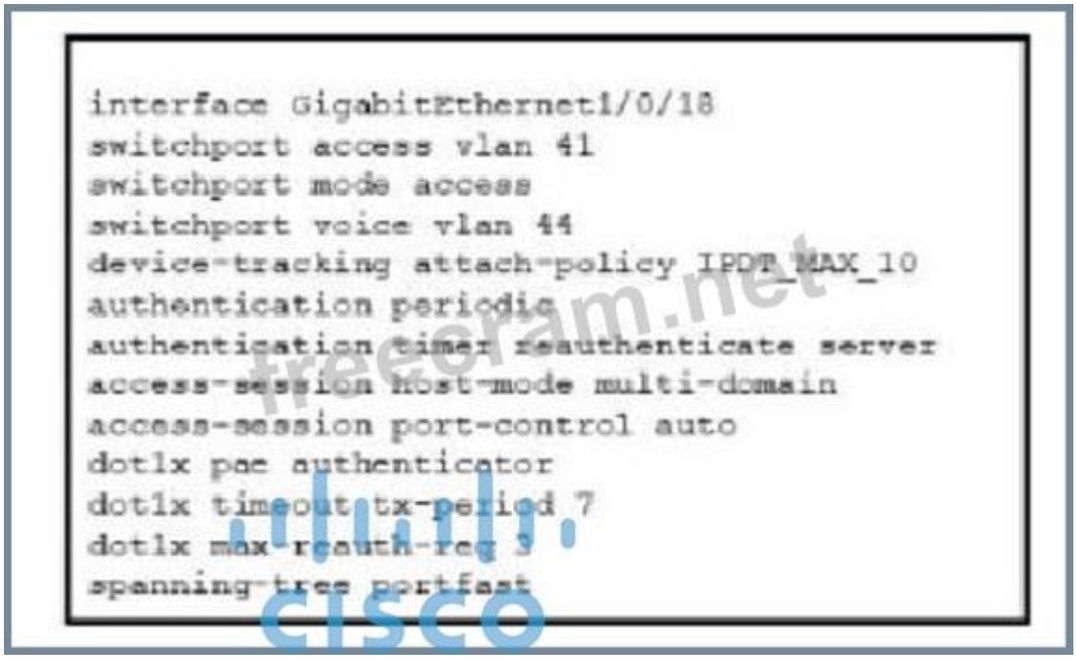
Cisco.350-701.v2021-12-14.q124

Exam Code:	350-701
Exam Name:	Implementing and Operating Cisco Security Core Technologies
Certification Provider:	Cisco
Free Question Number:	124
Version:	v2021-12-14
# of views:	1578
# of Questions views:	69003
https://www.freecram.net/torrent/Cisco.350-701.v2021-12-14.q124.html	

NEW QUESTION: 1
How is data sent out to the attacker during a DNS tunneling attack?
A. as part of the domain name
B. as part of the DNS response packet
C. as part of the TCP/53 packet header
D. as part of the UDP'53 packet payload
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Refer to the exhibit.



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

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

A. Add mab to the interface configuration.

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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 3

What is a characteristic of Dynamic ARP Inspection?

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

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

C. DAI associates a trust state with each switch.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 4

What are two advantages of using Cisco Any connect over DMVPN? (Choose two.)

A. It provides spoke-to-spoke communications without traversing the hub

B. It enables VPN access for individual users from their machines

C. It allows different routing protocols to work over the tunnel

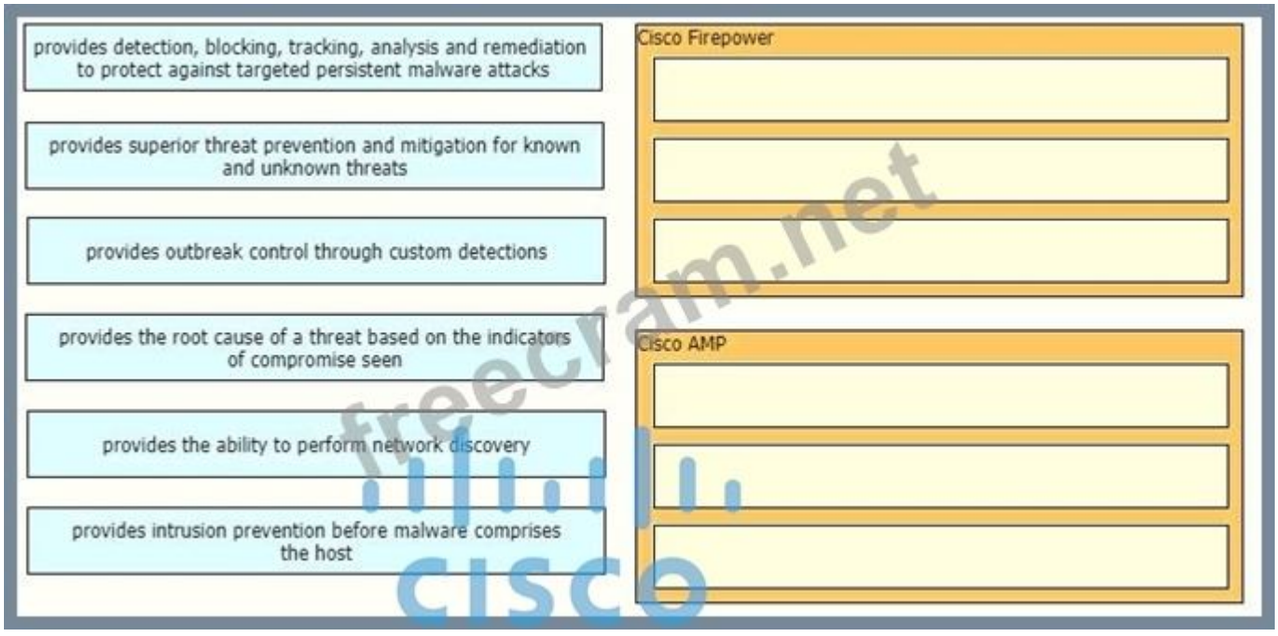
D. it allows multiple sites to connect to the data center

