Cisco.350-701.v2025-06-19.q238

Exam Code:	350-701
Exam Name:	Implementing and Operating Cisco Security Core Technologies
Certification Provider:	Cisco
Free Question Number:	238
Version:	v2025-06-19
# of views:	111
# of Questions views:	2380
https://www.exam-tests.com/350-701-exam/Cisco.350-701.v2025-06-19.q238.html	

NEW QUESTION: 1
What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.) The eDirectory client must be installed on each client workstation.
A. Create NTLM or Kerberos authentication realm and enable transparent user identification
B. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.
C. Create an LDAP authentication realm and disable transparent user identification.
D. Deploy a separate eDirectory server: the client IP address is recorded in this server
Answer: A,B (LEAVE A REPLY)
Transparently identify users with authentication realms - This option is available when one or more authentication realms are configured to support transparent identification using one of the following authentication servers:
Active Directory - Create an NTLM or Kerberos authentication realm and enable transparent user identification. In addition, you must deploy a separate Active Directory agent such as Cisco's Context Directory Agent. For more information, see Transparent User Identification with Active Directory.
LDAP - Create an LDAP authentication realm configured as an eDirectory, and enable transparent user identification. For more information, see Transparent User Identification with LDAP.
Details:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01001.html#:~:text=Transparently%20identify%20users%20with%20authentication,User%20Identification%20with%20LDAP.

NEW QUESTION: 2
Which information is required when adding a device to Firepower Management Center?
A. device serial number
B. encryption method
C. registration key
D. username and password
Answer: (SHOW ANSWER)

NEW QUESTION: 3

Why is it important to implement MFA inside of an organization?
A. To prevent man-the-middle attacks from being successful.
B. To prevent DoS attacks from being successful.
C. To prevent brute force attacks from being successful.
D. To prevent phishing attacks from being successful.
Answer: C (LEAVE A REPLY)
Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy1. MFA is important to implement inside of an organization because it can prevent brute force attacks from being successful. A brute force attack is a type of cyberattack that tries to guess the user's password or PIN by trying different combinations until it finds the correct one. This can be done manually or with automated tools. MFA can stop brute force attacks by requiring an additional factor of authentication that the attacker does not have, such as a phone, a token, a biometric, or a location. MFA can also reduce the risk of other types of attacks that rely on stealing or compromising the user's credentials, such as phishing, keylogging, or credential stuffing. References := 1:
What is Multi-Factor Authentication (MFA)? | OneLogin

NEW QUESTION: 4
An engineer is configuring web filtering for a network using Cisco Umbrella Secure Internet Gateway.
The requirement is that all traffic needs to be filtered. Using the SSL decryption feature, which type of certificate should be presented to the end-user to accomplish this goal?
A. third-party
B. organization owned root
C. SubCA
D. self-signed
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
Refer to the exhibit.

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

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

NEW QUESTION: 6
Refer to the exhibit. When creating an access rule for URL filtering, a network engineer adds certain categories and individual URLs to block. What is the result of the configuration?

A. Only URLs for botnets with reputation scores of 1-3 will be blocked.
B. Only URLs for botnets with a reputation score of 3 will be blocked.
C. Only URLs for botnets with reputation scores of 3-5 will be blocked.
D. Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked.
Answer: B (LEAVE A REPLY)
The exhibit shows an access rule for URL filtering that has the following conditions:
* The action is Block
* The URL category is Botnets
* The URL reputation is 3
* The URL list is empty
This means that the rule will block any URL that matches the category and reputation criteria, regardless of the individual URL. According to the Cisco documentation1, the URL reputation is a score from 1 to 5 that indicates the risk level of a URL, where 1 is the most risky and 5 is the least risky. Therefore, a reputation score of 3 means a moderate risk level. The rule will not block URLs for botnets with reputation scores of 1, 2,
4, or 5, nor will it block any other URL category or list. The rule will also not allow any URL, as the action is Block, not Allow.
References := 1: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4:
Securing the Cloud, Lesson 4.3: Cloud Application Security, Topic 4.3.2: Cisco Umbrella, page 4-58.

NEW QUESTION: 7
Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two)
A. DDoS
B. antispam
C. antivirus
D. encryption
E. DLP
Answer: D,E (LEAVE A REPLY)
Explanation Cisco Hybrid Email Security is a unique service offering that combines a cloud-based email security deployment with an appliance-based email security deployment (on premises) to provide maximum choice and control for your organization. The cloud-based infrastructure is typically used for inbound email cleansing, while the onpremises appliances provide granular control - protecting sensitive information with data loss prevention (DLP) and encryption technologies. Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf 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:
Explanation Cisco Hybrid Email Security is a unique service offering that combines a cloud-based email security deployment with an appliance-based email security deployment (on premises) to provide maximum choice and control for your organization. The cloud-based infrastructure is typically used for inbound email cleansing, while the onpremises appliances provide granular control - protecting sensitive information with data loss prevention (DLP) and encryption technologies. Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

NEW QUESTION: 8

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

Answer:

NEW QUESTION: 9

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: 10

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

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

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

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

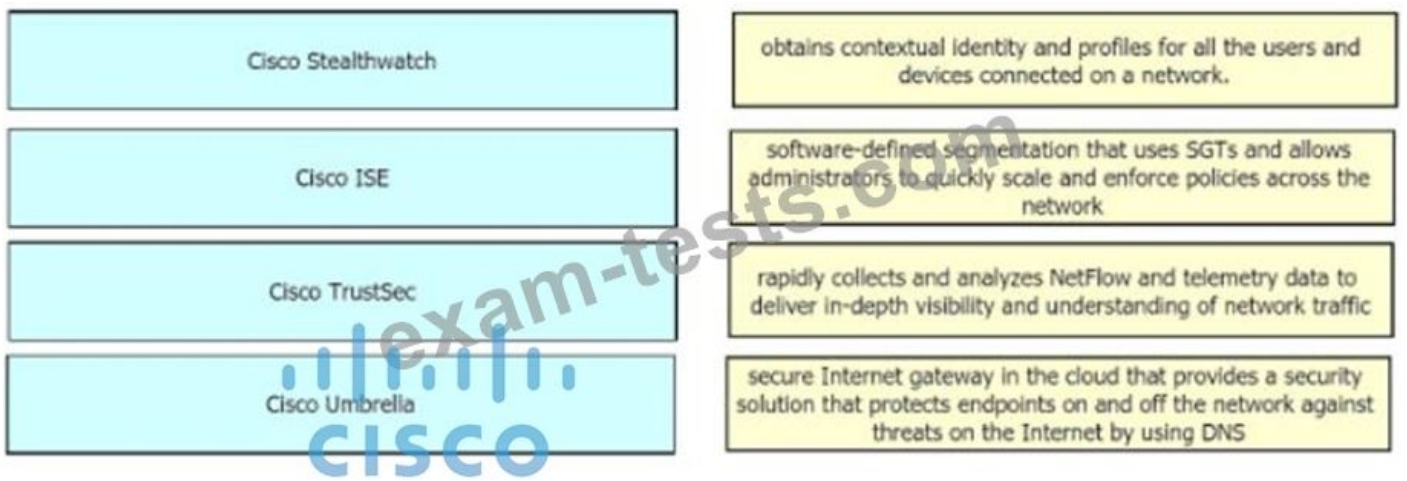
D. Messenger applications cannot be segmented with standard network controls.

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

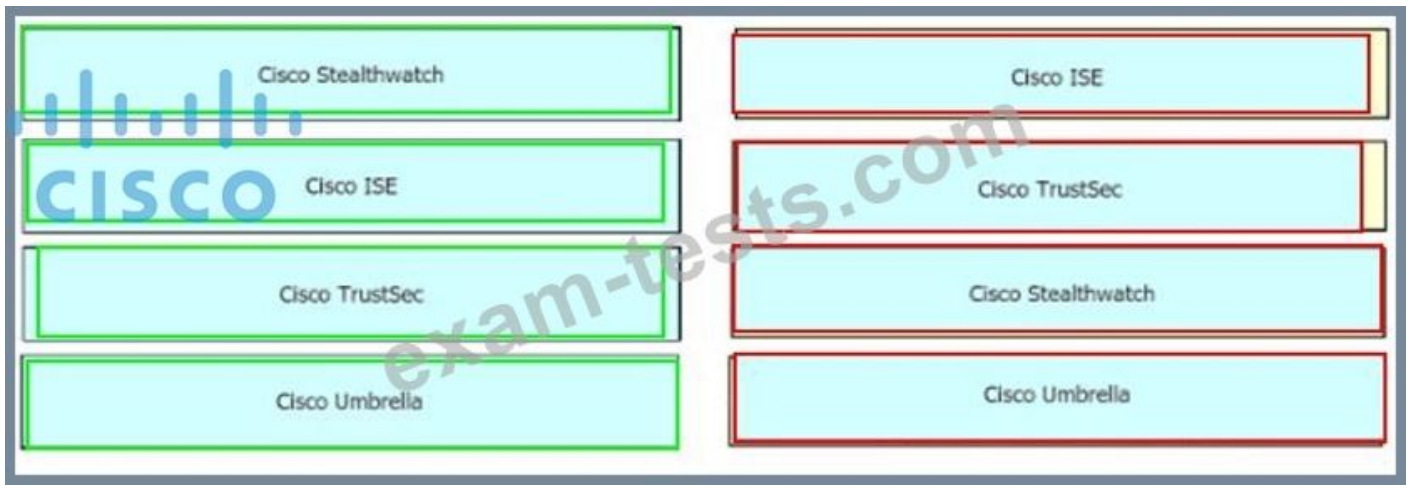
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 11
Which Cisco security solution secures public, private, hybrid, and community clouds?
A. Cisco Cloudlock
B. Cisco pxGrid
C. Cisco ISE
D. Cisco ASAv
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Drag and drop the solutions from the left onto the solution's benefits on the right.



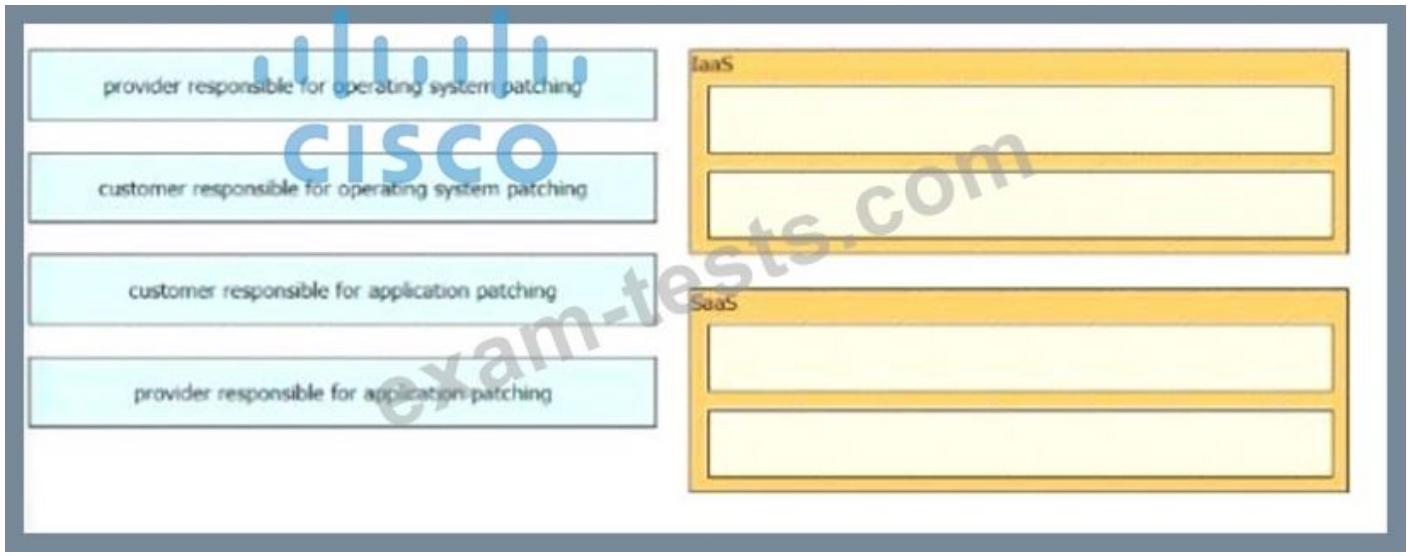
Answer:



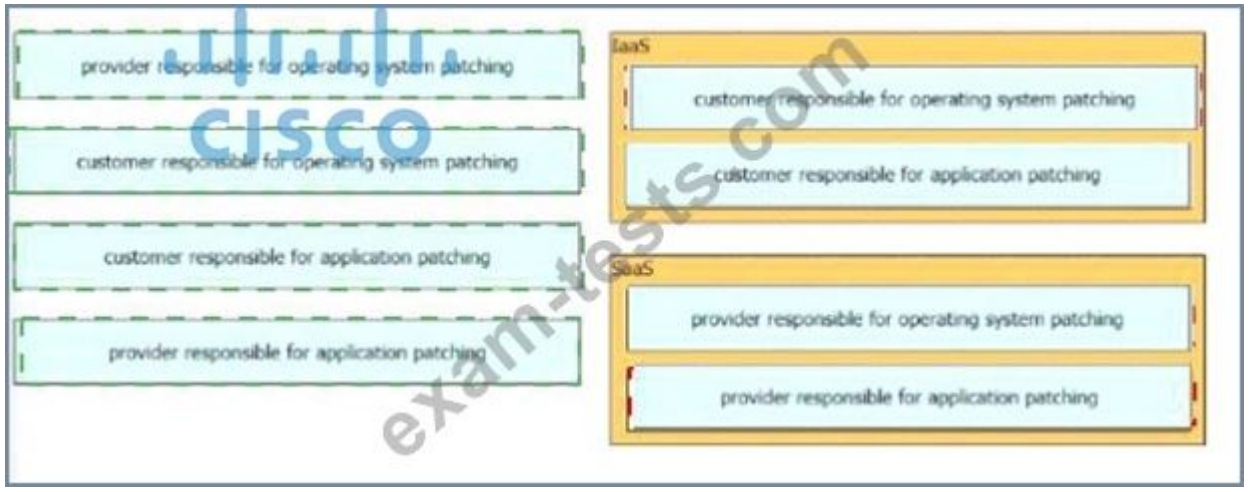
NEW QUESTION: 13
What is a benefit of a Cisco Secure Email Gateway Virtual as compared to a physical Secure Email Gateway?
A. simplifies the distribution of software updates
B. provides faster performance
C. provides an automated setup process
D. enables the allocation of additional resources
Answer: (SHOW ANSWER)

One of the benefits of a Cisco Secure Email Gateway Virtual appliance compared to a physical one is the ability to allocate additional resources as needed. Virtual appliances can be easily scaled up by allocating more CPU, memory, or storage resources, providing flexibility and scalability in response to changing demands or growth.

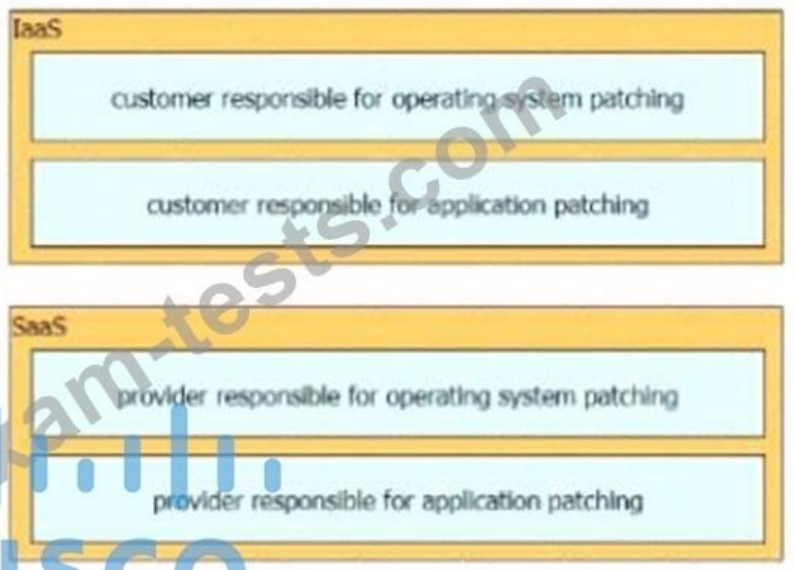
NEW QUESTION: 14
Drag and drop the security responsibilities from the left onto the corresponding cloud service models on the right.



Answer:



Explanation:

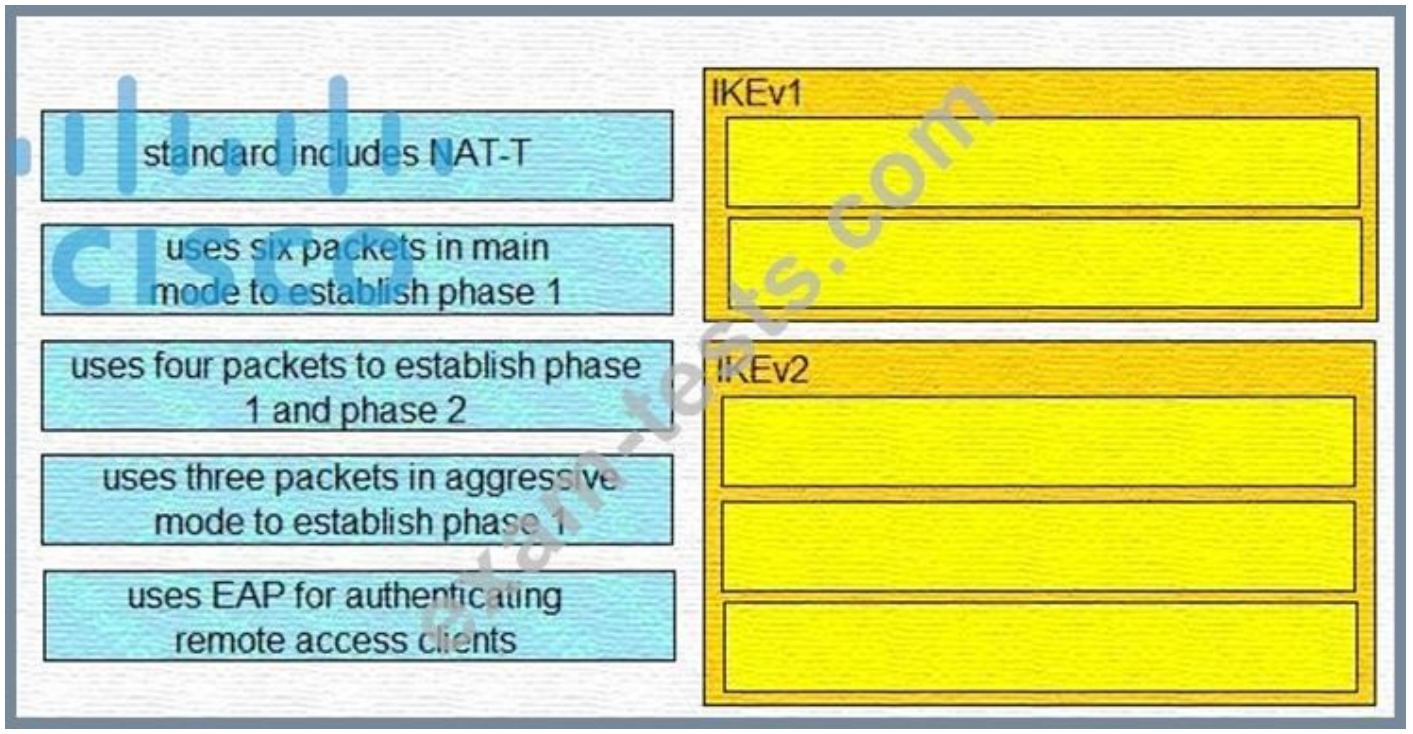


The cloud security shared responsibility model is a way of describing how the security tasks and obligations are divided between the cloud service provider (CSP) and the customer, depending on the type of cloud service model used. The cloud service models are:

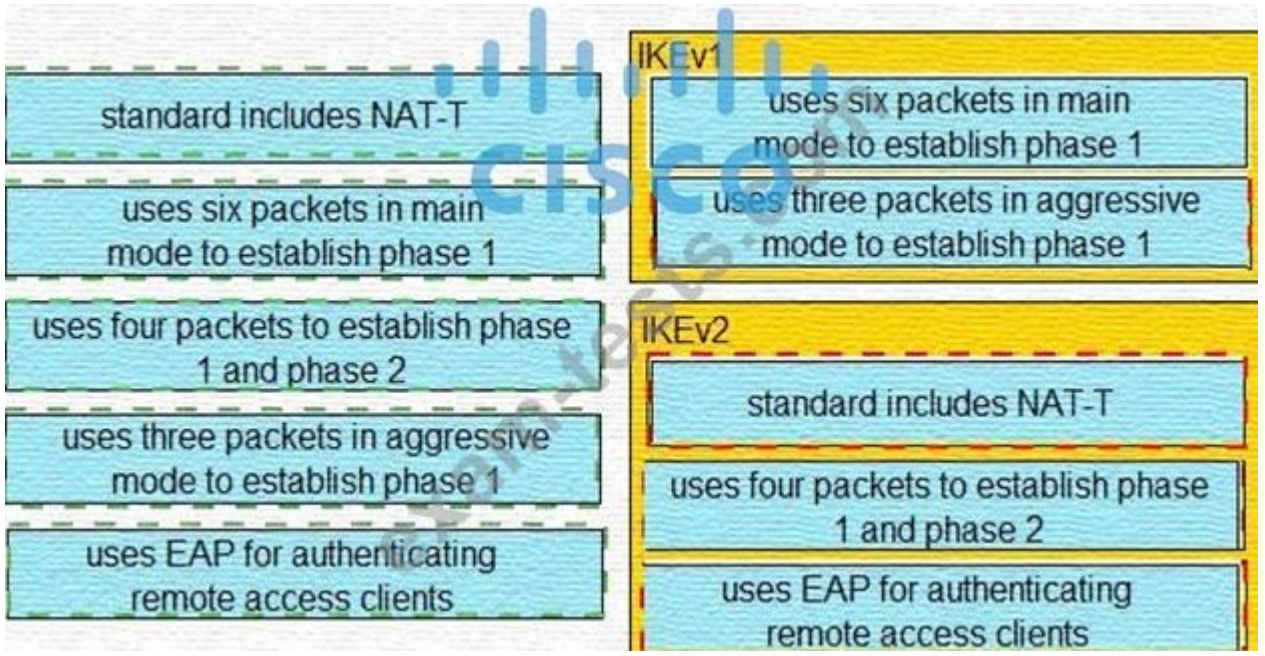
* Software as a Service (SaaS): The CSP provides and manages the entire software stack, including the applications, data, runtime, middleware, operating system, virtualization, servers, storage, and networking. The customer only needs to access the software through a web browser or an application.
The customer is responsible for managing their own data and identities, as well as configuring the security settings of the software. The CSP is responsible for everything else, including patching the operating system and the applications12
* Platform as a Service (PaaS): The CSP provides and manages the platform layer, including the runtime, middleware, operating system, virtualization, servers, storage, and networking. The customer can deploy and run their own applications and data on the platform, using the tools and languages supported by the CSP. The customer is responsible for managing their own applications and data, as well as configuring the security settings of the platform. The CSP is responsible for patching the operating system and the middleware12
* Infrastructure as a Service (IaaS): The CSP provides and manages the infrastructure layer, including the virtualization, servers, storage, and networking. The customer can provision and use virtual machines, containers, or bare metal servers, and install their own operating system, middleware, applications, and data. The customer is responsible for managing and patching their own operating system, middleware, applications, and data, as well as configuring the security settings of the infrastructure. The CSP is responsible for the physical security and availability of the infrastructure12 References := 1: Shared responsibility in the cloud - Microsoft Azure 2: Cloud security shared responsibility model - NCSC

NEW QUESTION: 15

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

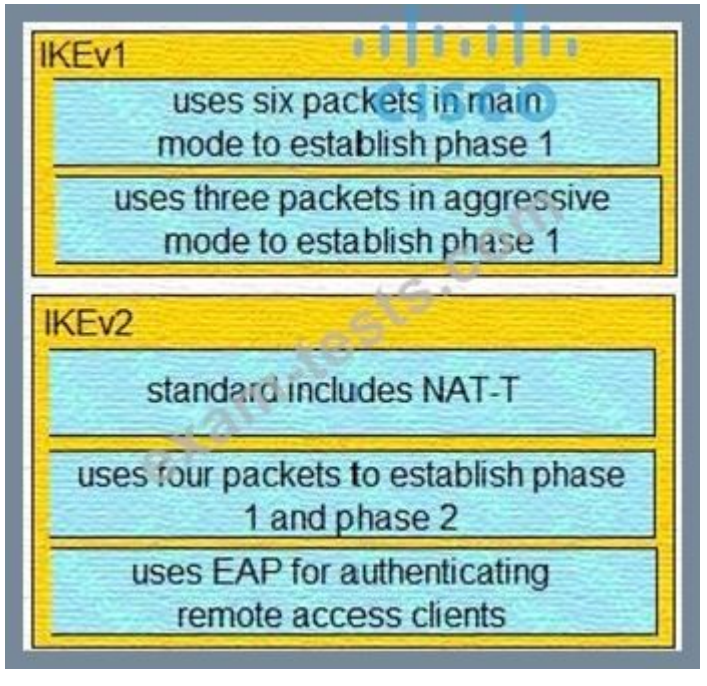


Answer:



Explanation:

Graphical user interface Description automatically generated with low confidence



NEW QUESTION: 16
Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two.)
A. RADIUS
B. TACACS+
C. DHCP
D. sFlow
E. SMTP
Answer: A,C (LEAVE A REPLY)
Explanation/Reference: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

NEW QUESTION: 17
Which term describes when the Cisco Firepower downloads threat intelligence updates from Cisco Talos?
A. consumption
B. sharing
C. analysis
D. authoring
Answer: (SHOW ANSWER)
Explanation Explanation ... we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's Firepower Management Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and

allows uploads/downloads of STIX and simple blacklists. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector Explanation
... we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's Firepower Explanation Explanation ... we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's Firepower Management Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector

NEW QUESTION: 18
Which security solution is used for posture assessment of the endpoints in a BYOD solution?
A. Cisco Umbrella
B. Cisco ISE
C. Cisco ASA
D. Cisco FTD
Answer: (SHOW ANSWER)

NEW QUESTION: 19
What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?
A. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously.
B. It discovers and controls cloud apps that are connected to a company's corporate environment.
C. It deletes any application that does not belong in the network.
D. It sends the application information to an administrator to act on.
Answer: (SHOW ANSWER)
The Cloudlock Apps Firewall is a feature of Cisco Cloudlock, which is a cloud-native cloud access security broker (CASB) that helps organizations move to the cloud safely. The Cloudlock Apps Firewall mitigates security concerns from an application perspective by discovering and controlling cloud apps that are connected to a company's corporate environment, such as Google G Suite or Microsoft Azure Active Directory (AD).
These cloud apps are authorized through OAuth to access corporate data and resources via APIs, and may pose risks such as data exfiltration, account compromise, or malicious behavior. The Cloudlock Apps Firewall provides visibility into the app ecosystem, including the app name, category, risk level, access scopes, and number of users. It also allows administrators to ban or allowlist apps based on their risk profile and compliance requirements.
Additionally, the Cloudlock Apps Firewall leverages a crowd-sourced Community Trust Rating for each app, which reflects the feedback from other Cloudlock customers on the app's security and functionality. References :=
* Cisco Content Security Products
* Cisco Cloudlock - Cisco
* Shadow IT Control with Apps Firewall - Cisco
* Test scor q151 - q200

NEW QUESTION: 20
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 themanagement 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.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmtnw.html

NEW QUESTION: 21
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: (SHOW ANSWER)
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: 22
Which Cisco DNA Center Intent API action is used to retrieve the number of devices known to a DNA Center?
A. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v
1/networkdevice/startIndex/recordsToReturn
B. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/network-device/count
C. GET
https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/networkdevice?parameter1=value&parameter2=va
D. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/network-device
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps. Which two actions must be taken to ensure that interfaces are put back into service? (Choose two)
A. Have Cisco Prime Infrastructure issue an SNMP set command to re-enable the ports after the preconfigured interval.
B. Use EEM to have the ports return to service automatically in less than 300 seconds.
C. Enter the shutdown and no shutdown commands on the interfaces.
D. Enable the snmp-server enable traps command and wait 300 seconds
E. Ensure that interfaces are configured with the error-disable detection and recovery feature
Answer: (SHOW ANSWER)
You can also bring up the port by using these commands:

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

NEW QUESTION: 24
Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two.)
A. modbus
B. inline normalization
C. SIP
D. packet decoder
E. SSL
Answer: (SHOW ANSWER)

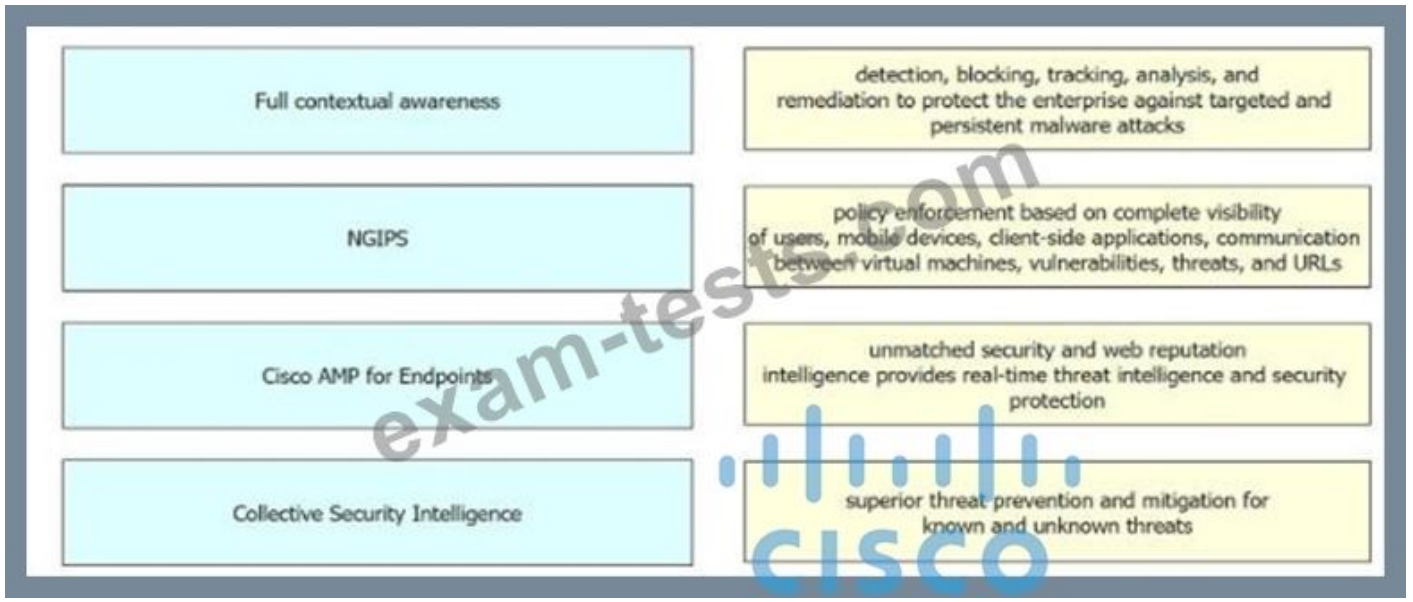
NEW QUESTION: 25
In which two ways does a system administrator send web traffic transparently to the Web Security Appliance? (Choose two.)
A. configure AD Group Policies to push proxy settings
B. configure policy-based routing on the network infrastructure
C. use Web Cache Communication Protocol
D. configure the proxy IP address in the web-browser settings
E. reference a Proxy Auto Config file
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 26
Which type of algorithm provides the highest level of protection against brute-force attacks?
A. SHA
B. PFS
C. MD5
D. HMAC
Answer: A (LEAVE A REPLY)

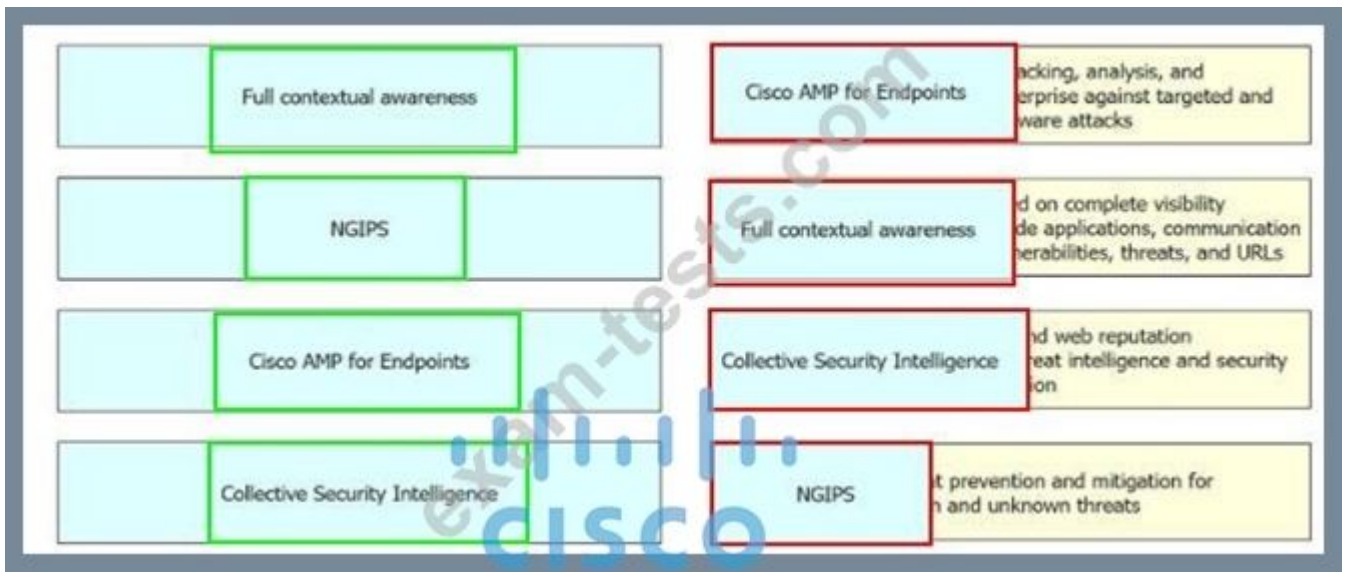
NEW QUESTION: 27
Which two kinds of attacks are prevented by multifactor authentication? (Choose two.)
A. phishing
B. brute force
C. man-in-the-middle
D. DDOS
E. tear drop
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 28

Drag and drop the security solutions from the left onto the benefits they provide on the right.



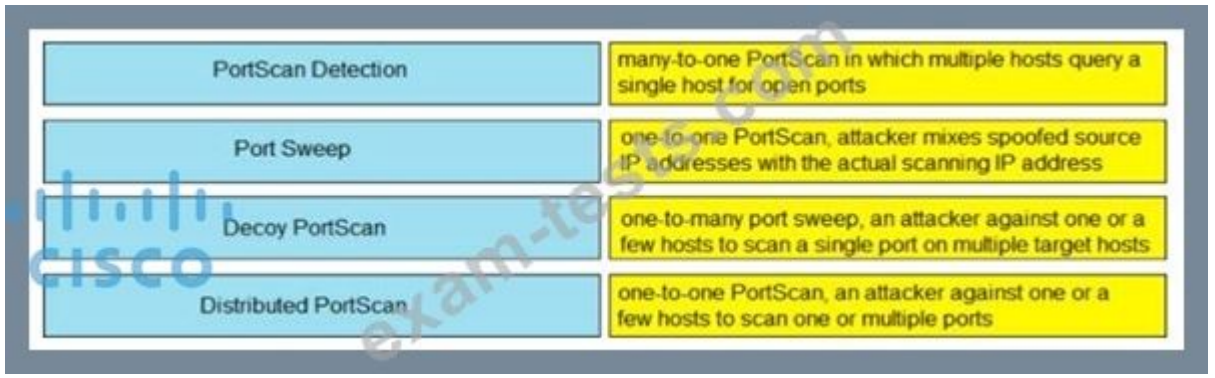
Answer:



NEW QUESTION: 29
What is a characteristic of Firepower NGIPS inline deployment mode?
A. ASA with Firepower module cannot be deployed.
B. It cannot take actions such as blocking traffic.
C. It is out-of-band from traffic.
D. It must have inline interface pairs configured.
Answer: (SHOW ANSWER)
Firepower NGIPS inline deployment mode is a mode where the NGIPS device is placed in the traffic path and can take actions such as blocking, modifying, or redirecting traffic based on the policies and rules. In this mode, the NGIPS device must have inline interface pairs configured, which are pairs of physical or logical interfaces that act as a single logical interface. The inline interface pairs are connected to the network devices on both sides of the NGIPS device, and the traffic flows through the NGIPS device from one interface to the other. The NGIPS device can inspect and modify the traffic as it passes through the inline interface pairs12. References := 1: Firepower Management Center Configuration Guide, Version 6.6 - Device Management Basics 2: Configure FTD Interfaces in Inline-Pair Mode

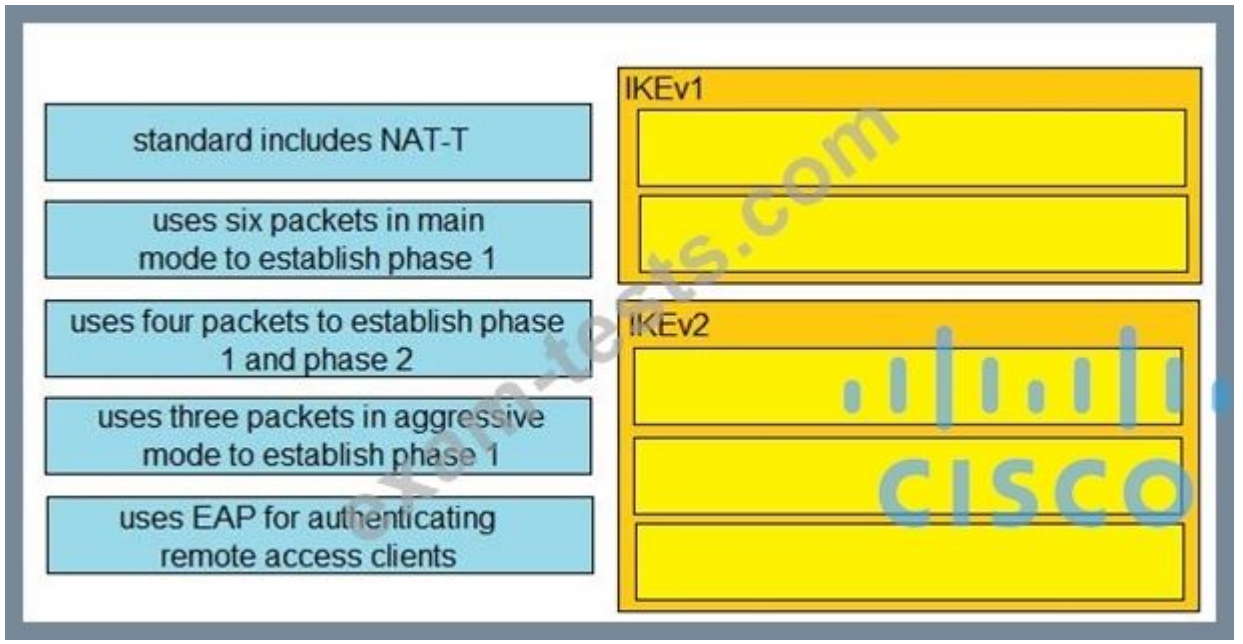
NEW QUESTION: 30
An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch was not installed, which left the endpoint vulnerable to WannaCry ransomware. Which two solutions mitigate the risk of this ransomware infection? (Choose two.)
A. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.
B. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.
C. Set up a profiling policy in Cisco Identity Service Engine to check and endpoint patch level before allowing access on the network.
D. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.
E. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.

