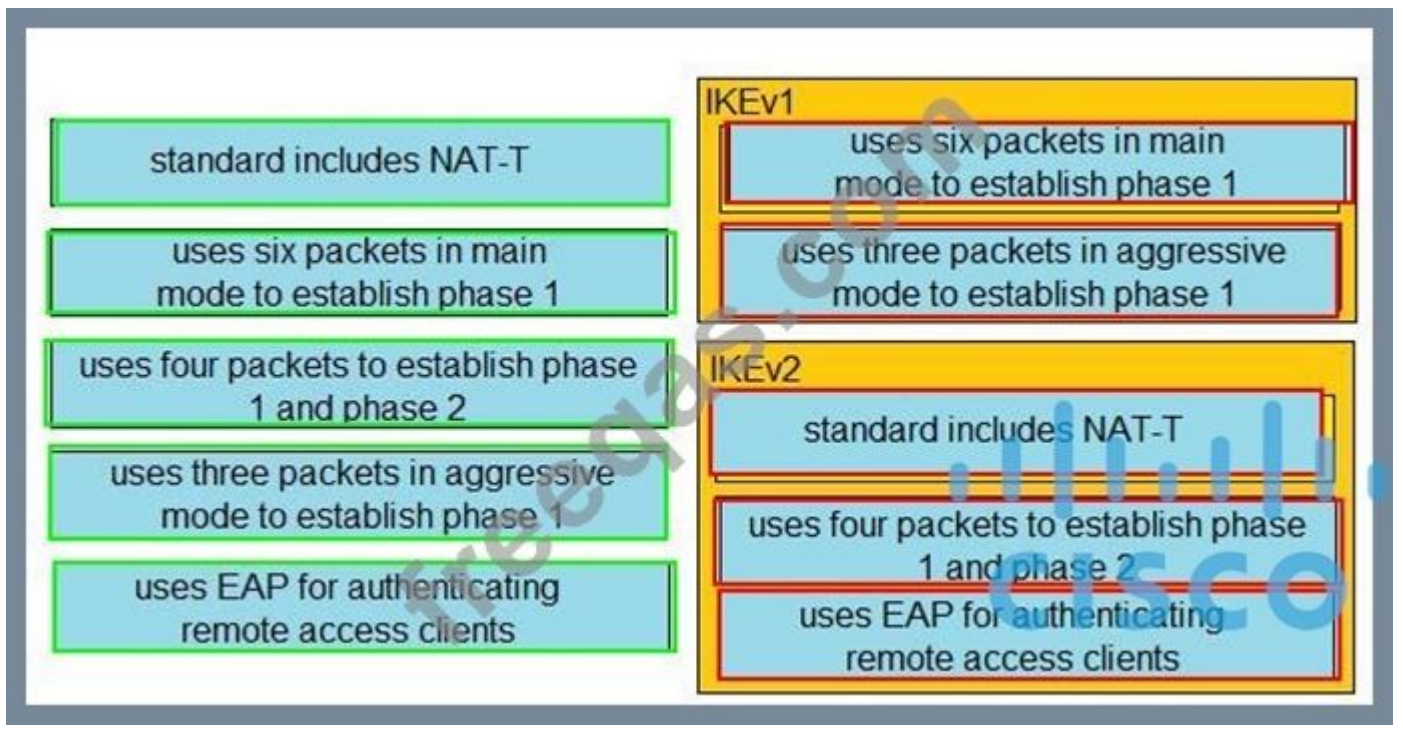
NEW QUESTION: 353
Refer to the exhibit.

Which configuration item makes it possible to have the AAA session on the network?
A. aaa authorization exec default ise
B. aaa authentication enable default enable
C. aaa authorization network default group ise
D. aaa authentication login console ise
Answer: (SHOW ANSWER)

NEW QUESTION: 354
Drag and drop the descriptions from the left onto the correct protocol versions on the right.



Answer:



NEW QUESTION: 355

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

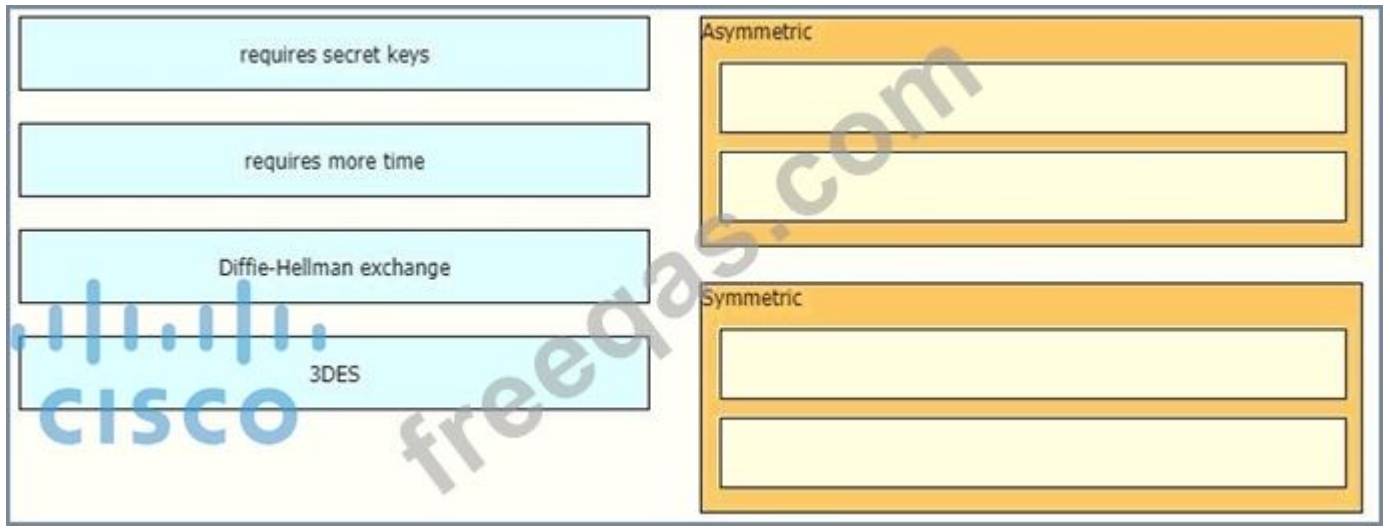
C. database

D. web page images

Answer: C (LEAVE A REPLY)

Explanation/Reference: https://tools.cisco.com/security/center/resources/sql_injection

NEW QUESTION: 356
Drag and drop the descriptions from the left onto the encryption algorithms on the right.



Answer:

NEW QUESTION: 357
Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.

Answer:

NEW QUESTION: 358
What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?
A. Telemetry uses a pull mehod, which makes it more reliable than SNMP
B. Telemetry uses push and pull, which makes it more scalable than SNMP
C. Telemetry uses push and pull which makes it more secure than SNMP
D. Telemetry uses a push method which makes it faster than SNMP
Answer: D (LEAVE A REPLY)
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: 359

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

Refer to the exhibit. What is the result of using this authentication protocol in the configuration?
A. There are separate authentication and authorization request packets.
B. The authentication request contains only a username.
C. The authentication request contains only a password.
D. The authentication and authorization requests are grouped in a single packet.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 360
Which CLI command is used to register a Cisco FirePOWER sensor to Firepower Management Center?
A. configure manager delete
B. configure system add <host><key>
C. configure manager add <host><key>
D. configure manager <key> add host
Answer: (SHOW ANSWER)

NEW QUESTION: 361
Which compliance status is shown when a configured posture policy requirement is not met?
A. compliant
B. unknown
C. authorized
D. noncompliant
Answer: (SHOW ANSWER)
Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. A posture policy is a collection of posture requirements that are associated with one or more identity groups and operating systems. Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. + If a mandatory requirement fails, the user will be moved to Non-Compliant state + If an optional requirement fails, the user is allowed to skip the specified optional requirements and the user is moved to Compliant state This Qdid not clearly specify the type of posture policy requirement (mandatory or optional) is not met so the user can be in Non-compliant or compliant state. But "noncompliant" is the best answer here. Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_010111.html known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies.
A posture policy is a collection of posture requirements that are associated with one or more identity groups and operating systems. Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies.
+ If a mandatory requirement fails, the user will be moved to Non-Compliant state
+ If an optional requirement fails, the user is allowed to skip the specified optional requirements and the user is moved to Compliant state This Qdid not clearly specify the type of posture policy requirement (mandatory or optional) is not met so the user can be in Non-compliant or compliant state. But "noncompliant" is the best answer here.
Reference:
Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. A posture policy is a collection of posture requirements that are associated with one or more identity groups and operating systems. Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. + If a mandatory requirement fails, the user will be moved to Non-Compliant state + If an optional requirement fails, the user is allowed to skip the specified optional requirements and the user is moved to Compliant state This Qdid not clearly specify the type of posture policy requirement (mandatory or optional) is not met so the user can be in Non-compliant or compliant state. But "noncompliant" is the best answer here. Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_010111.html

NEW QUESTION: 362
Which two protocols must be configured to authenticate end users to the Web Security Appliance? (Choose two.)
A. NTLMSSP
B. Kerberos
C. CHAP
D. TACACS+
E. RADIUS
Answer: A,B (LEAVE A REPLY)
The Web Security Appliance (WSA) supports different authentication protocols and schemes to acquire end-user credentials. The most common protocols are NTLMSSP and Kerberos, which are both supported by Active Directory realms. NTLMSSP is a challenge-response authentication protocol that uses a hash of the user's password to authenticate. Kerberos is a ticket-based authentication protocol that uses a trusted third-party (the Key Distribution Center) to issue tickets to the user and the service. Both protocols are more secure and widely supported than Basic authentication, which sends the user's credentials in clear text. CHAP, TACACS+, and RADIUS are not supported by the WSA for end-user authentication, although they can be used for external authentication of administrators or for credential encryption.
References: 1, 2, 3
https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/guide-c07-742373.html
https://frontegg.com/blog/authentication