E. It allows customization of access policies based on user identity

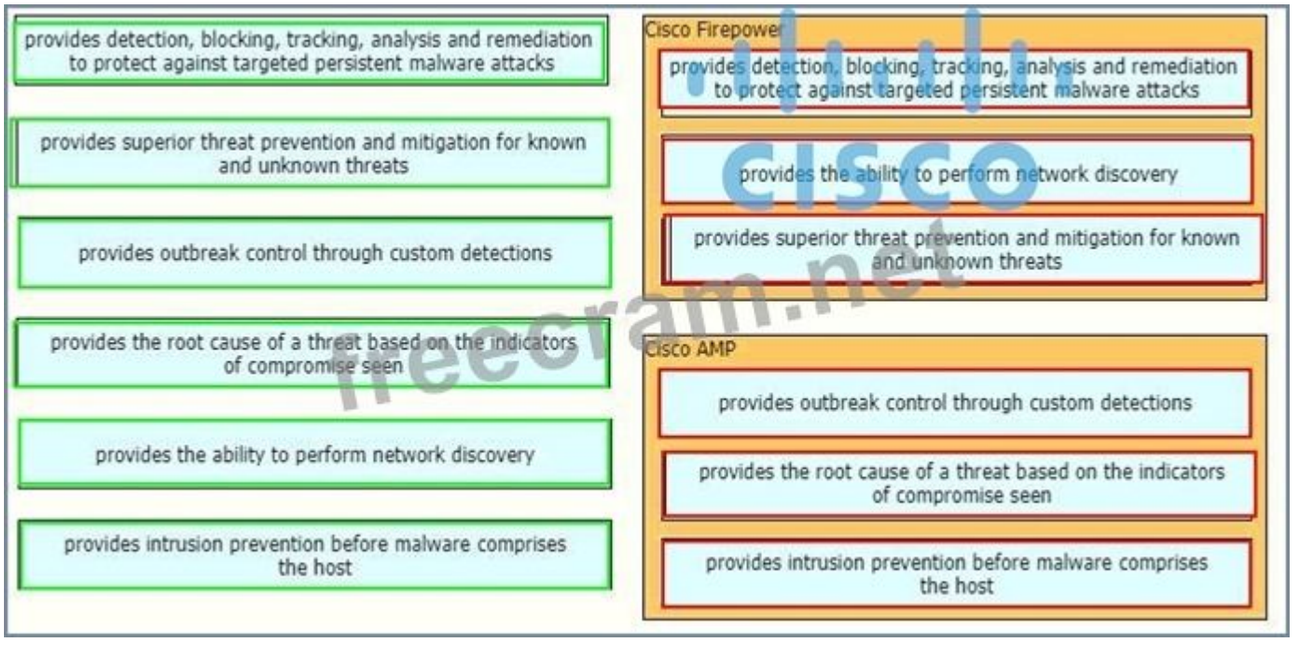
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 5

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



Answer:



NEW QUESTION: 6

Which license is required for Cisco Security Intelligence to work on the Cisco Next Generation Intrusion Prevention System?