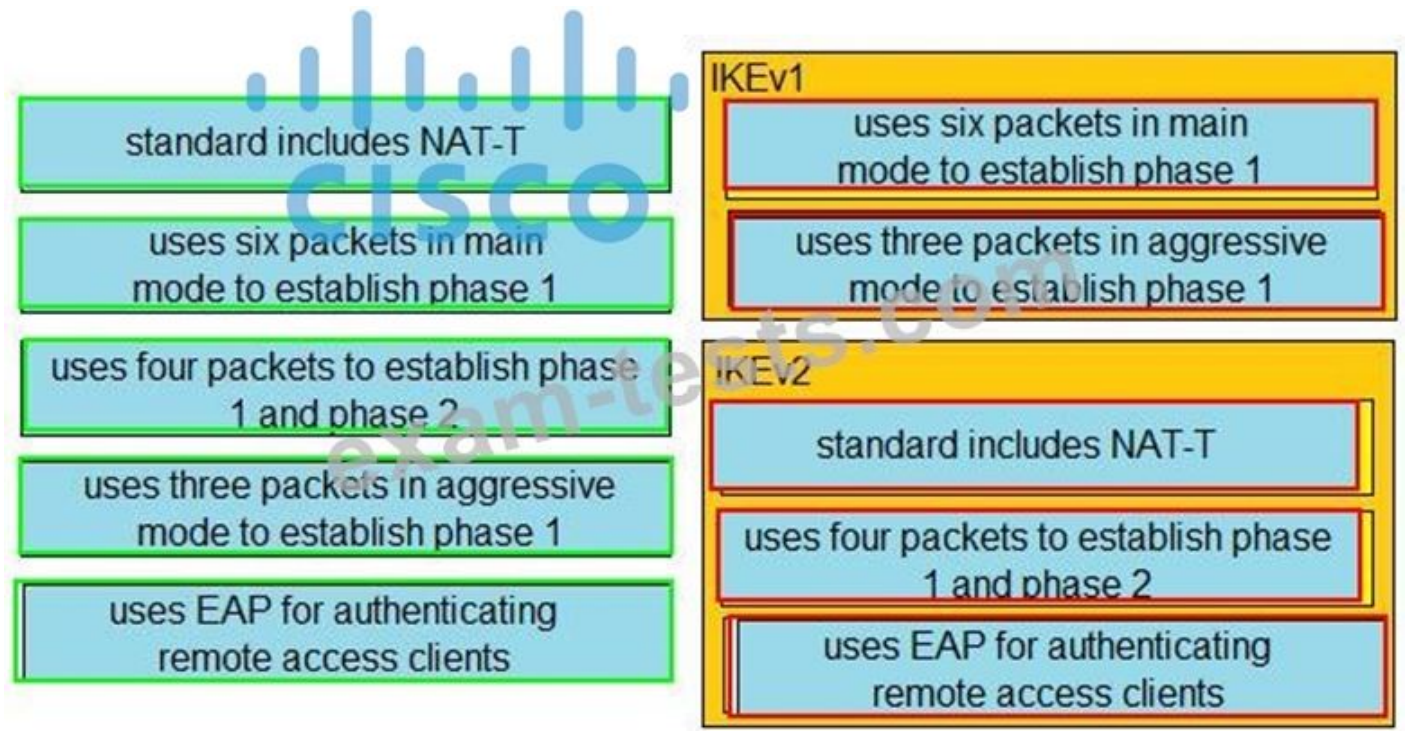


Answer:

NEW QUESTION: 32
Drag and drop the descriptions from the left onto the correct protocol versions on the right.

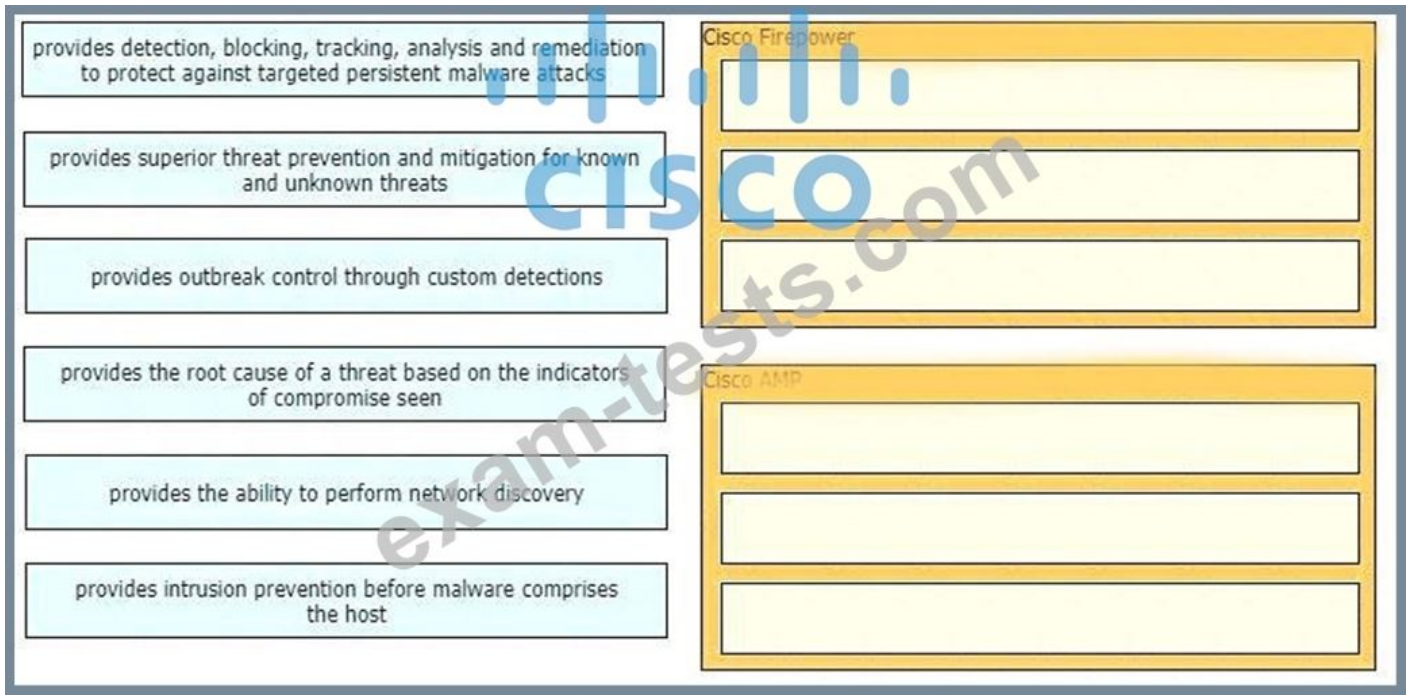


Answer:

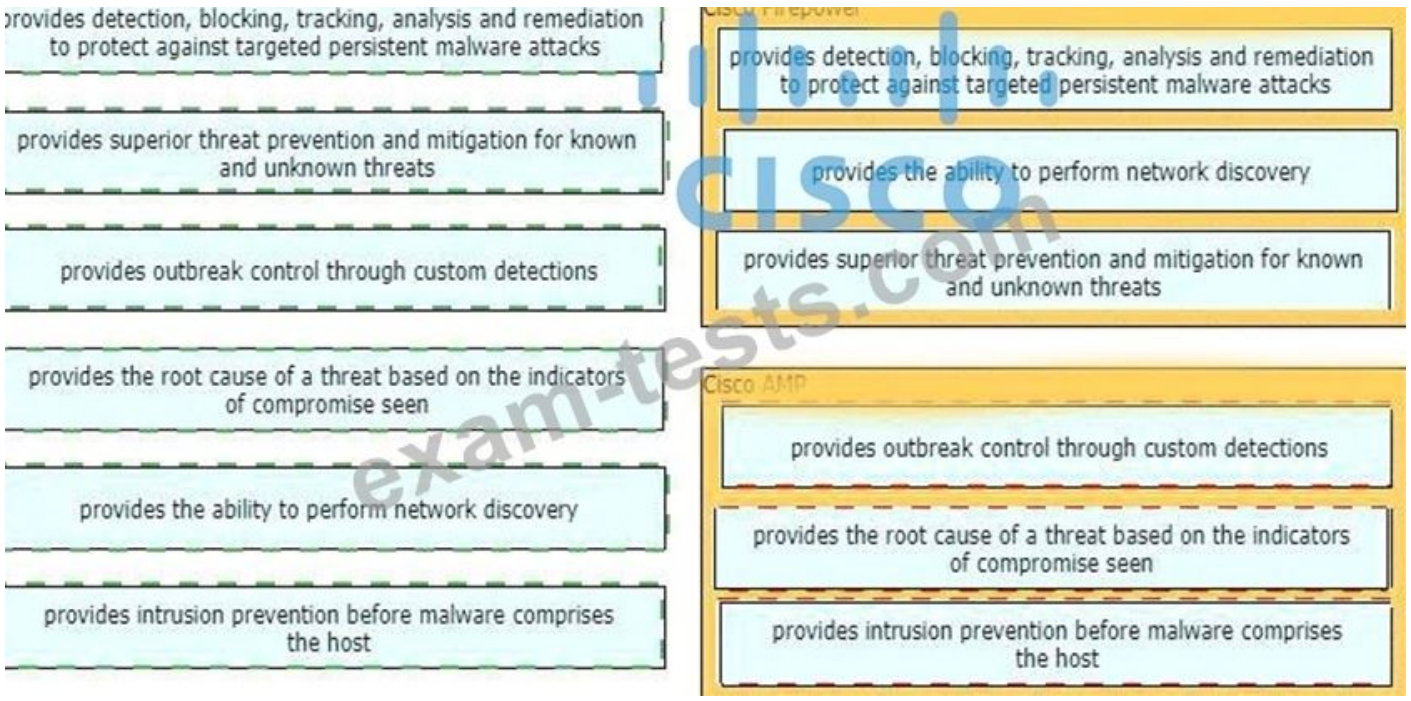


NEW QUESTION: 33

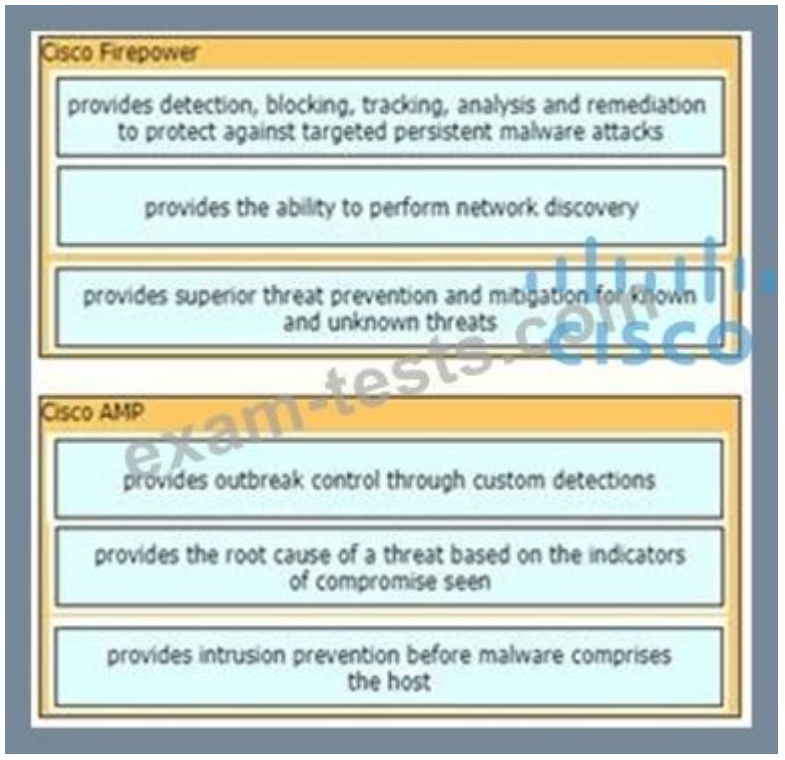
Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.



Answer:

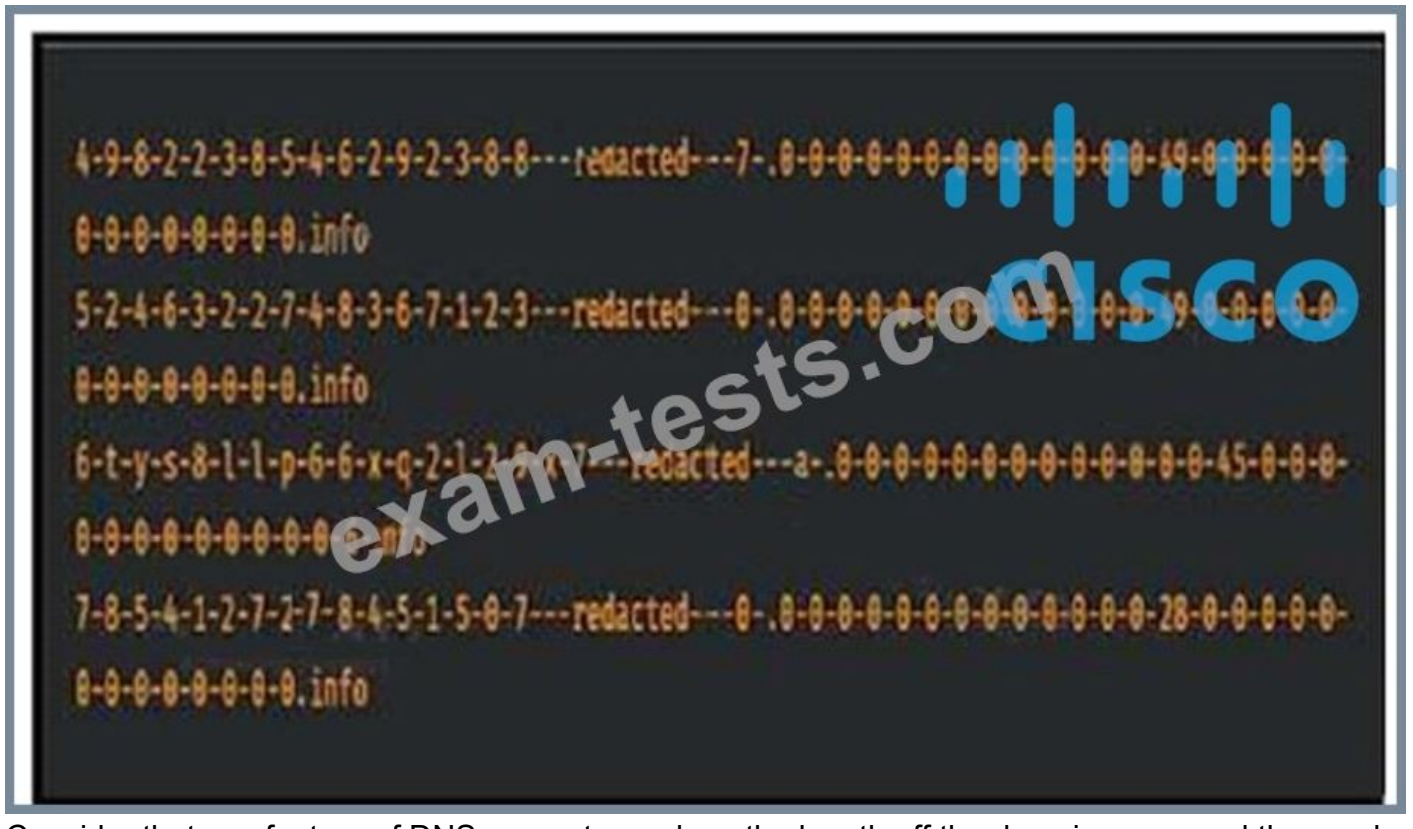


Explanation



https://www.cisco.com/c/en/us/products/collateral/security/ngips/datasheet-c78-742472.html
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Refere
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-ov

NEW QUESTION: 34
Refer to the exhibit.

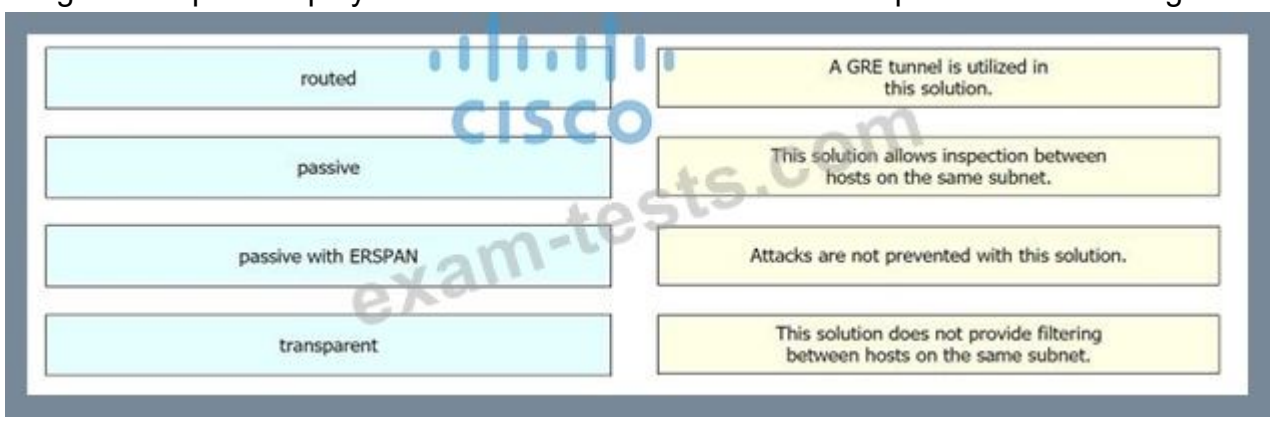


Consider that any feature of DNS requests, such as the length off the domain name and the number of subdomains, can be used to construct models of expected behavior to which observed values can be compared. Which type of malicious attack are these values associated with?

A. Heartbleed SSL Bug
B. Eternal Blue Windows
C. W32/AutoRun worm
D. Spectre Worm
Answer: C (LEAVE A REPLY)

NEW QUESTION: 35
Which statement about IOS zone-based firewalls is true?
A. An unassigned interface can communicate with assigned interfaces
B. Only one interface can be assigned to a zone.
C. An interface can be assigned to multiple zones.
D. An interface can be assigned only to one zone.
Answer: D (LEAVE A REPLY)
IOS zone-based firewalls (ZBFW) are a feature that provides stateful firewall policies between groups of interfaces known as zones. A zone is a logical grouping of one or more interfaces that have similar security requirements. A zone can be applied to physical interfaces, subinterfaces, port channels, VLAN interfaces, or tunnel interfaces. However, an interface can be assigned only to one zone, and it cannot be shared between zones. This is because the ZBFW policy is applied between zones, not interfaces, and it controls the bidirectional traffic flow between them. Therefore, an interface can belong to only one zone at a time, and it must be removed from one zone before it can be added to another zone. This ensures that the firewall policy is consistent and unambiguous for each interface.
References :=
* Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS XE Gibraltar 16.12.x, Configuring Zones
* Understand the Zone-Based Policy Firewall Design, Zone-Based Policy Overview
* IOS Zone Based Firewall Step-by-Step Basic Configuration, Zone Based Firewall Vs CBAC

NEW QUESTION: 36
Drag and drop the deployment models from the left onto the explanations on the right.

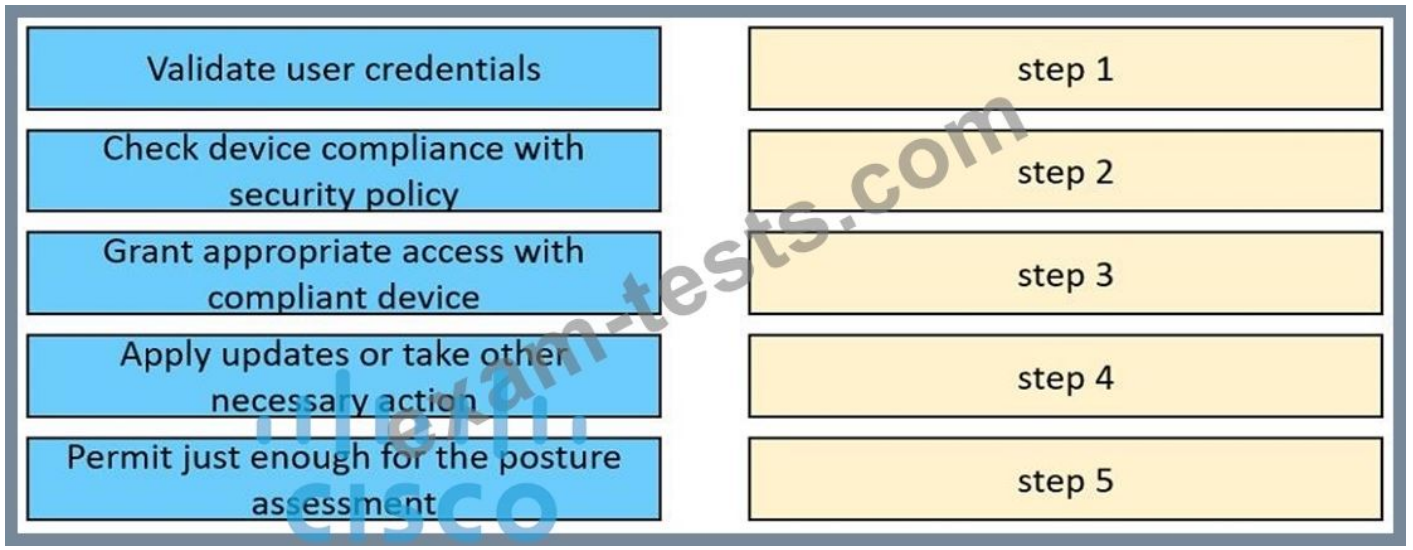


Answer:

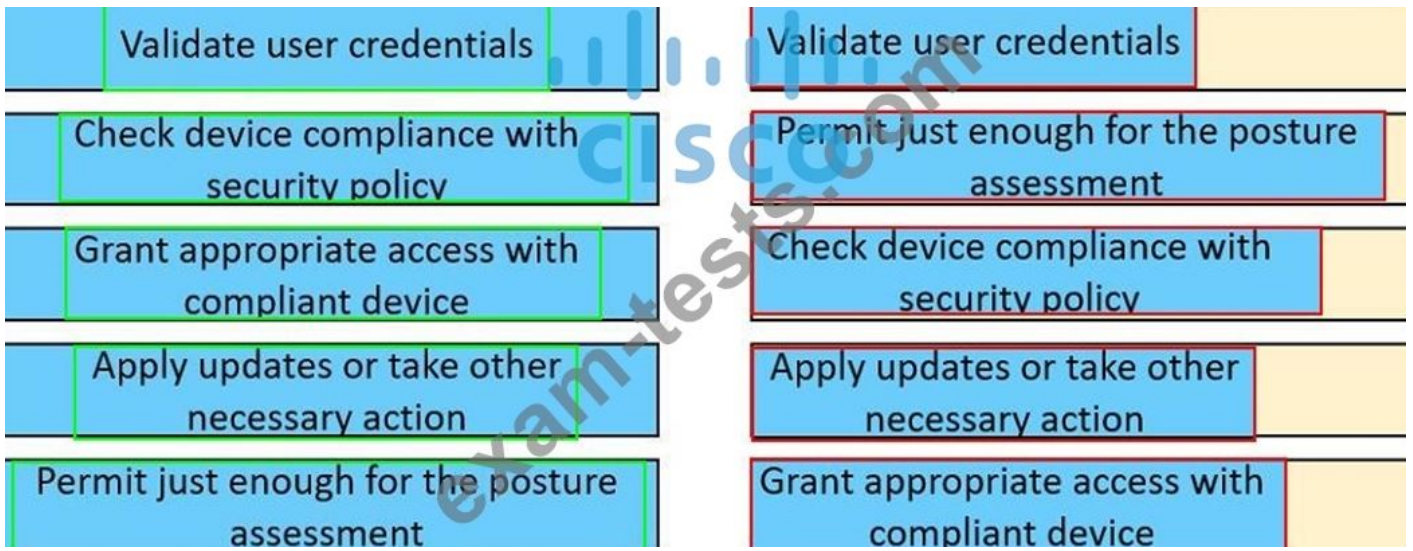
NEW QUESTION: 37
An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?
A. SIEM
B. CASB
C. Adaptive MFA
D. Cisco Cloudlock
Answer: D (LEAVE A REPLY)
+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy.
+ Cloudlock is API-based.
+ Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).
+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy.
+ Cloudlock is API-based.
+ Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).
Reference:
Note:
+ Security information and event management (SIEM) platforms collect log and event data from security systems, networks and computers, and turn it into actionable security insights.
+ An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when a condition of an alerting policy has been met.
+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy.
+ Cloudlock is API-based.
+ Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).
Note:

+ Security information and event management (SIEM) platforms collect log and event data from security systems, networks and computers, and turn it into actionable security insights.
+ An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when a Note:
+ Security information and event management (SIEM) platforms collect log and event data from security systems, networks and computers, and turn it into actionable security insights.
+ An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when a condition of an alerting policy has been met.

NEW QUESTION: 38
Drag and drop the posture assessment flow actions from the left into a sequence on the right.



Answer:



NEW QUESTION: 39
Refer to the exhibit.

```
*Jun 30 16:52:33.795: ISAKMP:(1002): retransmission skipped for phase 1 (time
since last transmission 504)
R1#
*Jun 30 16:52:40.103: ISAKMP:(1001):purging SA., sa=68CEE058, delme=68CEE058
R1#
*Jun 30 16:52:43.291: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:43.291: ISAKMP (1002): incrementing error counter on sa, attempt 5
of 5: retransmit phase 1
*Jun 30 16:52:43.295: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002): sending packet to 10.10.12.2 my_port 500
peer_port 500 (I) MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002):Sending an IKE IPv4 Packet.
R1#
*Jun 30 16:52:53.299: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:53.299: ISAKMP:(1002):peer does not do paranoid keepalives.

*Jun 30 16:52:53.299: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.303: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.307: ISAKMP: Unlocking peer struct 0x68287318 for
isadb_mark_sa_deleted(), count 0
*Jun 30 16:52:53.307: ISAKMP: Deleting peer node by peer_reap for 10.10.12.2:
68287318
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node 79875537 error FALSE reason "IKE
deleted"
R1#
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node -484575753 error FALSE reason
"IKE deleted"
*Jun 30 16:52:53.315: ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL
*Jun 30 16:52:53.319: ISAKMP:(1002):Old State = IKE_I_MM5 New State = IKE_DEST_SA
```

A network administrator configured a site-to-site VPN tunnel between two Cisco IOS routers, and hosts are unable to communicate between two sites of VPN. The network administrator runs the debug crypto isakmp sa command to track VPN status. What is the problem according to this command output?

A. encryption algorithm mismatch

B. interesting traffic was not applied

C. authentication key mismatch

D. hashing algorithm mismatch

Answer: C (LEAVE A REPLY)

NEW QUESTION: 40

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. set the IP address of an interface

C. complete all configurations

D. complete no configurations

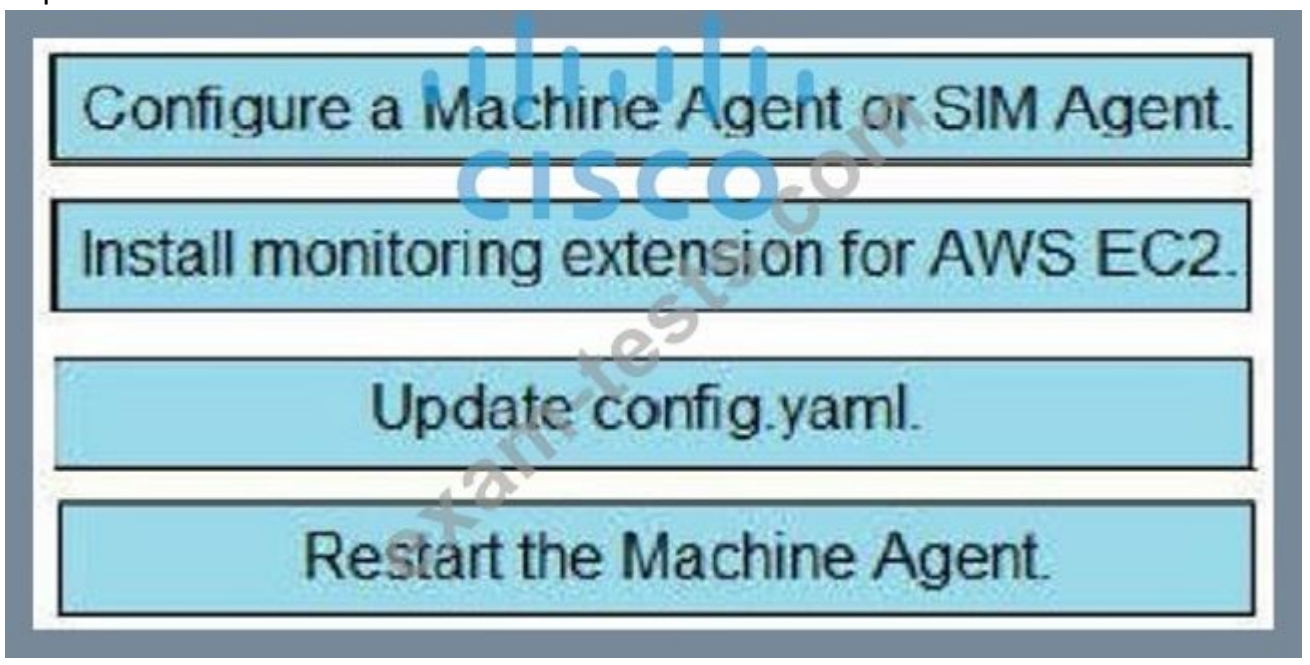
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41

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:

Explanation



NEW QUESTION: 42

A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https://<FMC IP>/capure/CAPI/pcap/test.pcap, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

A. Disable the proxy setting on the browser

B. Disable the HTTPS server and use HTTP instead

C. Use the Cisco FTD IP address as the proxy server setting on the browser

D. Enable the HTTPS server for the device platform policy

Answer: D (LEAVE A REPLY)

The error 403: Forbidden indicates that the web server denied access to the requested resource, which in this case is the PCAP file. One possible reason for this error is that the HTTPS server is not enabled for the device platform policy, which is a configuration that applies to the FTD devices managed by the

FMC. The device platform policy defines the settings for the management interface, the SSH access, the SNMP, the NTP, the DNS, and the HTTPS server. The HTTPS server allows the FMC to access the FTD devices via HTTPS and perform tasks such as packet capture, packet tracer, and file transfer. If the HTTPS server is not enabled for the device platform policy, the FMC cannot access the PCAP file from the FTD device via HTTPS. Therefore, the engineer must enable the HTTPS server for the device platform policy in order to resolve this issue. To enable the HTTPS server for the device platform policy, the engineer must follow these steps:

* Log in to the FMC web interface and navigate to Devices > Platform Settings.
* Select the device platform policy that applies to the FTD device and click Edit.
* In the General tab, check the Enable HTTPS Server checkbox and click Save.
* Deploy the policy changes to the FTD device and wait for the deployment to complete.
* Try to access the PCAP file again from the FMC web browser using the same address.

Alternatively, the engineer can also enable the HTTPS server for the FTD device from the FTD CLI using the command configure network https-server enable. However, this method is not recommended because it may cause a configuration conflict with the FMC123 References := 1: Use Firepower Threat Defense Captures and Packet Tracer - Cisco 2: Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.6 - Device Management Basics
[Cisco Firepower NGFW] - Cisco 3: Cisco Firepower Threat Defense Command Reference - C through D Commands [Cisco Firepower NGFW] - Cisco

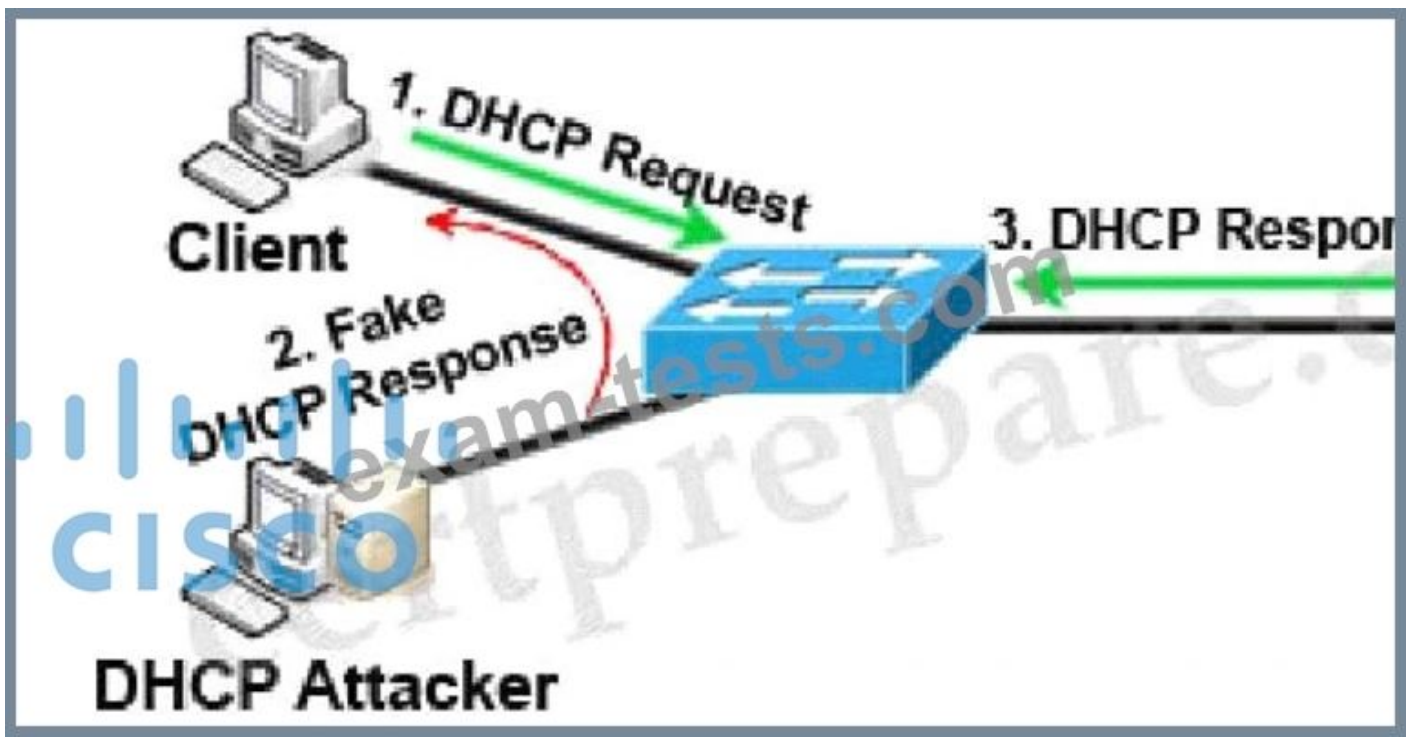
NEW QUESTION: 43
An organization has two systems in their DMZ that have an unencrypted link between them for communication.
The organization does not have a defined password policy and uses several default accounts on the systems.
The application used on those systems also have not gone through stringent code reviews. Which vulnerability would help an attacker brute force their way into the systems?
A. missing encryption
B. lack of file permission
C. lack of input validation
D. weak passwords
Answer: (SHOW ANSWER)

NEW QUESTION: 44
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

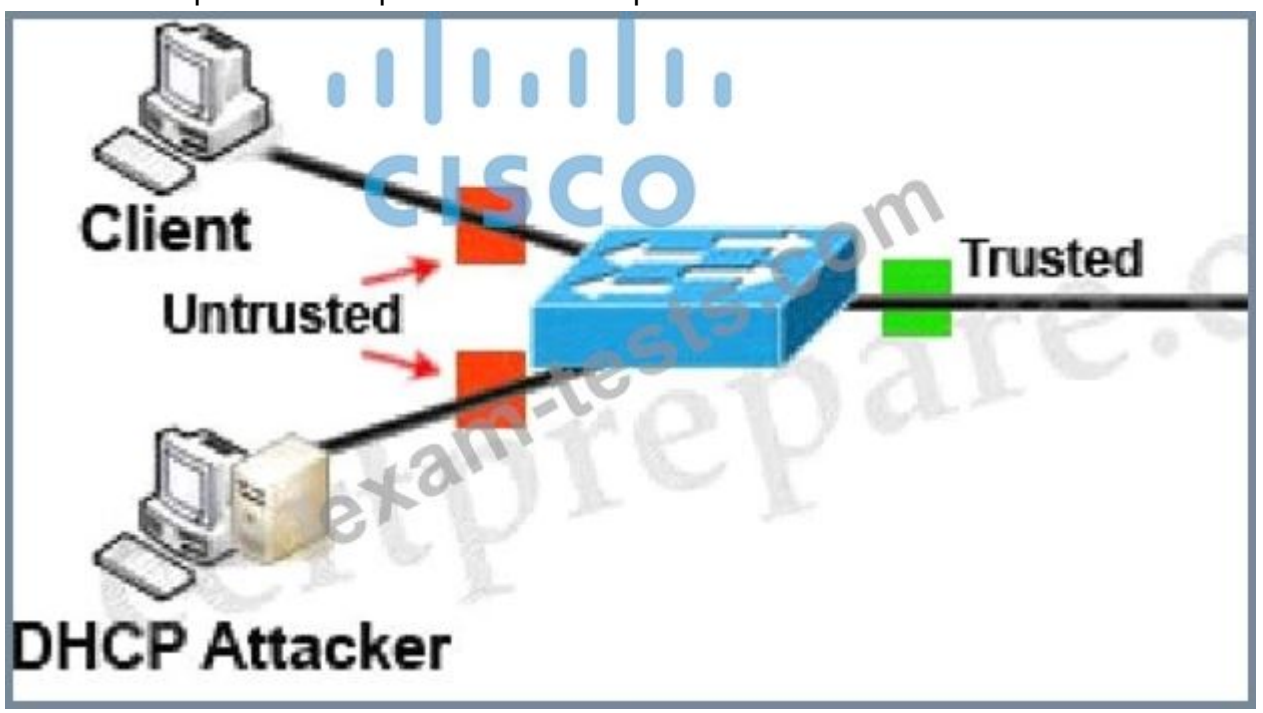
Cyber Threat Intelligence, STIX V2.1 and TAXII V2.1 OASIS Standards are published, What is STIX/TAXII? | Cloudflare, What is STIX / TAXII? Learn about the industry standards for Cyber ..., What are STIX/TAXII Standards I Resources I Anomali

NEW QUESTION: 45
Which industry standard is used to integrate Cisco ISE and pxGrid to each other and with other interoperable security platforms?
A. IEEE
B. IETF
C. NIST
D. ANSI
Answer: B (LEAVE A REPLY)
Cisco ISE and pxGrid use the IETF (Internet Engineering Task Force) standards to integrate with each other and with other interoperable security platforms. IETF is an open, international community of network designers, operators, vendors, and researchers who produce voluntary standards for the Internet. Cisco pxGrid is based on the IETF standards-track XMPP (Extensible Messaging and Presence Protocol) and RESTCONF (Representational State Transfer Configuration Protocol) technologies. These standards enable Cisco pxGrid to provide a scalable, secure, and open data-sharing platform that supports multiple security products and services. Cisco ISE uses the IETF standards-track RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) protocols to provide network access control and policy enforcement. Cisco ISE also supports the IETF standards-track SXP (Security Group Tag eXchange Protocol) to propagate security group tags across the network. By using the IETF standards, Cisco ISE and pxGrid can interoperate with other security platforms that support the same standards, such as Infoblox, Splunk, Rapid7, and more. References:
* Cisco pxGrid - Cisco
* ISE pxGrid General Information & FAQ - Cisco Community
* How To: Integrate Cisco WSA using ISE and TrustSec via pxGrid
* Infoblox DDI, Cisco ISE, and the pxGrid Solution Platform

NEW QUESTION: 46
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)
ExplanationTo 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 DHCPmessages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP responseis seen on an untrusted port, the port is shut down.