NEW QUESTION: 363
What is the difference between Cross-site Scripting and SQL Injection, attacks?
A. Cross-site Scripting is an attack where code is injected into a database, whereas SQL Injection is an attack where code is injected into a browser.
B. Cross-site Scripting is when executives in a corporation are attacked, whereas SQL Injection is when a database is manipulated.
C. Cross-site Scripting is a brute force attack targeting remote sites, whereas SQL Injection is a social engineering attack.
D. Cross-site Scripting is an attack where code is executed from the server side, whereas SQL Injection is an attack where code is executed from the client side.
Answer: (SHOW ANSWER)

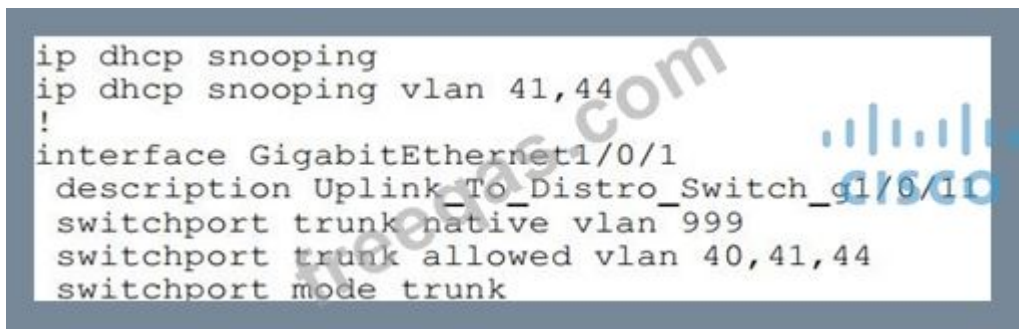
NEW QUESTION: 364
Refer to the exhibit.

```
snmp-server group SNMP v3 auth access 15
```

What does the number 15 represent in this configuration?

A. interval in seconds between SNMPv3 authentication attempts
B. privilege level for an authorized user to this router
C. number of possible failed attempts until the SNMPv3 user is locked out
D. access list that identifies the SNMP devices that can access the router
Answer: D (LEAVE A REPLY)

NEW QUESTION: 365
Refer to the exhibit.



An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained. Which command should be configured on the switch interface in order to provide the user with network connectivity?
A. ip dhcp snooping verify mac-address
B. ip dhcp snooping limit 41
C. ip dhcp snooping vlan 41
D. ip dhcp snooping trust
Answer: D (LEAVE A REPLY)
To understand DHCP snooping we need to learn about DHCP spoofing attack first.
DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle".
The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.
DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.
Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.
The port connected to a DHCP server should be configured as trusted port with the "ip dhcp snooping trust" command. Other ports connecting to hosts are untrusted ports by default.
In this question, we need to configure the uplink to "trust" (under interface Gi1/0/1) as shown below.

NEW QUESTION: 366
How many interfaces per bridge group does an ASA bridge group deployment support?
A. up to 2
B. up to 4
C. up to 8

D. up to 16

Answer: B (LEAVE A REPLY)

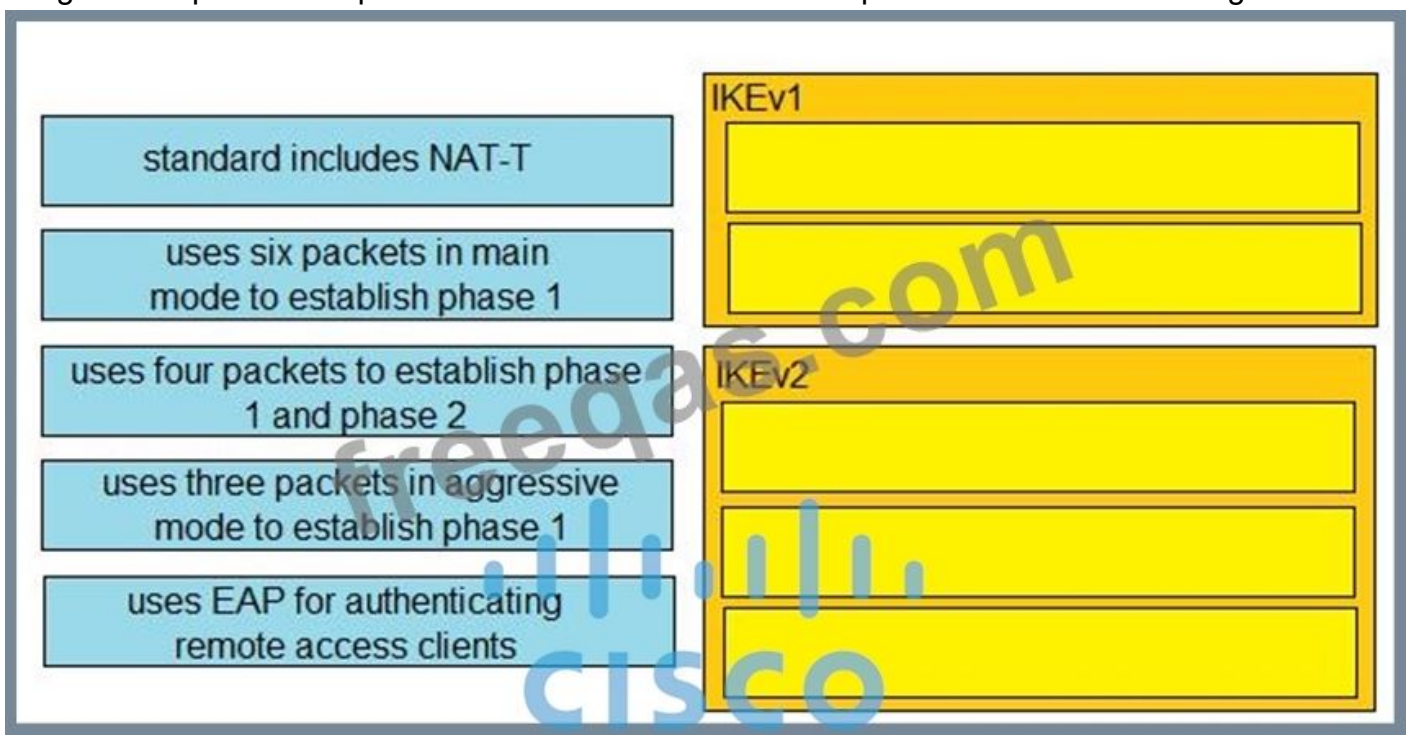
Each of the ASAs interfaces need to be grouped into one or more bridge groups. Each of these groups acts as an independent transparent firewall. It is not possible for one bridge group to communicate with another bridge group without assistance from an external router.

As of 8.4(1) upto 8 bridge groups are supported with 2-4 interface in each group. Prior to this only one bridge group was supported and only 2 interfaces.

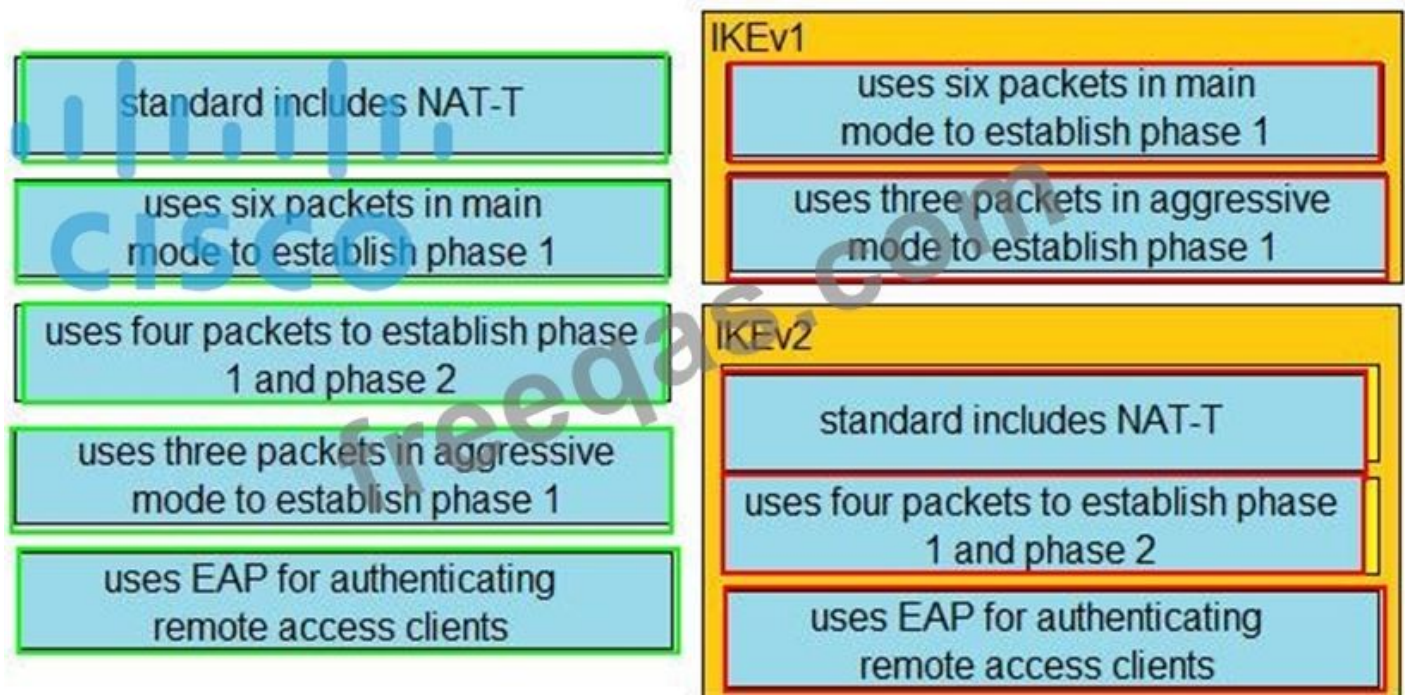
Up to 4 interfaces are permitted per bridge-group (inside, outside, DMZ1, DMZ2)

NEW QUESTION: 367

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



Answer:



NEW QUESTION: 368
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)
ExplanationA Proxy Auto-Configuration (PAC) file is a JavaScript function definition that determines whether web browserrequests (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 tosend traffic to the web proxy. The big advantage of PAC files is that they are usually relatively easy to createand maintain.