A. control

B. protect

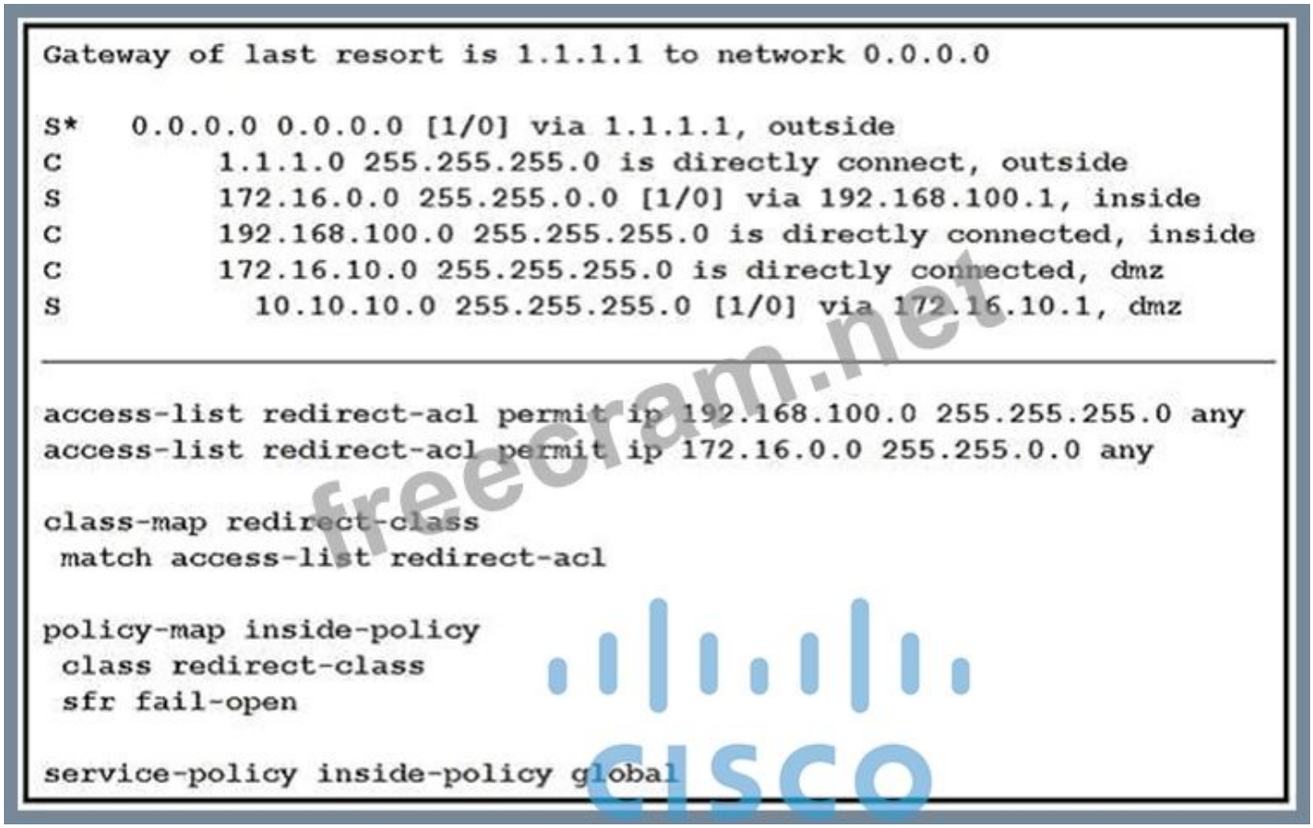
C. malware

D. URL filtering

Answer: (SHOW ANSWER)

NEW QUESTION: 7

Refer to the exhibit.



What is a result of the configuration?

A. Traffic from the DMZ network is redirected

B. Traffic from the inside network is redirected

C. All TCP traffic is redirected

D. Traffic from the inside and DMZ networks is redirected

Answer: (SHOW ANSWER)

Explanation: The purpose of above commands is to redirect traffic that matches the ACL "redirect-acl" to the Cisco FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and any other actions that are applied by policy are performed, the traffic is returned to the ASA for further processing and ultimate transmission. The command "service-policy global_policy global" applies the policy to all of the interfaces. Reference: https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.html The purpose of above commands is to redirect traffic that matches the ACL "redirect-acl" to the Cisco FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and any other actions that are applied by policy are performed, the traffic is returned to the ASA for further processing and ultimate transmission.

The command "service-policy global_policy global" applies the policy to all of the interfaces.

Explanation: The purpose of above commands is to redirect traffic that matches the ACL "redirect-acl" to the Cisco FirePOWER (SFR) module in the inline (normal) mode. In this mode, after the undesired traffic is dropped and any other actions that are applied by policy are performed, the traffic is returned to the ASA for further processing and ultimate transmission. The command "service-policy global_policy global" applies the policy to all of the interfaces. Reference: https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.html

NEW QUESTION: 8
What is a characteristic of traffic storm control behavior?
A. Traffic storm control cannot determine if the packet is unicast or broadcast.
B. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.
C. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
D. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which two features of Cisco Email Security can protect your organization against email threats? (Choose two)
A. Time-based one-time passwords
B. Data loss prevention
C. Heuristic-based filtering
D. Geolocation-based filtering
E. NetFlow
Answer: (SHOW ANSWER)
Explanation : Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution. Cisco Email Security appliance can now handle incoming mail connections and incoming messages from specific geolocations and perform appropriate actions on them, for example: - Prevent email threats coming from specific geographic regions. - Allow or disallow emails coming from specific geographic regions. Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_00.html Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution.
Cisco Email Security appliance can now handle incoming mail connections and incoming messages from specific geolocations and perform appropriate actions on them, for example:
- Prevent email threats coming from specific geographic regions.
- Allow or disallow emails coming from specific geographic regions.
Reference:
Explanation : Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution. Cisco Email Security appliance can now handle incoming mail connections and incoming messages from specific geolocations and perform appropriate actions on them, for example: - Prevent email threats coming from specific geographic regions. - Allow or disallow emails coming from specific geographic regions. Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_00.html

NEW QUESTION: 10

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

A. permit

B. trust

C. reset

D. allow

E. monitor

Answer: (SHOW ANSWER)

Each rule also has an action, which determines whether you monitor, trust, block, or allow matching traffic.

Note: With action "trust", Firepower does not do any more inspection on the traffic. There will be no intrusion protection and also no file-policy on this traffic.