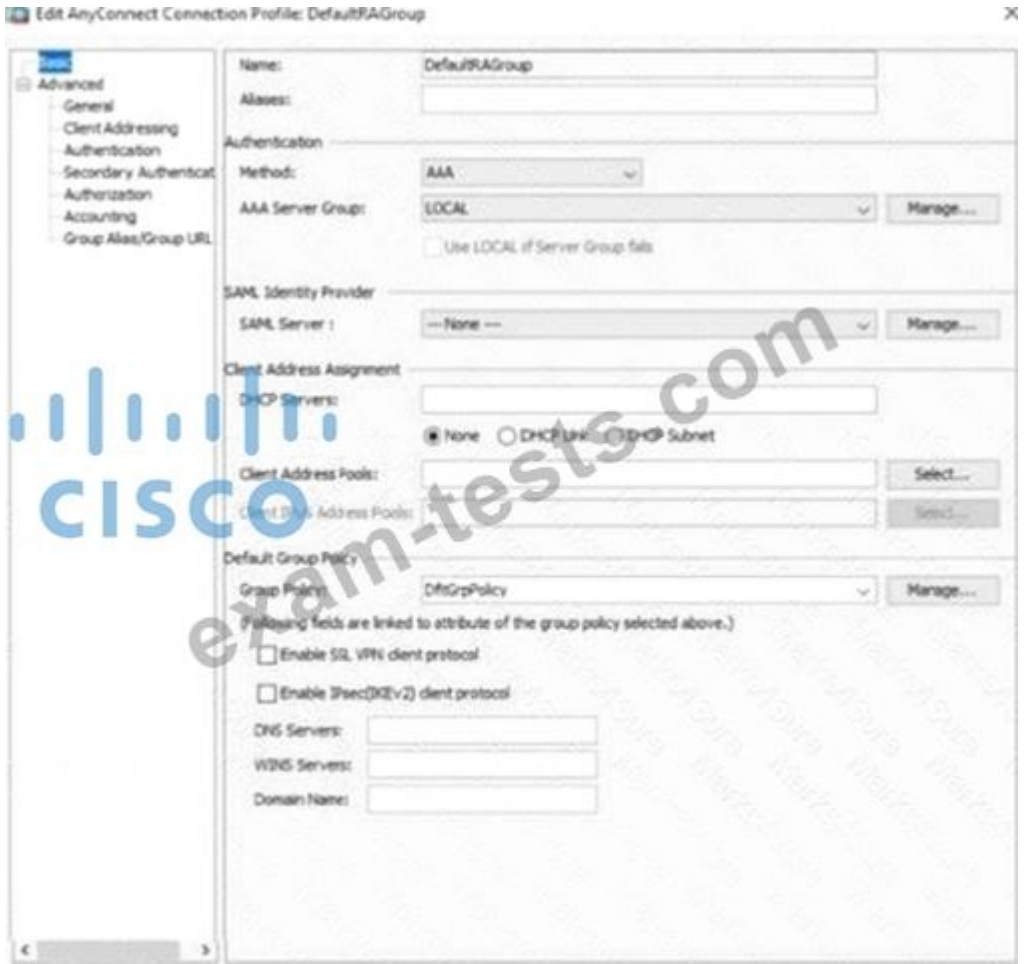
NEW QUESTION: 47
Which public cloud provider supports the Cisco Next Generation Firewall Virtual?
A. Google Cloud Platform
B. Red Hat Enterprise Visualization
C. VMware ESXi
D. Amazon Web Services
Answer: D (LEAVE A REPLY)
Reference:
https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/ white-paper-c11-740505.html

NEW QUESTION: 48
Which Cisco security solution provides patch management in the cloud?
A. Cisco Umbrella
B. Cisco ISE
C. Cisco CloudLock
D. Cisco Tetration
Answer: D (LEAVE A REPLY)
Cisco Tetration is a Cisco security solution that provides patch management in the cloud. Patch management is the process of identifying, acquiring, installing, and verifying patches for products and systems to correct security and functionality problems in software and firmware1. Cisco Tetration is a cloud-native platform that delivers comprehensive workload protection for multicloud data centers by enabling a zero-trust model using segmentation2. One of the features of Cisco Tetration is software vulnerability detection and patch management, which allows users to identify software vulnerabilities on workloads, prioritize patching based on risk scores, and automate patch deployment using orchestration tools3. Cisco Tetration leverages the National Vulnerability Database (NVD) and Cisco Talos Intelligence Group to provide up-to-date information on software vulnerabilities and their severity levels3. Cisco Tetration also supports patch management for both Windows and Linux operating systems, as well as third-party applications such as Apache, Java, MySQL, and Oracle4. Therefore, the correct answer is D. Cisco Tetration. References: 1: RFC 9232: Network Telemetry Framework - Internet Engineering Task Force 2: Cisco Tetration - Workload Protection - Cisco 3: Cisco Tetration Software Vulnerability Detection and Patch Management - Cisco 4: Cisco Tetration Platform Data Sheet - Cisco

NEW QUESTION: 49
What is an attribute of the DevSecOps process?
A. mandated security controls and check lists
B. security scanning and theoretical vulnerabilities
C. development security
D. isolated security team
Answer: (SHOW ANSWER)

Explanation
Explanation
DevSecOps (development, security, and operations) is a concept used in recent years to describe how to move security activities to the start of the development life cycle and have built-in security practices in the continuous integration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer to IT and business objectives.
Three key things make a real DevSecOps environment:
+ Security testing is done by the development team.
+ Issues found during that testing is managed by the development team.
+ Fixing those issues stays within the development team.

NEW QUESTION: 50
Refer to the exhibit.



When configuring a remote access VPN solution terminating on the Cisco ASA, an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication using machine certificates. Which configuration item must be modified to allow this?
A. Group Policy
B. Method
C. SAML Server
D. DHCP Servers
Answer: B (LEAVE A REPLY)
Explanation In order to use AAA along with an external token authentication mechanism, set the "Method" as "Both" inthe Authentication.

NEW QUESTION: 51

Refer to the exhibit.

```
> show crypto ipsec sa
interface: Outside
    Crypto map tag: CSM_Outside_map, seq num: 1, local addr:
209.165.200.225

      access-list CSM_IPSEC_ACL_1 extended permit ip 10.0.11.0
255.255.255.0 10.0.10.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.0.11.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.0.10.0/255.255.255.0/0/0)
      current_peer: 209.165.202.129


      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 17
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp
failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.200.225/500, remote crypto endpt.:
209.165.202.129/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: B6F5EA53
      current inbound spi : 84348DEE
```

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: A (LEAVE A REPLY)

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: 52

Which Cisco DNA Center RESTful PNP API adds and claims a device into a workflow?

A. api/v1/onboarding/pnp-device/import

B. api/v1/onboarding/pnp-device

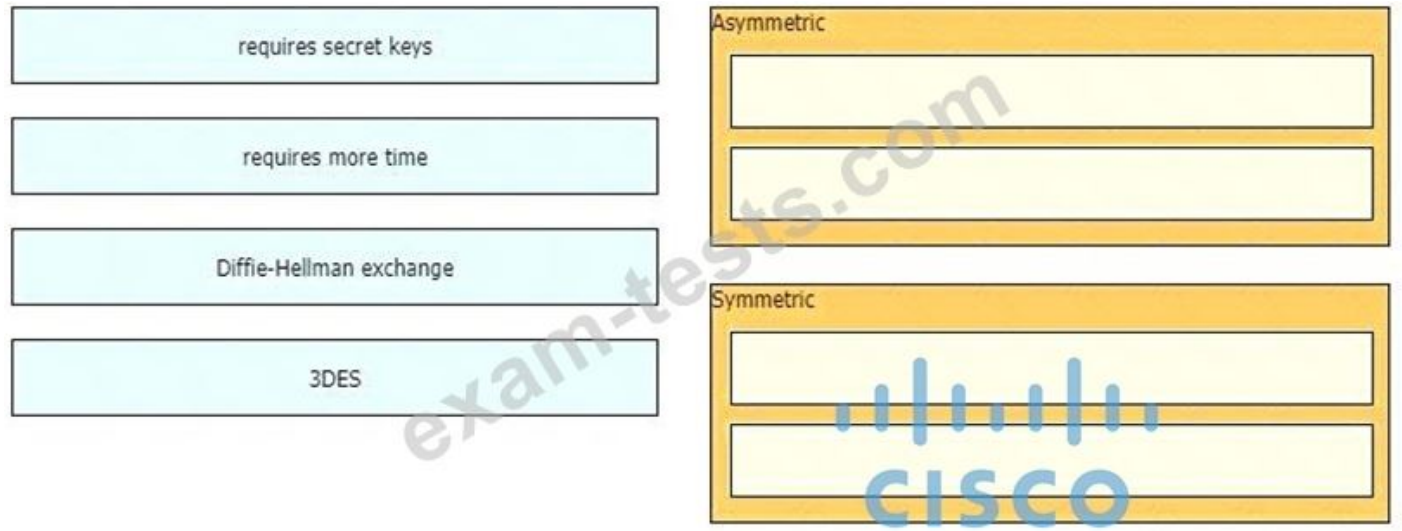
C. api/v1/fie/config

D. api/v1/onboarding/workflow

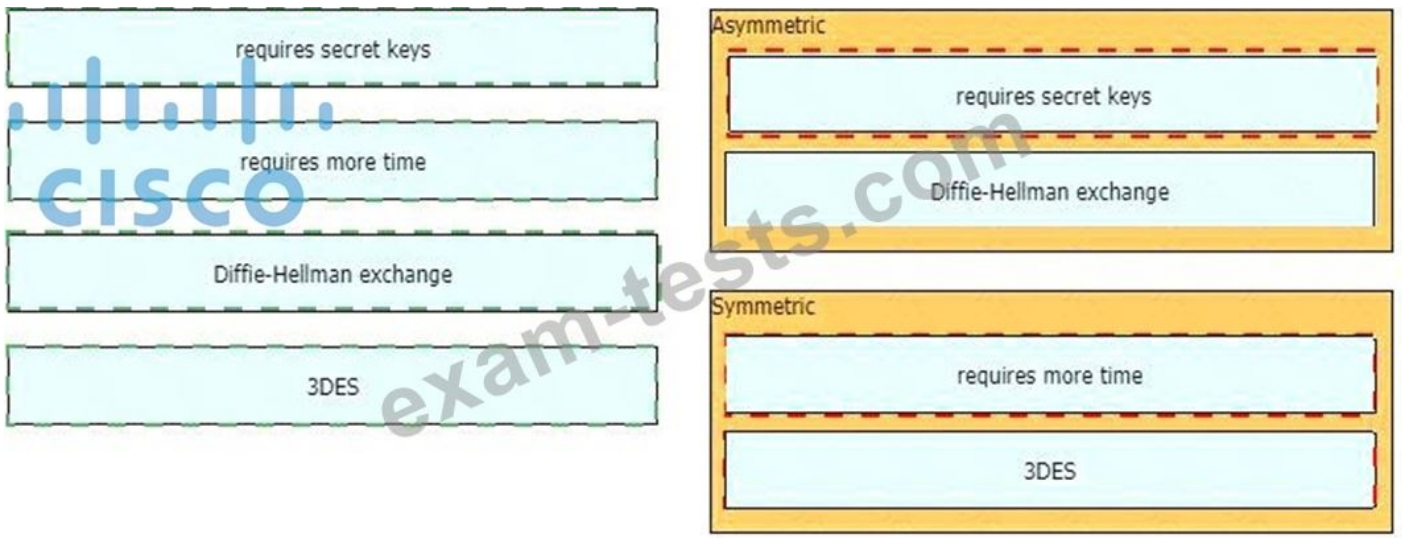
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
What is a difference between a DoS attack and a DDoS attack?
A. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where multiple systems target a single system with a DoS attack
B. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where a computer is used to flood multiple servers that are distributed over a LAN
C. A DoS attack is where a computer is used to flood a server with UDP packets whereas a DDoS attack is where a computer is used to flood a server with TCP packets
D. A DoS attack is where a computer is used to flood a server with TCP packets whereas a DDoS attack is where a computer is used to flood a server with UDP packets
Answer: A (LEAVE A REPLY)
A DoS (Denial of Service) attack is a type of cyberattack that aims to disrupt the normal functioning of a server, service, or network by overwhelming it with a large amount of traffic or requests. A DoS attack typically uses a single computer or device to launch the attack, sending TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) packets to the target server. TCP and UDP are two common protocols used to send data over the internet. TCP packets require a connection to be established between the sender and the receiver, and ensure that the data is delivered reliably and in order. UDP packets do not require a connection, and do not guarantee the delivery or order of the data. Both TCP and UDP packets can be used to flood a server with requests, consuming its resources and bandwidth, and preventing legitimate users from accessing the service.
A DDoS (Distributed Denial of Service) attack is a type of DoS attack that uses multiple computers or devices to launch the attack, creating a large network of attackers that can generate more traffic or requests than a single source. A DDoS attack often involves a botnet, which is a network of compromised computers or devices that are controlled by a malicious actor, usually through malware or hacking. The botnet can send TCP or UDP packets to the target server from different locations and IP addresses, making it harder to trace and block the attack. A DDoS attack can also target multiple servers or services that are distributed over a LAN (Local Area Network), such as a web hosting service or a cloud computing platform, affecting the availability and performance of the entire network.
The main difference between a DoS attack and a DDoS attack is the number and diversity of the sources that are involved in the attack. A DoS attack comes from a single source, while a DDoS attack comes from multiple sources. This makes a DDoS attack more powerful, faster, and harder to stop than a DoS attack.
References:
* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Malware Threats, Lesson 2: Identifying Network Attacks, Topic: DoS and DDoS Attacks
* DoS Attack vs. DDoS Attack: Key Differences? | Fortinet
* What's the Difference Between a DOS and DDoS Attack? - How-To Geek

NEW QUESTION: 54
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: 55
A user has a device in the network that is receiving too many connection requests from multiple machines. Which type of attack is the device undergoing?
A. SYN flood
B. slowloris
C. pharming
D. phishing
Answer: A (LEAVE A REPLY)
https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html#~types-of-ddos-attacks

NEW QUESTION: 56
In which two ways does a system administrator send web traffic transparently to the Web Security Appliance?
(Choose two.)
A. configure Active Directory Group Policies to push proxy settings
B. configure policy-based routing on the network infrastructure
C. configure the proxy IP address in the web-browser settings
D. use Web Cache Communication Protocol
E. reference a Proxy Auto Config file
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 57
An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?
A. Cisco Defense Orchestrator
B. Cisco Secureworks
C. Cisco DNA Center
D. Cisco Configuration Professional
Answer: A (LEAVE A REPLY)

NEW QUESTION: 58
Refer to the exhibit.

An administrator is adding a new Cisco FTD device to their network and wants to manage it with Cisco FMG. The Cisco FTD 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> 16

B. configure manager add DONTRESOLVE <registration key> FTD123

C. configure manager add <FMC IP address> <registration key>

D. configure manager add DONTRESOLVE kregistration key>

Answer: C (LEAVE A REPLY)

NEW QUESTION: 59

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: (SHOW ANSWER)

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: 60
Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?
A. interpacket variation
B. software package variation
C. flow insight variation
D. process details variation
Answer: (SHOW ANSWER)
The telemetry information consists of three types of data:
+ Flow information: This information contains details about endpoints, protocols, ports, when the flow started, how long the flow was active, etc.
+ Interpacket variation: This information captures any interpacket variations within the flow. Examples include variation in Time To Live (TTL), IP and TCP flags, payload length, etc
+ Context details: Context information is derived outside the packet header. It includes details about variation in buffer utilization, packet drops within a flow, association with tunnel endpoints, etc.
Reference:
cisco_nexus_9300_ex_platform_switches_white_paper_uki.pdf

NEW QUESTION: 61
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: 62
An engineer is configuring IPsec VPN and needs an authentication protocol that is reliable and supports ACK and sequence. Which protocol accomplishes this goal?
A. IKEv1
B. ESP
C. AES-256

D. AES-192

Answer: B (LEAVE A REPLY)

NEW QUESTION: 63

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. receives information about a switch

C. adds authentication to a switch

Answer: A (LEAVE A REPLY)

NEW QUESTION: 64

An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms.

Which software should be used to accomplish this goal?

A. Cisco Defense Orchestrator

B. Cisco Secureworks

C. Cisco DNA Center

D. Cisco Configuration Professional
Answer: A (LEAVE A REPLY)
Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms.
Cisco Defense Orchestrator features:
....
Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms.
Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms.
Cisco Defense Orchestrator features:
....
Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms.
Reference:
736847.html
Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms.
Cisco Defense Orchestrator features:
....
Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms.
736847.html

NEW QUESTION: 65
A Cisco ISE engineer configures Central Web Authentication (CWA) for wireless guest access and must have the guest endpoints redirect to the guest portal for authentication and authorization. While testing the policy, the engineer notices that the device is not redirected and instead gets full guest access. What must be done for the redirect to work?
A. Tag the guest portal in the CWA part of the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.
B. Create an advanced attribute setting of Cisco:cisco-gateway-id=guest within the authorization profile for the authorization policy line that the unauthenticated devices hit.
C. Use the track movement option within the authorization profile for the authorization policy line that the unauthenticated devices hit.
D. Add the DACL name for the Airespace ACL configured on the WLC in the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 66
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

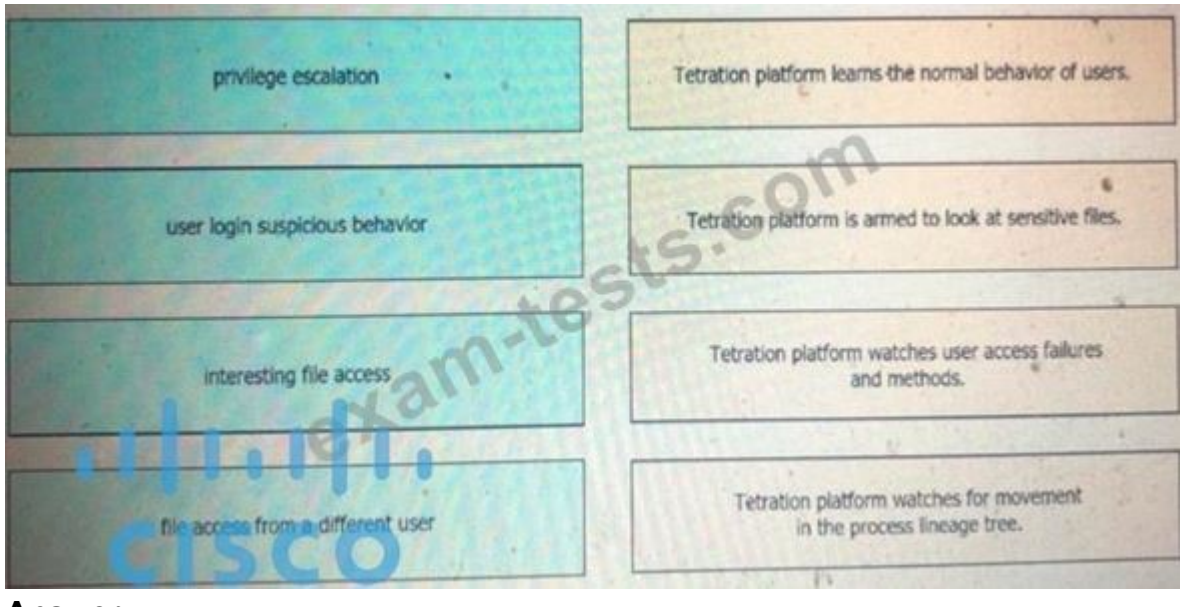
NEW QUESTION: 67
Which type of protection encrypts RSA keys when they are exported and imported?
A. nonexportable
B. file
C. passphrase
D. NGE
Answer: C (LEAVE A REPLY)

NEW QUESTION: 68
What are two workloaded security models? (Choose two)
A. SaaS
B. IaaS
C. on-premises
D. off-premises
E. PaaS
Answer: B,C (LEAVE A REPLY)
Workloaded security models are ways of protecting applications, services, and capabilities that run on a cloud resource. Virtual machines, databases, containers, and applications are all considered cloud workloads. There are different types of cloud deployment models, such as public, private, hybrid, and multicloud. Depending on the deployment model, the cloud workload security can vary in terms of responsibility, visibility, and control.
Infrastructure as a service (IaaS) is a cloud deployment model where the cloud provider offers the basic computing infrastructure, such as servers, storage, and networking, as a service. The customer is responsible for installing, configuring, and managing the operating systems, applications, and security of the workloads that run on the cloud infrastructure. IaaS provides the customer with more flexibility and control over the workload security, but also more complexity and overhead.
On-premises is a deployment model where the customer owns and operates the entire IT infrastructure, including the hardware, software, and security. The customer has full responsibility and control over the workload security, but also the highest cost and maintenance. On-premises deployment can offer more security and compliance than cloud deployment, depending on the customer's security posture and practices.
References:
https://www.cisco.com/site/us/en/products/security/secure-workload/index.html
https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-workload-security/

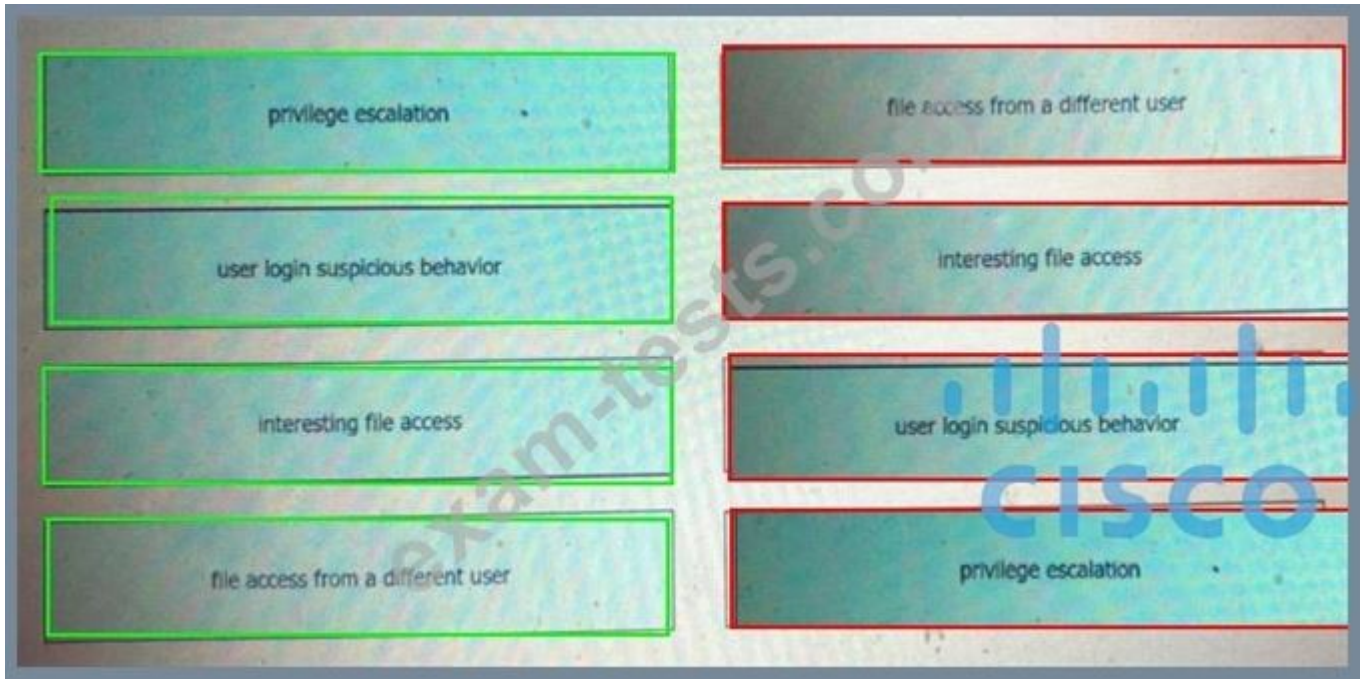
NEW QUESTION: 69
What are two reasons for implementing a multifactor authentication solution such as Duo Security provide to an organization? (Choose two.)
A. identification and correction of application vulnerabilities before allowing access to resources
B. secure access to on-premises and cloud applications

C. flexibility of different methods of 2FA such as phone callbacks, SMS passcodes. and push notifications
D. integration with 802.1x security using native Microsoft Windows supplicant
E. single sign-on access to on-premises and cloud applications
Answer: (SHOW ANSWER)

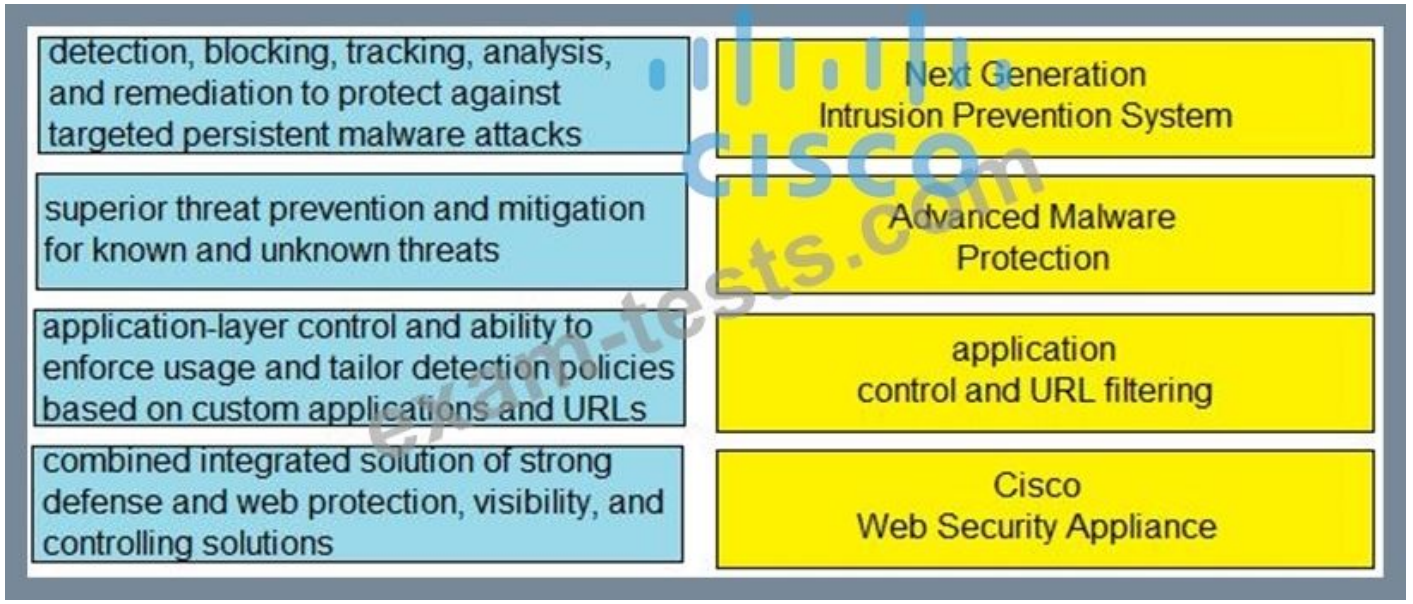
NEW QUESTION: 70
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.



Answer:



NEW QUESTION: 71
Drag and drop the capabilities from the left onto the correct technologies on the right.



Answer:

NEW QUESTION: 72

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 a brute force attack targeting remote sites, whereas SQL Injection is a social engineering attack.

C. Cross-site Scripting is when executives in a corporation are attacked, whereas SQL Injection is when a database is manipulated.

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)

Answer B is not correct because Cross-site Scripting (XSS) is not a brute force attack.

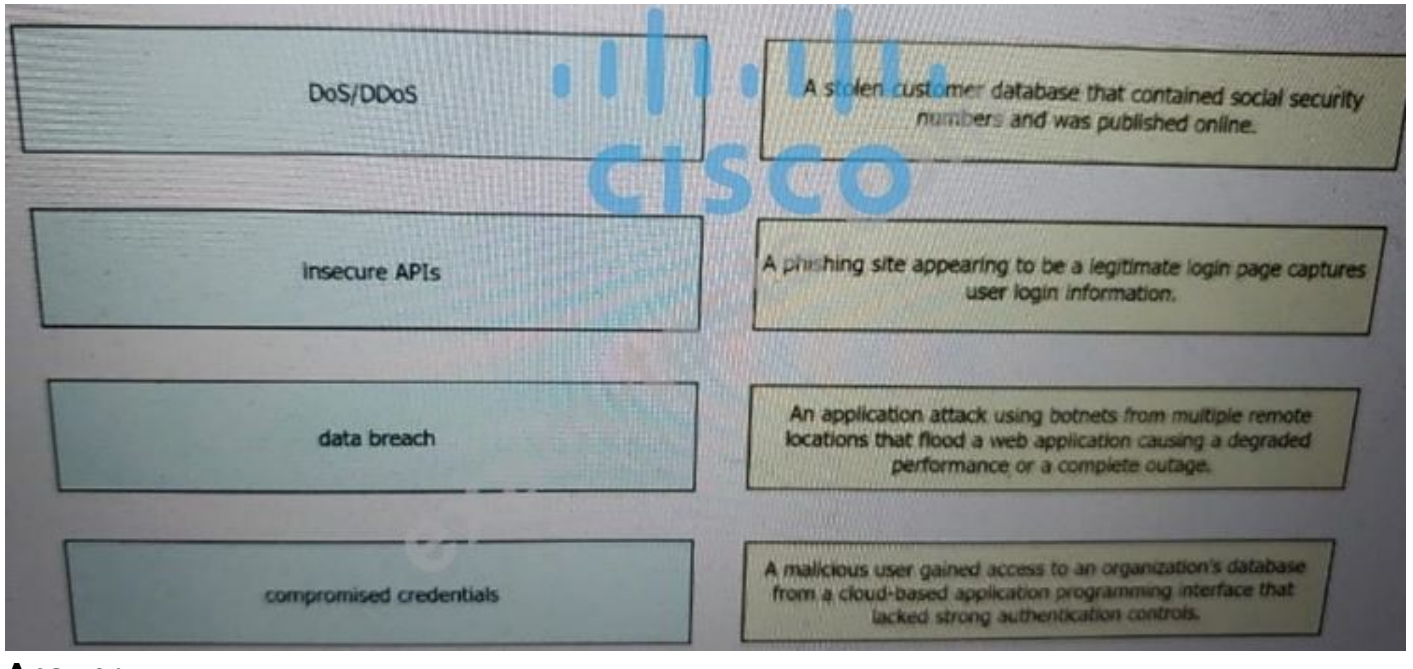
Answer C is not correct because the statement "Cross-site Scripting is when executives in a corporation are attacked" is not true. XSS is a client-side vulnerability that targets other application users.

Answer D is not correct because the statement "Cross-site Scripting is an attack where code is executed from the server side". In fact, XSS is a method that exploits website vulnerability by injecting scripts that will run at client's side.

Therefore only answer A is left. In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites where attackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POST parameters.

Note: The main difference between a SQL and XSS injection attack is that 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.

NEW QUESTION: 73
Drag and drop the threats from the left onto examples of that threat on the right



Answer:

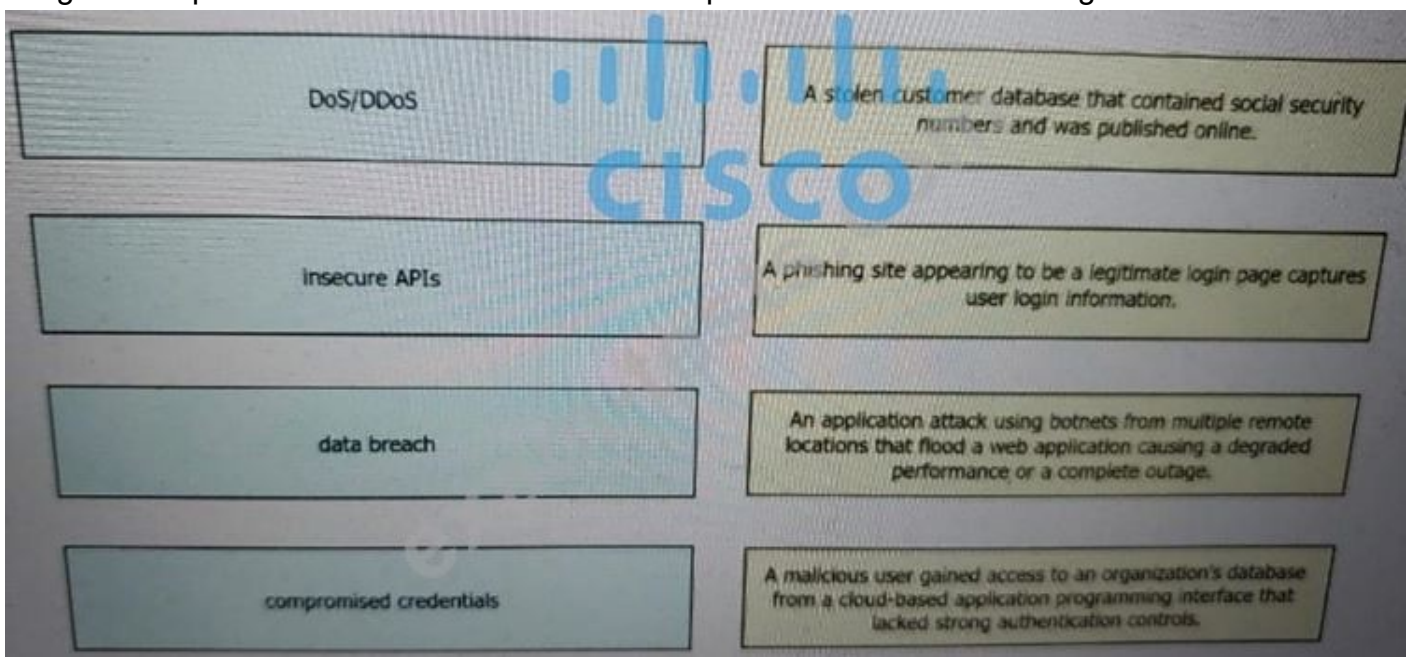
NEW QUESTION: 74
Refer to the exhibit.

```
crypto ikev2 name-mangler MANGLER
 dn organization-unit
```

An engineer is implementing a certificate based VPN. What is the result of the existing configuration?