NEW QUESTION: 369
How does Cisco Workload Optimization Manager help mitigate application performance issues?
A. It deploys an AWS Lambda system
B. It automates resource resizing
C. It optimizes a flow path
D. It sets up a workload forensic score
Answer: (SHOW ANSWER)
Cisco Workload Optimization Manager provides specific real-time actions that ensure workloads get the resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software). Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software).
Cisco Workload Optimization Manager provides specific real-time actions that ensure workloads get the resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software). Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf

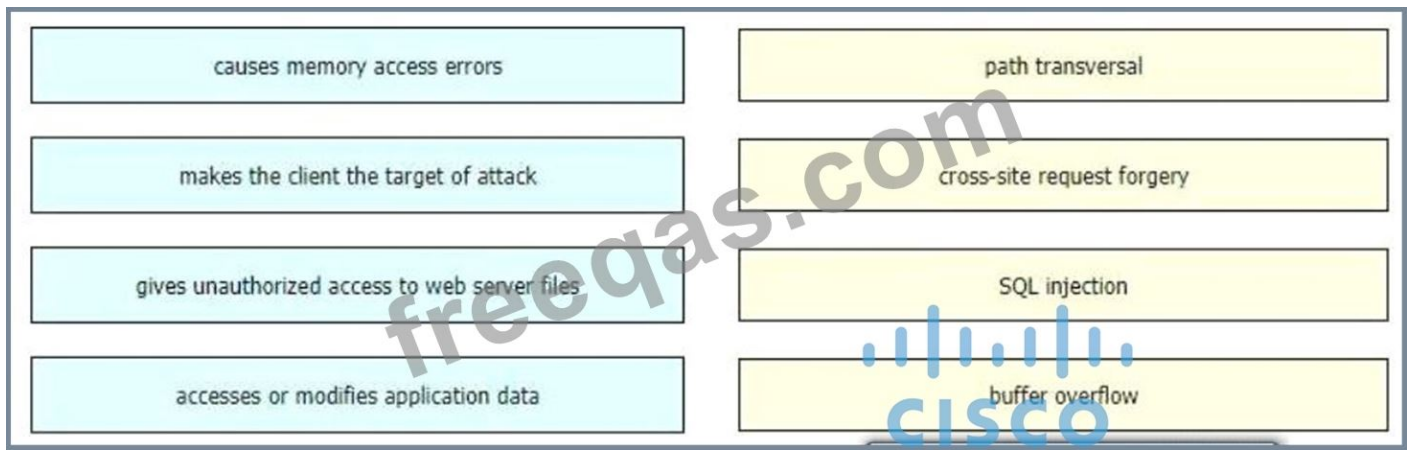
NEW QUESTION: 370
What are two functionalities of northbound and southbound APIs within Cisco SDN architecture? (Choose two.)
A. Southbound APIs are used to define how SDN controllers integrate with applications.
B. Southbound interfaces utilize device configurations such as VLANs and IP addresses.
C. Northbound APIs utilize RESTful API methods such as GET, POST, and DELETE.
D. Southbound APIs utilize CLI, SNMP, and RESTCONF.

E. Northbound interfaces utilize OpenFlow and OpFlex to integrate with network devices.
Answer: C,D (LEAVE A REPLY)
Northbound and southbound APIs are two types of interfaces that enable communication between different layers of the SDN architecture. Northbound APIs relay information between the controller and the applications or policy engines, while southbound APIs relay information between the controller and the network devices.
Northbound APIs allow applications to request network services or resources from the controller, such as bandwidth, latency, security, or routing. The controller then translates these requests into network configurations and applies them to the network devices via the southbound APIs. Northbound APIs typically use RESTful API methods such as GET, POST, and DELETE to communicate with the controller.
Southbound APIs allow the controller to program the network devices to perform forwarding and other functions. The controller can use different protocols or standards to communicate with the network devices, depending on their capabilities and vendor-specific features. Some common examples of southbound APIs are CLI, SNMP, RESTCONF, NETCONF, OpenFlow, and OpFlex.
References:
* Software-Defined Networking (SDN) Definition - Cisco
* Software-Defined Networking Security and Network ... - Cisco Press
* Cisco SDN - Software Defined Networking Explained - Study-CCNA
* SDN Network - Cisco Community

NEW QUESTION: 371
A network administrator configures Dynamic ARP Inspection on a switch. After Dynamic ARP Inspection is applied, all users on that switch are unable to communicate with any destination. The network administrator checks the Interface status of all interfaces, and there is no err-disabled interface. What is causing this problem?
A. DHCP snooping has not been enabled on all VLANs
B. Dynamic ARP inspection has not been enabled on all VLANs
C. The ip arp inspection limit command is applied on all interfaces and is blocking the traffic of all users
D. The no ip arp inspection trust command is applied on all user host interfaces
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 372
Which attack type attempts to shut down a machine or network so that users are not able to access it?
A. bluesnarfing
B. MAC spoofing
C. IP spoofing
D. smurf
Answer: D (LEAVE A REPLY)

NEW QUESTION: 373
Drag and drop the exploits from the left onto the type of security vulnerability on the right.



Answer:

NEW QUESTION: 374

How does Cisco AMP for Endpoints provide next-generation protection?

A. It leverages an endpoint protection platform and endpoint detection and response.

B. It utilizes Cisco pxGrid, which allows Cisco AMP to pull threat feeds from threat intelligence centers.

C. It encrypts data on user endpoints to protect against ransomware.

D. It integrates with Cisco FTD devices.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 375

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

A. Traffic is encrypted, which prevents visibility on firewalls and IPS systems.

B. Messenger applications cannot be segmented with standard network controls

C. Malware infects the messenger application on the user endpoint to send company data.

D. An exposed API for the messaging platform is used to send large amounts of data.

E. Outgoing traffic is allowed so users can communicate with outside organizations.

Answer: (SHOW ANSWER)

NEW QUESTION: 376

A network administrator is configuring a rule in an access control policy to block certain URLs and selects the "Chat and Instant Messaging" category. Which reputation score should be selected to accomplish this goal?