NEW QUESTION: 11

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

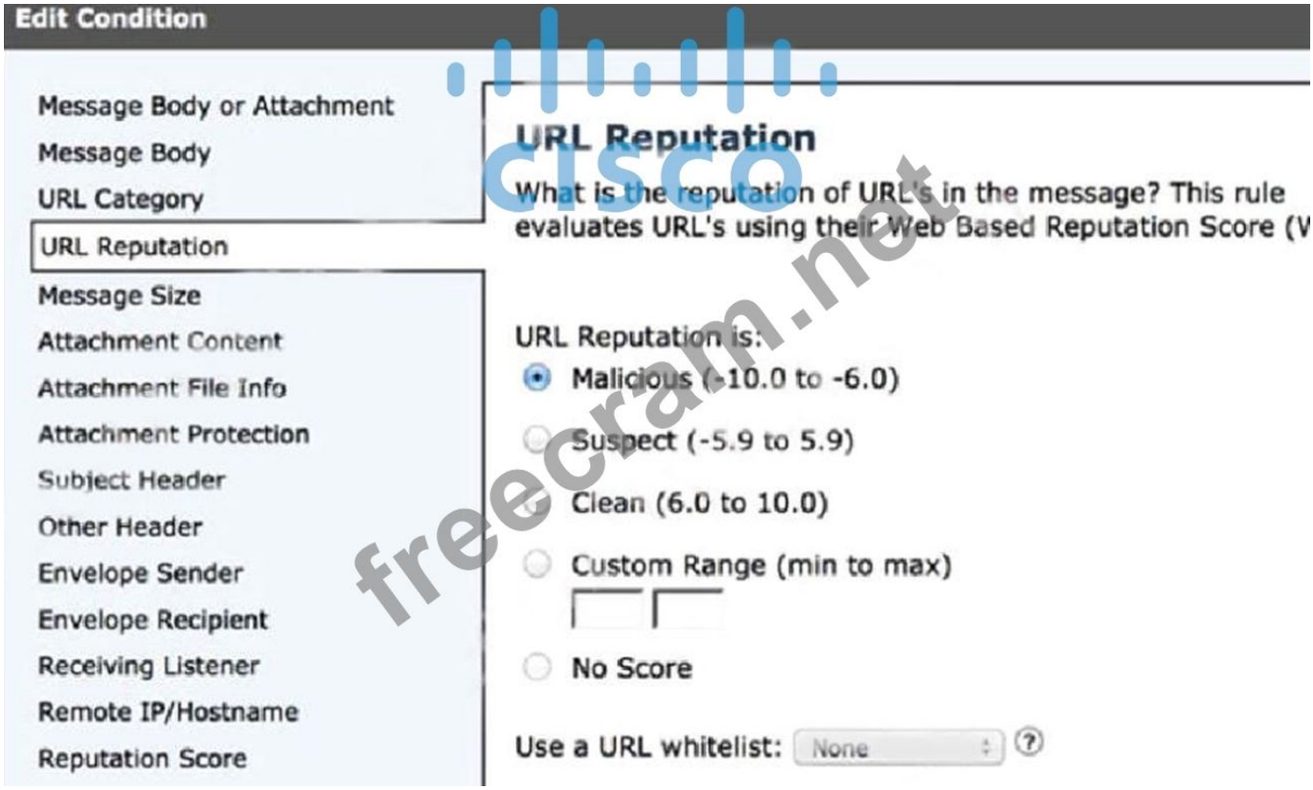
C. 5

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: 12

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

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

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

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

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

Answer: (SHOW ANSWER)

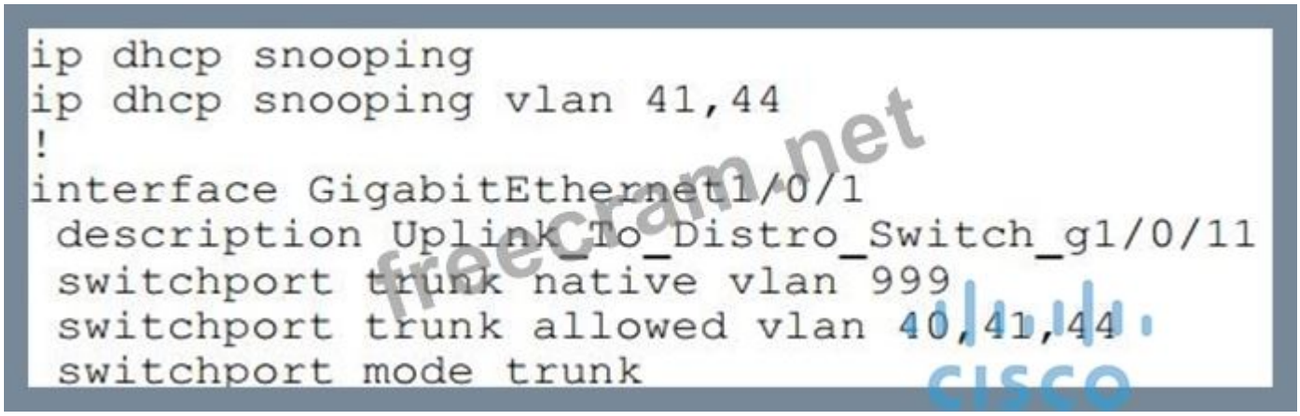
The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.

The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.

Reference:

The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.

NEW QUESTION: 13
Refer to the exhibit.