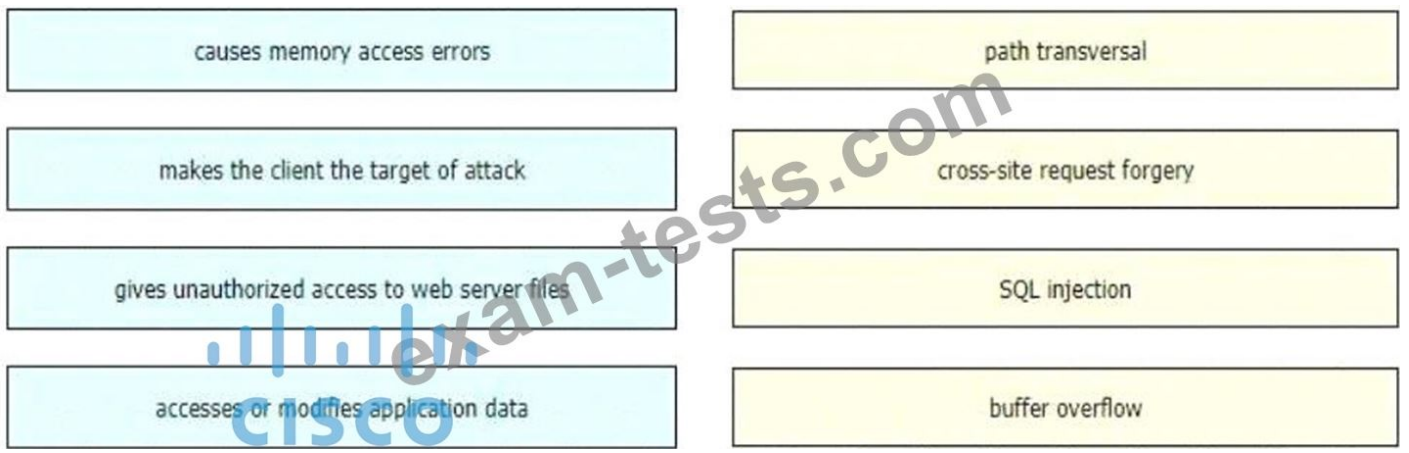
A. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER
B. Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully
C. The OU of the IKEv2 peer certificate is set to MANGLER
D. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
Drag and drop the threats from the left onto examples of that threat on the right

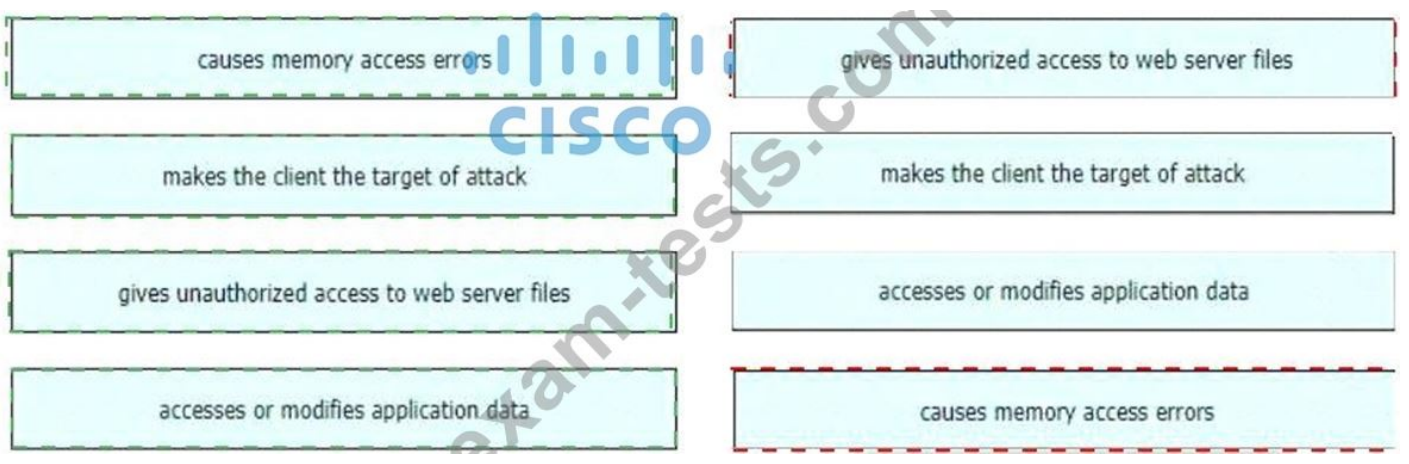


Answer:

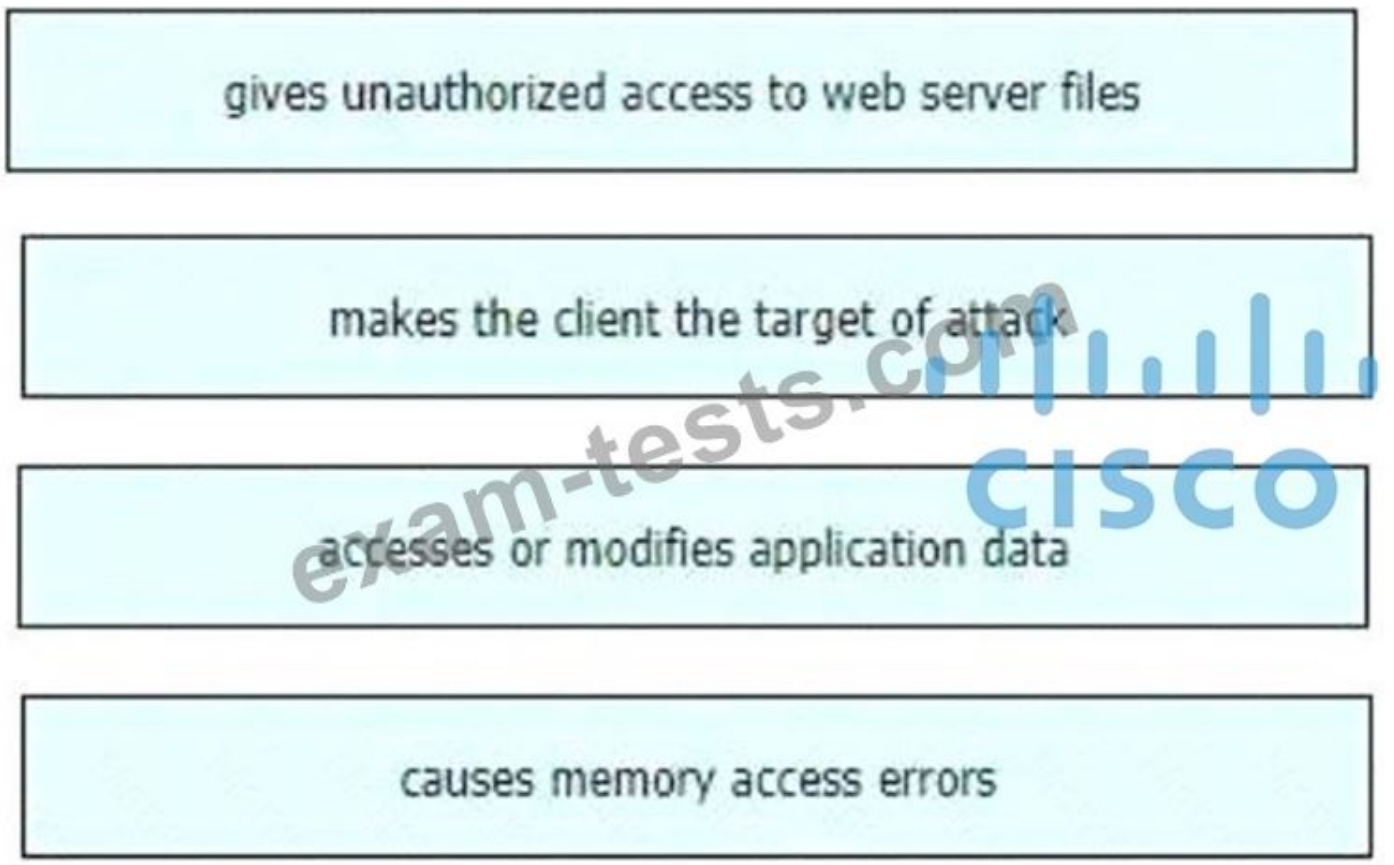
NEW QUESTION: 76
Drag and drop the exploits from the left onto the type of security vulnerability on the right.



Answer:



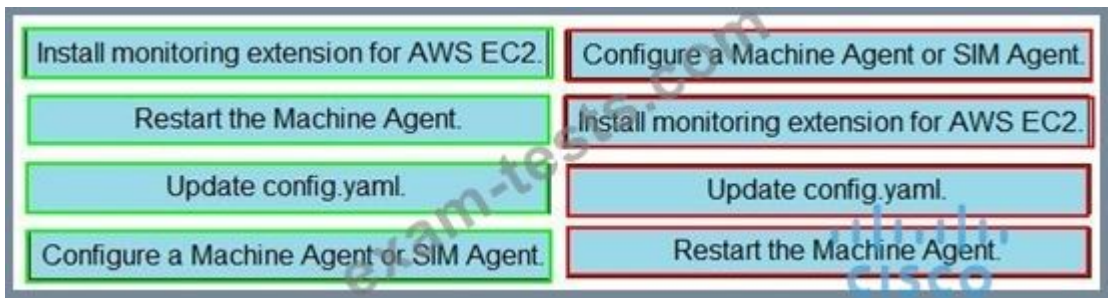
Explanation:



NEW QUESTION: 77

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: 78

An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA. Which Cisco ASA command must be used?

A. ip flow-export destination 1.1.1.1 2055

B. ip flow monitor<name> input

C. flow exporter <name>

D. flow-export destination inside 1.1.1.1 2055

Answer: D (LEAVE A REPLY)

NEW QUESTION: 79

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)

https://learningnetwork.cisco.com/s/question/0D53i00000KsrhK/rsa-key

NEW QUESTION: 80

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

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

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

C. when there is no firewall on the network

D. when there is a need to have more advanced detection capabilities

Answer: (SHOW ANSWER)

Endpoint protection platforms (EPP) prevent endpoint security threats like known and unknown malware.

Endpoint detection and response (EDR) solutions can detect and respond to threats that your EPP and other security tools did not catch.

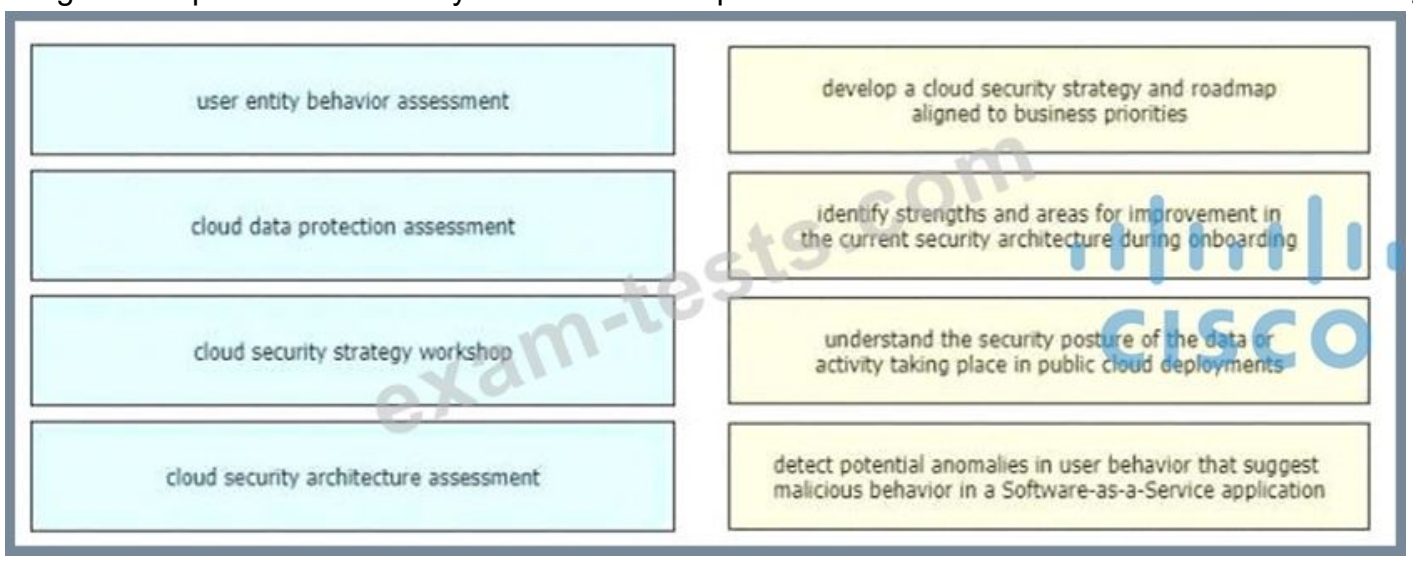
EDR and EPP have similar goals but are designed to fulfill different purposes. EPP is designed to provide device-level protection by identifying malicious files, detecting potentially malicious activity, and providing tools for incident investigation and response.

The preventative nature of EPP complements proactive EDR. EPP acts as the first line of defense, filtering out attacks that can be detected by the organization's deployed security solutions. EDR acts as a second layer of protection, enabling security analysts to perform threat hunting and identify more subtle threats to the endpoint.

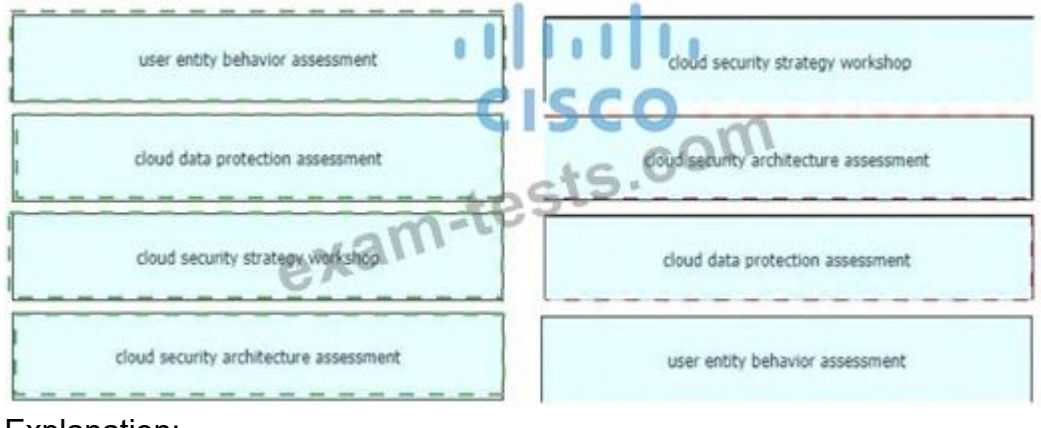
Effective endpoint defense requires a solution that integrates the capabilities of both EDR and EPP to provide protection against cyber threats without overwhelming an organization's security team.

NEW QUESTION: 81

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



Answer:

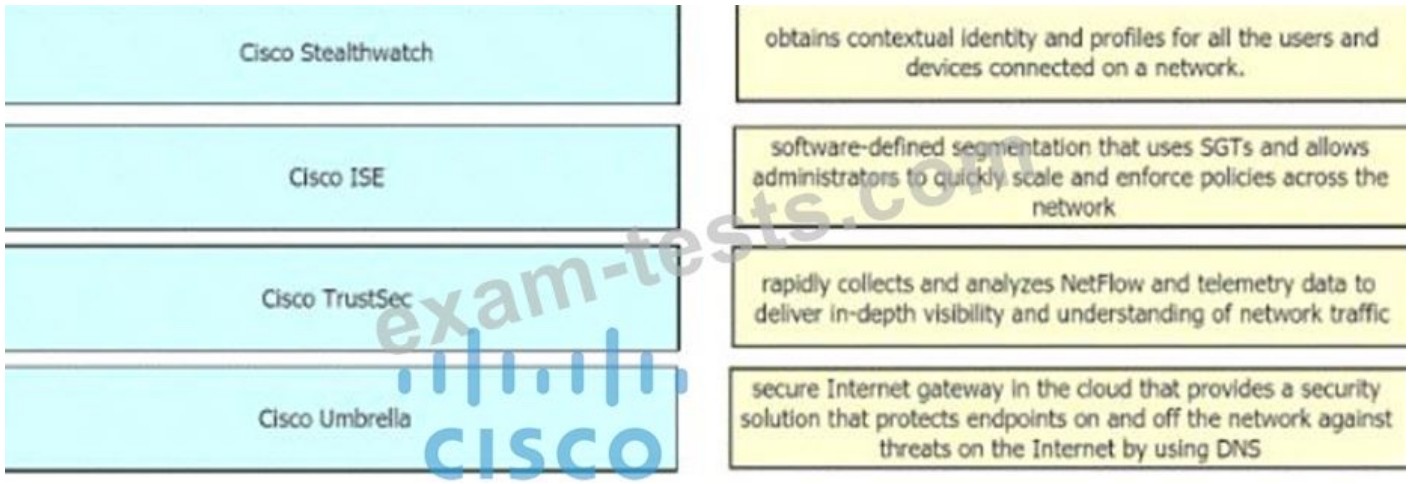


Explanation:

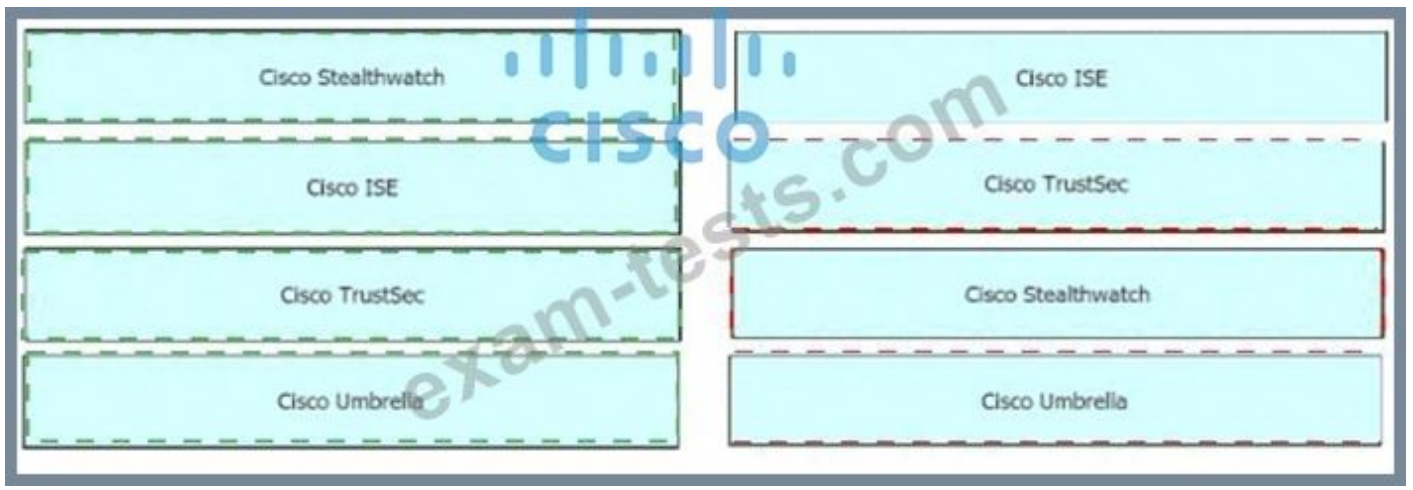
NEW QUESTION: 82
How does Cisco Advanced Phishing Protection protect users?
A. It validates the sender by using DKIM.
B. It determines which identities are perceived by the sender
C. It utilizes sensors that send messages securely.
D. It uses machine learning and real-time behavior analytics.
Answer: D (LEAVE A REPLY)
Cisco Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to protect against identity deception-based threats.
Cisco Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to protect against identity deception-based threats.
Reference:
Cisco Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to protect against identity deception-based threats.

NEW QUESTION: 83
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)
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.

NEW QUESTION: 84
Drag and drop the solutions from the left onto the solution's benefits on the right.



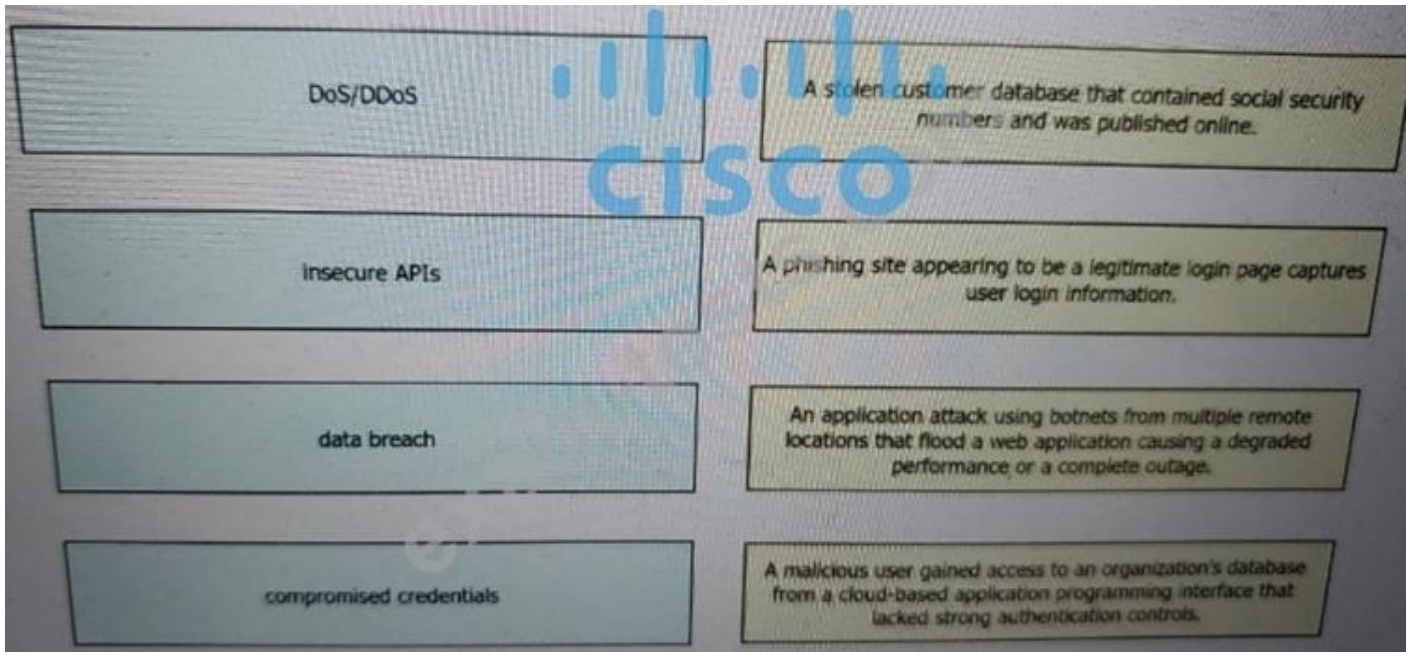
Answer:



Explanation:
Cisco Stealthwatch - rapidly collects and analyzes netflow and telemenly data to deliver in-depth visibility and understanding of network traffic Cisco ISE - obtains contextual identity and profiles for all users and device Cisco TrustSec - software defined segmentation that uses SGTs Cisco Umbrella - secure internet gateway ion the cloud that provides a security solution

NEW QUESTION: 85
The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic.
Where must the ASA be added on the Cisco UC Manager platform?
A. Certificate Trust List
B. Endpoint Trust List
C. Enterprise Proxy Service
D. Secured Collaboration Proxy
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/special/unified-communications/guide/unified- comm/unified-comm-tlsproxy.html

NEW QUESTION: 86
Drag and drop the threats from the left onto examples of that threat on the right



Answer:

NEW QUESTION: 87
On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed devices?
A. health awareness policy
B. system policy
C. correlation policy
D. access control policy
E. health policy
Answer: E (LEAVE A REPLY)

NEW QUESTION: 88
Which technology must De used to Implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

A. GET VPN
B. IPsec DVTI
C. DMVPN
D. FlexVPN
Answer: A (LEAVE A REPLY)
Group Encrypted Transport VPN (GET VPN) is used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity. GET VPN provides a way to encrypt traffic between sites without the need for point-to-point tunnels, supporting efficient, scalable, and secure communication across a broad network infrastructure.

NEW QUESTION: 89
What is the most commonly used protocol for network telemetry?
A. SMTP
B. SNMP
C. TFTP
D. NctFlow
Answer: B (LEAVE A REPLY)
SNMP (Simple Network Management Protocol) is the most commonly used protocol for network telemetry. SNMP is a standard protocol that allows network devices to exchange management information1.
SNMP agents run on network devices and collect data about their status, performance, configuration, and events. SNMP managers run on network management systems and query the agents for data or receive notifications from them. SNMP can also be used to configure or control network devices remotely2. SNMP is widely supported by various vendors and platforms, and it provides a simple and flexible way to monitor and manage networks3.
References: 1: What is SNMP? | Cisco 2: SNMP Basics: What is SNMP and How It Works | SolarWinds 3: Network Telemetry Explained: Frameworks, Applications & Standards | Splunk

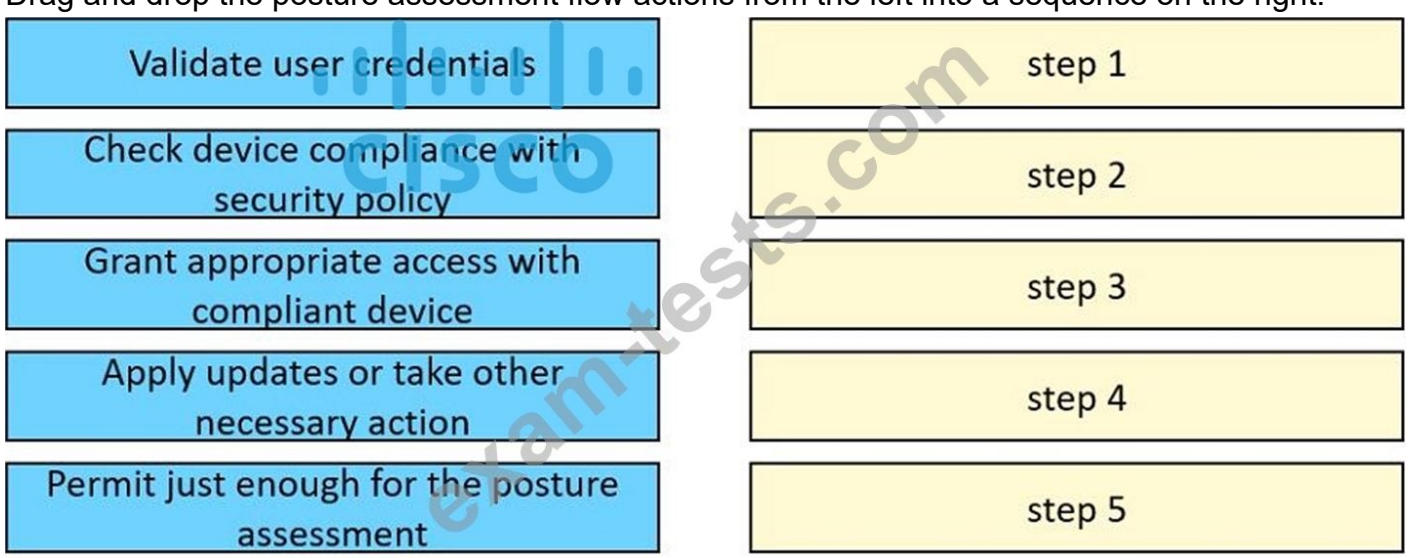
NEW QUESTION: 90
Refer to the exhibit.

```
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
```

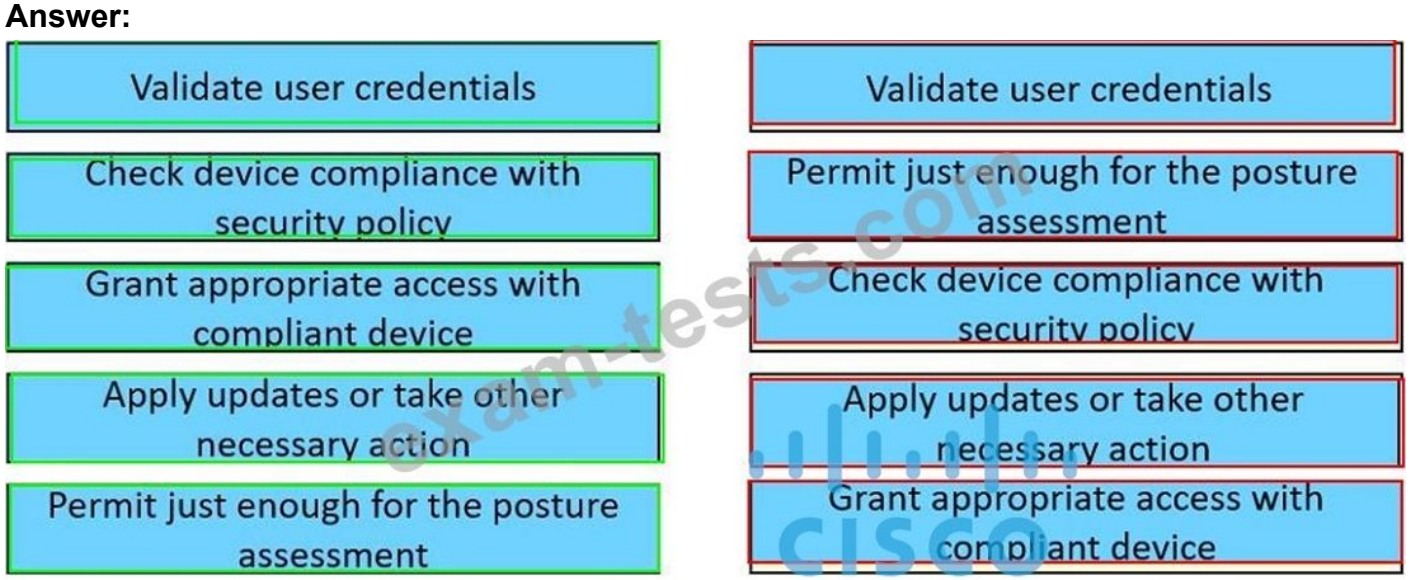
A network administrator configures command authorization for the admin5 user. What is the admin5 user able to do on HQ_Router after this configuration?
A. set the IP address of an interface
B. complete no configurations
C. complete all configurations
D. add subinterfaces
Answer: (SHOW ANSWER)

Explanation The user "admin5" was configured with privilege level 5. In order to allow configuration (enter global configuration mode), we must type this command: (config)#privilege exec level 5 configure terminal Without this command, this user cannot do any configuration. Note: Cisco IOS supports privilege levels from 0 to 15, but the privilege levels which are used by default are privilege level 1 (user EXEC) and level privilege 15 (privilege EXEC)

NEW QUESTION: 91
Drag and drop the posture assessment flow actions from the left into a sequence on the right.



Answer:



NEW QUESTION: 92
Refer to the exhibit.

Which statement about the authentication protocol used in the configuration is true

A. The authentication and authorization requests are grouped in a single packet

B. The authentication request contains only a password

C. The authentication request contains only a username

D. There are separate authentication and authorization request packets

Answer: A (LEAVE A REPLY)

NEW QUESTION: 93

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: 94

II

An engineer musi set up 200 new laptops on a network and wants to prevent the users from moving their laptops around to simplify administration Which switch port MAC address security setting must be used?

A. sticky

B. static

C. maximum

D. aging

Answer: A (LEAVE A REPLY)

NEW QUESTION: 95

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

A. Cisco ASAV

B. Cisco Cloud Orchestrator

C. Cisco WSAV

D. Cisco Stealthwatch Cloud

Answer: A (LEAVE A REPLY)

NEW QUESTION: 96
Which feature is supported when deploying Cisco ASAv within AWS public cloud?
A. IPv6
B. clustering
C. user deployment of Layer 3 networks
D. multiple context mode
Answer: (SHOW ANSWER)

NEW QUESTION: 97
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: C (LEAVE A REPLY)
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: 98
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)
Explanation
Cisco Hybrid Email Security is a unique service offering that facilitates the deployment of your email security infrastructure both on premises and in the cloud. You can change the number of on-premises versus cloud users 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: 99
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.

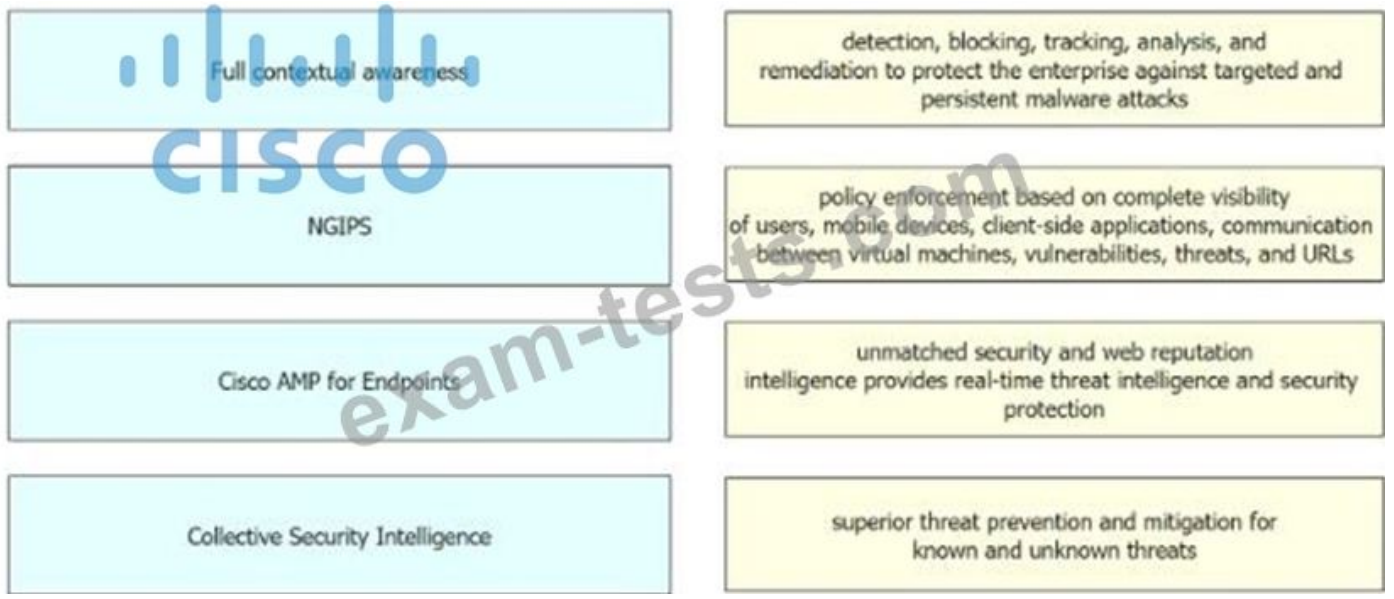
B. Configure policies to quarantine malicious emails.
C. Configure policies to stop and reject communication
D. Configure the Cisco ESA to reset the TCP connection.
Answer: B (LEAVE A REPLY)
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118219-configure-esa-00.html

NEW QUESTION: 100
Which VMware platform does Cisco ACI integrate with to provide enhanced visibility, provide policy integration and deployment, and implement security policies with access lists?
A. VMware APIC
B. VMwarevRealize
C. VMware fusion
D. VMware horizons
Answer: (SHOW ANSWER)
VMware APIC is a platform that integrates with Cisco ACI to provide enhanced visibility, policy integration and deployment, and security policies with access lists. VMware APIC is a virtual appliance that runs on VMware vSphere and communicates with the Cisco APIC controller. VMware APIC allows administrators to create and manage Cisco ACI policies for VMware virtual machines and networks. VMware APIC also provides a unified view of the physical and virtual network topology, health, and statistics. VMware APIC supports the following modes of Cisco ACI and VMware integration:
* VMware VDS: When integrated with Cisco ACI, the VMware vSphere Distributed Switch (VDS)
* enables administrators to configure VM networking in the ACI fabric.
* Cisco ACI Virtual Edge: Cisco ACI Virtual Edge is a distributed service that provides Layer 4 to Layer
7 services for applications running on VMware vSphere.
* Cisco Application Virtual Switch (AVS): Cisco AVS is a distributed virtual switch that provides policy-based network services for VMware vSphere environments. References:
* Cisco ACI with VMware VDS Integration
* Cisco ACI and VMware NSX-T Data Center Integration
* Cisco ACI and VMware: The Perfect Pair
* Setting the Record Straight: Confusion about ACI on VMware Technologies

NEW QUESTION: 101
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: (SHOW ANSWER)
Explanation
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118188-qanda-esa-00.html

NEW QUESTION: 102
What is the difference between a vulnerability and an exploit?
A. A vulnerability is a weakness that can be exploited by an attacker
B. A vulnerability is a hypothetical event for an attacker to exploit
C. An exploit is a hypothetical event that causes a vulnerability in the network
D. An exploit is a weakness that can cause a vulnerability in the network
Answer: (SHOW ANSWER)

NEW QUESTION: 103
Drag and drop the security solutions from the left onto the benefits they provide on the right.



Answer:

NEW QUESTION: 104
A network engineer has configured a NTP server on a Cisco ASA. The Cisco ASA has IP reachability to the NTP server and is not filtering any traffic. The show ntp association detail command indicates that the configured NTP server is unsynchronized and has a stratum of 16. What is the cause of this issue?
A. Resynchronization of NTP is not forced

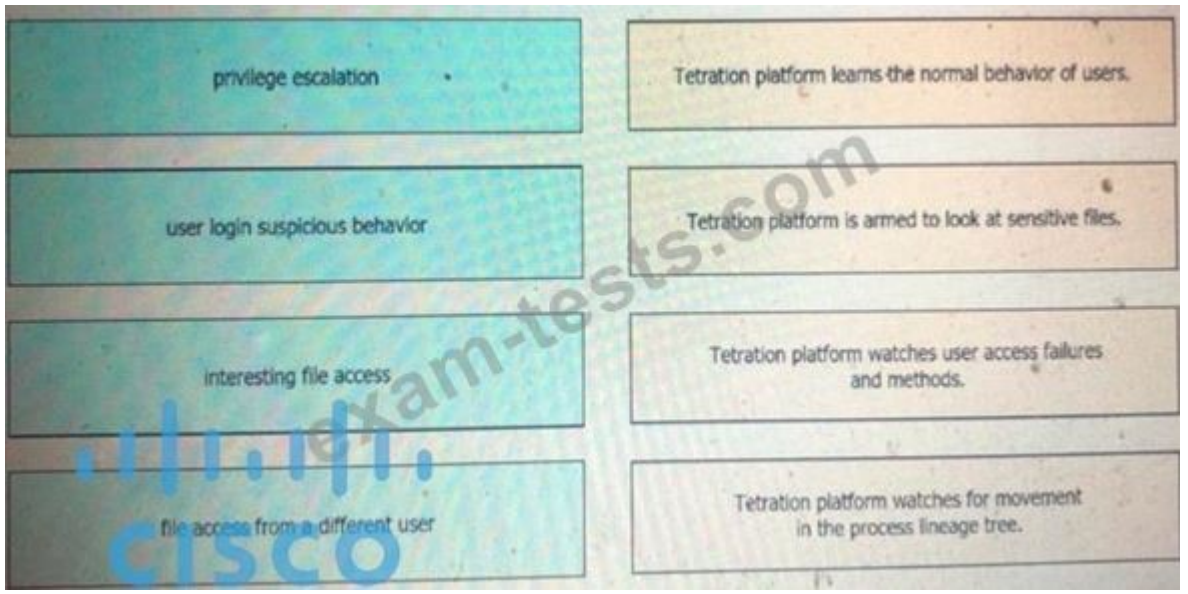
B. An access list entry for UDP port 123 on the outside interface is missing.
C. NTP is not configured to use a working server.
D. An access list entry for UDP port 123 on the inside interface is missing.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
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 discovers and controls cloud apps that are connected to a company's corporate environment.
C. It sends the application information to an administrator to act on.
D. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously.
Answer: B (LEAVE A REPLY)

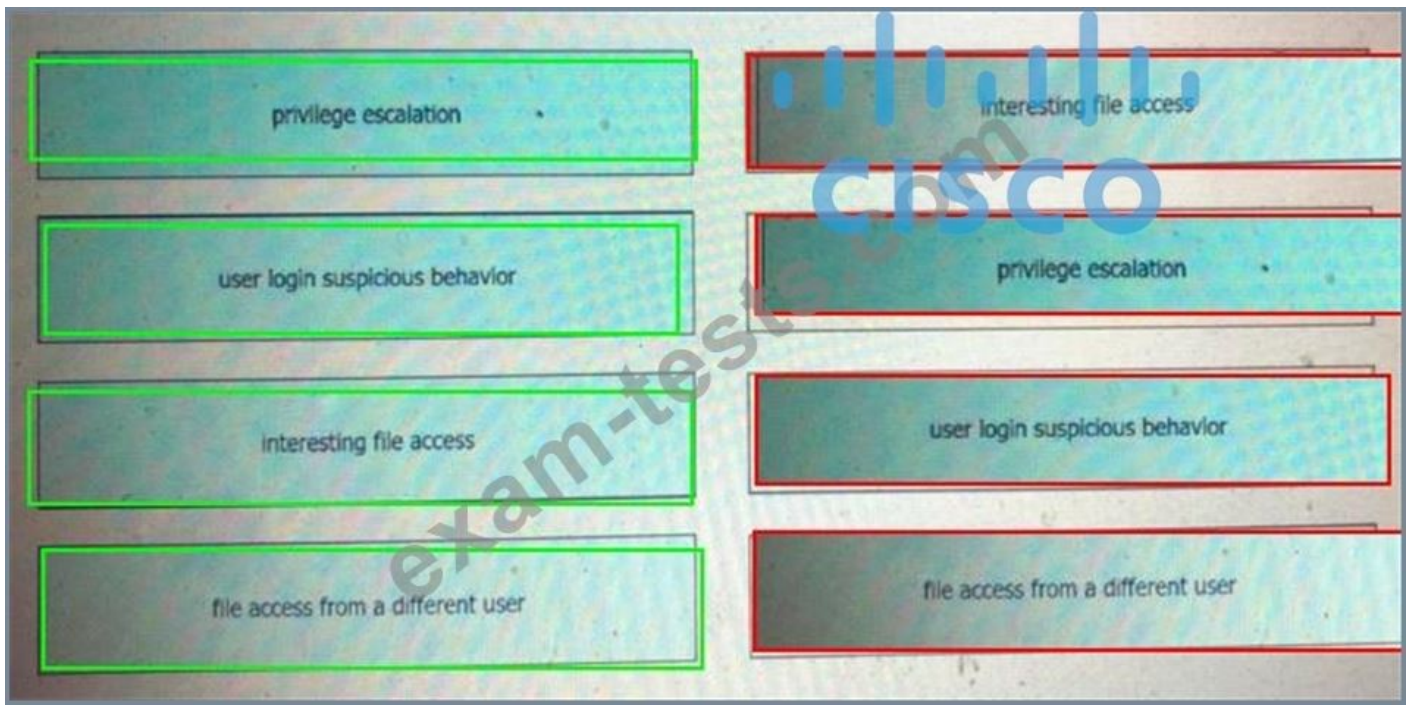
NEW QUESTION: 106
In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?
A. insecure API
B. LDAP injection
C. cross-site scripting
D. man-in-the-middle
Answer: D (LEAVE A REPLY)

NEW QUESTION: 107
A university policy must allow open access to resources on the Internet for research, but internal workstations are exposed to malware. Which Cisco AMP feature allows the engineering team to determine whether a file is installed on a selected few workstations?
A. file prevalence
B. file discovery
C. file conviction
D. file manager
Answer: (SHOW ANSWER)
File discovery is a feature of Cisco AMP that allows the engineering team to search for files across all endpoints in the network based on their SHA-256 hashes. File discovery can help identify whether a file is installed on a selected few workstations, and also provide information such as file name, path, size, date, and disposition. File discovery can be used to locate malicious files, unauthorized software, or sensitive data on the endpoints. File discovery can be accessed from the Outbreak Control menu in the AMP console1. References: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/215176-configure-a-s

NEW QUESTION: 108
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.