A. 1

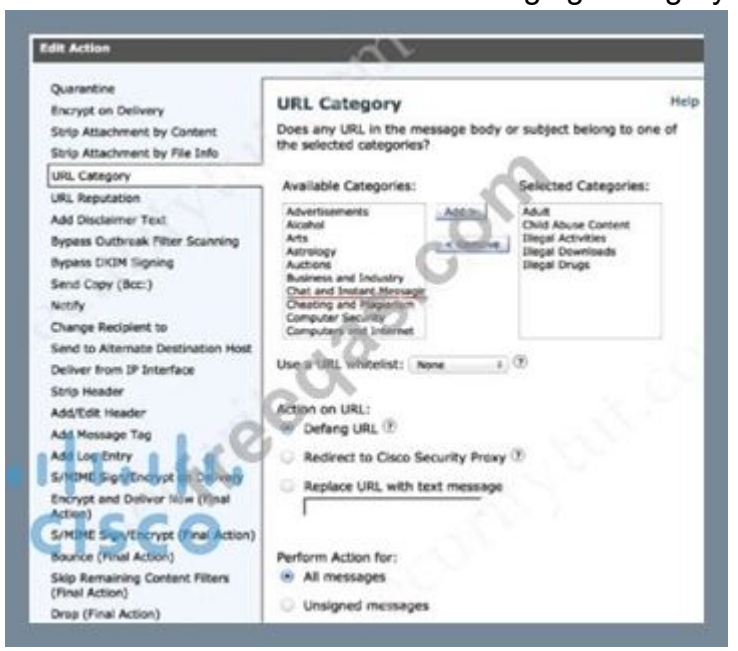
B. 3

C. 5

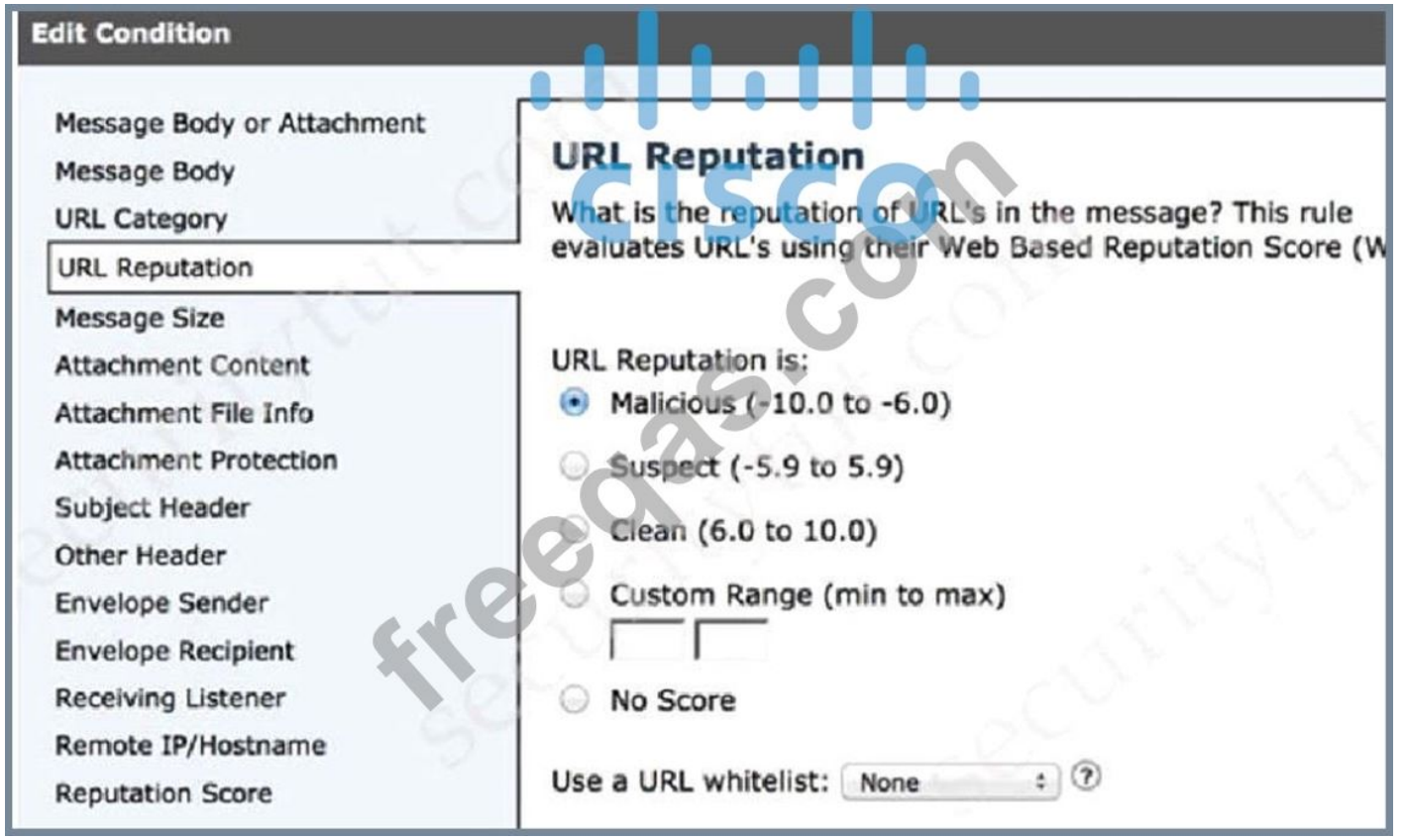
D. 10

Answer: D (LEAVE A REPLY)

We choose "Chat and Instant Messaging" category in "URL Category":



To block certain URLs we need to choose URL Reputation from 6 to 10.



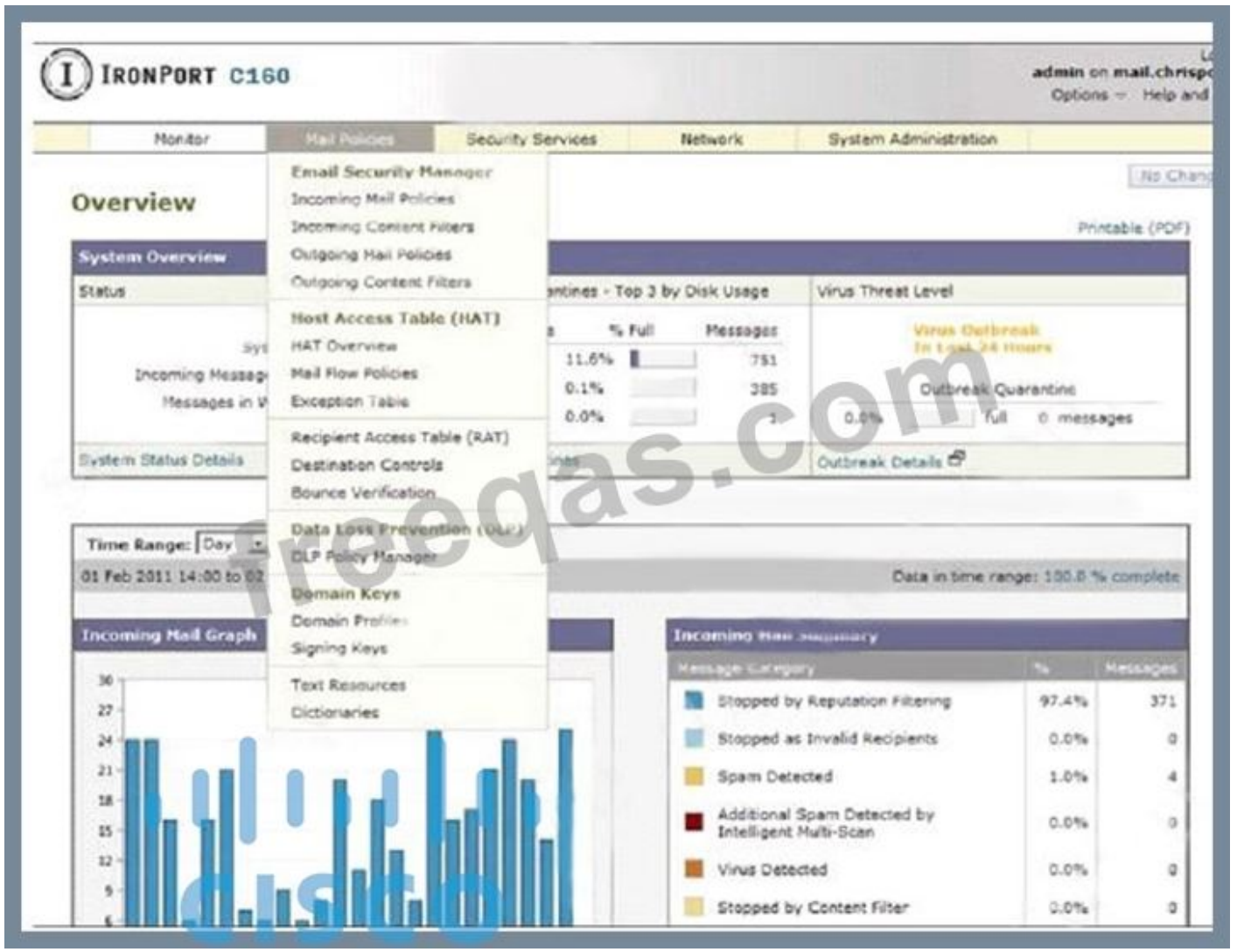
NEW QUESTION: 377
What do tools like Jenkins, Octopus Deploy, and Azure DevOps provide in terms of application and infrastructure automation?
A. continuous integration and continuous deployment
B. cloud application security broker
C. compile-time instrumentation
D. container orchestration
Answer: (SHOW ANSWER)
Tools like Jenkins, Octopus Deploy, and Azure DevOps provide continuous integration and continuous deployment (CI/CD) capabilities for application and infrastructure automation. CI/CD is a process that enables developers to deliver code changes more frequently and reliably by automating the building, testing, and deployment stages. CI/CD tools help to integrate various components of the software delivery pipeline, such as source control, testing frameworks, configuration management, security scanning, and deployment platforms. By using CI/CD tools, developers can achieve faster feedback loops, improved quality, reduced errors, and increased efficiency123.
According to the Cisco course on Implementing and Operating Cisco Security Core Technologies (SCOR), CI/CD is one of the key concepts of DevSecOps, which is a culture and practice that aims to embed security into every stage of the software development lifecycle. DevSecOps requires collaboration and communication between development, security, and operations teams, as well as the use of automation tools and techniques to ensure security is integrated throughout the process45. References: 1: Configuring Jenkins in Azure and deploying with Octopus 2: Octopus Deploy vs. Azure DevOps (VSTS/TFS) 3: Building .NET Core Apps in Azure DevOps and integrating Octopus Deploy 4: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 5: 350-701 SCOR - Cisco

NEW QUESTION: 378
A network administrator is using the Cisco ESA with AMP to upload files to the cloud for analysis. The network is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?
A. AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.
B. The file is queued for upload when connectivity is restored.
C. The file upload is abandoned.
D. The ESA immediately makes another attempt to upload the file.
Answer: C (LEAVE A REPLY)
Explanation The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more. Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technoteesa-00.html In this question, it stated "the network is congested" (not the file analysis server was overloaded) so the appliance will not try to upload the file again.
The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.
Reference:

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

NEW QUESTION: 379
Which two capabilities does TAXII support? (Choose two)
A. Exchange
B. Pull messaging
C. Binding
D. Correlation
E. Mitigating
Answer: B,C (LEAVE A REPLY)
The Trusted Automated eXchangeof Indicator Information (TAXII) specifies mechanisms for exchanging structured cyber threat information between parties over the network.
TAXII exists to provide specific capabilities to those interested in sharing structured cyber threat information.
TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilities that this version of TAXII supports: push messaging, pull messaging, and discovery.
Although there is no "binding" capability in the list but it is the best answer here.

NEW QUESTION: 380
An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically.
What must be configured to accomplish this?
A. Configure the Cisco WSA to modify policies based on the traffic seen
B. Configure the Cisco ESA to receive real-time updates from Talos
C. Configure the Cisco WSA to receive real-time updates from Talos
D. Configure the Cisco ESA to modify policies based on the traffic seen
Answer: D (LEAVE A REPLY)
The Mail Policies menu is where almost all of the controls related to email filtering happens. All the security and content filtering policies are set here, so it's likely that, as an ESA administrator, the pages on this menu are where you are likely to spend most of your time.