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

NEW QUESTION: 14
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: (SHOW ANSWER)
Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Reference:
Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system
"You cannot use an FMC to manage ASA firewall functions."
The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management.
Cisco FTD devices, Cisco Firepower devices, and the Cisco ASA FirePOWER modules can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center -> Answer D is not correct Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system
"You cannot use an FMC to manage ASA firewall functions."
The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management.
Note: The ASA FirePOWER module runs on the separately upgraded ASA operating system
"You cannot use an FMC to manage ASA firewall functions."
The Cisco Secure Firewall Threat Defense Manager (Firepower Management Center) increases the effectiveness of your Cisco network security solutions by providing centralized, integrated, and streamlined management.

NEW QUESTION: 15
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 must have inline interface pairs configured.
D. It is out-of-band from traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
A customer has various external HTTP resources available including Intranet. Extranet, and Internet, with a proxy configuration running in explicit mode Which method allows the client desktop browsers to be configured to select when to connect direct or when to use the proxy?
A. Forward file
B. Transparent mode
C. PAC file

D. Bridge mode
Answer: (SHOW ANSWER)

NEW QUESTION: 17
What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?
A. Cisco Umbrella
B. External Threat Feeds
C. Cisco Threat Grid
D. Cisco Stealthwatch
Answer: (SHOW ANSWER)
Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically.
Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically.
Reference:
Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically.

NEW QUESTION: 18
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: 19
Which form of attack is launched using botnets?

A. EIDDOS
B. virus
C. DDOS
D. TCP flood
Answer: (SHOW ANSWER)
A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them. Cyber criminals use botnets to instigate botnet attacks, which include malicious activities such as credentials leaks, unauthorized access, data theft and DDoS attacks.

NEW QUESTION: 20
Which component of Cisco umbrella architecture increases reliability of the service?
A. Cisco Talos
B. Anycast IP
C. AMP Threat grid
D. BGP route reflector
Answer: (SHOW ANSWER)

NEW QUESTION: 21
What is the purpose of CA in a PKI?
A. To issue and revoke digital certificates
B. To validate the authenticity of a digital certificate
C. To create the private key for a digital certificate
D. To certify the ownership of a public key by the named subject
Answer: (SHOW ANSWER)
A trusted CA is the only entity that can issue trusted digital certificates. This is extremely important because while PKI manages more of the encryption side of these certificates, authentication is vital to understanding which entities own what keys. Without a trusted CA, anyone can issue their own keys, authentication goes out the window and chaos ensues.
A trusted CA is the only entity that can issue trusted digital certificates. This is extremely important because while PKI manages more of the encryption side of these certificates, authentication is vital to understanding which entities own what keys. Without a trusted CA, anyone can issue their own keys, authentication goes out the window and chaos ensues.
Reference:
A trusted CA is the only entity that can issue trusted digital certificates. This is extremely important because while PKI manages more of the encryption side of these certificates, authentication is vital to understanding which entities own what keys. Without a trusted CA, anyone can issue their own keys, authentication goes out the window and chaos ensues.

NEW QUESTION: 22
Elliptic curve cryptography is a stronger more efficient cryptography method meant to replace which current encryption technology?

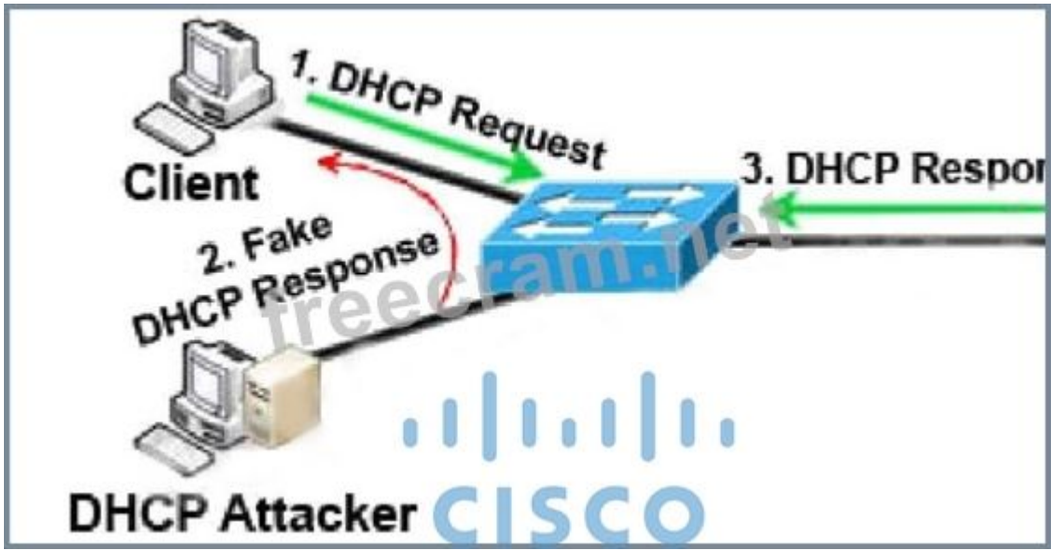
A. 3DES
B. RSA
C. DES
D. AES
Answer: (SHOW ANSWER)
Compared to RSA, the prevalent public-key cryptography of the Internet today, Elliptic Curve Cryptography (ECC) offers smaller key sizes, faster computation,as well as memory, energy and bandwidth savings and is thus better suited forsmall devices.