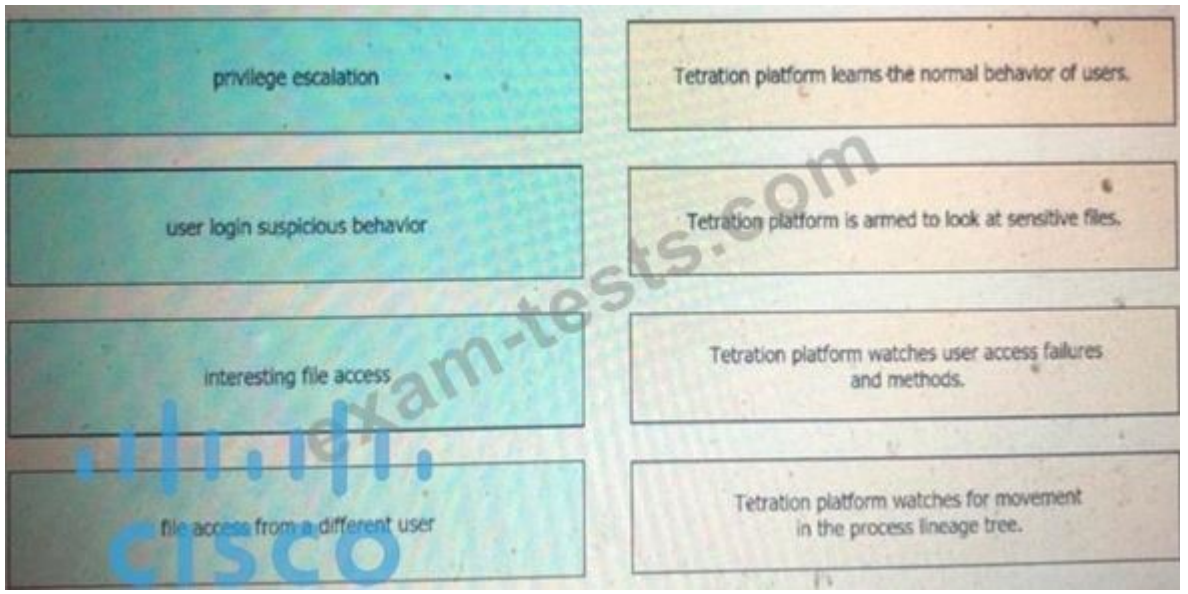


Answer:

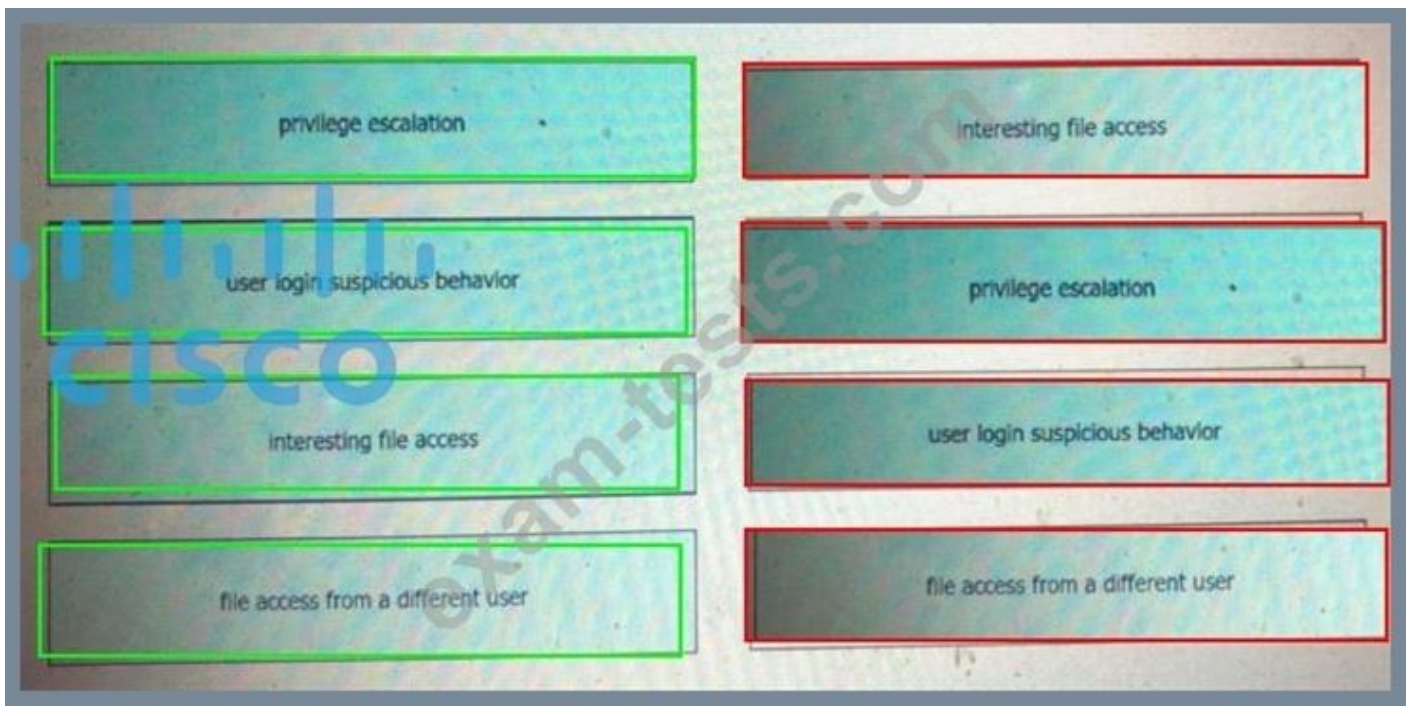


NEW QUESTION: 109
What is a benefit of using Cisco FMC over Cisco ASDM?
A. Cisco FMC uses Java while Cisco ASDM uses HTML5.
B. Cisco FMC provides centralized management while Cisco ASDM does not.
C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.
D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices
Answer: B (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html

NEW QUESTION: 110
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.



Answer:



NEW QUESTION: 111
What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?
A. It decrypts HTTPS application traffic for unauthenticated users.
B. It provides enhanced HTTPS application detection for AsyncOS.
C. It alerts users when the WSA decrypts their traffic.
D. It decrypts HTTPS application traffic for authenticated users.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 112

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

A. Use an access policy group to configure application control settings.

B. Use security services to configure the traffic monitor, .

C. Use web security reporting to validate engine functionality

D. Use URL categorization to prevent the application traffic.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 113

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)

Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn- availability-15-mt-book/sec-state-fail-ipsec.html

NEW QUESTION: 114

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)

Explanation

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

As of 8.4(1) 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: 115

Which two conditions are prerequisites for stateful failover for IPsec? (Choose two.)

A. The IPsec configuration that is set up on the active device must be duplicated on the standby device.

B. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device.

C. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.

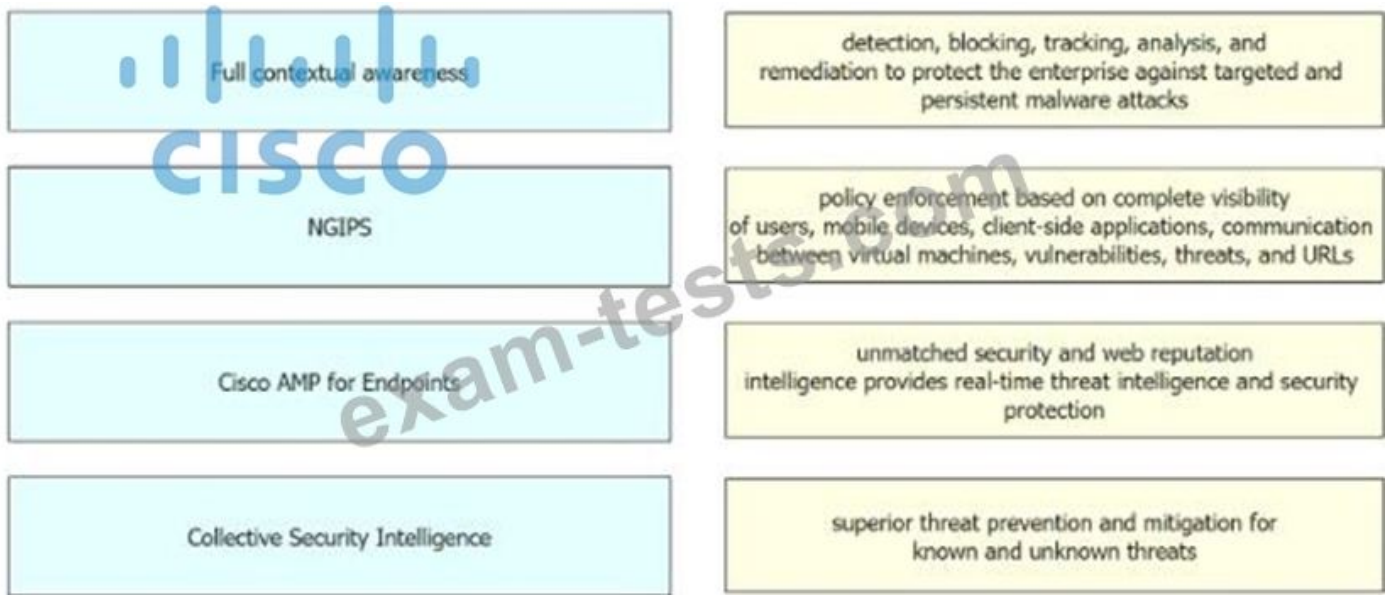
D. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically.

E. 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.

Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which component of Cisco umbrella architecture increases reliability of the service?
A. BGP route reflector
B. AMP Threat grid
C. Anycast IP
D. Cisco Talos
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
Drag and drop the security solutions from the left onto the benefits they provide on the right.



Answer:

NEW QUESTION: 118
Drag and drop the NetFlow export formats from the left onto the descriptions on the right.

Answer:

NEW QUESTION: 119

What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?

A. EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.

B. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.

C. EPP focuses on network security, and EDR focuses on device security.

D. EDR focuses on network security, and EPP focuses on device security.

Answer: A (LEAVE A REPLY)

Explanation/Reference: https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection- response-edr.html

NEW QUESTION: 120

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.

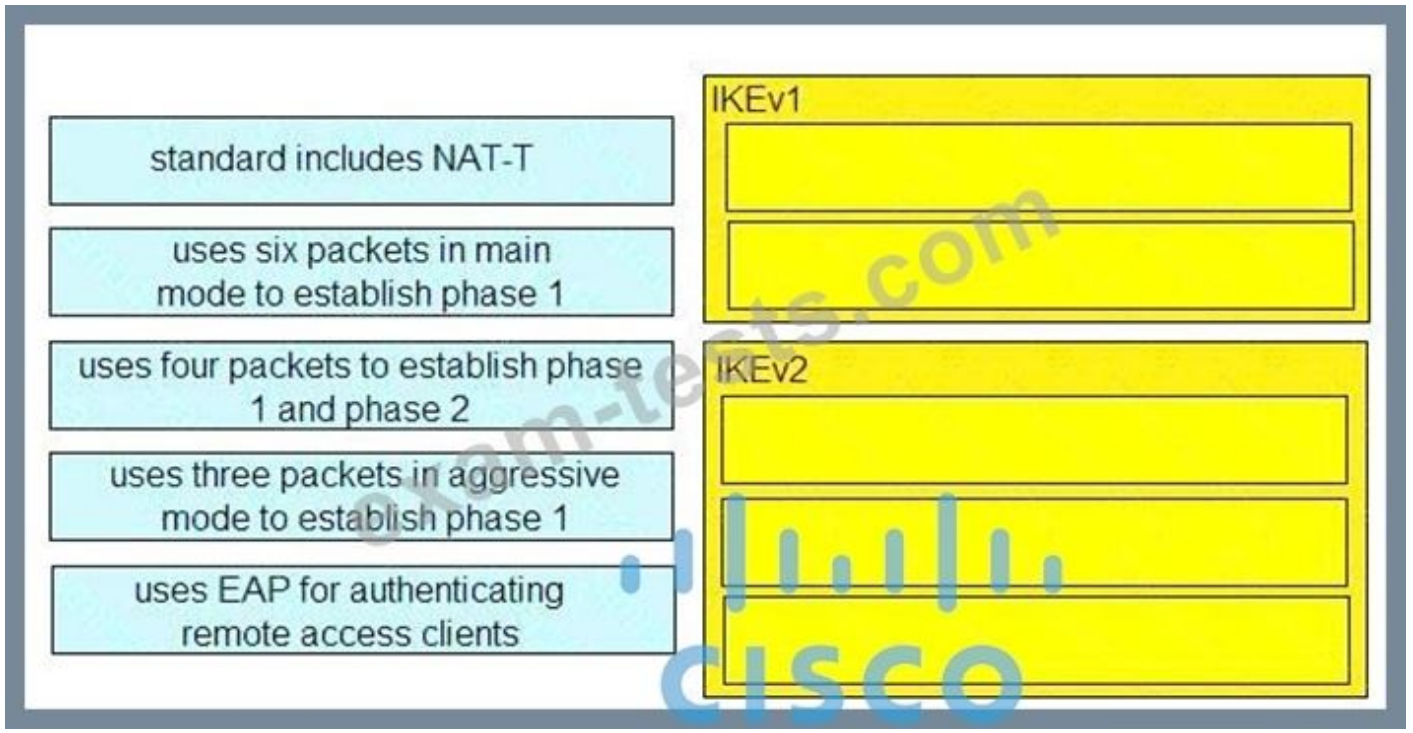
Answer: (SHOW ANSWER)

Explanation

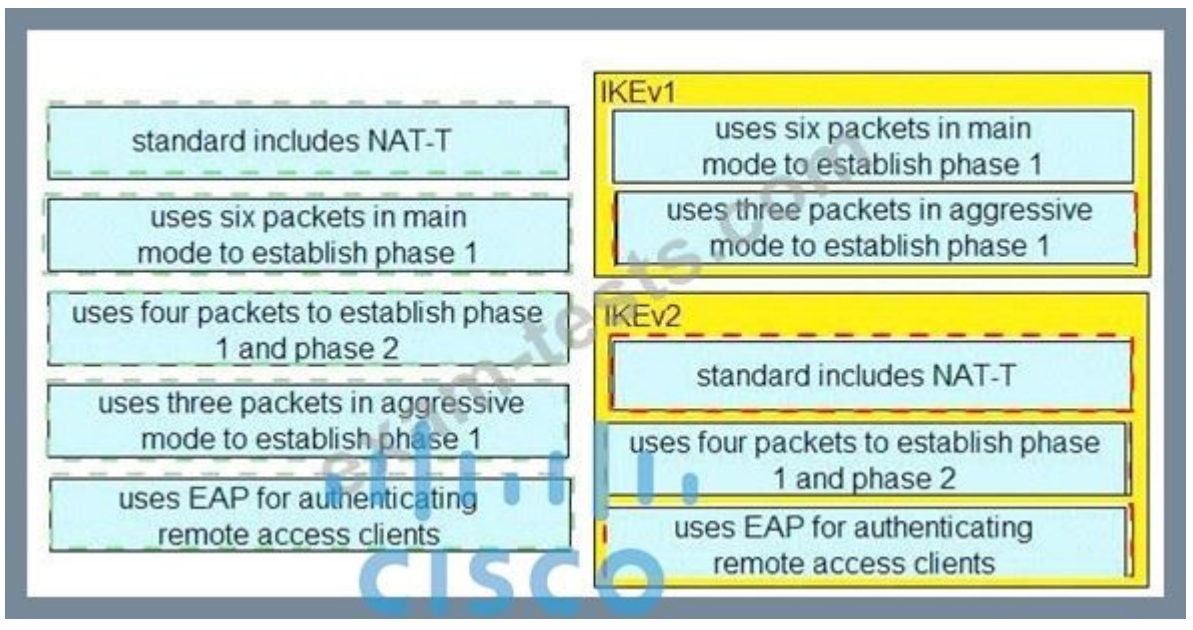
https://learningnetwork.cisco.com/s/question/0D53i00000KsrhK/rsa-key

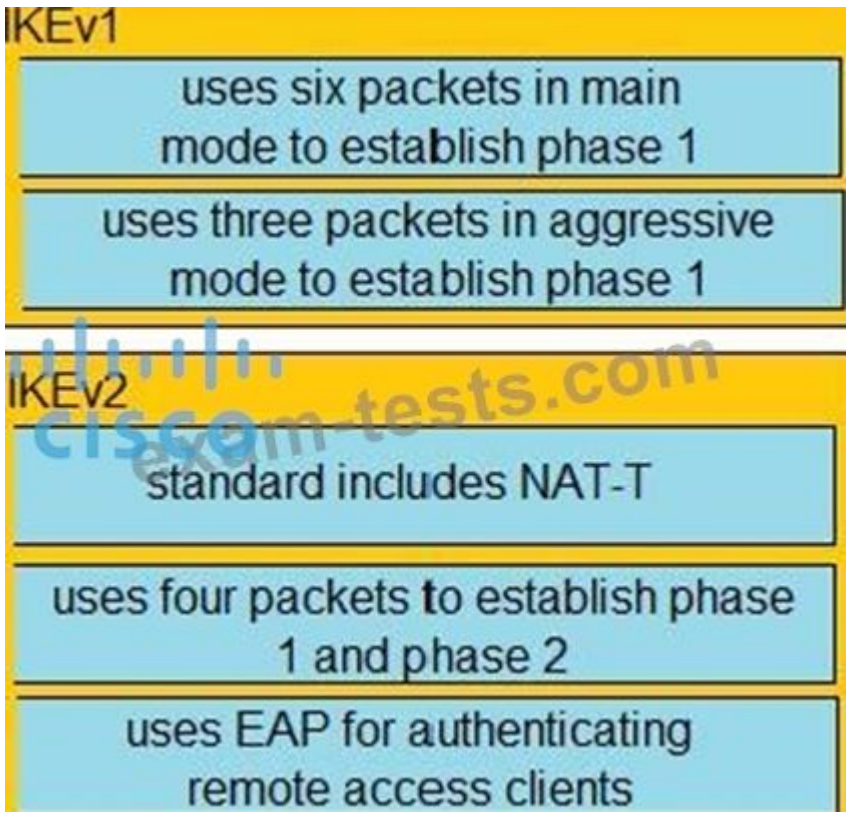
NEW QUESTION: 121

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



Answer:





NEW QUESTION: 122
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: B,D (LEAVE A REPLY)
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: 123

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

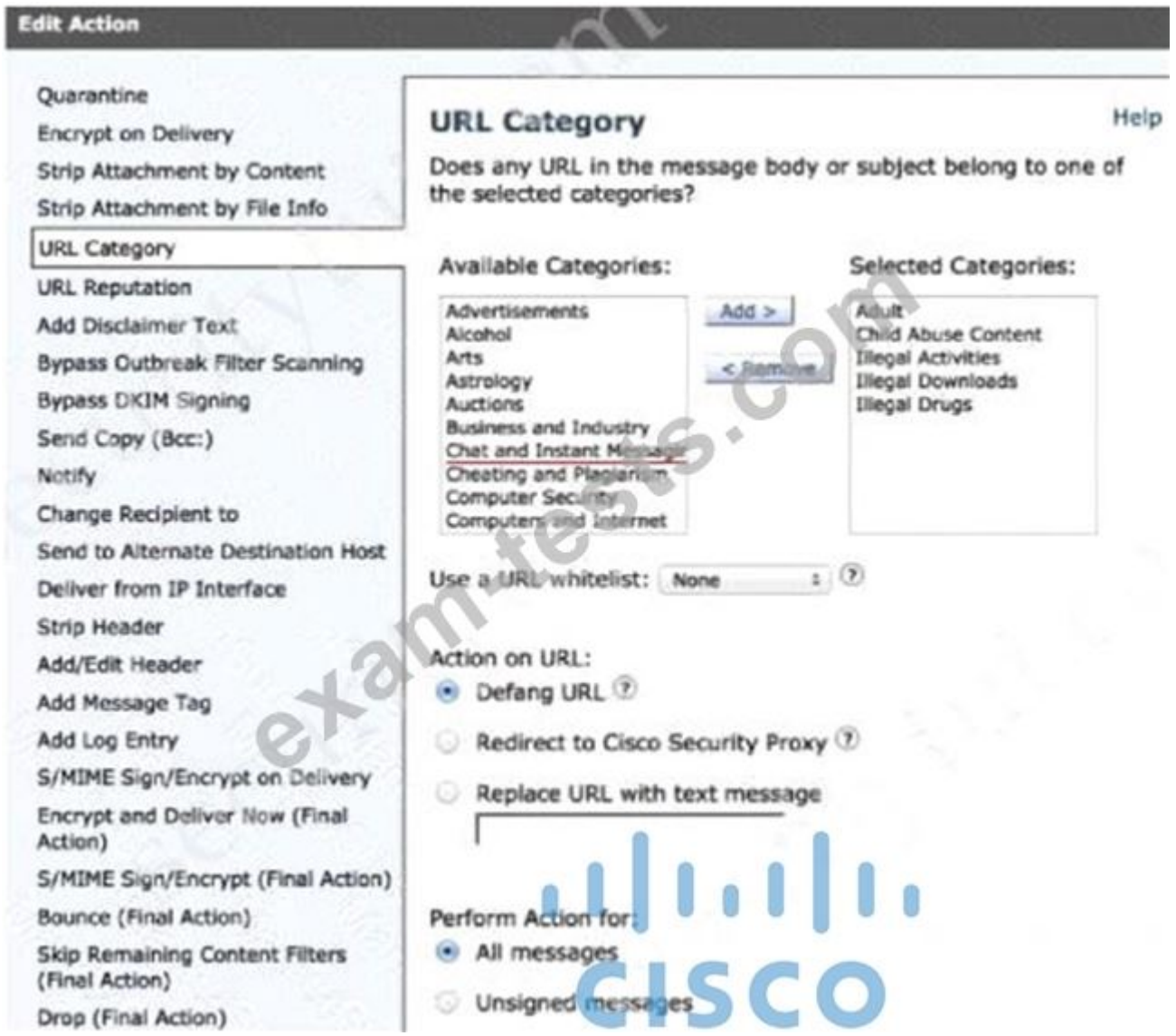
B. 3

C. 5

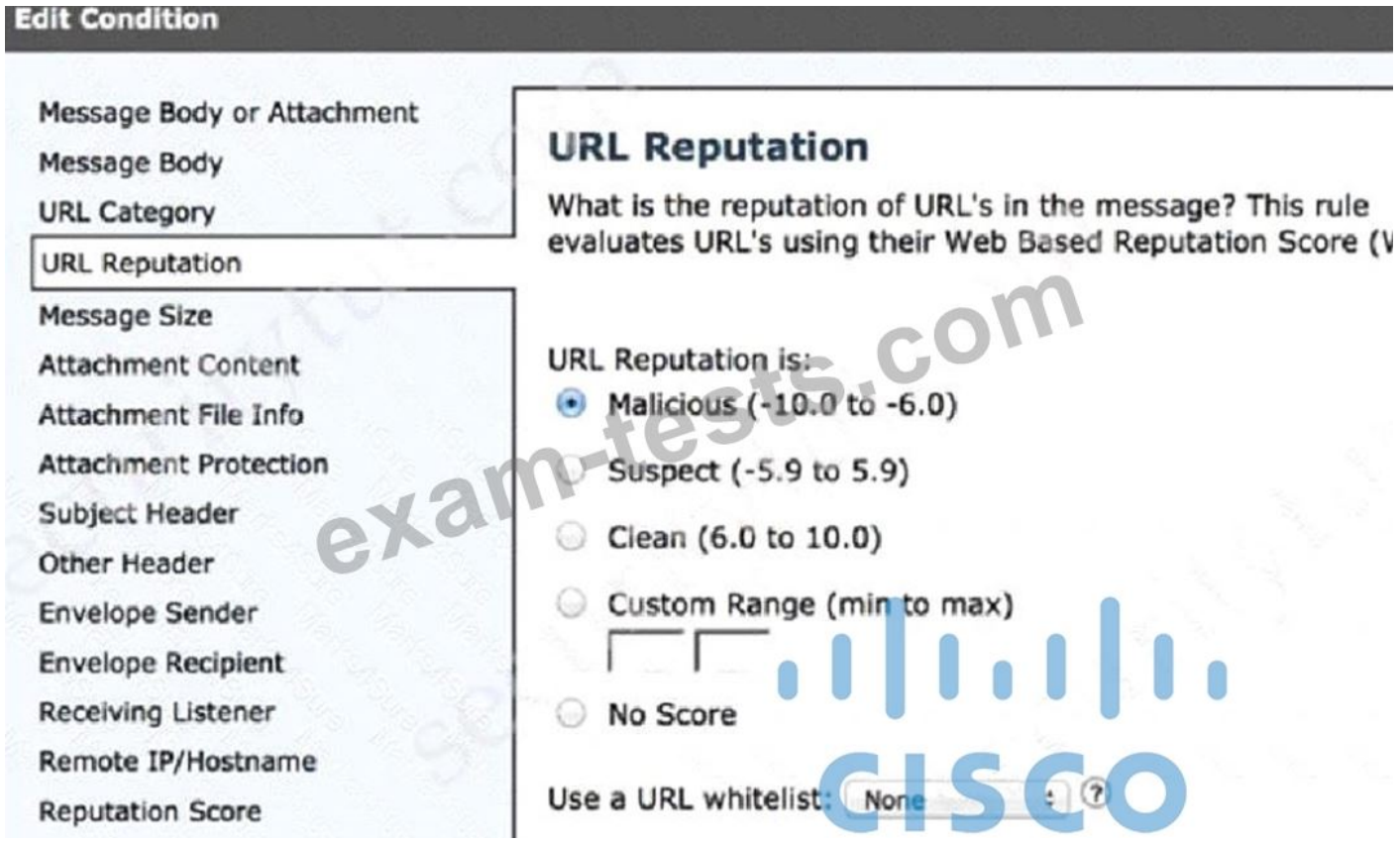
D. 10

Answer: D (LEAVE A REPLY)

ExplanationWe 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: 124
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. CDO
B. Cisco FDM
C. Cisco FMC
D. CSM
Answer: D (LEAVE A REPLY)

NEW QUESTION: 125

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

Refer to the exhibit. 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. number of possible failed attempts until the SNMPv3 user is locked out
D. privilege level for an authorized user to this router
Answer: (SHOW ANSWER)

NEW QUESTION: 126
An engineer needs to configure an access control policy rule to always send traffic for inspection without using the default action. Which action should be configured for this rule?
A. allow

B. trust

C. monitor

D. block

Answer: C (LEAVE A REPLY)

NEW QUESTION: 127

Refer to the exhibit.

```
nterface: Outside
    Crypto map tag: CSM_Outside_map, seq num: 1, local addr:
09.165.200.225

      access-list CSM_IPSEC_ACL_1 extended permit ip 10.0.11.0
55.255.255.0 10.0.10.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.0.11.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.0.10.0/255.255.255.0/0/0
      current_peer: 209.165.202.129


      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 17
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp
ailed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments
reated: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
eassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.200.225/500, remote crypto endpt.:
09.165.202.129/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: B6F5EA53
```

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.

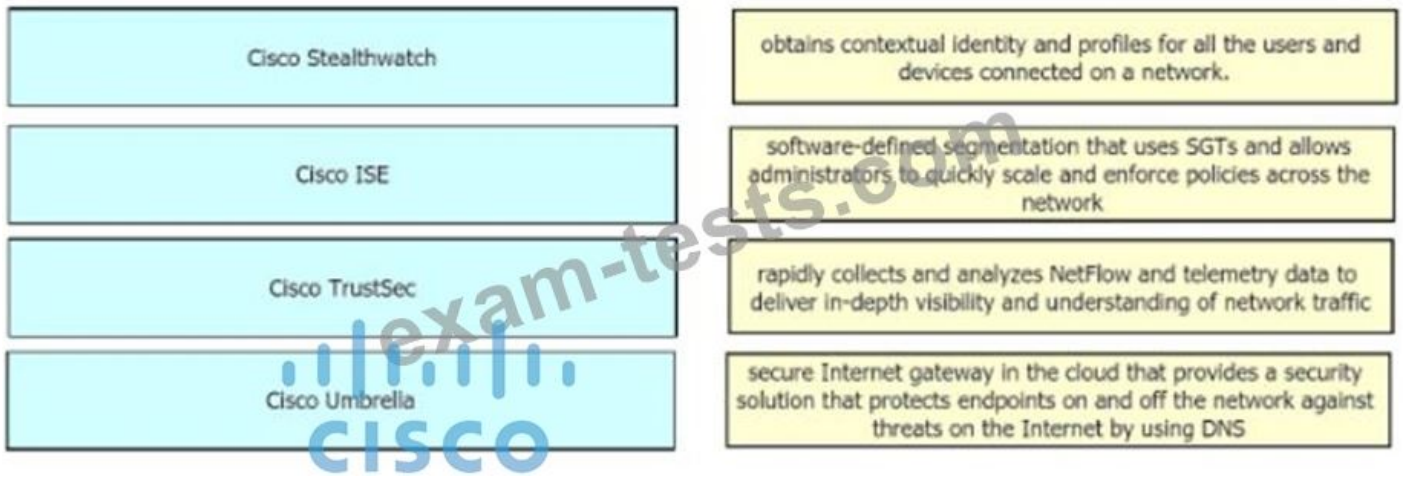
D. Site-to-site VPN preshared keys are mismatched.

Answer: A (LEAVE A REPLY)

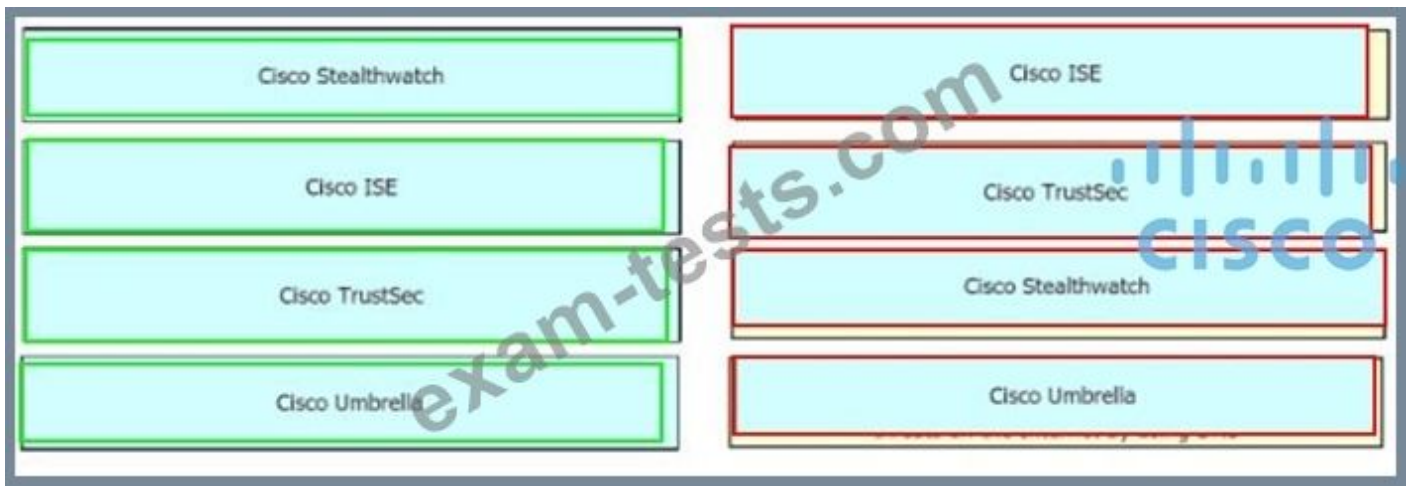
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html

NEW QUESTION: 128

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



Answer:



NEW QUESTION: 129

A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?

A. Use MAB with profiling

B. Use MAB with posture assessment.

C. Use 802.1X with posture assessment.

D. Use 802.1X with profiling.

Answer: A (LEAVE A REPLY)

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

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

NEW QUESTION: 130
Which type of dashboard does Cisco DNA Center provide for complete control of the network?
A. service management
B. centralized management
C. application management
D. distributed management
Answer: (SHOW ANSWER)
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- dna-center-faq-cte-en.html

NEW QUESTION: 131

```
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)# switchport access vlan 12
```

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

A. dot1x reauthentication

B. cisp enable

C. dot1x pae authenticator

D. authentication open

Answer: C (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 132

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

A. data exfiltration

B. snort

C. command and control communication

D. intelligent proxy

E. URL categorization

Answer: (SHOW ANSWER)

NEW QUESTION: 133

What is managed by Cisco Security Manager?

A. WSA

B. ASA

C. access point O

D. ESA

Answer: B (LEAVE A REPLY)

Explanation

https://www.cisco.com/c/en/us/products/collateral/security/security-manager/datasheet-C78-737182.html

NEW QUESTION: 134

Which two cryptographic algorithms are used with IPsec? {Choose two.)

A. AES-BAC

B. AES-ABC

C. HMAC-SHA1/SHA2

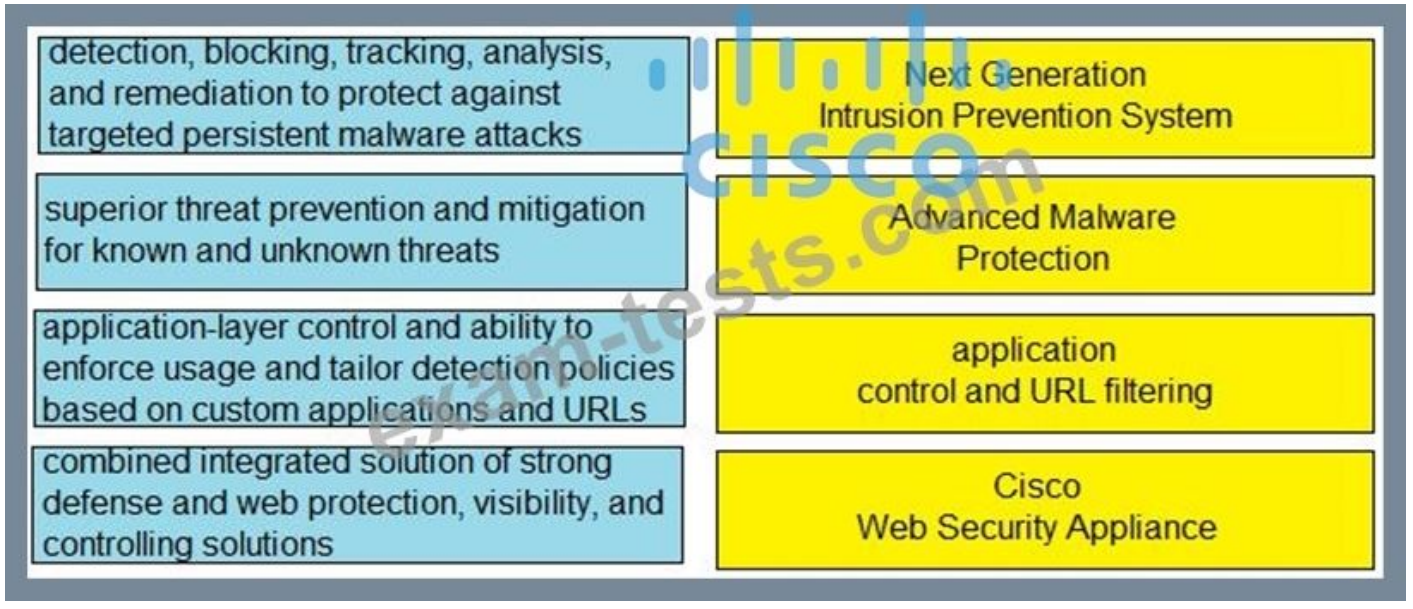
D. Triple AMC-CBC

E. AES-CBC

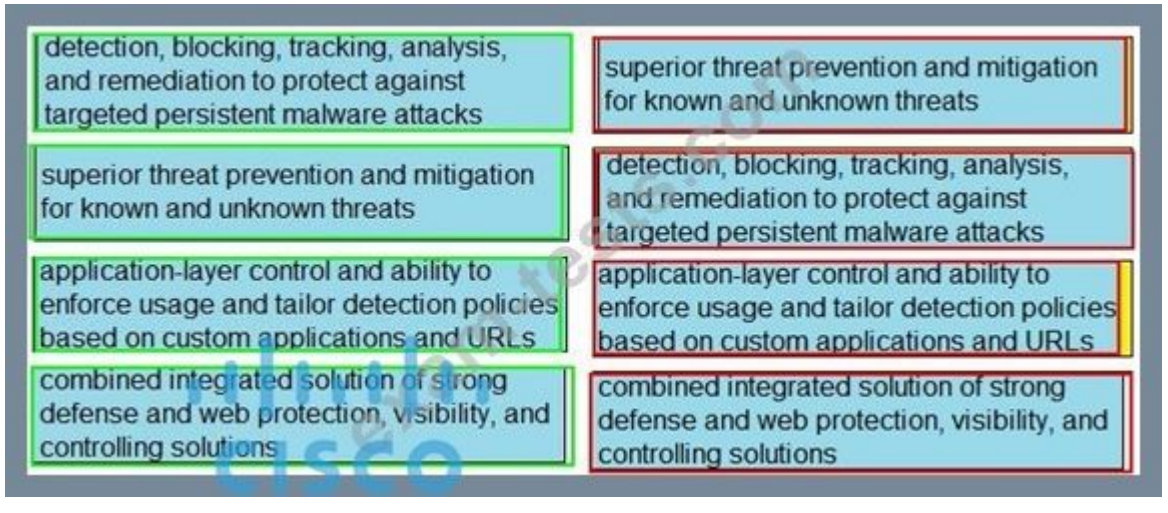
Answer: (SHOW ANSWER)
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-mt/sec-sec-for-vpns-w-ipsec-15-mt-book/sec-cfg-vpn-ipsec.html

NEW QUESTION: 135
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.