NEW QUESTION: 381
What is a functional difference between a cisco ASA and a cisco IOS router with Zone-based policy firewall?
A. The Cisco IOS router with Zone-Based Policy Firewall can be configured for high availability, whereas the Cisco ASA cannot
B. The Cisco ASA can be configured for high availability whereas the Cisco IOS router with Zone-Based Policy Firewall cannot
C. The Cisco IOS router with Zone-Based Policy Firewall denies all traffic by default, whereas the Cisco ASA starts out by allowing all traffic until rules are added
D. The Cisco ASA denies all traffic by default whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 382
What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two.)
A. snort
B. intelligent proxy
C. URL categorization
D. data exfiltration
E. command and control communication

Answer: (SHOW ANSWER)

NEW QUESTION: 383
When configuring ISAKMP for IKEv1 Phase 1on a Cisco IOS router, an administrator needs to input the command crypto isakmp key cisco address 0.0.0.0. The administrator is not sure what the IP address in this command is used for. What would he the effect of changing the IP address from 0,0.0 0 to 1,2.3.4?
A. The key server that is managing the keys for the connection will be at 1.2.3.4.
B. The address that will be used as the crypto validation authority
C. All IP addresses other than 1.2.3.4 will be allowed
D. The remote connection will only be allowed from 1.2.3.4
Answer: (SHOW ANSWER)

NEW QUESTION: 384
An email administrator is setting up a new Cisco ESA. The administrator wants to enable the blocking of greymail for the end user. Which feature must the administrator enable first?
A. File Analysis
B. IP Reputation Filtering
C. Intelligent Multi-Scan
D. Anti-Virus Filtering
Answer: C (LEAVE A REPLY)
Intelligent Multi-Scan (IMS) is a feature that enables the Cisco ESA to perform multiple anti-spam scans on each message and apply different actions based on the results. IMS also includes the Graymail Detection and Safe Unsubscribe services, which allow the ESA to identify and filter messages that are not strictly spam, but are low-priority or unwanted by the end user, such as newsletters, social media notifications, or marketing emails. The Graymail Detection service can classify messages into different categories, such as bulk, mass, or subscription, and assign different scores and verdicts to them. The Safe Unsubscribe service can provide a link for the end user to safely unsubscribe from the sender's mailing list, without revealing their email address or opening a malicious URL. To enable the blocking of greymail for the end user, the administrator must first enable the IMS feature globally and then configure the Graymail and Safe Unsubscribe settings in the mail policies. The administrator can also enable the centralized spam quarantine and the end-user quarantine interface to allow the end user to manage their own quarantined messages. References :=
* Best Practice Guide for Anti-Spam, Anti-Virus, Graymail and Outbreak Filters
* Graymail Detection and Safe Unsubscribing Functionality

NEW QUESTION: 385
Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'

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']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
            mac = network_interface.get('mac')
            ip = network_interface.get('ip')
            ipv6 = network_interface.get('ipv6')
            print(mac, ip, ipv6)
```

What does the API do when connected to a Cisco security appliance?

A. get the process and PID information from the computers in the network

B. create an SNMP pull mechanism for managing AMP

C. gather network telemetry information from AMP for endpoints

D. gather the network interface information about the computers AMP sees

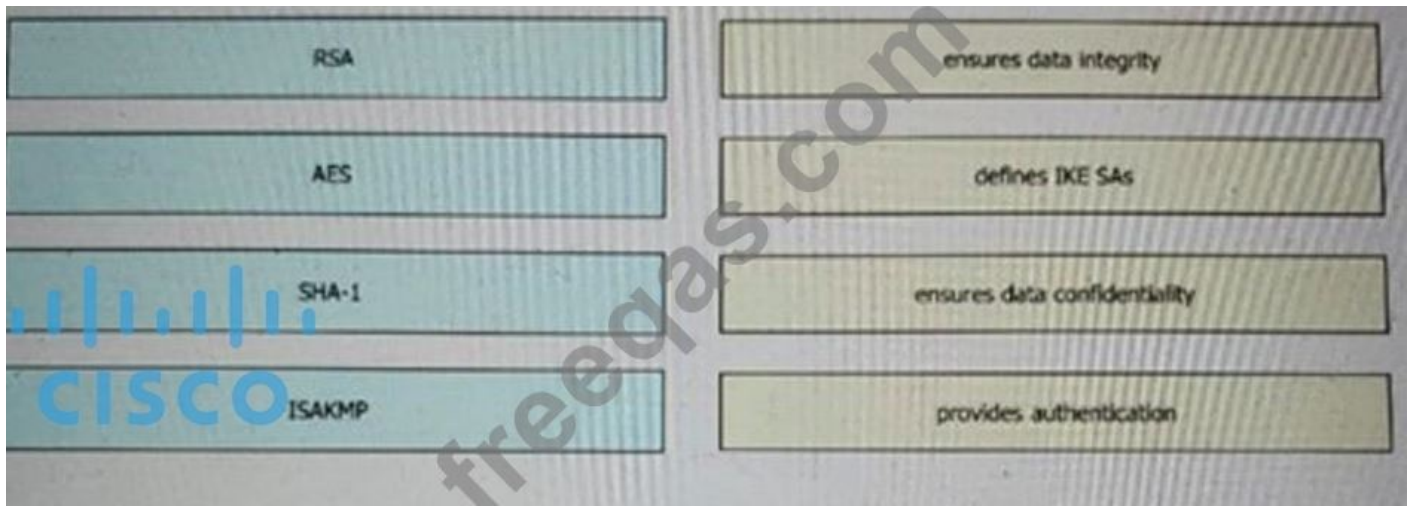
Answer: (SHOW ANSWER)

The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across your organization that Advanced Malware Protection (AMP) sees. Reference: 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 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: 386

Drag and drop the VPN functions from the left onto the description on the right.



Answer:

NEW QUESTION: 387
A network administrator is configuring a role in an access control policy to block certain URLs and selects the "Chat and instant Messaging" category. which reputation score should be selected to accomplish this goal?
A. 10
B. 1
C. 3
D. 5
Answer: A (LEAVE A REPLY)

NEW QUESTION: 388
What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group?
A. posture assessment
B. CoA
C. external identity source
D. SNMP probe
Answer: B (LEAVE A REPLY)
Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated. One of the settings to configure the CoA type is "Reauth". This option

is used to enforce reauthentication of an already authenticated endpoint when it is profiled. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_010101.html page that enables the profiling service with more control over endpoints that are already authenticated.
One of the settings to configure the CoA type is "Reauth". This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.
Reference:
Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated. One of the settings to configure the CoA type is "Reauth". This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_010101.html

NEW QUESTION: 389
In an IaaS cloud services model, which security function is the provider responsible for managing?
A. Internet proxy
B. firewalling virtual machines
C. CASB
D. hypervisor OS hardening
Answer: B (LEAVE A REPLY)
Explanation
In this IaaS model, cloud providers offer resources to users/machines that include computers as virtual machines, raw (block) storage, firewalls, load balancers, and network devices.
Note: Cloud access security broker (CASB) provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware such as ransomware.

NEW QUESTION: 390
Which term describes when the Cisco Secure Firewall downloads threat intelligence updates from Cisco Tables?
A. analysis
B. sharing
C. authoring
D. consumption
Answer: D (LEAVE A REPLY)
When the Cisco Secure Firewall downloads threat intelligence updates from Cisco Talos, it is engaged in "consumption." This term refers to the process of receiving and utilizing threat intelligence data to enhance security measures. Cisco Talos provides comprehensive threat intelligence that Cisco Secure Firewall consumes to update its threat detection and prevention capabilities.

NEW QUESTION: 391
Which Cisco DNA Center RESTful PNP API adds and claims a device into a workflow?
A. api/v1/fie/config
B. api/v1/onboarding/pnp-device/import

C. api/v1/onboarding/pnp-device
D. api/v1/onboarding/workflow
Answer: (SHOW ANSWER)

NEW QUESTION: 392
Which RADIUS attribute can you use to filter MAB requests in an 802.1 x deployment?
A. 1
B. 2
C. 6
D. 31
Answer: C (LEAVE A REPLY)
Because MAB uses the MAC address as a username and password, you should make sure that the RADIUS server can differentiate MAB requests from other types of requests for network access. This precaution will prevent other clients from attempting to use a MAC address as a valid credential. Cisco switches uniquely identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB Access-Request message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server. Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networkingservices/config_guide_c17-663759.html identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB Access-Request message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server.
Because MAB uses the MAC address as a username and password, you should make sure that the RADIUS server can differentiate MAB requests from other types of requests for network access. This precaution will prevent other clients from attempting to use a MAC address as a valid credential. Cisco switches uniquely identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB Access-Request message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server. Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networkingservices/config_guide_c17-663759.html

NEW QUESTION: 393
Which attack is commonly associated with C and C++ programming languages?
A. cross-site scripting
B. water holing
C. DDoS
D. buffer overflow
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://en.wikipedia.org/wiki/Buffer_overflow

NEW QUESTION: 394

Refer to the exhibit. What does this python script accomplish?
A. It authenticates to a Cisco ISE server using the username of ersad
B. It allows authentication with TLSv1 SSL protocol
C. It lists the LDAP users from the external identity store configured on Cisco ISE
D. It authenticates to a Cisco ISE with an SSH connection
Answer: B (LEAVE A REPLY)

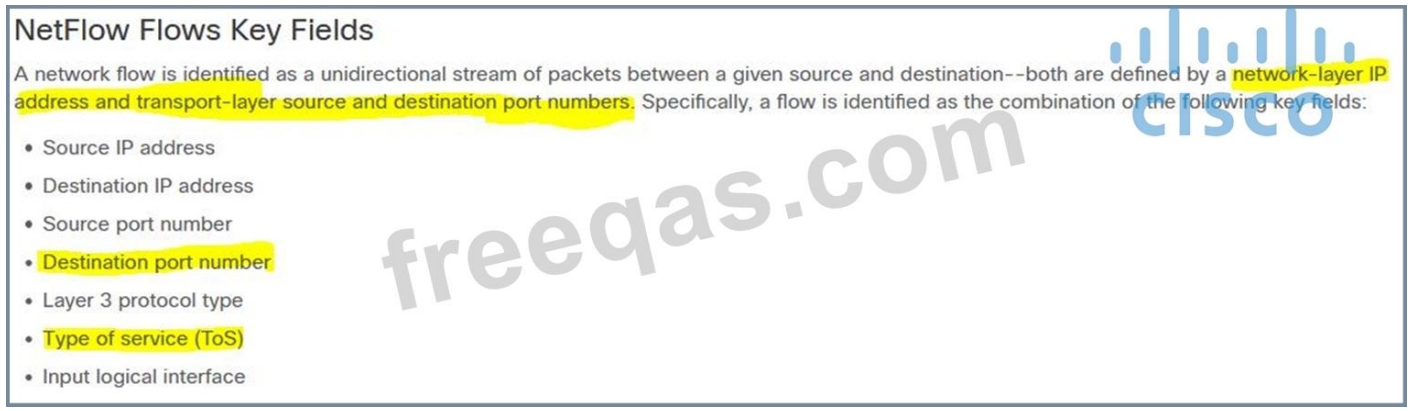
NEW QUESTION: 395
An engineer has enabled LDAP accept queries on a listener. Malicious actors must be prevented from quickly identifying all valid recipients.
What must be done on the Cisco ESA to accomplish this goal?
A. Use Bounce Verification
B. Configure incoming content filters.
C. Bypass LDAP access queries in the recipient access table.
D. Configure Directory Harvest Attack Prevention
Answer: D (LEAVE A REPLY)

NEW QUESTION: 396
An administrator is establishing a new site-to-site VPN connection on a Cisco IOS router. The organization needs to ensure that the ISAKMP key on the hub is used only for terminating traffic from the IP address of
172.19.20.24. Which command on the hub will allow the administrator to accomplish this?
A. crypto ca identity 172.19.20.24
B. crypto isakmp key Cisco0123456789 172.19.20.24
C. crypto enrollment peer address 172.19.20.24
D. crypto isakmp identity address 172.19.20.24
Answer: B (LEAVE A REPLY)
The command "crypto isakmp identity address 172.19.20.24" is not valid. We can only use "crypto isakmp identity {address | hostname}. The following example uses preshared keys at two peers and sets both their ISAKMP identities to the IP address.
At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified:
crypto isakmp identity address
crypto isakmp key sharedkeystring address 192.168.1.33
At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified:
crypto isakmp identity address
crypto isakmp key sharedkeystring address 10.0.0.1
Reference:
The command "crypto enrollment peer address" is not valid either.
The command "crypto ca identity ..." is only used to declare a trusted CA for the router and puts you in the caidentity configuration mode. Also it should be followed by a name, not an IP address. For example: "crypto ca identity CA-Server" -> Answer A is not correct.
Only answer B is the best choice left.

NEW QUESTION: 397
An MDM provides which two advantages to an organization with regards to device management? (Choose two.)

A. Active Directory group policy management
B. asset inventory management
C. critical device management
D. network device management
E. allowed application management
Answer: (SHOW ANSWER)

NEW QUESTION: 398
Which two fields are defined in the NetFlow flow? {Choose two.)
A. type of service byte
B. Layer 4 protocol type
C. class of service bits
D. output logical interface
E. destination port
Answer: (SHOW ANSWER)



NEW QUESTION: 399
Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?
A. Correlation
B. Intrusion
C. Access Control
D. Network Discovery
Answer: D (LEAVE A REPLY)
Explanation 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 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.
Explanation 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: 400
What is provided by the Secure Hash Algorithm in a VPN?
A. encryption
B. authentication
C. integrity
D. key exchange
Answer: (SHOW ANSWER)

NEW QUESTION: 401
Which Cisco solution provides a comprehensive view of Internet domains. IP addresses, and autonomous systems to help pinpoint attackers and malicious infrastructures?
A. Cisco Threat Indication Database
B. Cisco Advanced Malware Investigate
C. Cisco Umbrella Investigate
D. Cisco Secure Workload Cloud
Answer: C (LEAVE A REPLY)
Cisco Umbrella Investigate provides a comprehensive view of Internet domains, IP addresses, and autonomous systems, offering a wealth of information about the infrastructure of the internet. It helps security analysts and threat investigators to pinpoint current and emerging threats by providing access to data from Cisco's global network, thereby enabling the identification of attackers and malicious infrastructures.

NEW QUESTION: 402
An engineer needs to configure a Cisco Secure Email Gateway (SEG) to prompt users to enter multiple forms of identification before gaining access to the SEG. The SEG must also join a cluster using the preshared key of cisc421555367. What steps must be taken to support this?
A. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG GUI.
B. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG CLI.
C. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG CLI
D. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG GUI.
Answer: C (LEAVE A REPLY)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_

NEW QUESTION: 403
An organization has two systems in their DMZ that have an unencrypted link between them for communication.

The organization does not have a defined password policy and uses several default accounts on the systems.
The application used on those systems also have not gone through stringent code reviews. Which vulnerability would help an attacker brute force their way into the systems?
A. weak passwords
B. lack of input validation
C. missing encryption
D. lack of file permission
Answer: A (LEAVE A REPLY)

NEW QUESTION: 404
What is a benefit of using Cisco FMC over Cisco ASDM?
A. Cisco FMC uses Java while Cisco ASDM uses HTML5.
B. Cisco FMC provides centralized management while Cisco ASDM does not.
C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.
D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices
Answer: B (LEAVE A REPLY)
Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Reference:
Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system
"You cannot use an FMC to manage ASA firewall functions."
The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management.
Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system
"You cannot use an FMC to manage ASA firewall functions."
The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management.
Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system
"You cannot use an FMC to manage ASA firewall functions."
The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management.

NEW QUESTION: 405
In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint Protection Platform?
A. when there is a need for traditional anti-malware detection
B. when there is no need to have the solution centrally managed
C. when there is no firewall on the network
D. when there is a need to have more advanced detection capabilities

Answer: D (LEAVE A REPLY)
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: 406
Refer to the exhibit.

How does Cisco Umbrella manage traffic that is directed toward risky domains?
A. Traffic is allowed but logged.
B. Traffic is managed by the application settings, unhandled and allowed.
C. Traffic is proximed through the intelligent proxy.
D. Traffic is managed by the security settings and blocked.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 407
What is a prerequisite when integrating a Cisco ISE server and an AD domain?
A. Place the Cisco ISE server and the AD server in the same subnet
B. Configure a common administrator account
C. Configure a common DNS server
D. Synchronize the clocks of the Cisco ISE server and the AD server
Answer: D (LEAVE A REPLY)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_

NEW QUESTION: 408
Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?
A. DTLSv1
B. TLSv1
C. TLSv1.1
D. TLSv1.2
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/215331- anyconnect-implementation-and-performanc.html

NEW QUESTION: 409
Refer to the exhibit.