NEW QUESTION: 23
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)
A. Patch for cross-site scripting.
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.
D. Install a spam and virus email filter.
E. Protect systems with an up-to-date antimalware program
Answer: (SHOW ANSWER)
Explanation : Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

NEW QUESTION: 24
What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?
A. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not
B. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA.
C. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA
D. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA
Answer: (SHOW ANSWER)

NEW QUESTION: 25
An administrator is configuring a DHCP server to better secure their environment. They need to be able to ratelimit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?
A. Set a trusted interface for the DHCP server
B. Set the DHCP snooping bit to 1
C. Add entries in the DHCP snooping database
D. Enable ARP inspection for the required VLAN
Answer: (SHOW ANSWER)

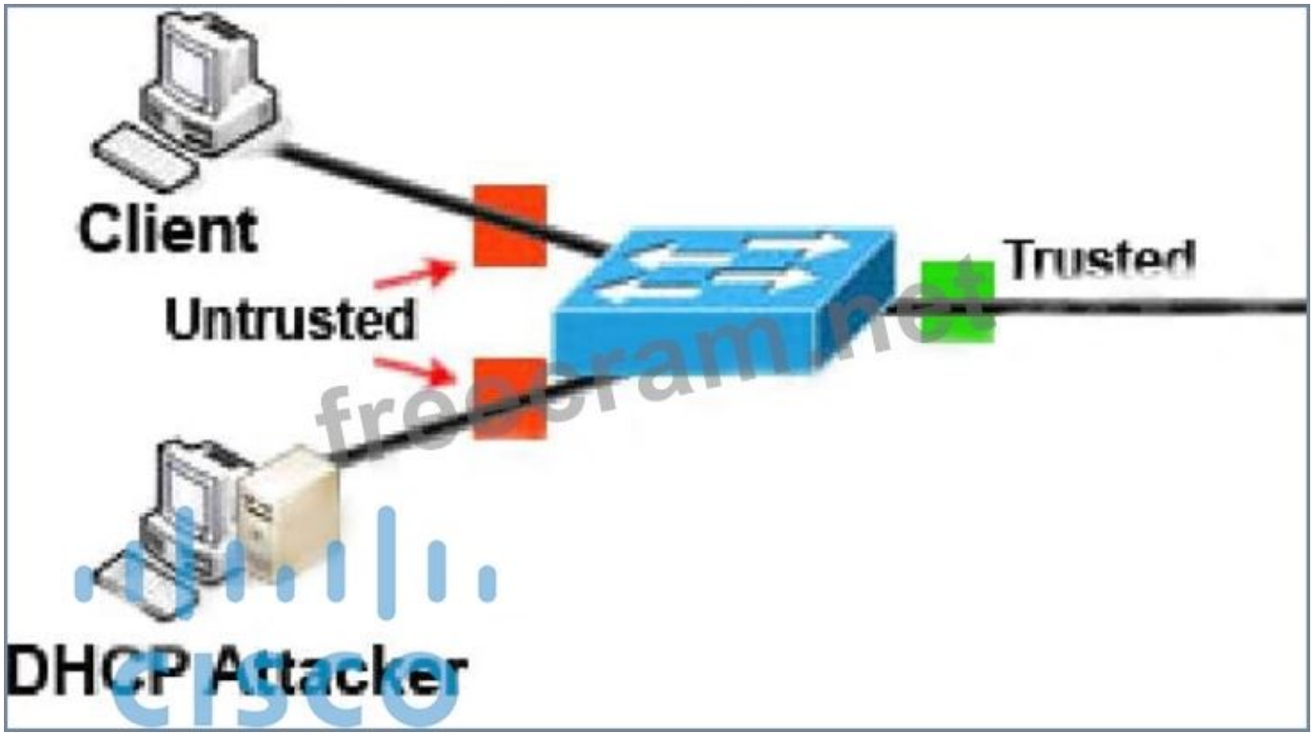
To understand DHCP snooping we need to learn about DHCP spoofing attack first.



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

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

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



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

NEW QUESTION: 26
In which two ways does a system administrator send web traffic transparently to the Web Security Appliance? (Choose two.)
A. configure policy-based routing on the network infrastructure
B. use Web Cache Communication Protocol
C. configure Active Directory Group Policies to push proxy settings
D. reference a Proxy Auto Config file
E. configure the proxy IP address in the web-browser settings
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which type of API is being used when a security application notifies a controller within a software-defined network architecture about a specific security threat? (Choose Two)
A. southbound API
B. northbound API
C. westbound AP
D. eastbound API
Answer: (SHOW ANSWER)

NEW QUESTION: 28
A malicious user gained network access by spoofing printer connections that were authorized using MAB on four different switch ports at the same time. What two catalyst switch security features will prevent further violations? (Choose two)
A. DHCP Snooping
B. IP Device track
C. 802.1AE MacSec
D. Private VLANs
E. Dynamic ARP inspection
F. Port security
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which information is required when adding a device to Firepower Management Center?
A. encryption method
B. device serial number
C. username and password
D. registration key

Answer: (SHOW ANSWER)

NEW QUESTION: 30

What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?