NEW QUESTION: 136
Drag and drop the capabilities from the left onto the correct technologies on the right.



Answer:



NEW QUESTION: 137
Which feature is supported when deploying Cisco ASAv within AWS public cloud?
A. multiple context mode
B. user deployment of Layer 3 networks
C. IPv6
D. clustering
Answer: B (LEAVE A REPLY)
The ASAv on AWS supports the following features:
+ Support for Amazon EC2 C5 instances, the next generation of the Amazon EC2 Compute Optimized instance family.
+ Deployment in the Virtual Private Cloud (VPC)
+ Enhanced networking (SR-IOV) where available
+ Deployment from Amazon Marketplace
+ Maximum of four vCPUs per instance
+ User deployment of L3 networks
+ Routed mode (default)
Note: The Cisco Adaptive Security Virtual Appliance (ASAv) runs the same software as physical Cisco ASAs to deliver proven security functionality in a virtual form factor. The ASAv can be deployed in the public AWS cloud.
It can then be configured to protect virtual and physical data center workloads that expand, contract, or shift their location over time. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96 qsg/asavaws.html The ASAv on AWS supports the following features:
+ Support for Amazon EC2 C5 instances, the next generation of the Amazon EC2 Compute Optimized instance family.
+ Deployment in the Virtual Private Cloud (VPC)
+ Enhanced networking (SR-IOV) where available
+ Deployment from Amazon Marketplace
+ Maximum of four vCPUs per instance
+ User deployment of L3 networks
+ Routed mode (default)
Note: The Cisco Adaptive Security Virtual Appliance (ASAv) runs the same software as physical Cisco ASAs to deliver proven security functionality in a virtual form factor. The ASAv can be deployed in the public AWS cloud.
The ASAv on AWS supports the following features:
+ Support for Amazon EC2 C5 instances, the next generation of the Amazon EC2 Compute Optimized instance family.
+ Deployment in the Virtual Private Cloud (VPC)
+ Enhanced networking (SR-IOV) where available

+ Deployment from Amazon Marketplace
+ Maximum of four vCPUs per instance
+ User deployment of L3 networks
+ Routed mode (default)
Note: The Cisco Adaptive Security Virtual Appliance (ASAv) runs the same software as physical Cisco ASAs to deliver proven security functionality in a virtual form factor. The ASAv can be deployed in the public AWS cloud.
It can then be configured to protect virtual and physical data center workloads that expand, contract, or shift their location over time. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96 qsg/asavaws.html

NEW QUESTION: 138
How does Cisco Workload Optimization Manager help mitigate application performance issues?
A. It automates resource resizing.
B. It optimizes a flow path
C. It deploys an AWS Lambda system
D. it sets up a workload forensic score
Answer: A (LEAVE A REPLY)

NEW QUESTION: 139
A network administrator is setting up Cisco FMC to send logs to Cisco Security Analytics and Logging (SaaS). The network administrator is anticipating a high volume of logging events from the firewalls and wants lo limit the strain on firewall resources. Which method must the administrator use to send these logs to Cisco Security Analytics and Logging?
A. SFTP using the FMCCLI
B. syslog using the Secure Event Connector
C. direct connection using SNMP traps
D. HTTP POST using the Security Analytics FMC plugin
Answer: B (LEAVE A REPLY)
The Secure Event Connector is a component of the Security Analytics and Logging (SaaS) solution that enables the FMC to send logs to the cloud-based service. The Secure Event Connector uses syslog to forward events from the FMC and the managed devices to the cloud. This method reduces the load on the firewall resources, as the events are sent in batches and compressed before transmission. The Secure Event Connector also provides encryption, authentication, and reliability for the log data. The other methods are not supported by the Security Analytics and Logging (SaaS) solution12 References := 1: Cisco Security Analytics and Logging (On Premises)

NEW QUESTION: 140
An administrator enables Cisco Threat Intelligence Director on a Cisco FMC. Which process uses STIX and allows uploads and downloads of block lists?
A. consumption
B. sharing
C. editing
D. authoring
Answer: B (LEAVE A REPLY)
The process that uses STIX and allows uploads and downloads of block lists is sharing. STIX (Structured Threat Information Expression) is a standard language and format for exchanging cyber threat intelligence data. Block lists are collections of observables, such as IP addresses, URLs, or domains, that

are associated with malicious activity and can be used to block or monitor network traffic. Cisco Threat Intelligence Director (TID) is a feature that operationalizes threat intelligence data by consuming, normalizing, publishing, and correlating data from various sources, including third-party STIX feeds. TID enables the administrator to upload STIX files from local or remote sources, or download STIX files from the Firepower Management Center (FMC) to share with other systems. TID also allows the administrator to configure actions (such as block or monitor) based on the indicators and observables in the STIX files, and generate incidents and observations when the system detects traffic that matches the threat intelligence data123 References := 1: Firepower Management Center Configuration Guide, Version 6.2.3 - Threat Intelligence Director 2 2: Introduction to STIX - GitHub Pages 4 3: Third-Party Integration of Security Feeds with FMC (Cisco Threat Intelligence Director) - Cisco Community 3

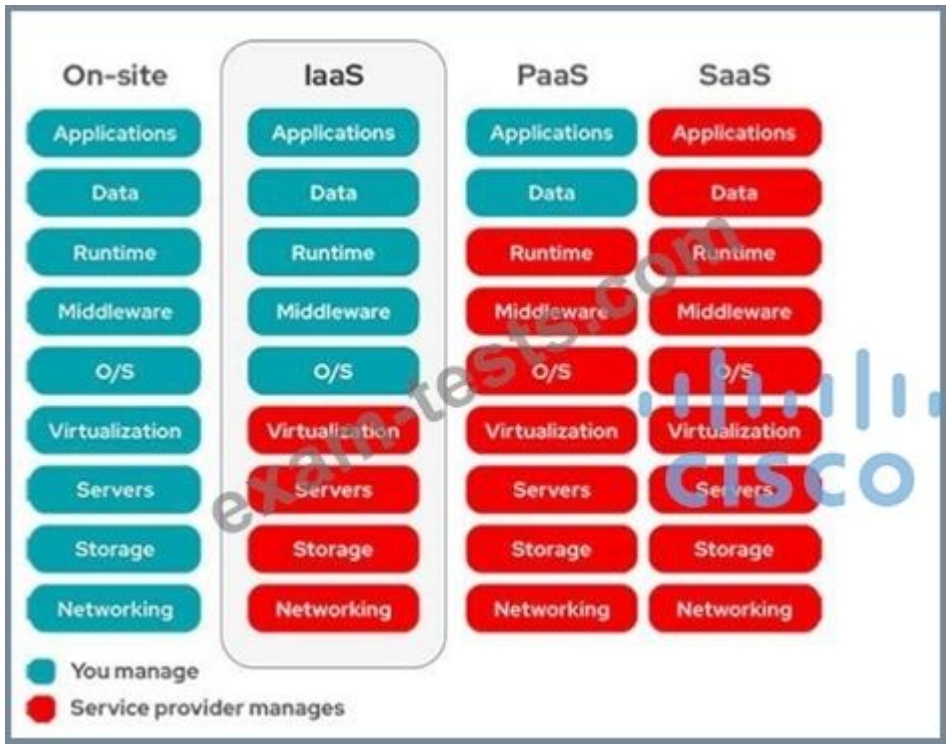
NEW QUESTION: 141
Which SNMPv3 configuration must be used to support the strongest security possible?
A. asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
B. asa-host(config)#snmp-server group myv3 v3 noauth
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
C. asa-host(config)#snmp-server group myv3 v3 noauth
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
D. asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 142
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)
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: 143
Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?
A. PaaS
B. XaaS
C. IaaS

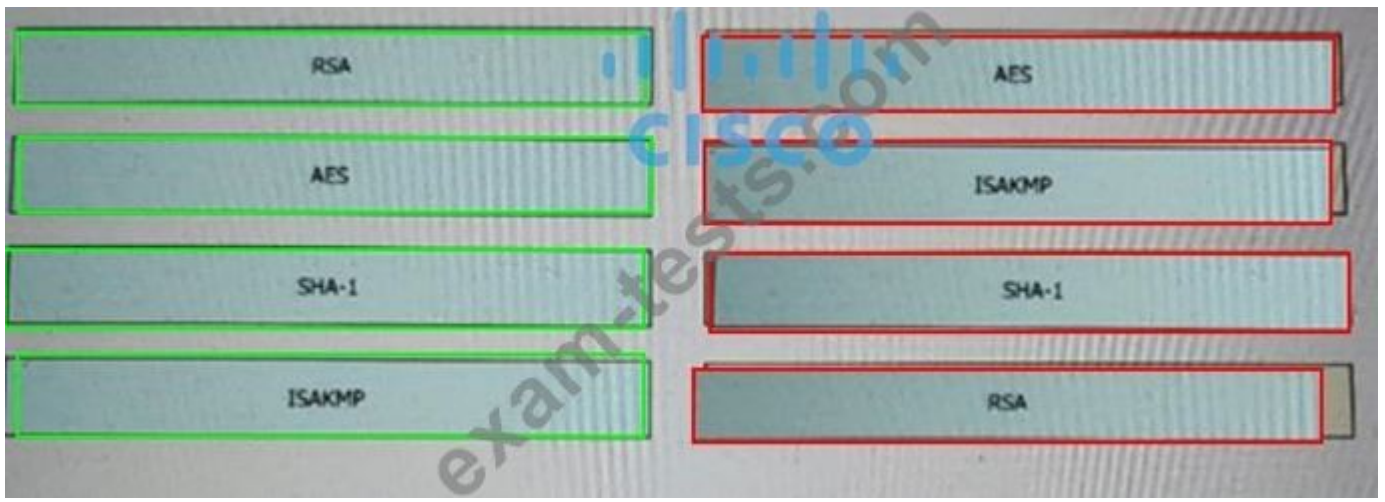
D. SaaS
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 144
In which cloud services model is the tenant responsible for virtual machine OS patching?
A. IaaS
B. UCaaS
C. PaaS
D. SaaS
Answer: A (LEAVE A REPLY)
Only in On-site (on-premises) and IaaS we (tenant) manage O/S (Operating System).



NEW QUESTION: 145
Drag and drop the VPN functions from the left onto the description on the right.

Answer:



NEW QUESTION: 146
How does Cisco Stealthwatch Cloud provide security for cloud environments?
A. It delivers visibility and threat detection.
B. It prevents exfiltration of sensitive data.
C. It assigns Internet-based DNS protection for clients and servers.
D. It facilitates secure connectivity between public and private networks.
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.content.shi.com/SHIcom/ContentAttachmentImages/SharedResources/FBLP/Cisco/ Cisco-091919-Simple-IT-Whitepaper.pdf

NEW QUESTION: 147
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. Spear phishing is when the attack is aimed at the C-level executives of an organization
C. Deceptive phishing is an attacked aimed at a specific user in the organization who holds a C-level role.
D. A spear phishing campaign is aimed at a specific person versus a group of people.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 148
What must be used to share data between multiple security products?
A. Cisco Platform Exchange Grid
B. Cisco Stealthwatch Cloud
C. Cisco Advanced Malware Protection
D. Cisco Rapid Threat Containment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 149
What is the purpose of the My Devices Portal in a Cisco ISE environment?
A. to manage and deploy antivirus definitions and patches on systems owned by the end user

B. to register new laptops and mobile devices
C. to provision userless and agentless systems
D. to request a newly provisioned mobile device
Answer: D (LEAVE A REPLY)
Explanation

Employees can use the My Devices portal to register and manage their personal devices. The My Devices portal includes online help that provides

NEW QUESTION: 150
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: 151
Which two characteristics of messenger protocols make data exfiltration difficult to detect and prevent?
(Choose two.)
A. An exposed API for the messaging platform is used to send large amounts of data.
B. Traffic is encrypted, which prevents visibility on firewalls and IPS systems.
C. Malware infects the messenger application on the user endpoint to send company data.
D. Outgoing traffic is allowed so users can communicate with outside organizations.
E. Messenger applications cannot be segmented with standard network controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 152
An administrator is adding a new switch onto the network and has configured AAA for network access control. When testing the configuration, the RADIUS authenticates to Cisco ISE but is being rejected. Why is the ip radius source-interface command needed for this configuration?
A. RADIUS requests are generated only by a router if a RADIUS source interface is defined.
B. Only requests that originate from a configured NAS IP are accepted by a RADIUS server
C. The RADIUS authentication key is transmitted only from the defined RADIUS source interface
D. Encrypted RADIUS authentication requires the RADIUS source interface be defined
Answer: (SHOW ANSWER)

NEW QUESTION: 153
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 uses methods such as GET, PUT, POST, and DELETE.
D. REST codes can be compiled with any programming language.
E. REST is a Linux platform-based architecture.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 154
Which cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group?
A. Hybrid
B. Community
C. Private
D. Public
Answer: B (LEAVE A REPLY)
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: 155
When NetFlow is applied to an interface, which component creates the flow monitor cache that is used to collect traffic based on the key and nonkey fields in the configured record?
A. records
B. flow exporter
C. flow sampler
D. flow monitor
Answer: D (LEAVE A REPLY)
A flow monitor is a component of Flexible NetFlow that is used to store and export flow data. A flow monitor consists of a record, an optional exporter, and a cache. The cache is a section of memory that stores flow entries before they are exported to an external collector. The cache is created by the flow monitor when NetFlow is applied to an interface. The cache collects traffic based on the key and nonkey fields in the configured record. The key fields are used to identify a flow uniquely, while the nonkey fields are used to provide additional information about the flow. The cache can be configured with various

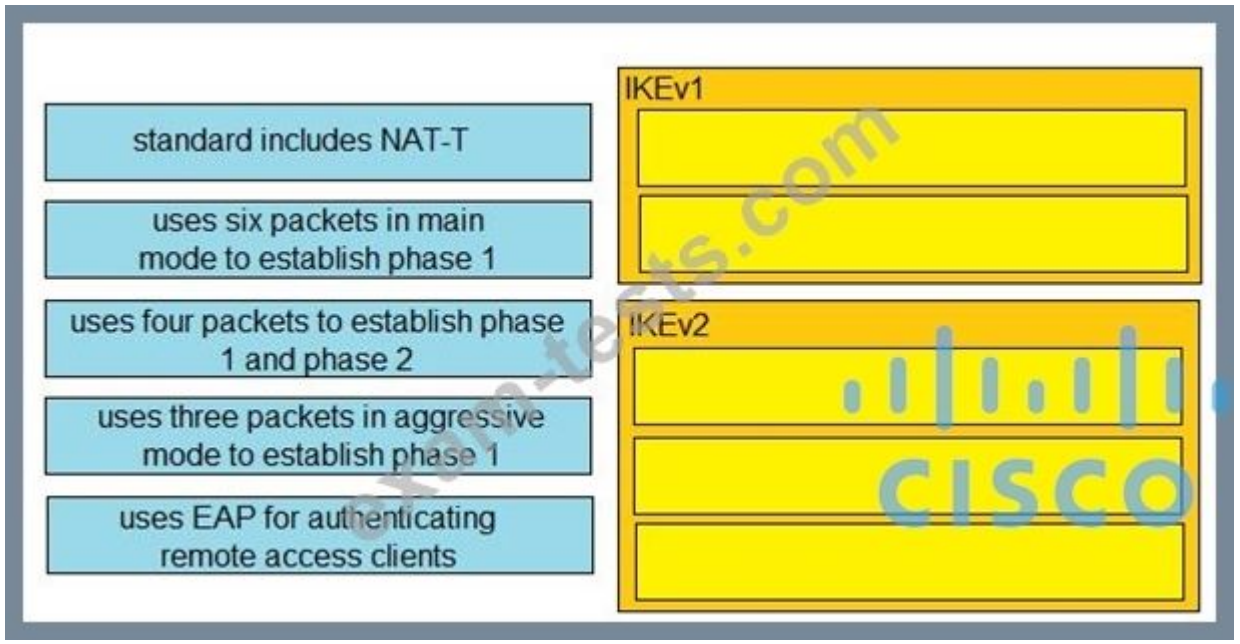
parameters, such as the number of entries, the timeout values, and the type of cache. The cache can also be viewed and cleared using show and clear commands. References := Some possible references are:
* Flexible Netflow Configuration Guide, Cisco IOS Release 15M&T
* ASR9000/XR Netflow Architecture and overview
* Cisco IOS Flexible NetFlow Command Reference - cache (Flexible NetFlow) through match flow

NEW QUESTION: 156
Which type of DNS abuse exchanges data between two computers even when there is no direct connection?
A. Malware installation
B. Command-and-control communication
C. Network footprinting
D. Data exfiltration
Answer: D (LEAVE A REPLY)
Reference: https://www.netsurion.com/articles/5-types-of-dns-attacks-and-how-to-detect-them

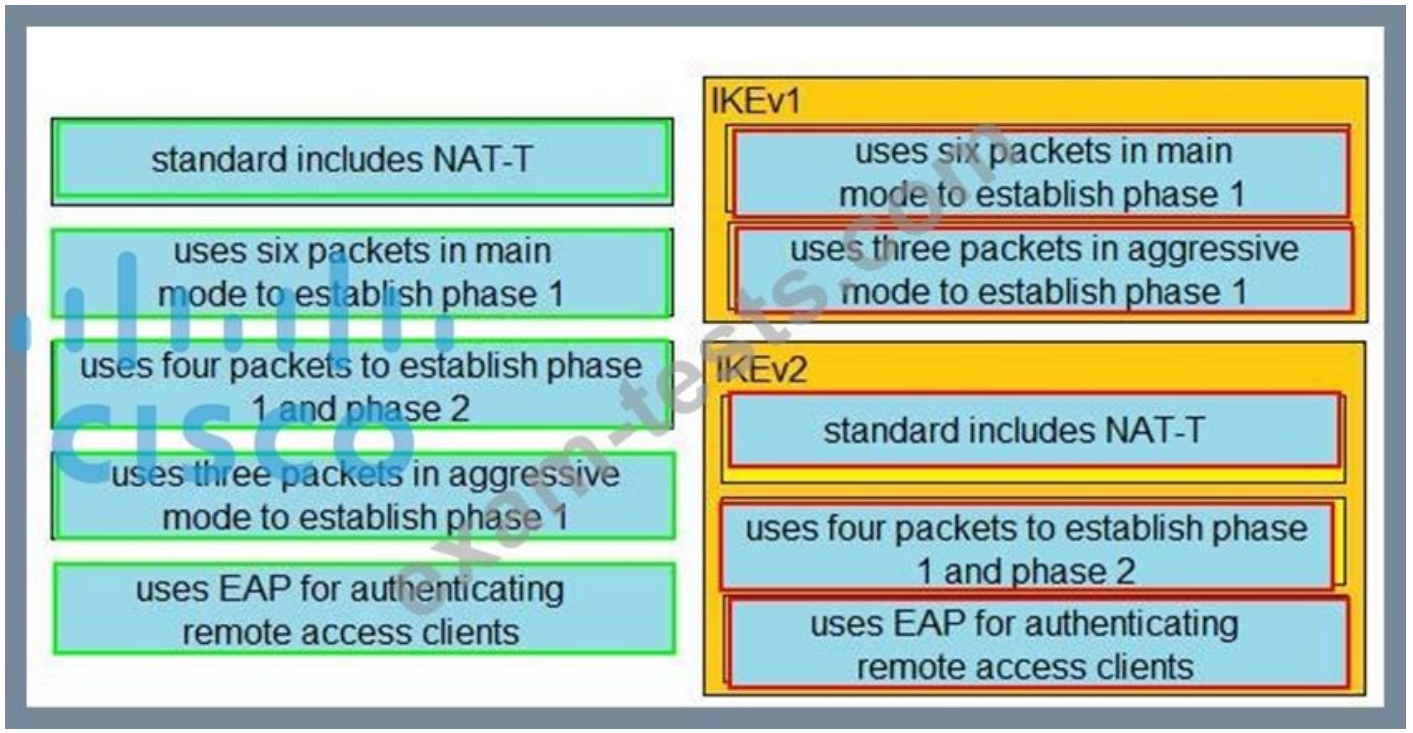
NEW QUESTION: 157
An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices. The default management port conflicts with other communications on the network and must be changed. What must be done to ensure that all devices can communicate together?
A. Manually change the management 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: A (LEAVE A REPLY)
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: 158
In which two ways does Easy Connect help control network access when used with Cisco TrustSec? (Choose two)
A. It allows multiple security products to share information and work together to enhance security posture in the network.
B. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.
C. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.
D. It integrates with third-party products to provide better visibility throughout the network.
E. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).
Answer: C,E (LEAVE A REPLY)
Explanation
Easy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity.
Reference:
easy-connect-configuration-guide.pdf

NEW QUESTION: 159
Drag and drop the descriptions from the left onto the correct protocol versions on the right.



Answer:

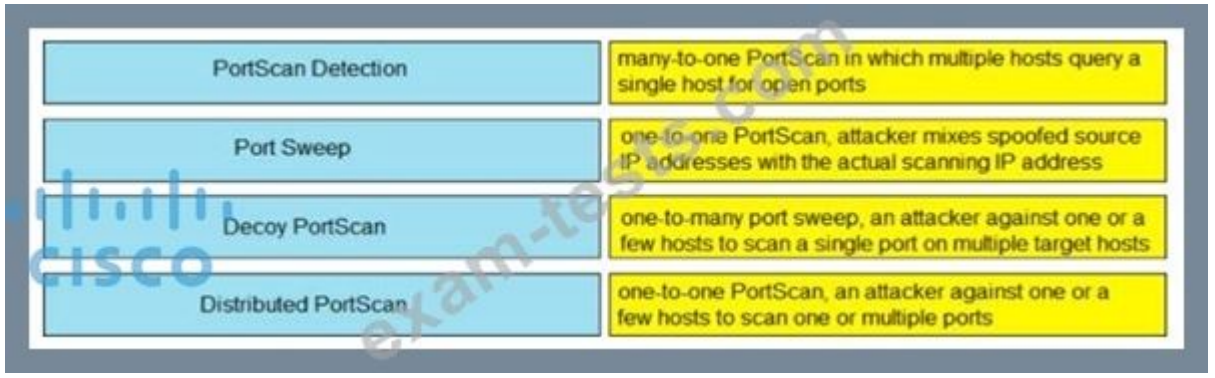


NEW QUESTION: 160
An administrator configures a new destination list in Cisco Umbrella so that the organization can block specific domains for its devices. What should be done to ensure that all subdomains of domain.com are blocked?
A. Configure the *.com address in the block list.
B. Configure the *.domain.com address in the block list
C. Configure the *.domain.com address in the block list
D. Configure the domain.com address in the block list

Answer: D (LEAVE A REPLY)
To block all subdomains of domain.com, the administrator should configure the domain.com address in the block list. This is because Umbrella automatically applies a left side and right side wildcard to every domain in a block or allow destination list. Therefore, adding domain.com to a block list will result in requests to domain.com or its subdomains, such as www.domain.com, being blocked. Adding a wildcard character (*) is not supported and will not work. Adding the *.com address in the block list will block all domains that end with .com, which is not the desired outcome. References:
* Understanding Destination lists supported entries and error messages
* Wildcards and Destination Lists

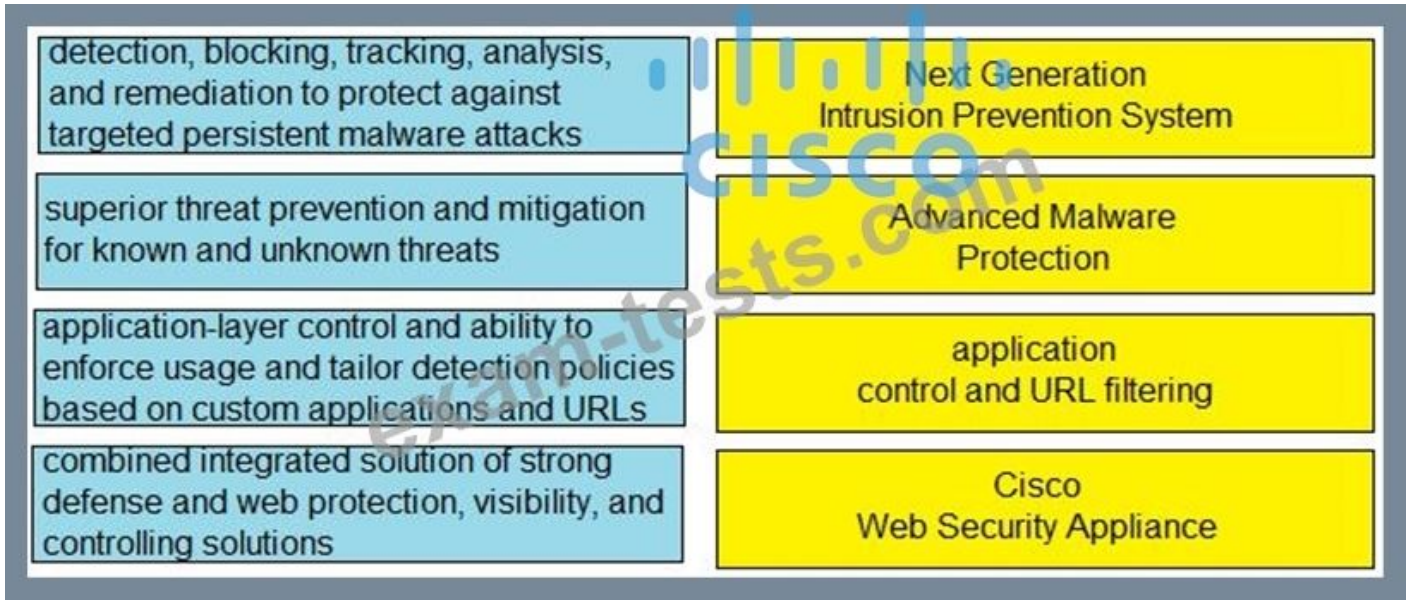
NEW QUESTION: 161
What are two rootkit types? (Choose two)
A. virtual
B. user mode
C. bootloader
D. registry
E. buffer mode
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 162
Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.

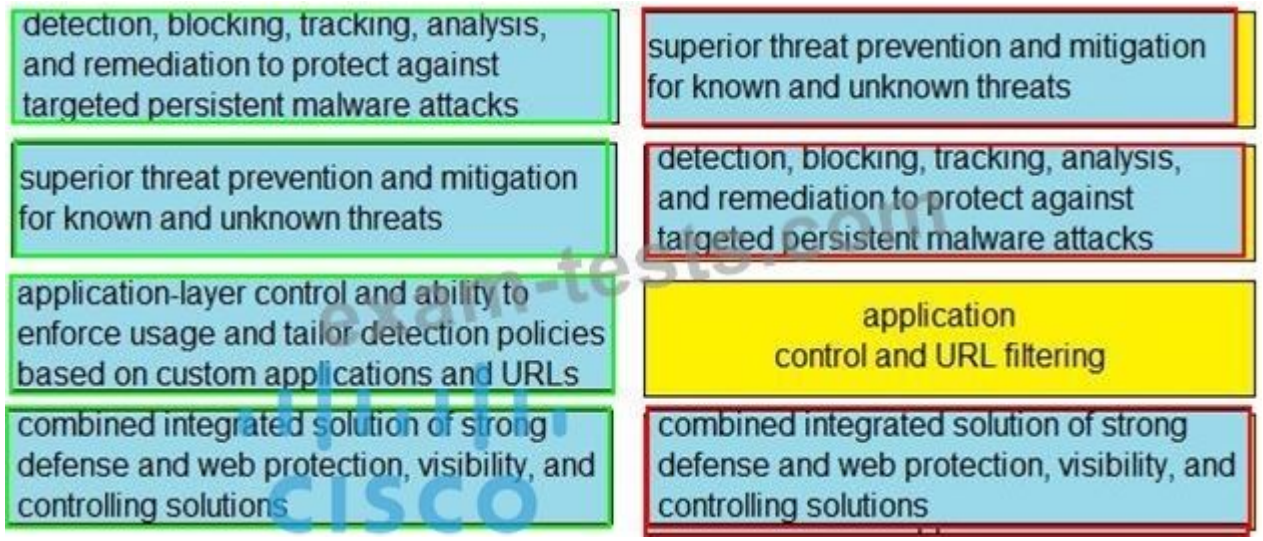


Answer:

NEW QUESTION: 163
Drag and drop the capabilities from the left onto the correct technologies on the right.

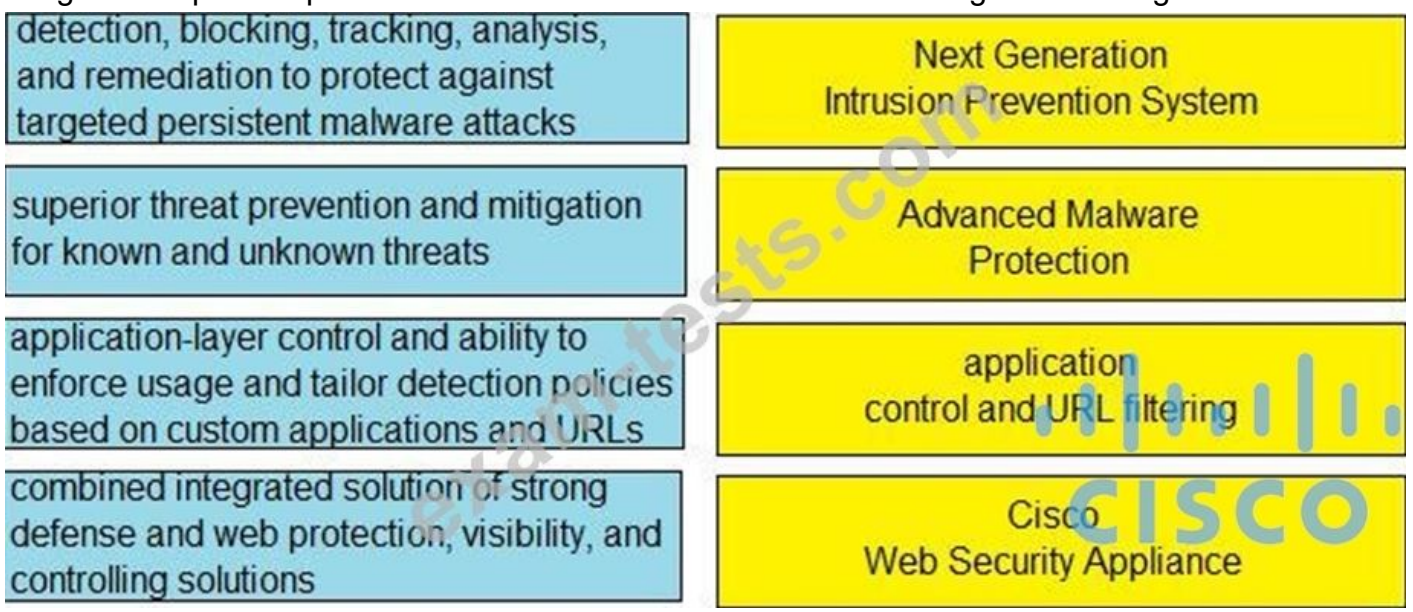


Answer:



NEW QUESTION: 164

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



Answer:

NEW QUESTION: 165

An organization wants to implement a cloud-delivered and SaaS-based solution to provide visibility and threat detection across the AWS network. The solution must be deployed without software agents and rely on AWS VPC flow logs instead. Which solution meets these requirements?

A. Cisco Umbrella

B. Cisco Stealthwatch Cloud

C. NetFlow collectors

D. Cisco Cloudlock

Answer: (SHOW ANSWER)

NEW QUESTION: 166

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)

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.

Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming.

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.

Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming.
Reference:
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.
Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming.

NEW QUESTION: 167
Refer to the exhibit.

An administrator is adding a new Cisco FTD device to their network and wants to manage it with Cisco FMC.
The Cisco FTD is not behind a NAT device. Which command is needed to enable this on the Cisco FTD?
A. configure manager add DONTRESOLVE kregistration key>
B. configure manager add <FMC IP address> <registration key> 16
C. configure manager add DONTRESOLVE <registration key> FTD123
D. configure manager add <FMC IP address> <registration key>
Answer: D (LEAVE A REPLY)
To let FMC manages FTD, first we need to add manager from the FTD and assign a register key of your choice. The command configure manager add 1.1.1.2 the_registration_key_you_want, where 1.1.1.2 is the IP address of the FMC, you need to use the same registration key in FMC when adding this FTD as a managed device. Reference: https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/ choice. The command configure manager add

1.1.1.2 the_registration_key_you_want, where 1.1.1.2 is the IP address of the FMC, you need to use the same registration key in FMC when adding this FTD as a managed device.
To let FMC manages FTD, first we need to add manager from the FTD and assign a register key of your choice. The command configure manager add 1.1.1.2 the_registration_key_you_want, where 1.1.1.2 is the IP address of the FMC, you need to use the same registration key in FMC when adding this FTD as a managed device. Reference: https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/

NEW QUESTION: 168
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.
Reference:
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: 169
Client workstations are experiencing extremely poor response time. An engineer suspects that an attacker is eavesdropping and making independent connections while relaying messages between victims to make them think they are talking to each other over a private connection. Which feature must be enabled and configured to provide relief from this type of attack?
A. private VLANs
B. Dynamic ARP Inspection
C. Reverse ARP
D. Link Aggregation
Answer: (SHOW ANSWER)

NEW QUESTION: 170
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: A (LEAVE A REPLY)
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: 171
How is ICMP used as an exfiltration technique?
A. by flooding the destination host with unreachable packets
B. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host
C. by overwhelming a targeted host with ICMP echo-request packets
D. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address
Answer: (SHOW ANSWER)

NEW QUESTION: 172
Which CoA response code is sent if an authorization state is changed successfully on a Cisco IOS device?
A. CoA-NCL
B. COA-MAB
C. CoA-ACK
D. CoA-NAK
Answer: C (LEAVE A REPLY)

NEW QUESTION: 173
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)
ExplanationThe 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: 174

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. unencrypted links for traffic

C. software bugs on applications

D. improper file security

Answer: B (LEAVE A REPLY)

The vulnerability that allows the attacker to see the passwords being transmitted in clear text is the lack of encryption on the VPN links. Encryption is a process of transforming data into an unreadable form, so that only authorized parties can access it. VPN (Virtual Private Network) is a technology that creates a secure tunnel between two or more devices over a public network, such as the Internet. VPN links should be encrypted to prevent eavesdropping, tampering, or spoofing of the data that passes through them. If the VPN links are not encrypted, an attacker can use a packet sniffer to intercept and read the data, including the passwords, that are sent over the network. This is called a sniffing attack, and it can lead to credential theft, identity spoofing, or data manipulation. Therefore, VPN links should always use strong encryption protocols, such as IPsec or SSL/TLS, to protect the confidentiality and integrity of the data. References := Some possible references are:

* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 - Cisco: This is the official course page for the SCOR 350-701 exam, which covers the topics of implementing and operating Cisco security core technologies. It provides the course objectives, outline, duration, and prerequisites. It also offers various learning options, such as instructor-led training, e-learning, and practice exams.
* SCOR 350-701 Official Cert Guide - Cisco Press: This is the official study guide for the SCOR 350-701 exam, written by Omar Santos, a principal engineer at Cisco's Security Research and Operations group.

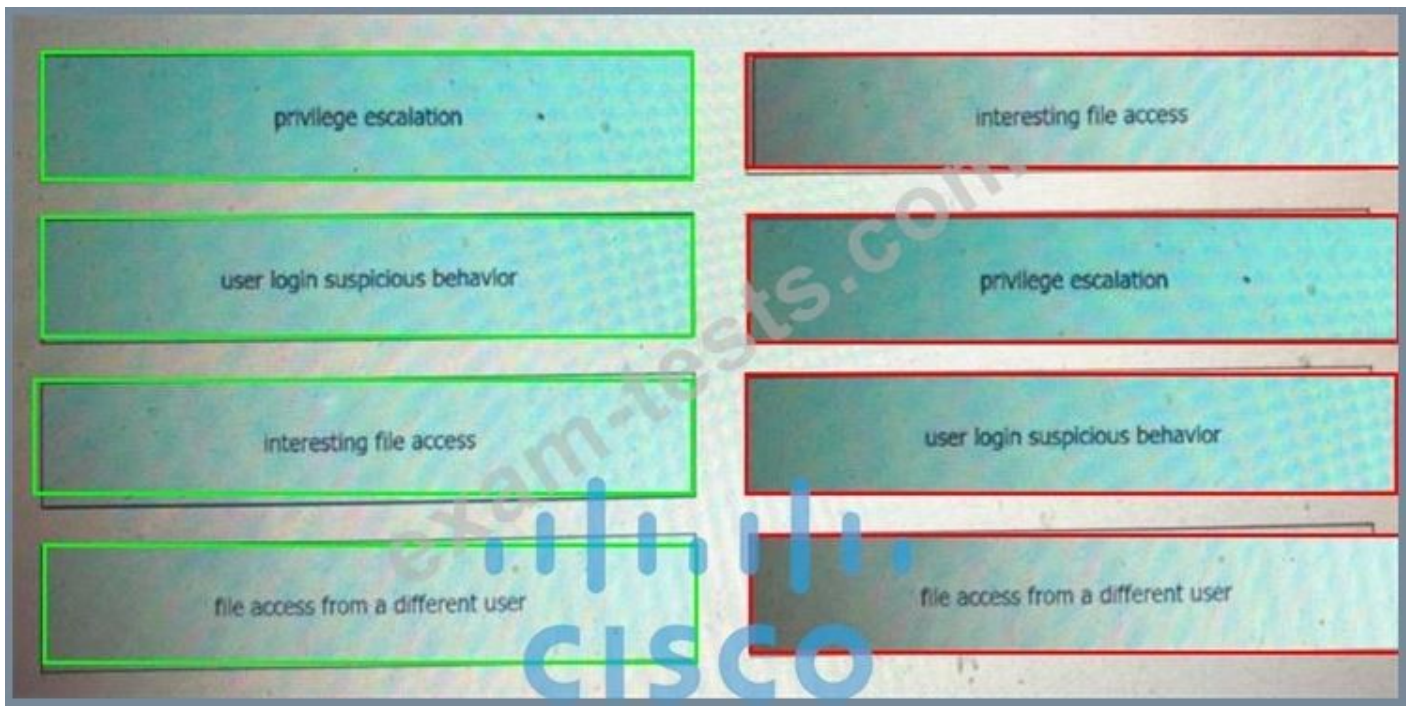
It covers all the exam topics in depth, with explanations, examples, exercises, and practice questions. It also includes a companion website with online resources, such as videos, quizzes, flashcards, and more.