```
snmp-server group SNMP v3 auth access 15
```

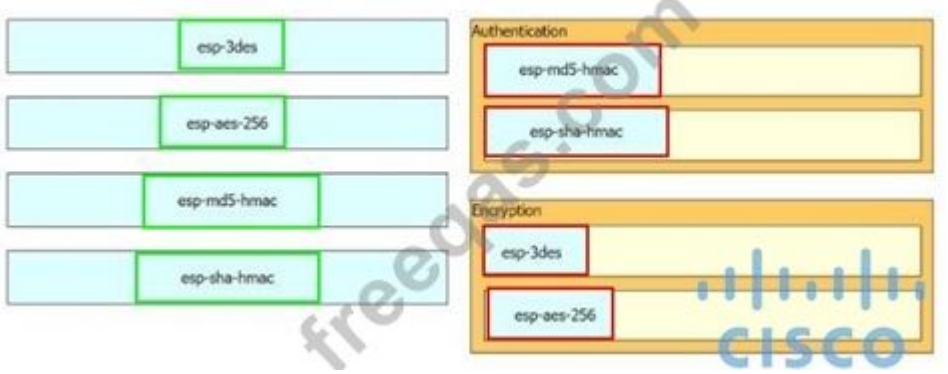
What does the number 15 represent in this configuration?
A. access list that identifies the SNMP devices that can access the router
B. privilege level for an authorized user to this router
C. interval in seconds between SNMPv3 authentication attempts
D. number of possible failed attempts until the SNMPv3 user is locked out
Answer: (SHOW ANSWER)

NEW QUESTION: 410
An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users.
A. Upload the organization root CA to the Umbrella admin portal
B. Modify the user's browser settings to suppress errors from Umbrella.
C. Restrict access to only websites with trusted third-party signed certificates.
D. Import the Umbrella root CA into the trusted root store on the user's device.

Answer: D (LEAVE A REPLY)
SSL decryption allows the intelligent proxy to inspect traffic over HTTPS. Some websites may use self-signed certificates or certificates that are not trusted by the user's device. This may cause the browser to display a warning or an error message when accessing those websites through the intelligent proxy. To avoid this, the user's device needs to trust the Umbrella root CA, which is the certificate authority that signs the certificates for the websites that are proxied by Umbrella. By importing the Umbrella root CA into the trusted root store on the user's device, the browser will recognize the certificates as valid and will not alert the end-users12. References: 1: Enable SSL Decryption - Umbrella User Guide 2: Intelligent Proxy and SSL Decryption with Cisco Umbrella

NEW QUESTION: 411
Drag and drop the cryptographic algorithms for IPsec from the left onto the cryptographic processes on the right.

Answer:



NEW QUESTION: 412
Which benefit does DMVPN provide over GETVPN?
A. DMVPN supports QoS, multicast, and routing, and GETVPN supports only QoS.
B. DMVPN can be used over the public Internet, and GETVPN requires a private network.
C. DMVPN supports non-IP protocols, and GETVPN supports only IP protocols.
D. DMVPN is a tunnel-less VPN, and GETVPN is tunnel-based.
Answer: (SHOW ANSWER)

NEW QUESTION: 413
What are the two types of managed Intercloud Fabric deployment models? (Choose two)
A. Service Provider managed
B. Public managed
C. Hybrid managed

D. User managed
E. Enterprise managed
Answer: (SHOW ANSWER)
Many enterprises prefer to deploy development workloads in the public cloud, primarily for convenience and faster deployment. This approach can cause concern for IT administrators, who must control the flow of IT traffic and spending and help ensure the security of data and intellectual property. Without the proper controls, data and intellectual property can escape this oversight. The Cisco Intercloud Fabric solution helps control this shadow IT, discovering resources deployed in the public cloud outside IT control and placing these resources under Cisco Intercloud Fabric control. Cisco Intercloud Fabric addresses the cloud deployment requirements appropriate for two hybrid cloud deployment models: Enterprise Managed (an enterprise manages its own cloud environments) and Service Provider Managed (the service provider administers and controls all cloud resources). Reference: https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric.pdf The Cisco Intercloud Fabric architecture provides two product configurations to address the following two consumption models: + Cisco Intercloud Fabric for Business + Cisco Intercloud Fabric for Providers Reference: https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric/Intercloud_Fabric_2.html

NEW QUESTION: 414
In a PaaS model, which layer is the tenant responsible for maintaining and patching?
A. hypervisor
B. virtual machine
C. network
D. application
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

NEW QUESTION: 415
A switch with Dynamic ARP inspection enabled has received a spoofed ARP response on a trusted interface. How does the switch behave in this situation?
A. It drops the packet after validation by using the IP & MAC Binding Table.
B. It drops the packet Without validation.
C. It forwards the packet without validation.
D. It forwards the packet after validation by using the MAC Binding Table.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 416
A company is experiencing exfiltration of credit card numbers that are not being stored on-premise. The company needs to be able to protect sensitive data throughout the full environment. Which tool should be used to accomplish this goal?
A. Security Manager
B. Cloudlock
C. Web Security Appliance
D. Cisco ISE
Answer: B (LEAVE A REPLY)

Explanation
Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

NEW QUESTION: 417
Which Cisco security solution stops exfiltration using HTTPS?
A. Cisco FTD
B. Cisco AnyConnect
C. Cisco CTA
D. Cisco ASA
Answer: C (LEAVE A REPLY)
https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf

NEW QUESTION: 418
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
```