A. It discovers and controls cloud apps that are connected to a company's corporate environment

B. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously

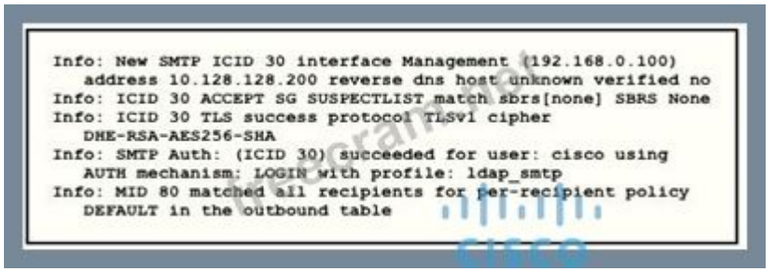
C. It sends the application information to an administrator to act on

D. It deletes any application that does not belong in the network

Answer: (SHOW ANSWER)

NEW QUESTION: 31

Refer to the exhibit.



Which type of authentication is in use?

A. LDAP authentication for Microsoft Outlook

B. POP3 authentication

C. SMTP relay server authentication

D. external user and relay mail authentication

Answer: (SHOW ANSWER)

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

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

Reference:

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

The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS

connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.
The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

NEW QUESTION: 32
Which public cloud provider supports the Cisco Next Generation Firewall Virtual?
A. Google Cloud Platform
B. Red Hat Enterprise Visualization
C. VMware ESXi
D. Amazon Web Services
Answer: (SHOW ANSWER)
Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco's Firepower next generation firewall.
The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure.
In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet.
In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions.
Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco's Firepower next generation firewall.
The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure.
In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet.
In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions.
Reference:
Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco's Firepower next generation firewall.

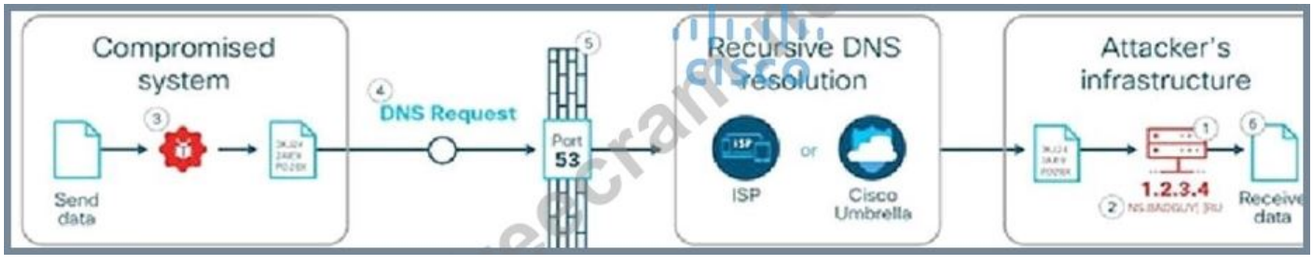
The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure.
In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet.
In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions.

NEW QUESTION: 33
What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?
A. Multiple NetFlow collectors are supported
B. Advanced NetFlow v9 templates and legacy v5 formatting are supported
C. Secure NetFlow connections are optimized for Cisco Prime Infrastructure
D. Flow-create events are delayed
Answer: (SHOW ANSWER)
The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions:
...
- Delays the export of flow-create events.
The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions:
...
- Delays the export of flow-create events.
Reference:
The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide the following major functions:
...
- Delays the export of flow-create events.

NEW QUESTION: 34
How is DNS tunneling used to exfiltrate data out of a corporate network?
A. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.
B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.
C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network.
D. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.
Answer: (SHOW ANSWER)
Domain name system (DNS) is the protocol that translates human-friendly URLs, such as securitytut.com, into IP addresses, such as 183.33.24.13. Because DNS messages are only used as the beginning of each

communication and they are not intended for data transfer, many organizations do not monitor their DNS traffic for malicious activity. As a result, DNS-based attacks can be effective if launched against their networks. DNS tunneling is one such attack.

An example of DNS Tunneling is shown below:



The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNS nameserver (NS) and malicious payload.

2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. attackerdomain.com) is registered or reused. The registrar informs the top-level domain (.com) nameservers to refer requests for attackerdomain.com to ns.attackerdomain.com, which has a DNS record mapped to 1.2.3.4

3. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, P028X977W,...).

4. The payload initiates thousands of unique DNS record requests to the attacker's domain with each string as a part of the domain name (e.g. 3KJ242AIE9.attackerdomain.com). Depending on the attacker's patience and stealth, requests can be spaced out over days or months to avoid suspicious network activity. 5. The requests are forwarded to a recursive DNS resolver. During resolution, the requests are sent to the attacker's authoritative DNS nameserver, 6. The tunneling kit parses the encoded strings and rebuilds the exfiltrated data. Reference: https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0

5. The requests are forwarded to a recursive DNS resolver. During resolution, the requests are sent to the attacker's authoritative DNS nameserver,

6. The tunneling kit parses the encoded strings and rebuilds the exfiltrated data.

a part of the domain name (e.g. 3KJ242AIE9.attackerdomain.com). Depending on the attacker's patience and stealth, requests can be spaced out over days or months to avoid suspicious network activity. 5. The requests are forwarded to a recursive DNS resolver. During resolution, the requests are sent to the attacker's authoritative DNS nameserver, 6. The tunneling kit parses the encoded strings and rebuilds the exfiltrated data. Reference: https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0

NEW QUESTION: 35

How many interfaces per bridge group does an ASA bridge group deployment support?