* Cleartext submission of password - PortSwigger: This is a web security article that explains the vulnerability of transmitting passwords over unencrypted connections, and how to exploit it using Burp Suite, a web application testing tool. It also provides some remediation advice, such as using HTTPS and HSTS to enforce encryption.
* What Are Sniffing Attacks, and How Can You Protect Yourself? - EC-Council: This is a blog post that describes what sniffing attacks are, how they work, and what are the common types and tools of sniffing attacks. It also provides some tips on how to prevent or detect sniffing attacks, such as using encryption, VPN, firewall, IDS, and anti-sniffing software.
* OWASP Application Security FAQ | OWASP Foundation: This is a frequently asked questions page about application security, maintained by the Open Web Application Security Project (OWASP), a non-profit organization that promotes web security awareness and best practices. It covers various topics, such as authentication, authorization, session management, input validation, output encoding, cryptography, error handling, logging, and more.

NEW QUESTION: 175

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

Answer:



NEW QUESTION: 176
What is the recommendation in a zero-trust model before granting access to corporate applications and resources?
A. to use multifactor authentication
B. to use strong passwords
C. to disconnect from the network when inactive
D. to use a wired network, not wireless
Answer: A (LEAVE A REPLY)

NEW QUESTION: 177
What is the purpose of the My Devices Portal in a Cisco ISE environment?
A. to register new laptops and mobile devices
B. to request a newly provisioned mobile device

C. to provision userless and agentless systems
D. to manage and deploy antivirus definitions and patches on systems owned by the end user
Answer: A (LEAVE A REPLY)
Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network.

NEW QUESTION: 178
Refer to the exhibit.

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.528a	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	0A02198200001
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

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

NEW QUESTION: 179
What is the most common type of data exfiltration that organizations currently experience?
A. encrypted SMTP
B. Microsoft Windows network shares
C. SQL database injections
D. HTTPS file upload site
Answer: D (LEAVE A REPLY)

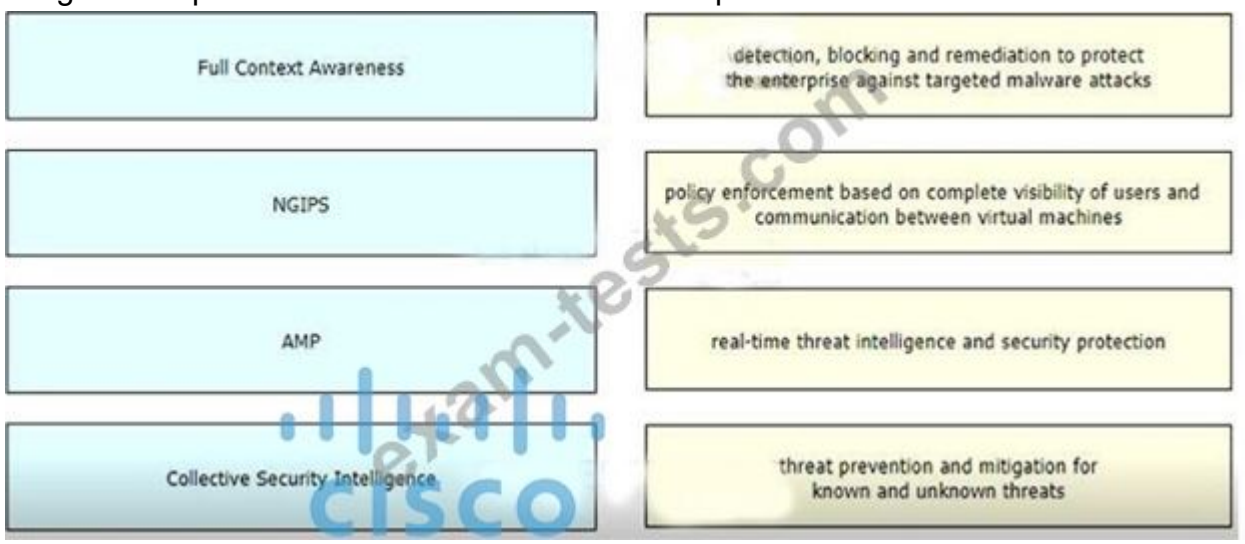
NEW QUESTION: 180
Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?
A. auth-type all
B. aaa server radius dynamic-author
C. aaa new-model

D. ip device-tracking

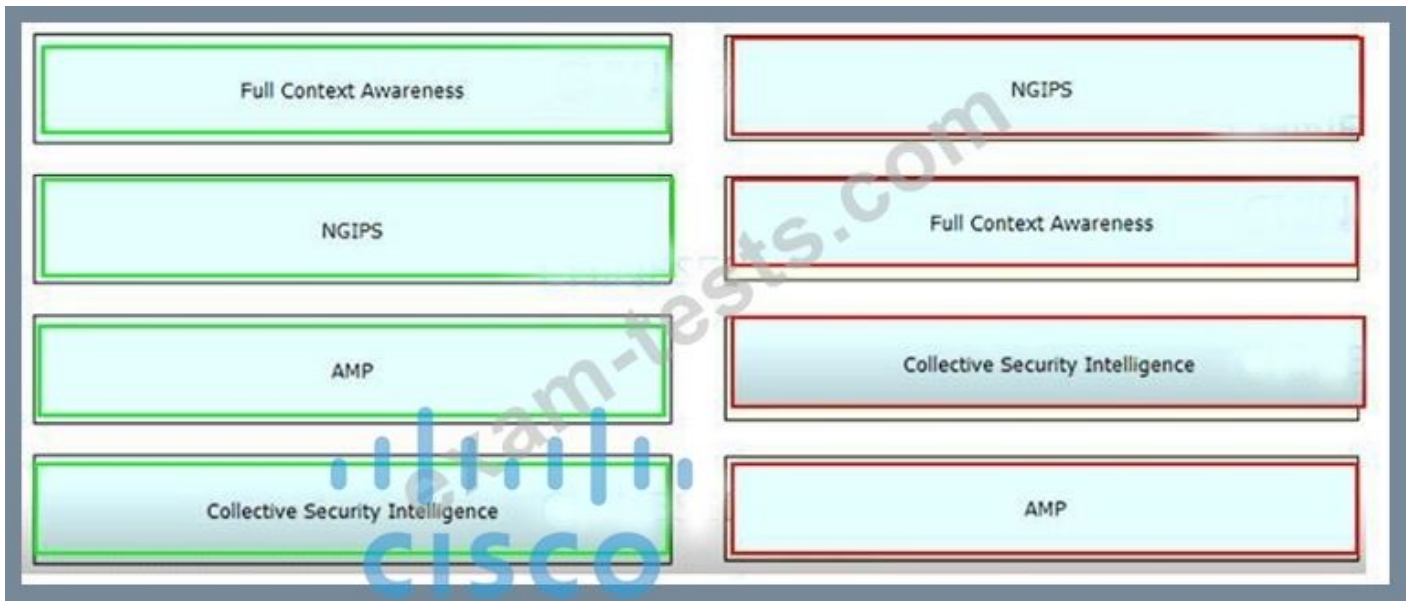
Answer: C (LEAVE A REPLY)

NEW QUESTION: 181

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



Answer:



NEW QUESTION: 182

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

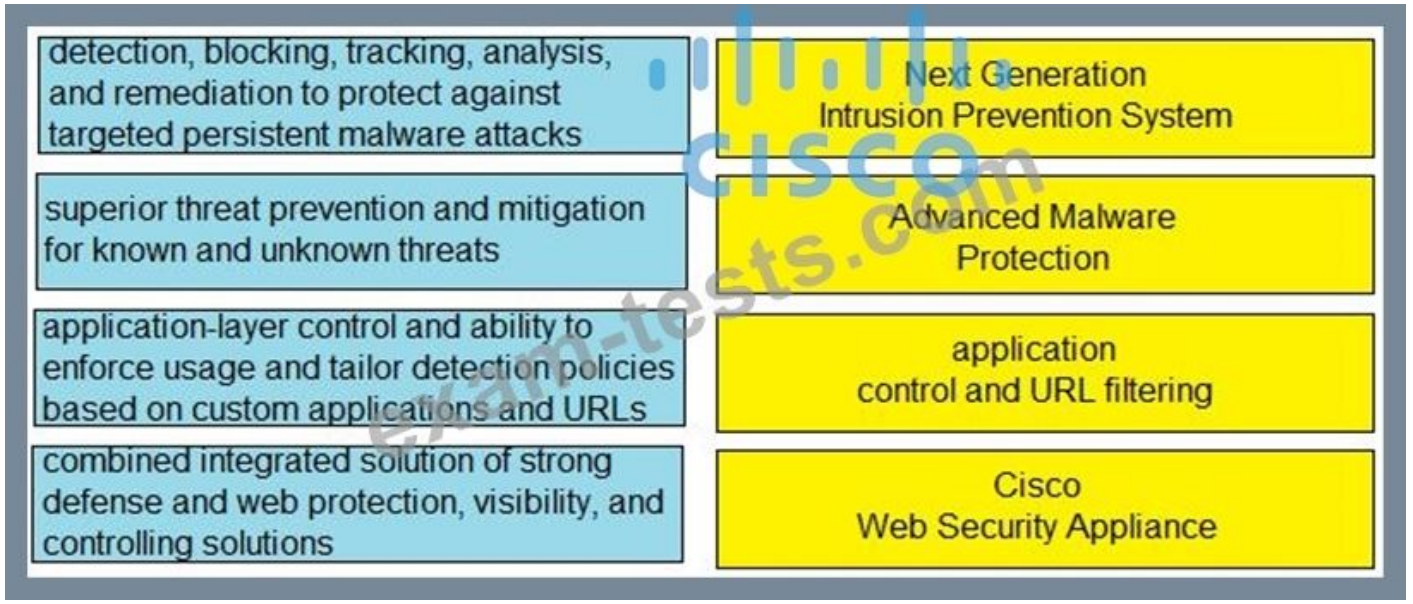
NEW QUESTION: 183
What does Cisco AMP for Endpoints use to help an organization detect different families of malware?
A. Ethos Engine to perform fuzzy fingerprinting
B. Tetra Engine to detect malware when me endpoint is connected to the cloud
C. Clam AV Engine to perform email scanning
D. Spero Engine with machine learning to perform dynamic analysis
Answer: (SHOW ANSWER)
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.
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:
ETHOS = Fuzzy Fingerprinting using static/passive heuristics
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.
ETHOS = Fuzzy Fingerprinting using static/passive heuristics

NEW QUESTION: 184
Which endpoint solution protects a user from a phishing attack?
A. Cisco Identity Services Engine
B. Cisco AnyConnect with ISE Posture module
C. Cisco AnyConnect with Network Access Manager module
D. Cisco AnyConnect with Umbrella Roaming Security module
Answer: D (LEAVE A REPLY)
Cisco AnyConnect with Umbrella Roaming Security module protects a user from a phishing attack by enforcing security at the DNS layer and blocking malicious domains that are used for phishing campaigns. The Umbrella Roaming Security module integrates with the Cisco AnyConnect client and provides always-on security even when no VPN is active. The Umbrella Roaming Security module can replace the existing Cisco Umbrella roaming client or be part of a new AnyConnect deployment12.

Cisco Identity Services Engine (ISE) is not an endpoint solution, but a network access control and policy enforcement platform that can integrate with AnyConnect for posture assessment and compliance3. Cisco AnyConnect with ISE Posture module is used to check the compliance status of the endpoint device and apply the appropriate network access policy based on the posture result4. Cisco AnyConnect with Network Access Manager module is used to manage the network connections and profiles of the endpoint device and support various authentication methods5. Neither of these modules directly protect the user from a phishing attack.
References :=
* Roaming Client: Umbrella Roaming Security (Integration with AnyConnect)
* Secure Umbrella Roaming: Cisco Secure Client (Formerly AnyConnect)
* Cisco Identity Services Engine
* [Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.9 - Posture Module]
* [Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.9 - Network Access Manager Module]

NEW QUESTION: 185
An engineer needs to detect and quarantine a file named abc424400664 zip based on the MD5 signature of the file using the Outbreak Control list feature within Cisco Advanced Malware Protection (AMP) for Endpoints The configured detection method must work on files of unknown disposition Which Outbreak Control list must be configured to provide this?
A. Blocked Application
B. Simple Custom Detection
C. Advanced Custom Detection
D. Android Custom Detection
Answer: B (LEAVE A REPLY)
Simple Custom Detection is a feature of Cisco AMP for Endpoints that allows administrators to block specific files based on their SHA-256 or MD5 hashes. This feature can be used to detect and quarantine files of unknown disposition, such as abc424400664.zip, by adding their hashes to a custom list in the AMP portal.
The list can then be applied to a policy that is assigned to the endpoints. Simple Custom Detection works on files of any type, size, or platform, unlike the other options that are either platform-specific (Android Custom Detection), size-limited (Blocked Application), or signature-based (Advanced Custom Detection). References: 1, 2, 3

NEW QUESTION: 186
Drag and drop the capabilities from the left onto the correct technologies on the right.



Answer:

NEW QUESTION: 187

An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA.

Which Cisco ASA command must be used?

A. flow exporter <name>

B. ip flow monitor<name> input

C. flow-export destination inside 1.1.1.1 2055

D. ip flow-export destination 1.1.1.1 2055

Answer: (SHOW ANSWER)

NEW QUESTION: 188

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

A. TLSv1.1

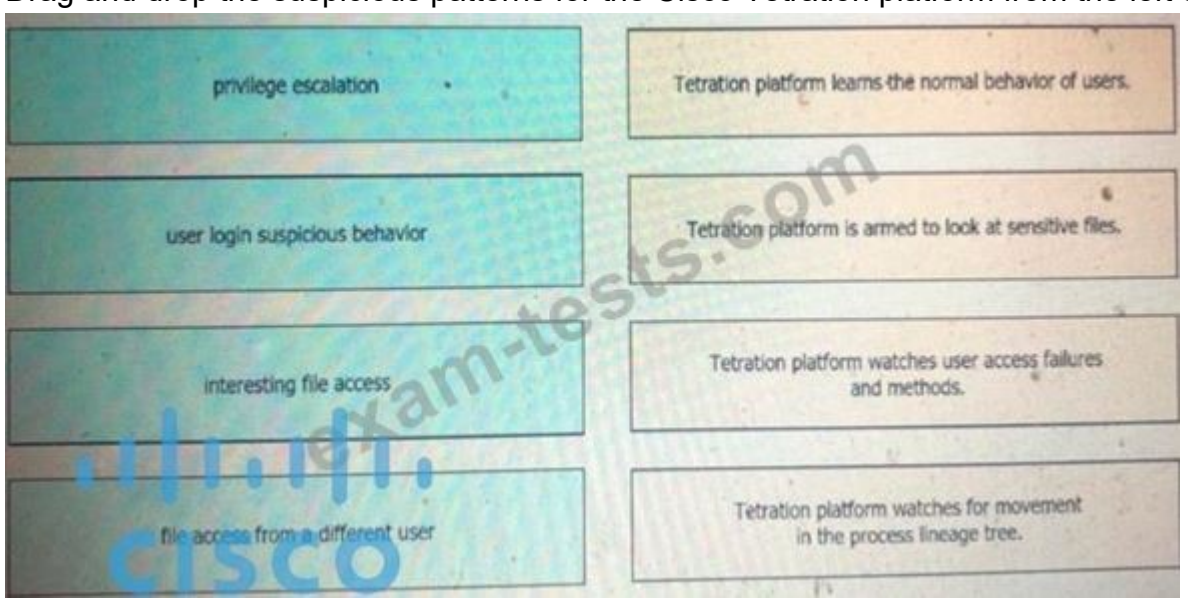
B. TLSvl

C. DTLSv1

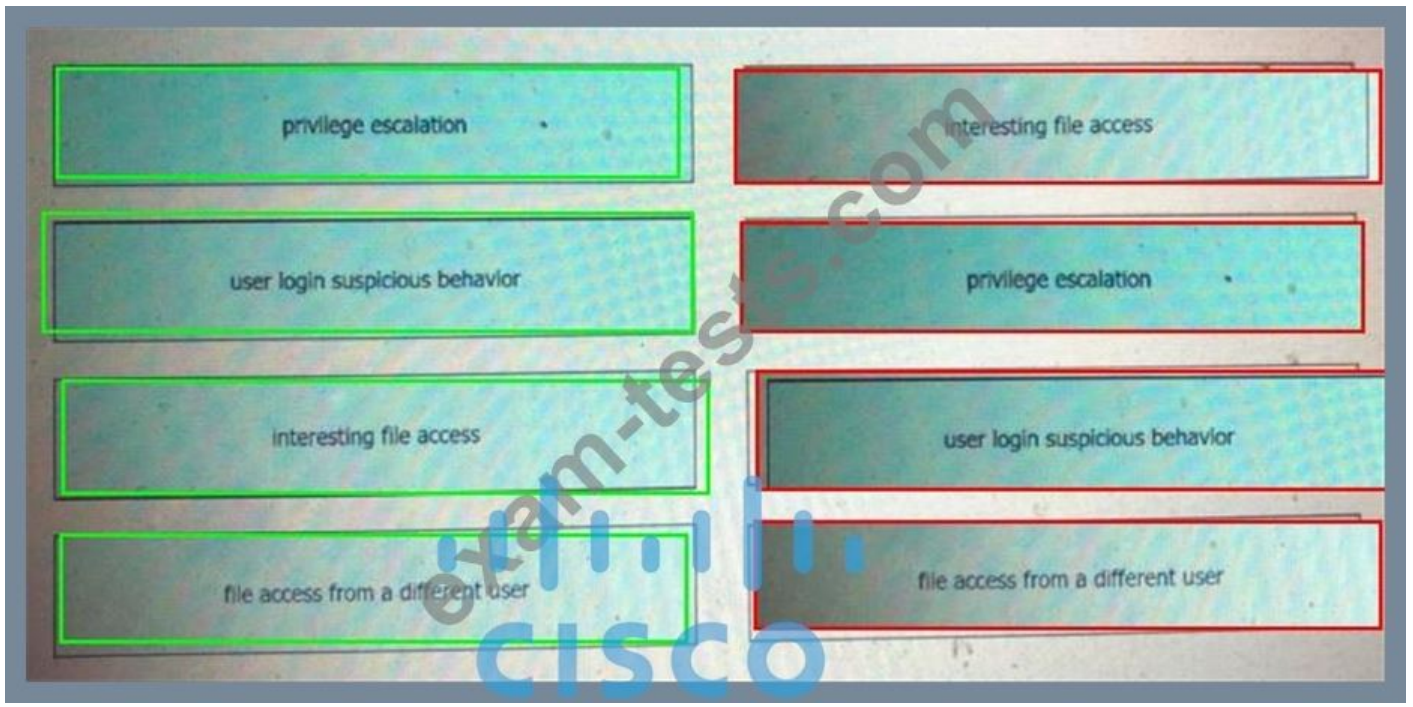
D. TLSv1.2
Answer: C (LEAVE A REPLY)

NEW QUESTION: 189
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: C (LEAVE A REPLY)
The best way to prevent the session during the initial TCP communication is to configure policies to stop and reject communication from the known malicious domain. This will prevent the ESA from accepting any messages from that domain and send a negative SMTP response code back to the sender. This will also save the ESA's resources and bandwidth, as it will not have to process or store the malicious emails. This can be done by creating a sender group in the Host Access Table (HAT) that matches the malicious domain and setting the mail flow policy to "Reject" or "Throttle". Alternatively, a message filter can be created that checks the envelope sender against the malicious domain and applies the "stop_connection" or "reject_connection" action12.
The other options are not as effective as stopping and rejecting the communication at the TCP level.
Configuring the Cisco ESA to drop the malicious emails (option A) will still allow the ESA to accept the messages and then silently discard them, which will consume the ESA's resources and bandwidth, and also not notify the sender of the rejection. Configuring policies to quarantine malicious emails (option B) will also require the ESA to accept and store the messages, which will take up disk space and require manual or automated management of the quarantine. Configuring the Cisco ESA to reset the TCP connection (option D) will abruptly terminate the connection without sending a proper SMTP response code, which may cause the sender to retry the delivery and generate more traffic. Resetting the TCP connection is also considered a less polite and less compliant way of rejecting messages than sending a negative SMTP response code34. References: 1: How to Block a Sender Domain on the Email Security Appliance 2: Message Filters on the Cisco Email Security Appliance 3: How to Configure the Cisco Email Security Appliance to Reject or Drop Messages 4: Cisco Email Security Appliance User Guide - Configuring Mail Policies

NEW QUESTION: 190
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.



Answer:



NEW QUESTION: 191
A Cisco ESA administrator has been tasked with configuring the Cisco ESA to ensure there are no viruses before quarantined emails are delivered. In addition, delivery of mail from known bad mail servers must be prevented. Which two actions must be taken in order to meet these requirements? (Choose two)
A. Use outbreak filters from SenderBase
B. Enable a message tracking service
C. Configure a recipient access table
D. Deploy the Cisco ESA in the DMZ
E. Scan quarantined emails using AntiVirus signatures
Answer: (SHOW ANSWER)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Ad Therefore Outbreak filters can be used to block emails from bad mail servers.Web servers and email gateways are generally located in the DMZ soNote: 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: 192
Which RADIUS attribute can you use to filter MAB requests in an 802.1 x deployment?
A. 1
B. 2
C. 6
D. 31
Answer: (SHOW ANSWER)
Because MAB uses the MAC address as a username and password, you should make sure that the RADIUS server can differentiate MAB requests from other types of requests for network access. This precaution will prevent other clients from attempting to use a MAC address as a valid credential. Cisco

switches uniquely identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB Access-Request message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server.

NEW QUESTION: 193
What is the purpose of the Cisco Endpoint IoC feature?
A. It is an incident response tool.
B. It provides stealth threat prevention.
C. It is a signature-based engine.
D. It provides precompromise detection.
Answer: A (LEAVE A REPLY)
Reference: https://docs.amp.cisco.com/Cisco%20Endpoint%20IOC%20Attributes.pdf The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

NEW QUESTION: 194
What is a difference between Cisco AMP for Endpoints and Cisco Umbrella?
A. Cisco AMP for Endpoints prevents, detects, and responds to attacks before and against Internet threats.
B. Cisco AMP for Endpoints automatically researches indicators of compromise ..
C. Cisco AMP for Endpoints prevents connections to malicious destinations, and C malware.
D. Cisco AMP for Endpoints is a cloud-based service, and Cisco Umbrella is not.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 195
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:
ETHOS = Fuzzy Fingerprinting using static/passive heuristics

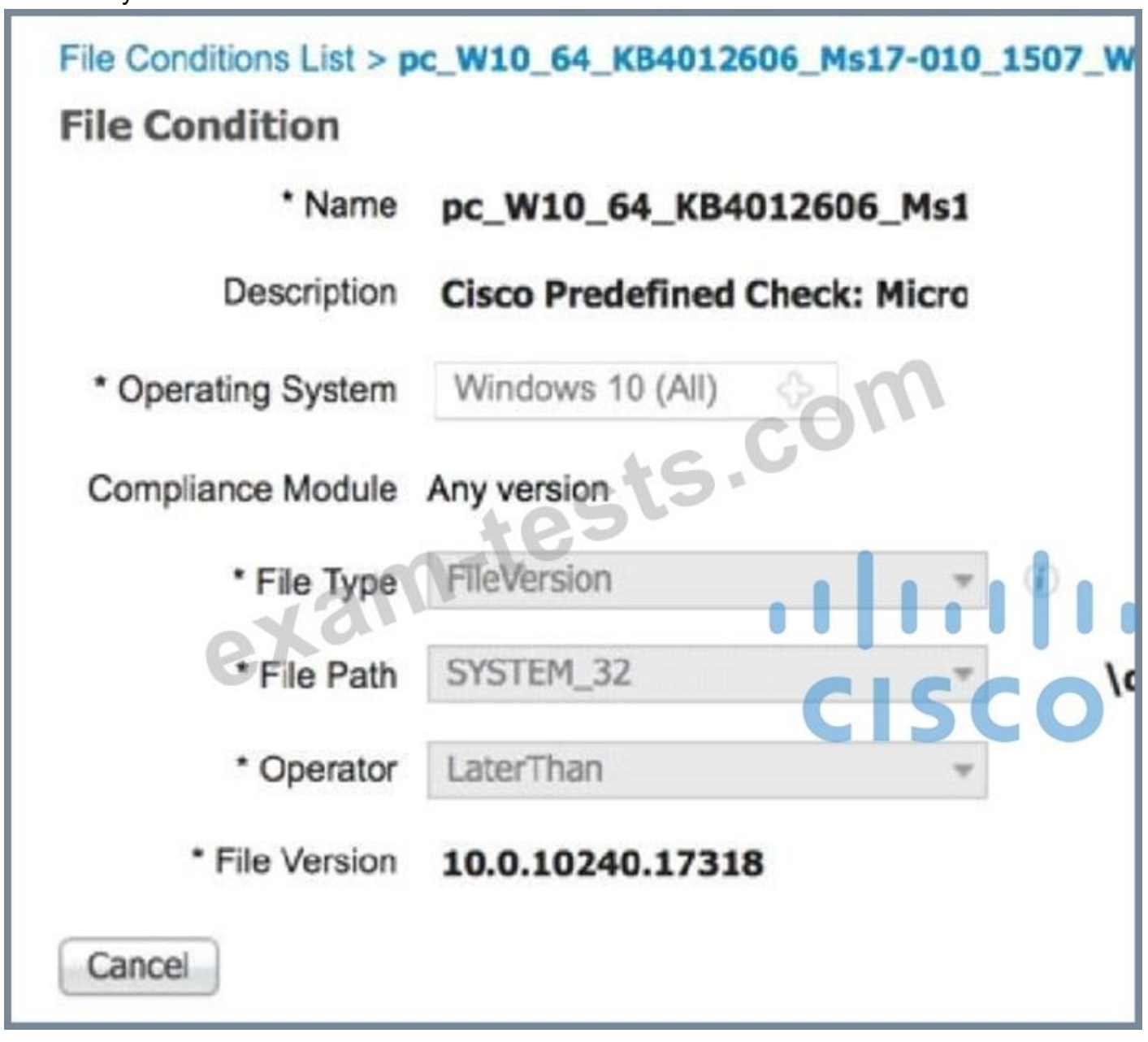
NEW QUESTION: 196
What is the intent of a basic SYN flood attack?
A. to solicit DNS responses
B. to exceed the threshold limit of the connection queue
C. to flush the register stack to re-initiate the buffers
D. to cause the buffer to overflow
Answer: B (LEAVE A REPLY)

A basic SYN flood attack is a type of denial-of-service (DoS) attack that aims to exhaust the resources of a server by sending a large number of SYN packets and not completing the TCP three-way handshake. The intent of this attack is to exceed the threshold limit of the connection queue, which is the data structure that stores the information about the pending connections. By doing so, the attacker prevents legitimate clients from establishing connections with the server, as the server cannot accept any more SYN requests. A SYN flood attack can be performed with spoofed IP addresses or without IP spoofing, depending on the attacker's strategy and the server's configuration. References: [Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 3: Securing Networks with Firewalls, Lesson 3.2: Firewall Technologies,

NEW QUESTION: 197
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)
Explanation Explanation 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: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mtbook/sec-pki-overview.html Explanation 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) Explanation Explanation 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: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mtbook/sec-pki-overview.html

NEW QUESTION: 198
An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch was not installed, which left the endpoint vulnerable to WannaCry ransomware. Which two solutions mitigate the risk of this ransom ware infection? (Choose two)
A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.
B. Set up a profiling policy in Cisco Identity Service Engine to check and endpoint patch level before allowing access on the network.

C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.
D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.
E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.
Answer: (SHOW ANSWER)
A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. We can configure ISE to check for the Windows patch at Work Centers > Posture > Posture Elements > Conditions > File.
In this example, we are going to use the predefined file check to ensure that our Windows 10 clients have the critical security patch installed to prevent the Wanna Cry malware.

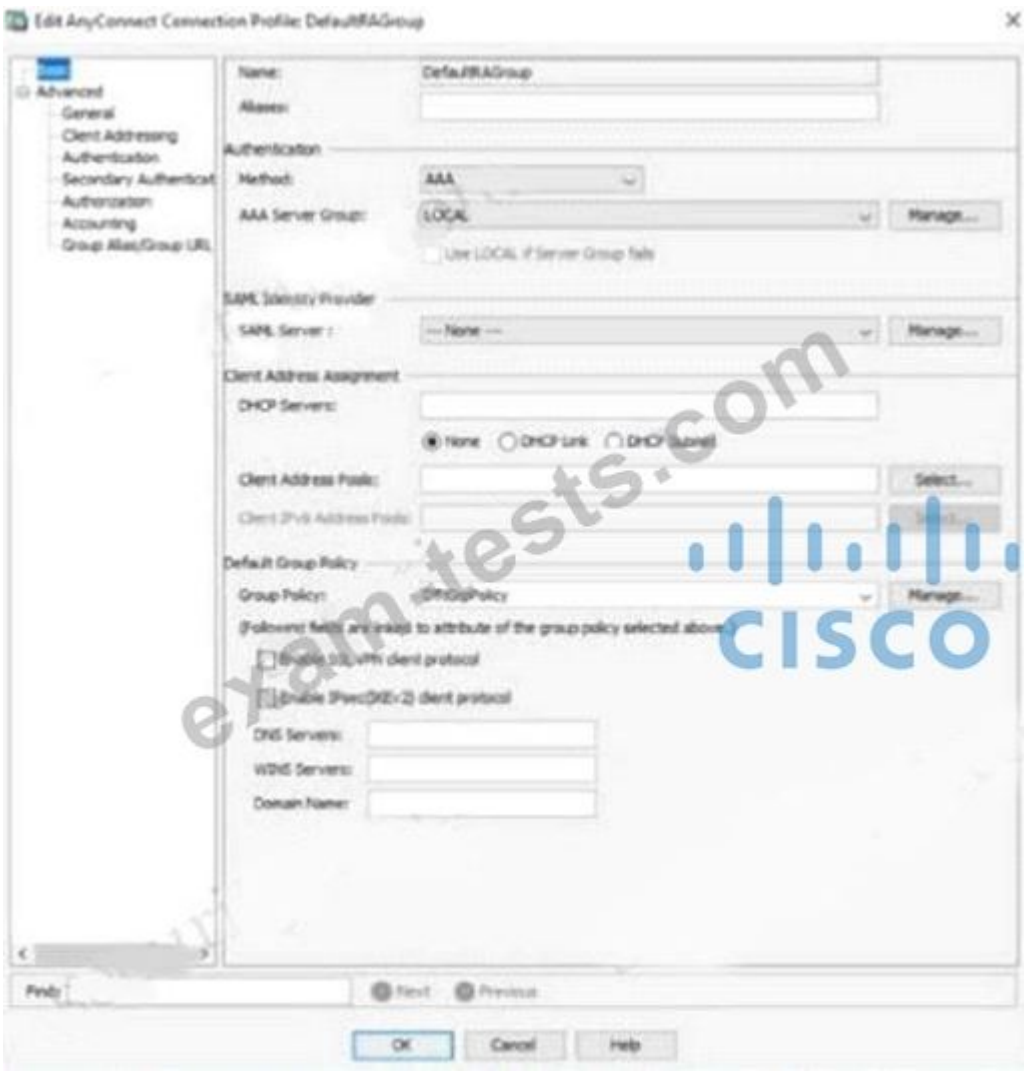


NEW QUESTION: 199
An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users.
A. Upload the organization root CA to the Umbrella admin portal
B. Modify the user's browser settings to suppress errors from Umbrella.
C. 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: 200
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: 201
Refer to the exhibit.



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

A. Group Policy

B. Method

C. SAML Server

D. DHCP Servers

Answer: (SHOW ANSWER)

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

NEW QUESTION: 202

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. 10

C. 5

D. 3

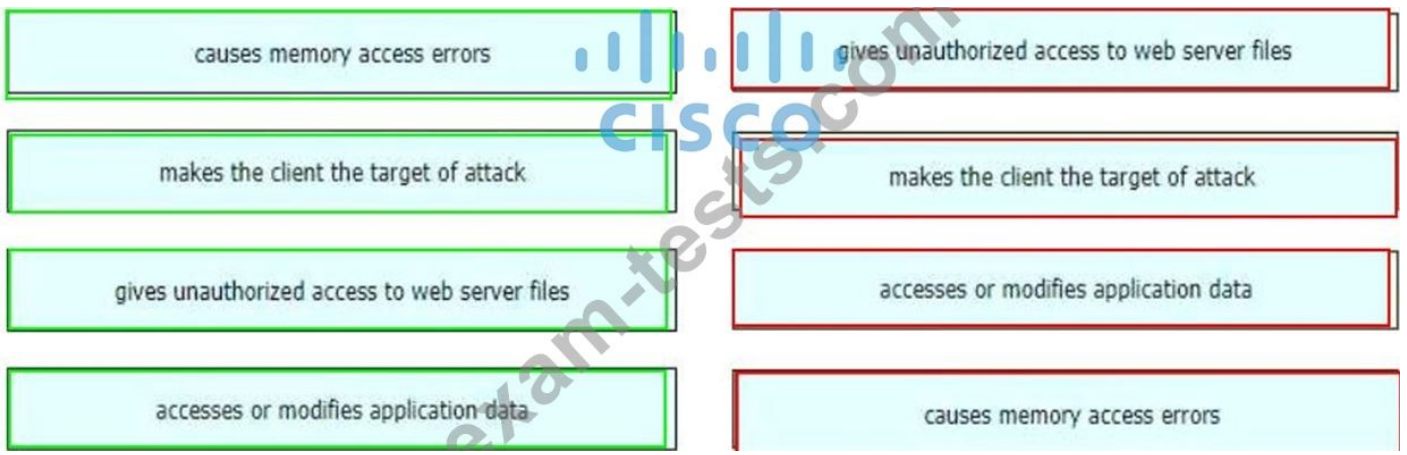
Answer: (SHOW ANSWER)

https://www.cisco.com/c/en/us/td/docs/security/esa/esa111/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_01111.html

NEW QUESTION: 203

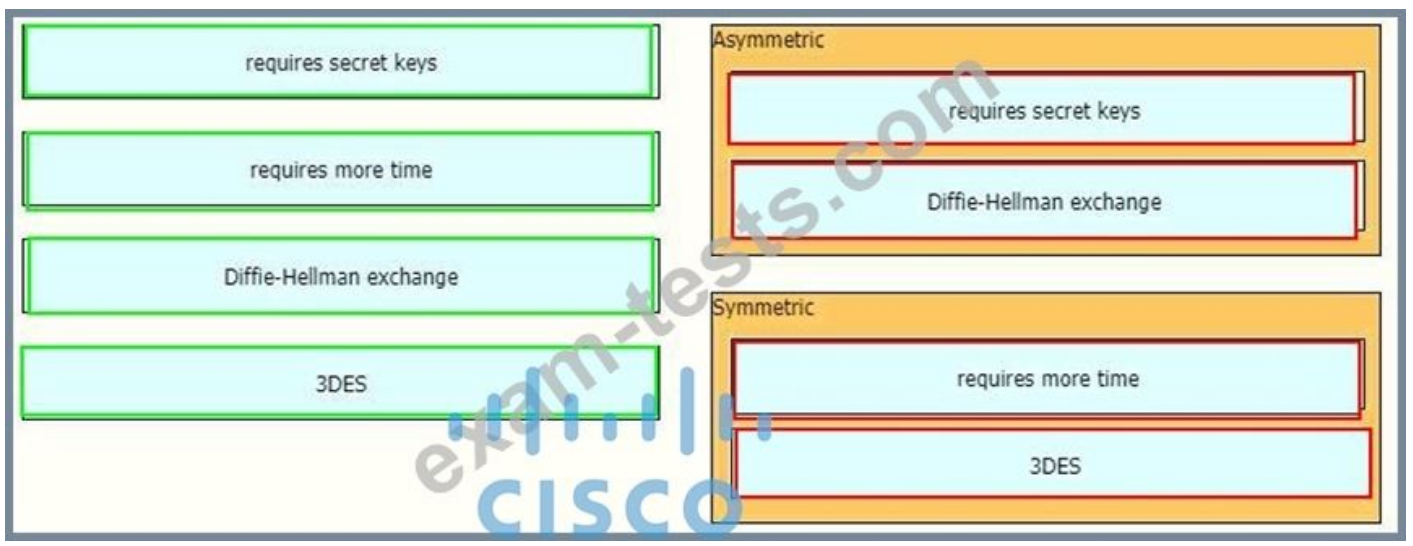
Drag and drop the exploits from the left onto the type of security vulnerability on the right.

Answer:



NEW QUESTION: 204
Drag and drop the descriptions from the left onto the encryption algorithms on the right.

Answer:



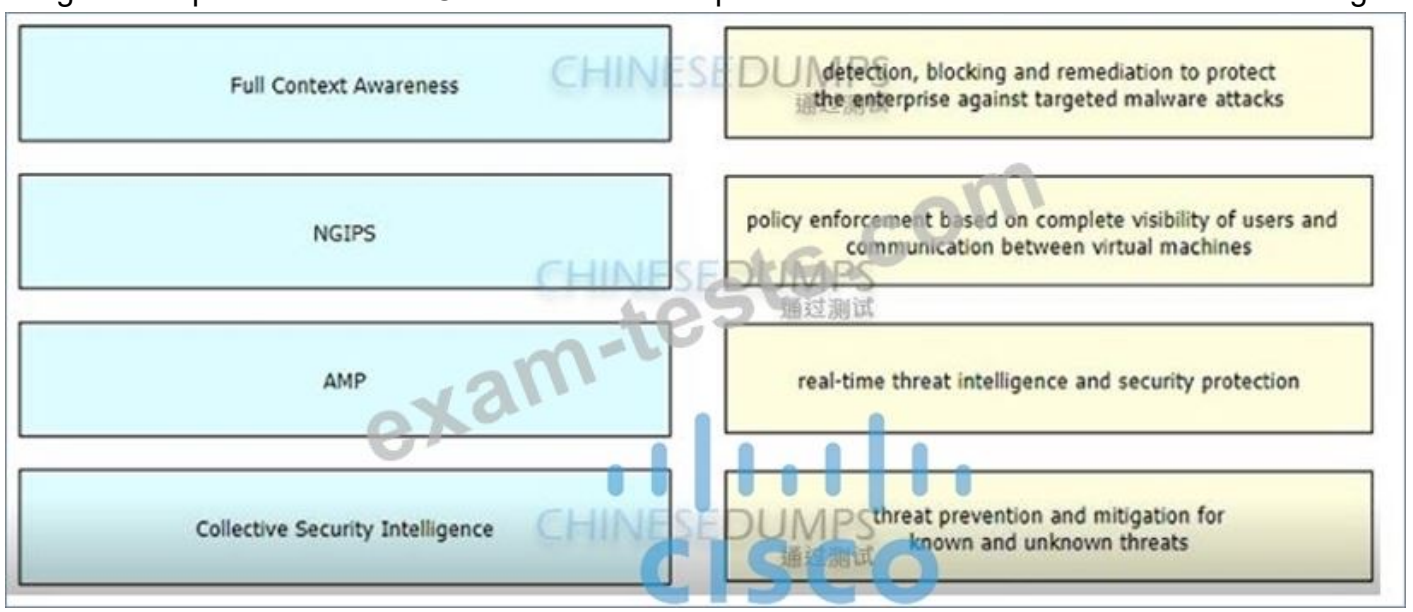
NEW QUESTION: 205
Which Cisco DNA Center RESTful PNP API adds and claims a device into a workflow?
A. api/v1/onboarding/pnp-device/import
B. api/v1/onboarding/pnp-device
C. api/v1/onboarding/workflow
D. api/v1/fie/config
Answer: A (LEAVE A REPLY)

NEW QUESTION: 206
Based on the NIST 800-145 guide, which cloud architecture may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises?
A. hybrid cloud
B. private cloud
C. public cloud
D. community cloud
Answer: D (LEAVE A REPLY)

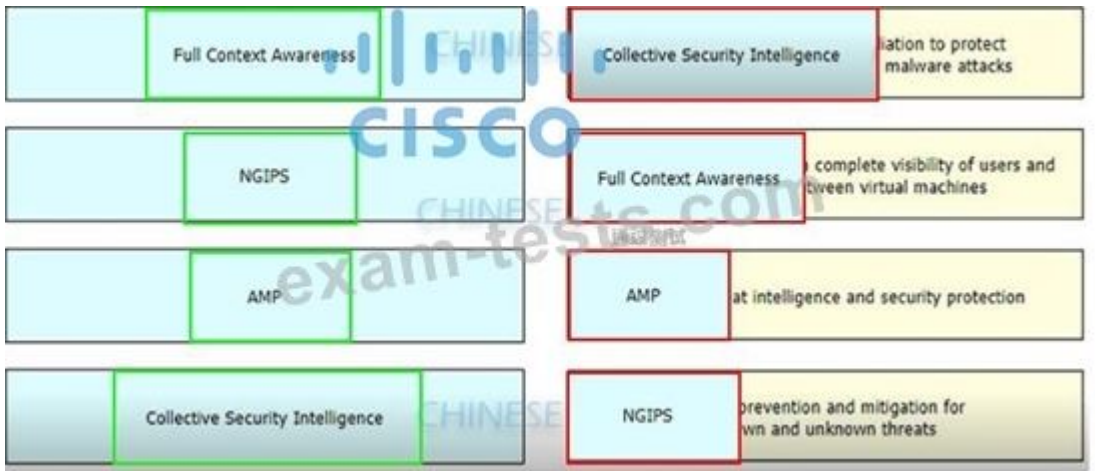
According to the NIST 800-145 guide1, a community cloud is a cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. A community cloud is different from a hybrid cloud, which is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). A private cloud is a cloud infrastructure that is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. A public cloud is a cloud infrastructure that is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. References := Some possible references are:
1: NIST SP 800-145, The NIST Definition of Cloud Computing, 1 2: Evaluation of Cloud Computing Services Based on NIST SP 800-145, 3 3: What Is Community Cloud? Definition, Architecture, Examples, and Best Practices, 6

NEW QUESTION: 207
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)
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/esa-content-filters.pdf

NEW QUESTION: 208
Drag and drop the features of Cisco ASA with Firepower from the left onto the benefits on the right.