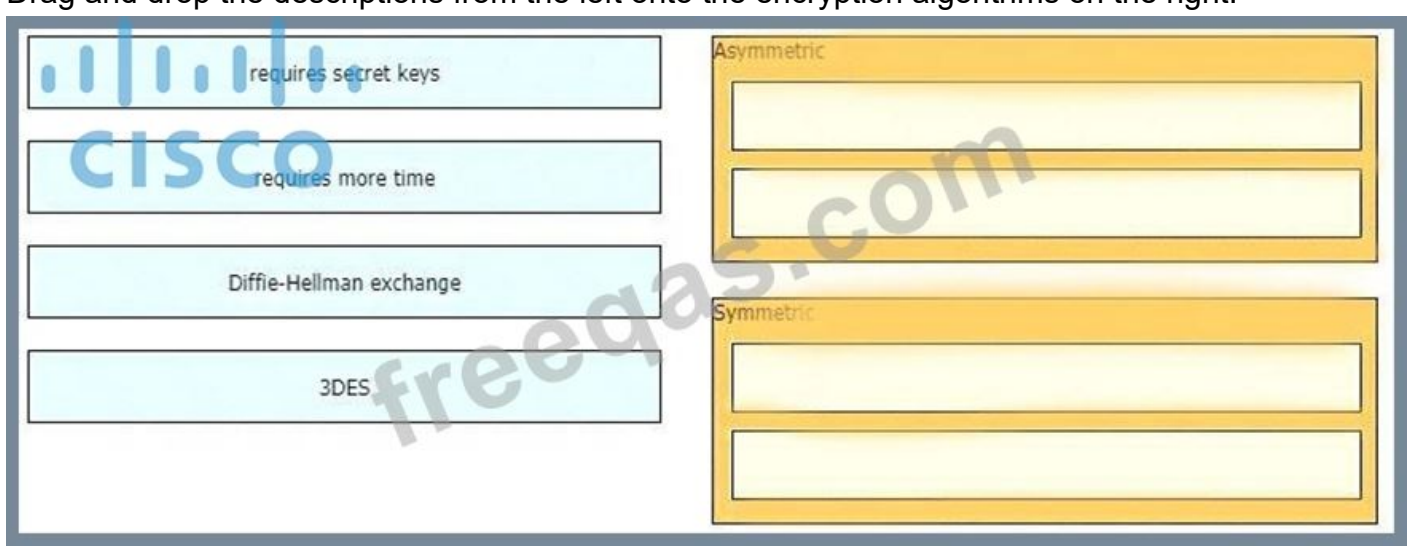
An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained. Which command should be configured on the switch interface in order to provide the user with network connectivity?
A. ip dhcp snooping verify mac-address
B. ip dhcp snooping limit 41
C. ip dhcp snooping vlan 41
D. ip dhcp snooping trust
Answer: (SHOW ANSWER)
Explanation
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp

NEW QUESTION: 419
Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.

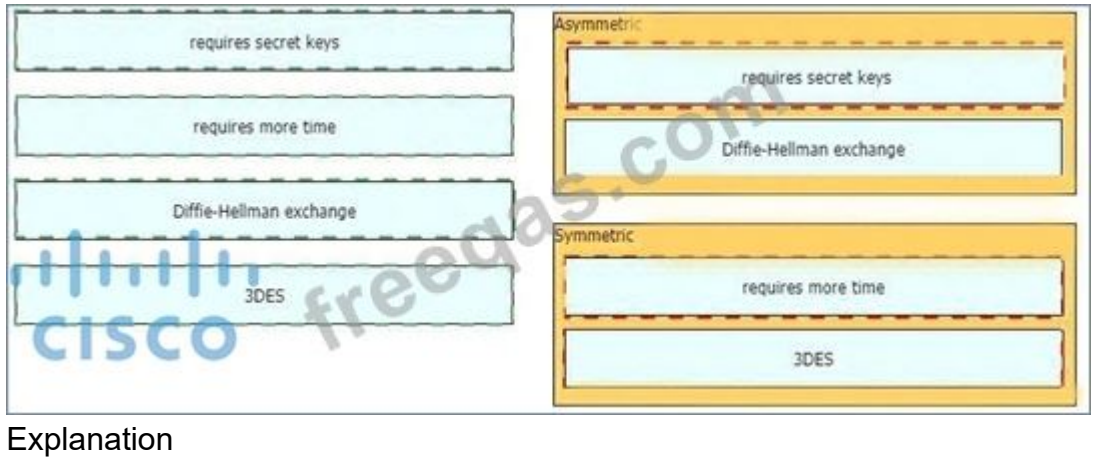
Answer:

NEW QUESTION: 420

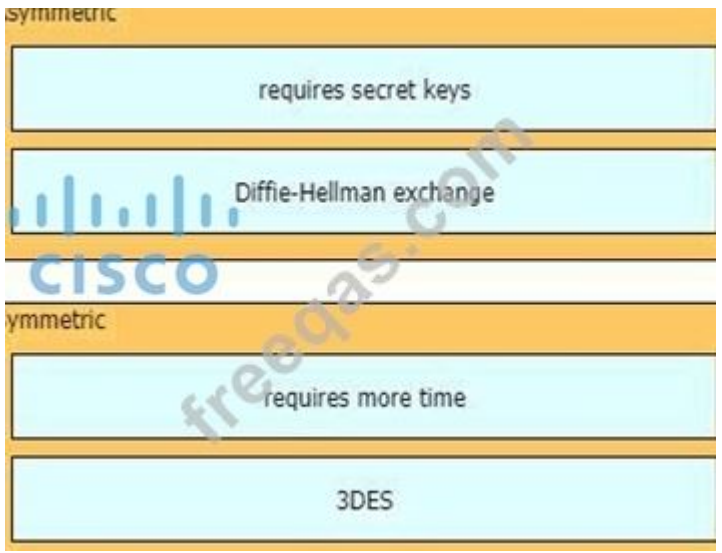
Drag and drop the descriptions from the left onto the encryption algorithms on the right.



Answer:



Explanation

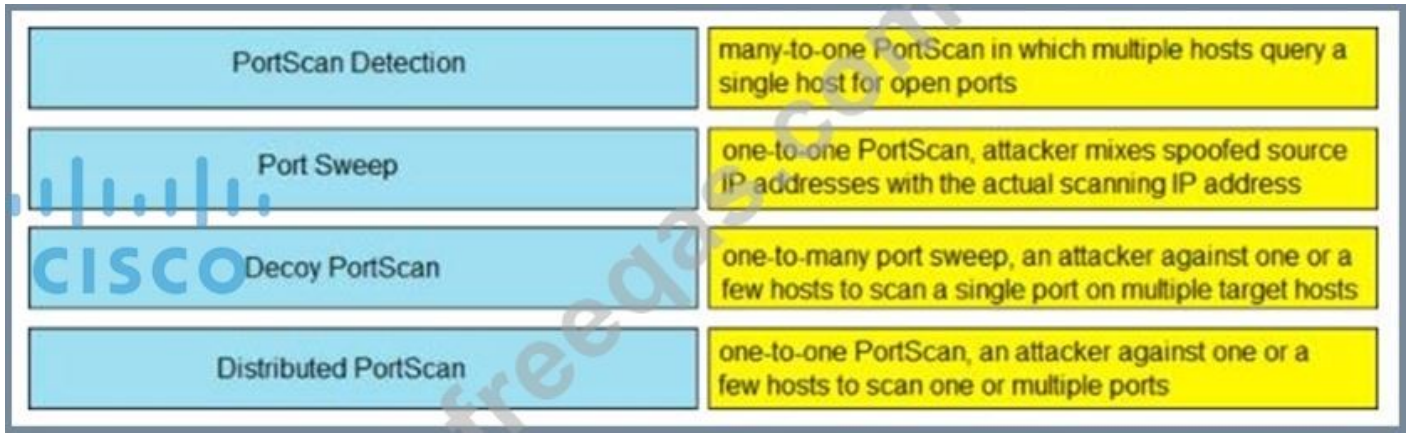


NEW QUESTION: 421
What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services?(Choose two)
A. multiple factor auth
B. local web auth
C. single sign-on
D. central web auth
E. TACACS+
Answer: B,D (LEAVE A REPLY)
Local web authentication (LWA) and central web authentication (CWA) are two mechanisms that are used to redirect users to a web portal to authenticate to ISE for guest services.
Both methods involve the use of a redirect access control list (ACL) that allows the user to access only the web portal URL and blocks all other traffic until the user is authenticated.
The difference between LWA and CWA is where the web portal and the authentication logic are hosted.
* LWA: The web portal and the authentication logic are hosted on the wireless LAN controller (WLC).
The WLC sends a RADIUS access-accept message to the network access device (NAD) along with the redirect ACL and the web portal URL. The NAD then redirects the user to the web portal on the WLC, where the user enters their credentials. The WLC verifies the credentials with the ISE and grants or denies access to the user.
The advantage of LWA is that it does not require any configuration on the ISE, but the disadvantage is that it does not support advanced features such as posture assessment, profiling, or authorization policies.
* CWA: The web portal and the authentication logic are hosted on the ISE.
The WLC sends a RADIUS access-challenge message to the NAD along with the redirect ACL and the web portal URL. The NAD then redirects the user to the web portal on the ISE, where the user enters their credentials. The ISE verifies the credentials and sends a RADIUS access-accept message to the WLC with the authorization profile and the final ACL. The WLC then applies the authorization profile and the final ACL to the user session. The advantage of CWA is that it supports advanced features such as posture assessment, profiling, or authorization policies, but the disadvantage is that it requires more configuration on the ISE.
References:
* Configure Guest Access
* Web Authentication Redirection to Original URL

* Configure Local Web Authentication with External Authentication

NEW QUESTION: 422

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



Answer:

NEW QUESTION: 423

Refer to the exhibit.

```
snmp-server group SNMP v3 auth access 15
```

What does the number 15 represent in this configuration?

A. interval in seconds between SNMPv3 authentication attempts

B. access list that identifies the SNMP devices that can access the router

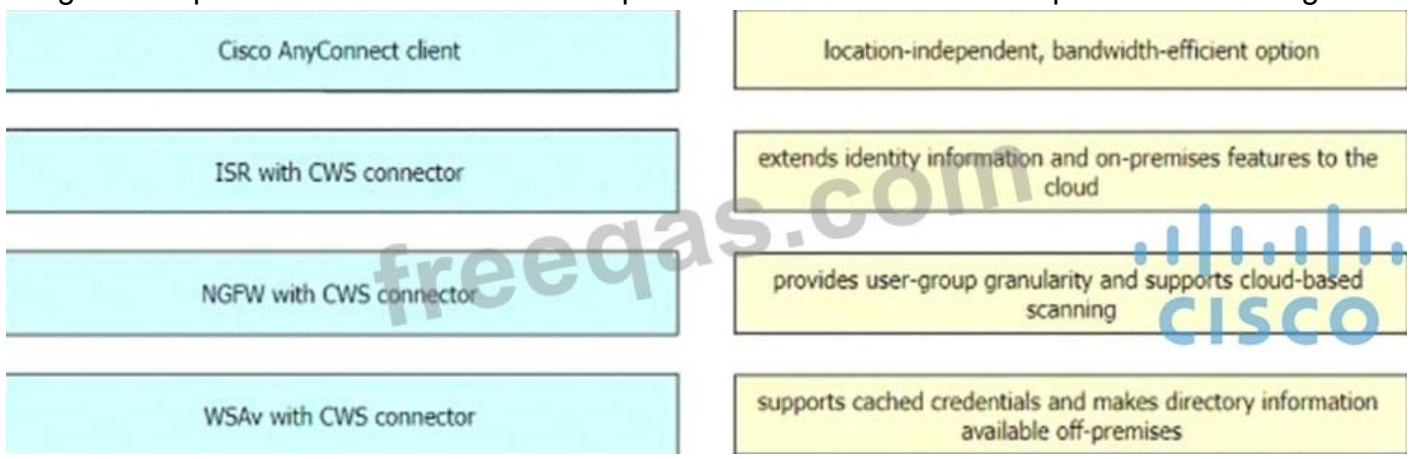
C. privilege level for an authorized user to this router

D. number of possible failed attempts until the SNMPv3 user is locked out

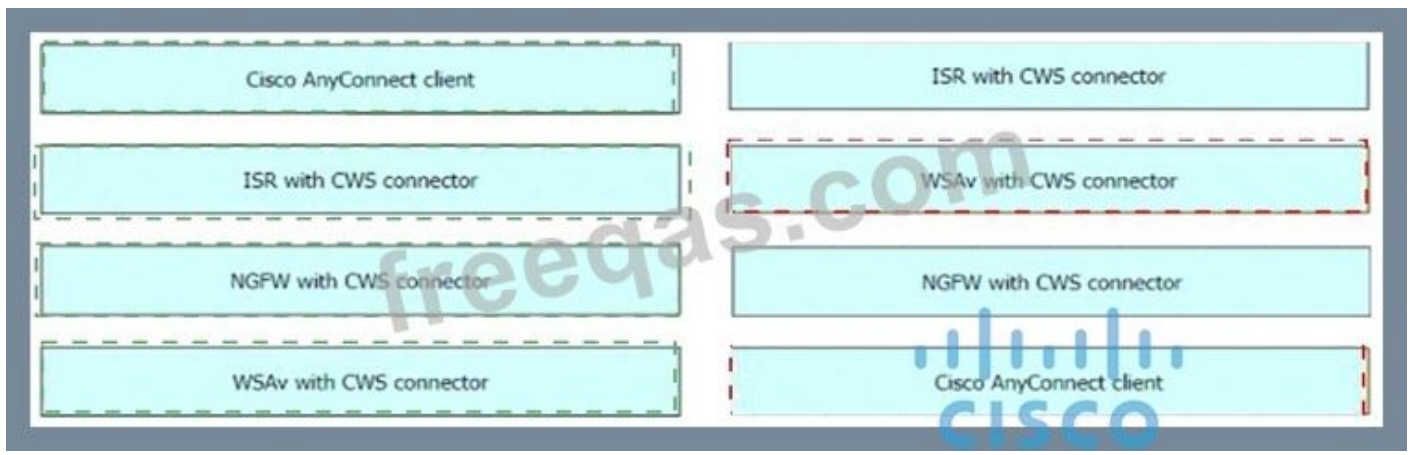
Answer: B (LEAVE A REPLY)

NEW QUESTION: 424

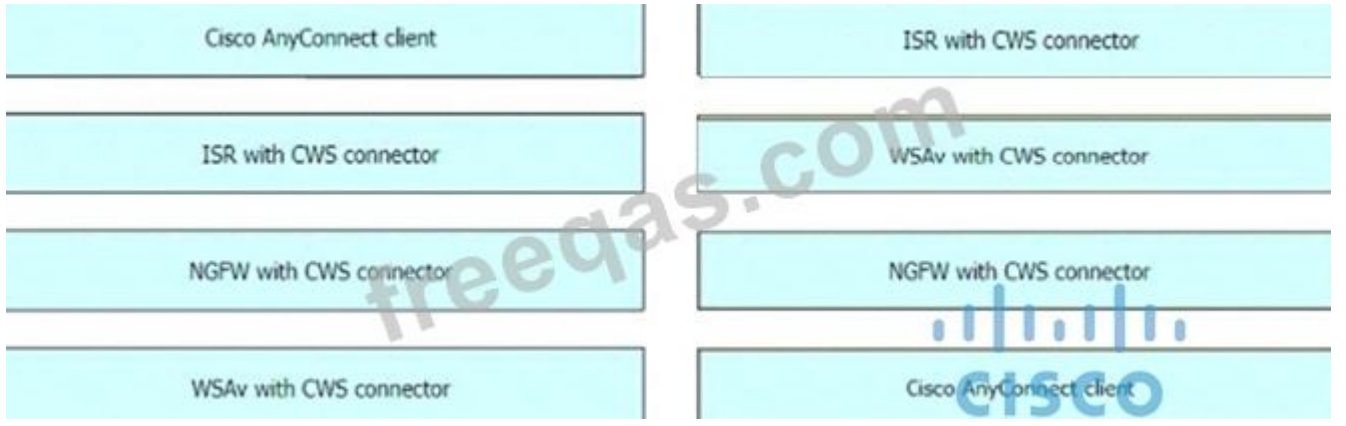
Drag and drop the Cisco CWS redirection options from the left onto the capabilities on the right.



Answer:



Explanation:



Reference:

https://www.westconcomstor.com/medias/CWS-data-sheet-c78-729637-1-.pdf?context=bWFzdGVyfHJvb3R8M