Answer:



NEW QUESTION: 209
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: 210
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: (SHOW ANSWER)
This command uses RADIUS which combines authentication and authorization in one function (packet).

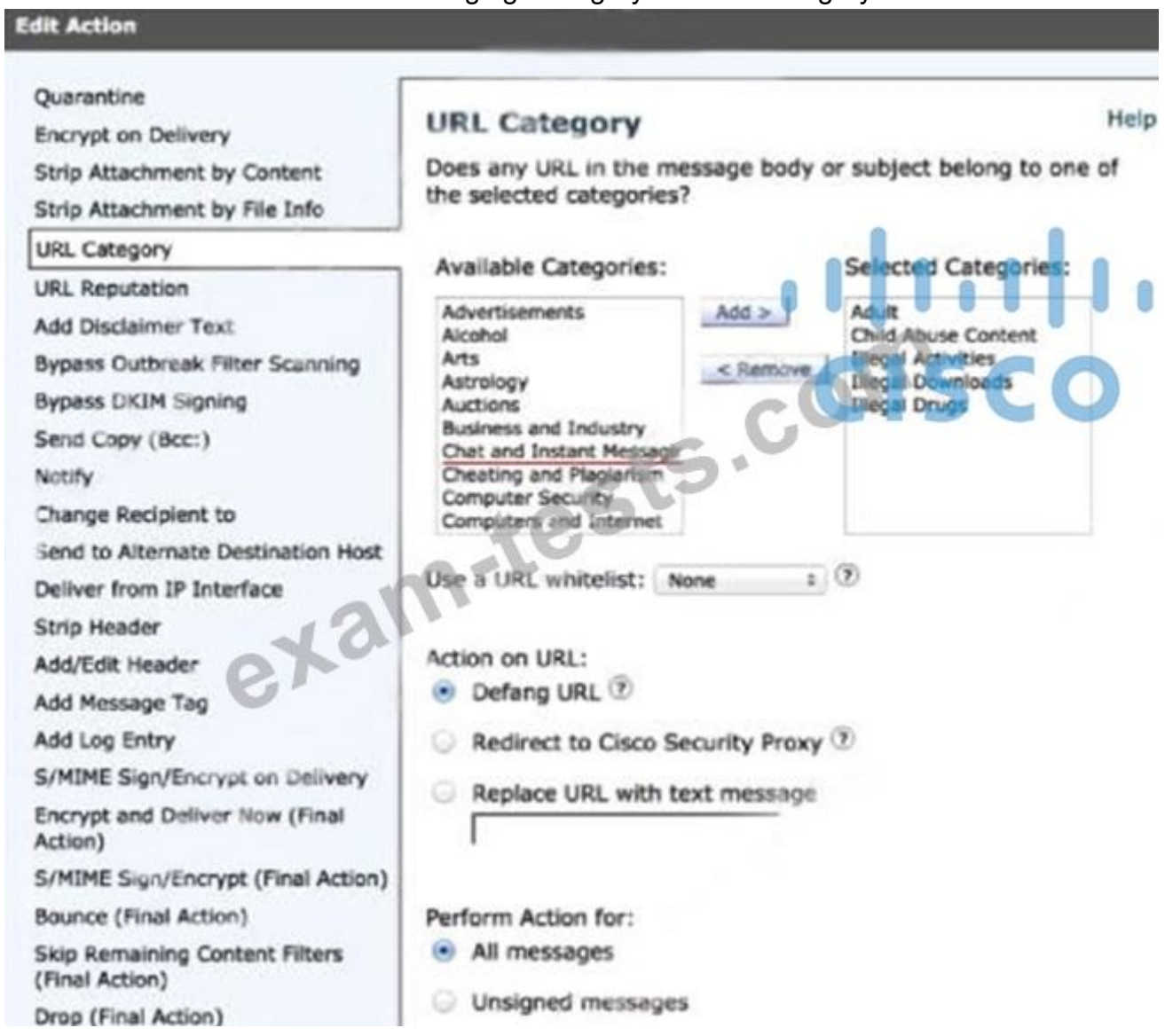
NEW QUESTION: 211
Refer to the exhibit.

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

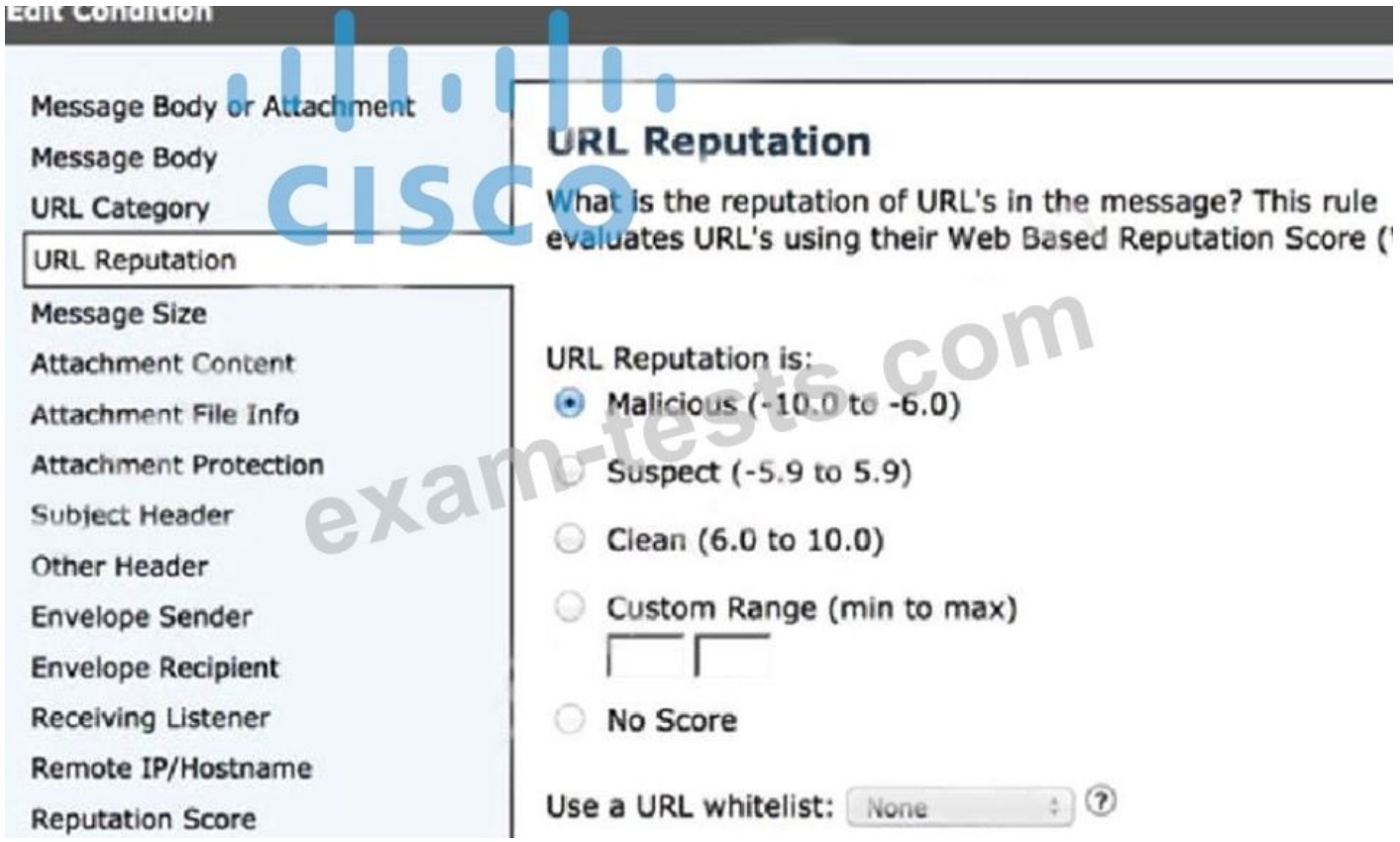
Which statement about the authentication protocol used in the configuration is true?
A. The authentication request contains only a password
B. The authentication request contains only a username
C. The authentication and authorization requests are grouped in a single packet
D. There are separate authentication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

NEW QUESTION: 212
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: 213
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. confidentiality factor
B. biometric factor
C. knowledge factor
D. encryption factor
E. time factor
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 214
Refer to the exhibit.

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

A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced
What is the cause of this issue?
A. The key was configured in plain text.
B. NTP authentication is not enabled.
C. The router was not rebooted after the NTP configuration updated.

D. The hashing algorithm that was used was MD5. which is unsupported.
Answer: (SHOW ANSWER)

NEW QUESTION: 215
A company identified a phishing vulnerability during a pentest What are two ways the company can protect employees from the attack? (Choose two.)
A. using Cisco ESA
B. using Cisco Umbrella
C. using an inline IPS/IDS in the network
D. using Cisco FTD
E. using Cisco ISE
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 216
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: 217
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)
Explanation Explanation 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
Explanation 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:
Explanation Explanation 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: 218
Which feature requires that network telemetry be enabled?
A. central syslog system
B. Layer 2 device discovery
C. per-interface stats
D. SNMP trap notification
Answer: A (LEAVE A REPLY)

NEW QUESTION: 219
What are two workload security models? (Choose two.)
A. SaaS
B. PaaS
C. off-premises
D. on-premises
E. IaaS
Answer: C,D (LEAVE A REPLY)
Workload security models refer to the ways of protecting applications, services, and capabilities that run on a cloud resource. There are different types of cloud deployment models, such as public, private, hybrid, and multicloud, and different types of cloud service models, such as IaaS, PaaS, and SaaS. However, these are not workload security models, but rather ways of describing the cloud environment and the level of abstraction.
Workload security models are more focused on the location and ownership of the workloads, and how they are secured. The two main workload security models are off-premises and on-premises. Off-premises workload security model means that the workloads are hosted and managed by a third-party cloud service provider, such as AWS, Azure, or GCP. The cloud service provider is responsible for the security of the underlying infrastructure, such as the physical servers, network devices, storage systems, and hypervisors. The customer is responsible for the security of the workloads themselves, such as the

guest operating systems, applications, data, and users. The customer can use various tools and techniques to secure their workloads, such as encryption, firewalls, identity and access management, vulnerability scanning, and logging and monitoring.
On-premises workload security model means that the workloads are hosted and managed by the customer on their own data center or private cloud. The customer is responsible for the security of both the infrastructure and the workloads, and has full control and visibility over them. The customer can use similar tools and techniques as the off-premises model, but also has to deal with the physical security, network security, and compliance requirements of their own environment. References:
* What Is Workload Security? On-Premises, Cloud, Kubernetes, and More
* What is Cloud Workload Security? - CyberArk
* What is Cloud Workload Protection? | Workload Security | VMware
* What is Cloud Workload Security? - Check Point Software
* Introduction To Classic Security Models - GeeksforGeeks

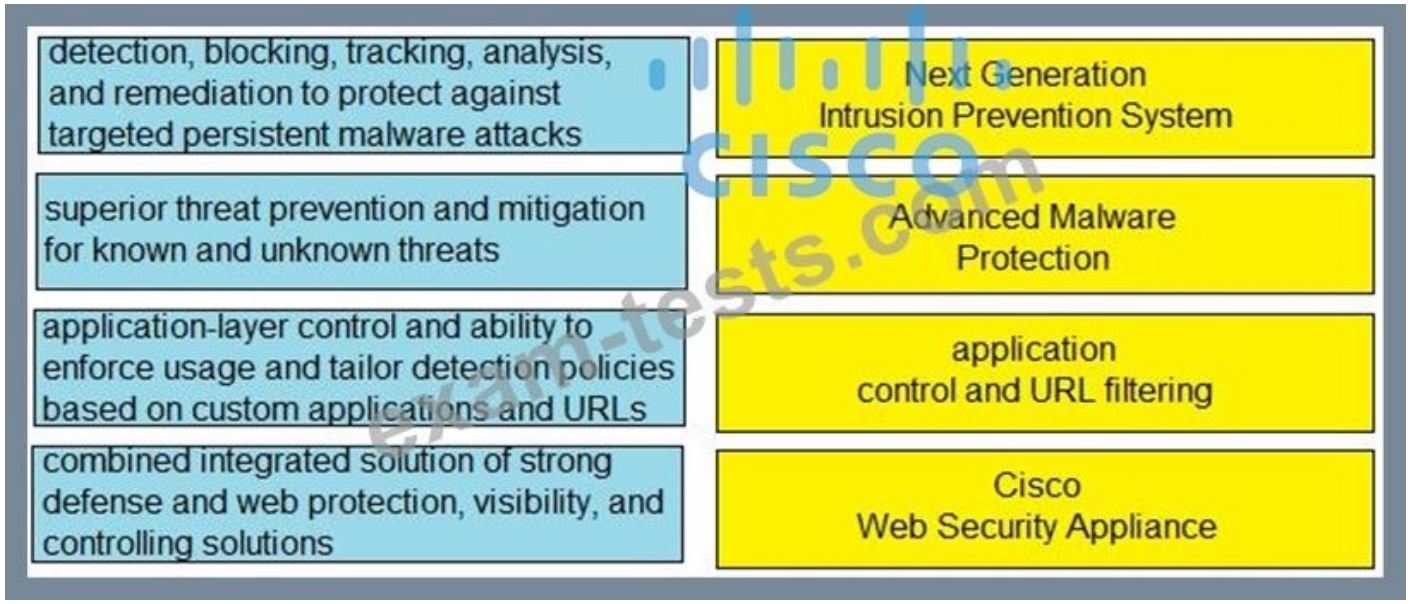
NEW QUESTION: 220

Refer to the exhibit. Which command was used to display this output?
A. show dot1x all
B. show dot1x
C. show dot1x all summary
D. show dot1x interface gi1/0/12
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec- user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

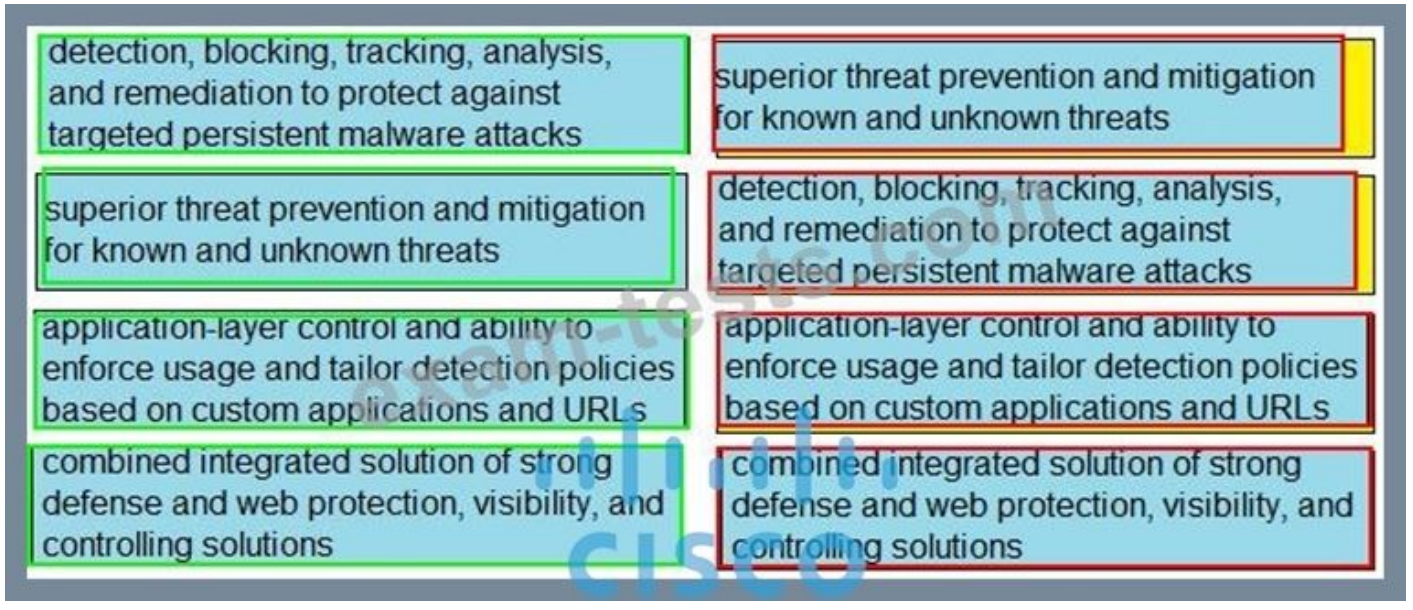
NEW QUESTION: 221
What is the benefit of integrating Cisco ISE with a MDM solution?
A. It provides compliance checks for access to the network
B. It provides the ability to update other applications on the mobile device
C. It provides the ability to add applications to the mobile device through Cisco ISE
D. It provides network device administration access
Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 222
Drag and drop the capabilities from the left onto the correct technologies on the right.

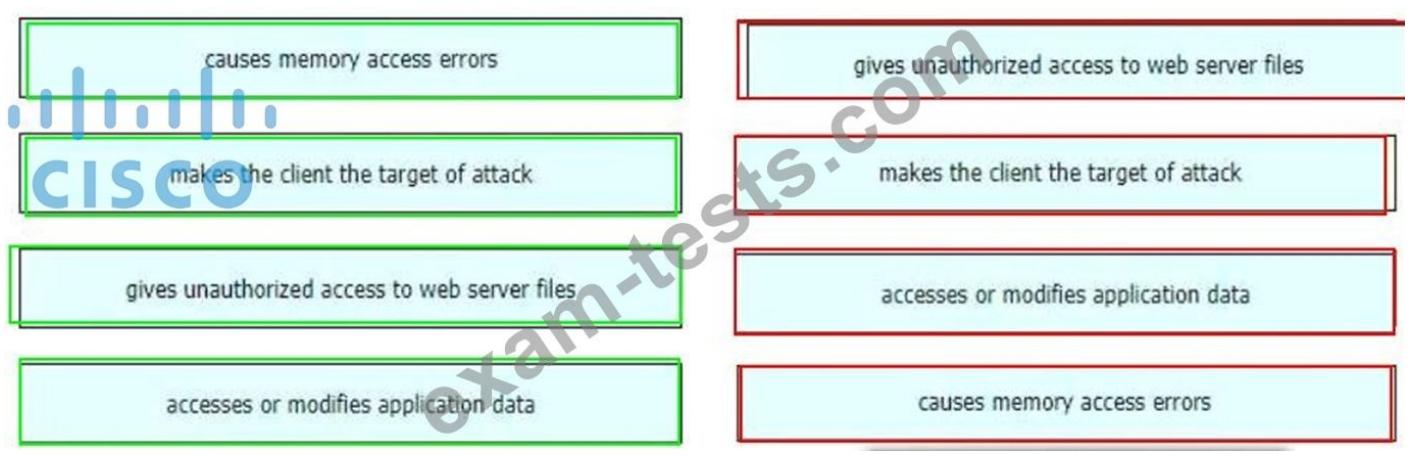


Answer:



NEW QUESTION: 223
Drag and drop the exploits from the left onto the type of security vulnerability on the right.

Answer:



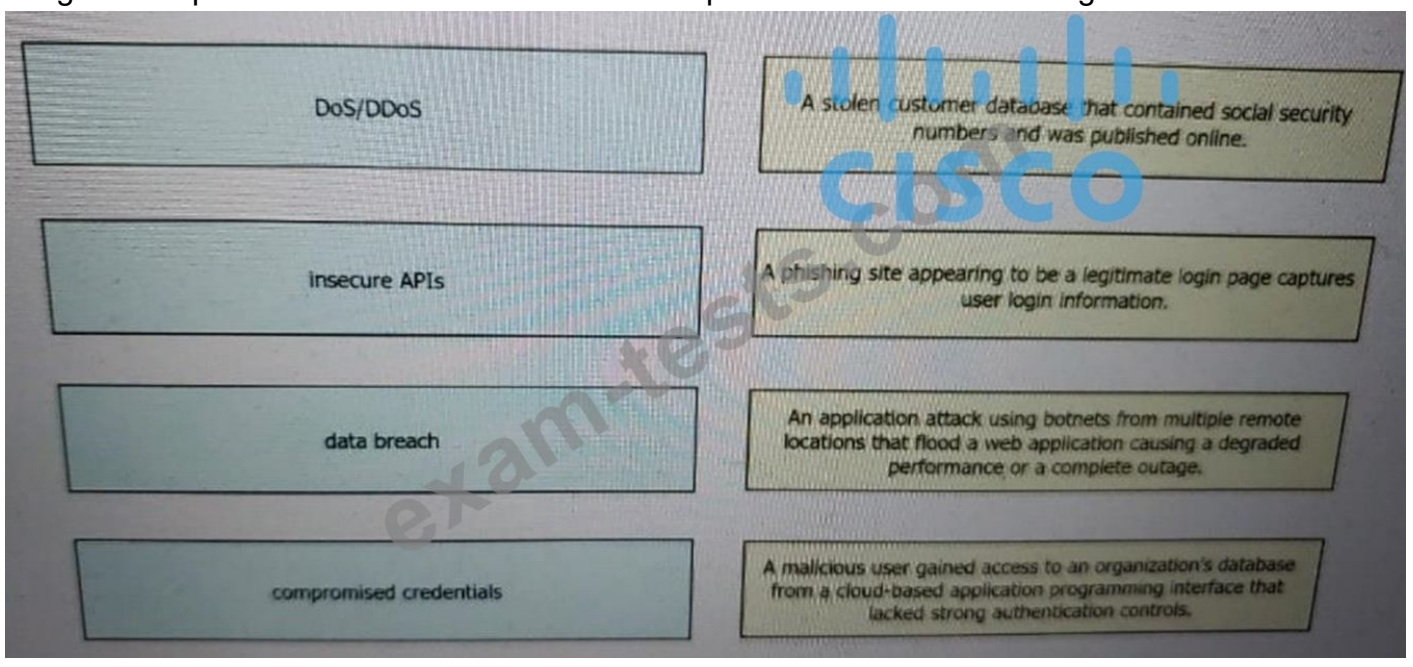
NEW QUESTION: 224
Which parameter is required when configuring a Netflow exporter on a Cisco Router?
A. DSCP value
B. Source interface
C. Exporter name
D. Exporter description
Answer: C (LEAVE A REPLY)
ExplanationAn example of configuring a NetFlow exporter is shown below:flow exporter Exporterdestination 192.168.100.22transport udp 2055

NEW QUESTION: 225
An engineer needs behavioral analysis to detect malicious activity on the hosts, and is configuring the organization's public cloud to send telemetry using the cloud provider's mechanisms to a security device. Which mechanism should the engineer configure to accomplish this goal?
A. Flow
B. NetFlow
C. mirror port
D. VPC flow logs
Answer: B (LEAVE A REPLY)

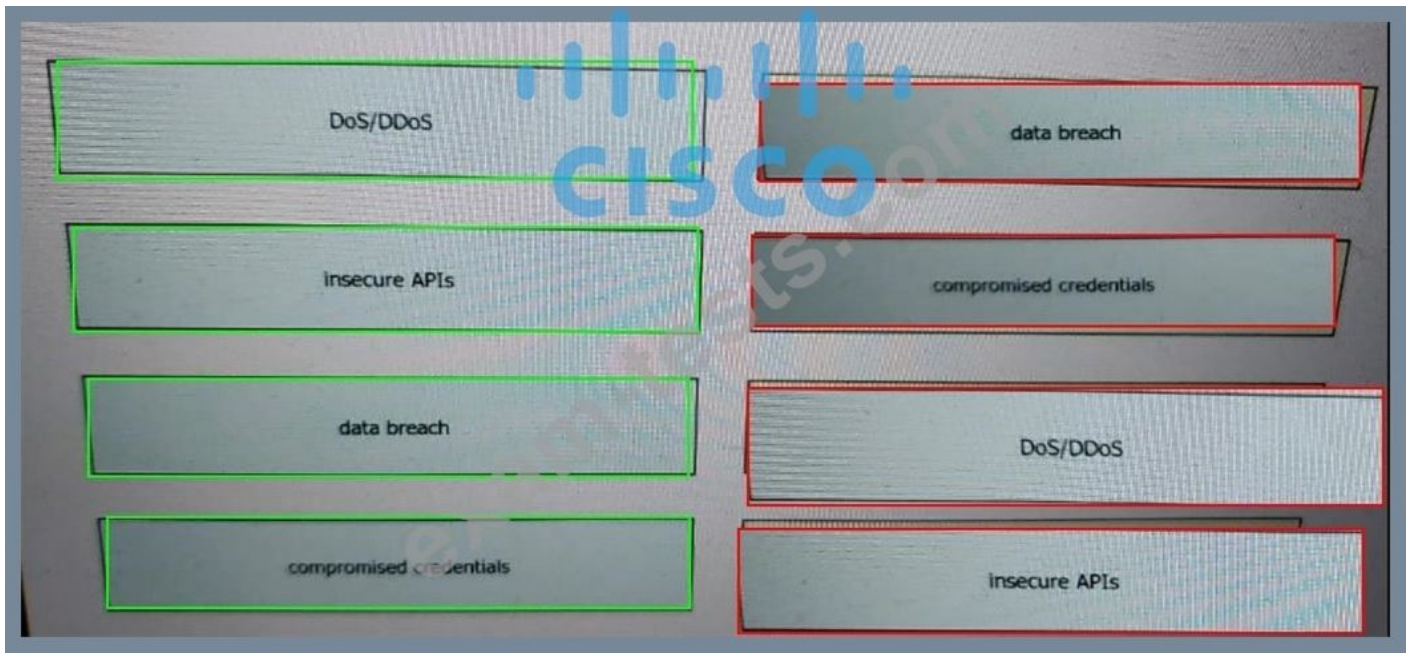
NEW QUESTION: 226

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 without validation.
B. It forwards the packet after validation by using the MAC Binding Table.
C. It drops the packet without validation.
D. It drops the packet after validation by using the IP & MAC Binding Table.
Answer: (SHOW ANSWER)

NEW QUESTION: 227
Drag and drop the threats from the left onto examples of that threat on the right



Answer:



NEW QUESTION: 228
Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?
A. PaaS
B. XaaS
C. IaaS
D. SaaS
Answer: (SHOW ANSWER)
Explanation
Cloud computing can be broken into the following three basic models:
+ Infrastructure as a Service (IaaS): IaaS describes a cloud solution where you are renting infrastructure. You purchase virtual power to execute your software as needed. This is much like running a virtual server on your own equipment, except you are now running a virtual server on a virtual disk. This model is similar to a utility company model because you pay for what you use.
+ Platform as a Service (PaaS): PaaS provides everything except applications. Services provided by this model include all phases of the system development life cycle (SDLC) and can use application programming interfaces (APIs), website portals, or gateway software. These solutions tend to be proprietary, which can cause problems if the customer moves away from the provider's platform.
+ Software as a Service (SaaS): SaaS is designed to provide a complete packaged solution. The software is rented out to the user. The service is usually provided through some type of front end or web portal. While the end user is free to use the service from anywhere, the company pays a peruse fee.

NEW QUESTION: 229
Which public cloud provider supports the Cisco Next Generation Firewall Virtual?
A. Google Cloud Platform
B. Red Hat Enterprise Visualization
C. VMware ESXi
D. Amazon Web Services
Answer: D (LEAVE A REPLY)

Reference:

Cisco Firepower NGFWv in Amazon Web Services (AWS) or Microsoft Azure must be managed by a Cisco Firepower Management Center (FMC) residing in AWS or on-premises. The virtual FCM can be deployed on VMware ESXi, on KVM, and in AWS. Figure 1 shows the various FMC dashboards.

NEW QUESTION: 230

Which two behavioral patterns characterize a ping of death attack? (Choose two)

A. The attack is fragmented into groups of 16 octets before transmission.

B. The attack is fragmented into groups of 8 octets before transmission.

C. Short synchronized bursts of traffic are used to disrupt TCP connections.

D. Malformed packets are used to crash systems.

E. Publicly accessible DNS servers are typically used to execute the attack.

Answer: B,D (LEAVE A REPLY)

Ping of Death (PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.

A correctly-formed ping packet is typically 56 bytes in size, or 64 bytes when the ICMP header is considered, and 84 including Internet Protocol version 4 header. However, any IPv4 packet (including pings) may be as large as 65,535 bytes. Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented Like other large but well-formed packets, a ping of death is fragmented into groups of 8 octets before transmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code.

NEW QUESTION: 231

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)

Reference:

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

NEW QUESTION: 232

Which two configurations must be made on Cisco ISE and on Cisco TrustSec devices to force a session to be adjusted after a policy change is made? (Choose two)

A. aaa server radius dynamic-author

B. posture assessment

C. CoA

D. tacacs-server host 10.1.1.250 key password

E. aaa authorization exec default local

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 233

Why is it important for the organization to have an endpoint patching strategy?

A. so the network administrator is notified when an existing bug is encountered

B. so the internal PSIRT organization is aware of the latest bugs

C. so the latest security fixes are installed on the endpoints

D. so the organization can identify endpoint vulnerabilities

Answer: A (LEAVE A REPLY)

NEW QUESTION: 234

What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?

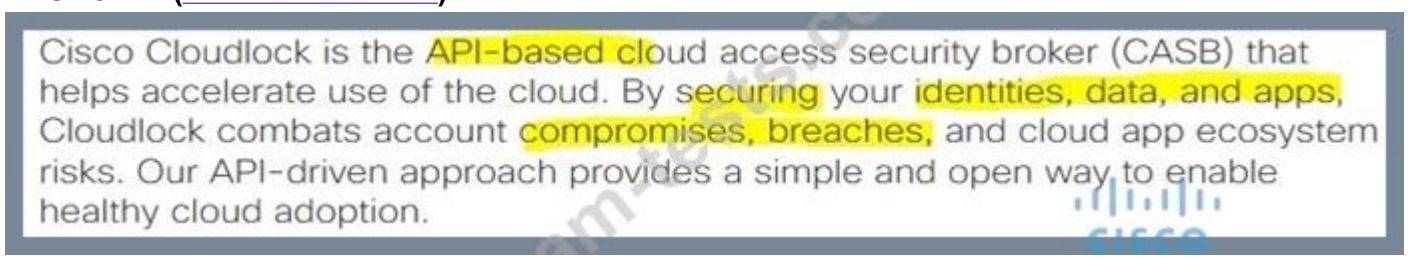
A. Cisco Cloudlock

B. Cisco Umbrella

C. Cisco AMP

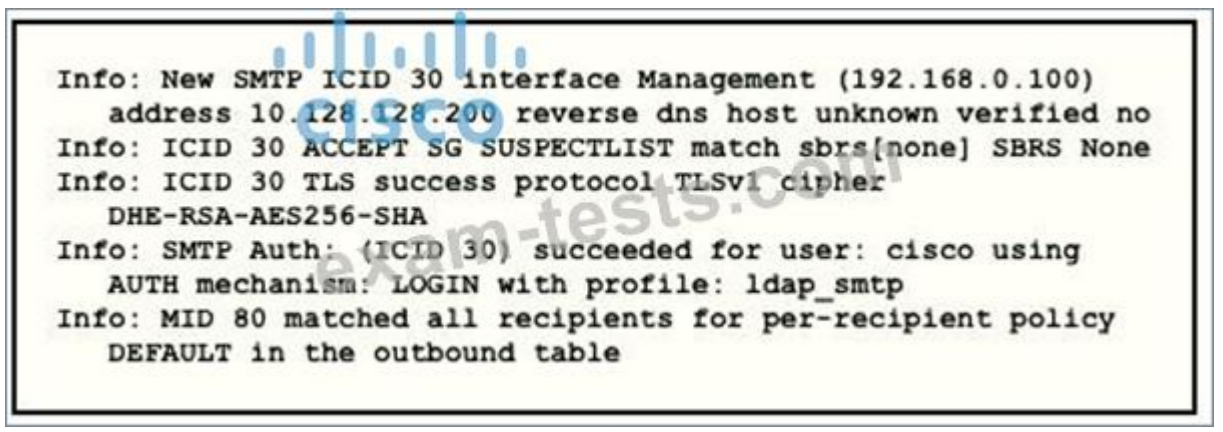
D. Cisco App Dynamics

Answer: A (LEAVE A REPLY)



NEW QUESTION: 235

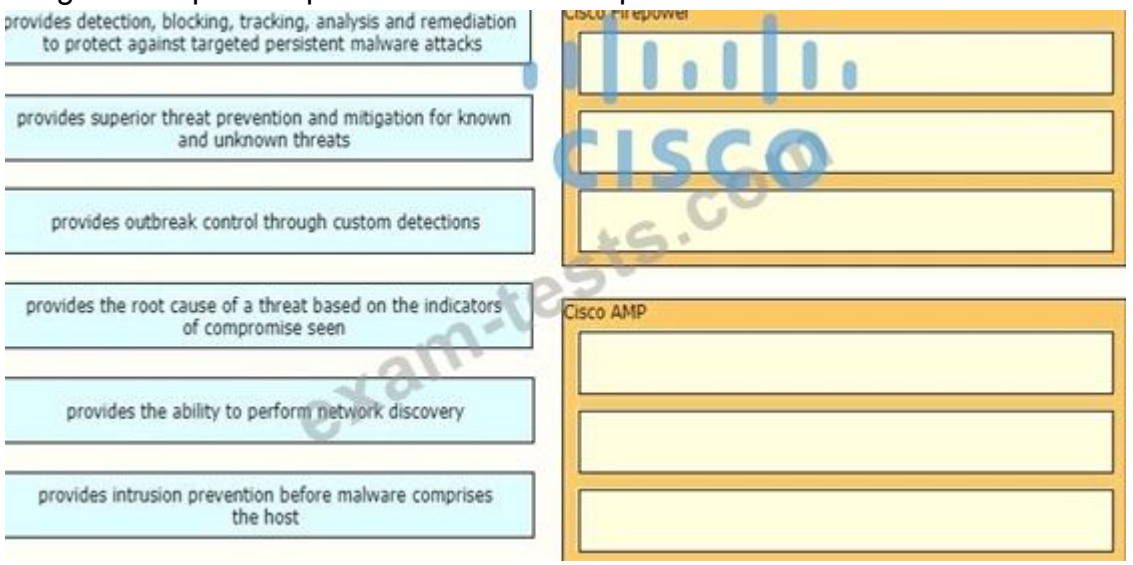
Refer to the exhibit.



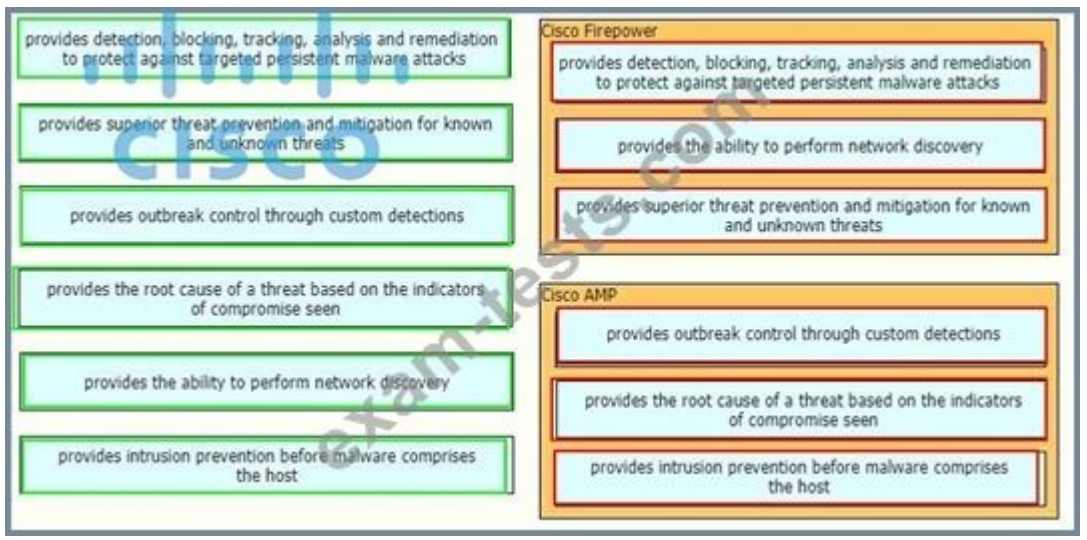
Which type of authentication is in use?
A. LDAP authentication for Microsoft Outlook
B. POP3 authentication
C. SMTP relay server authentication
D. external user and relay mail authentication
Answer: A (LEAVE A REPLY)

NEW QUESTION: 236
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: 237
Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.



Answer:



NEW QUESTION: 238

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 defense-in-depth stops at the network

B. to expose the endpoint to more threats

C. because human error or insider threats will still exist

D. to prevent theft of the endpoints

Answer: C (LEAVE A REPLY)