A. up to 2

B. up to 4

C. up to 8

D. up to 16

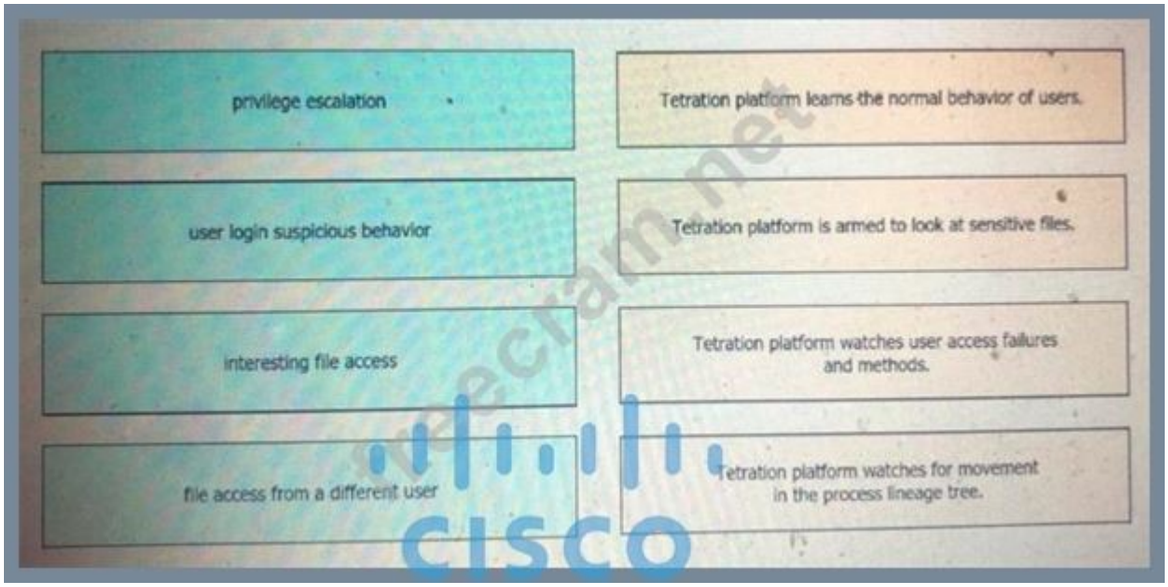
Answer: (SHOW ANSWER)

Each of the ASAs interfaces need to be grouped into one or more bridge groups. Each of these groups acts as an independent transparent firewall. It is not possible for one bridge group to communicate with another bridge group without assistance from an external router.
As of 8.4(1) upto 8 bridge groups are supported with 2-4 interface in each group. Prior to this only one bridge group was supported and only 2 interfaces.
Up to 4 interfaces are permitted per bridge-group (inside, outside, DMZ1, DMZ2)

NEW QUESTION: 36
Which parameter is required when configuring a Netflow exporter on a Cisco Router?
A. DSCP value
B. Source interface
C. Exporter name
D. Exporter description
Answer: (SHOW ANSWER)
An example of configuring a NetFlow exporter is shown below:
flow exporter Exporter
destination 192.168.100.22
transport udp 2055

NEW QUESTION: 37
Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?
A. network AMP
B. cloud web services
C. public cloud
D. private cloud
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.



Answer:

NEW QUESTION: 39

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)

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: 40
What is the function of the Context Directory Agent?
A. maintains users' group memberships
B. relays user authentication requests from Web Security Appliance to Active Directory
C. reads the Active Directory logs to map IP addresses to usernames
D. accepts user authentication requests on behalf of Web Security Appliance for user identification
Answer: (SHOW ANSWER)
Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to).
CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices.
Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to).
CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices.
Reference:
cda_oveviw.html
Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to).
CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices.
cda_oveviw.html

NEW QUESTION: 41
Which two tasks allow NetFlow on a Cisco ASA 5500 Series firewall? (Choose two.)
A. Create an ACL to allow UDP traffic on port 9996.
B. Enable NetFlow Version 9.
C. Define a NetFlow collector by using the flow-export command.
D. Apply NetFlow Exporter to the outside interface in the inbound direction.
E. Create a class map to match interesting traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 42
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: (SHOW ANSWER)
Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.
One of the settings to configure the CoA type is "Reauth". This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.
Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.
One of the settings to configure the CoA type is "Reauth". This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.
Reference:
b_ise_admin_guide_sample_chapter_010101.html
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.
b_ise_admin_guide_sample_chapter_010101.html

NEW QUESTION: 43
An administrator is establishing a new site-to-site VPN connection on a Cisco IOS router. The organization needs to ensure that the ISAKMP key on the hub is used only for terminating traffic from the IP address of 172.19.20.24. Which command on the hub will allow the administrator to accomplish this?
A. crypto ca identity 172.19.20.24
B. crypto isakmp key Cisco0123456789 172.19.20.24
C. crypto enrollment peer address 172.19.20.24

D. crypto isakmp identity address 172.19.20.24

Answer: (SHOW ANSWER)

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

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

crypto isakmp identity address

crypto isakmp key sharedkeystring address 192.168.1.33

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

crypto isakmp identity address

crypto isakmp key sharedkeystring address 10.0.0.1

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

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

crypto isakmp identity address

crypto isakmp key sharedkeystring address 192.168.1.33

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

crypto isakmp identity address

crypto isakmp key sharedkeystring address 10.0.0.1

Reference:

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

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

Only answer B is the best choice left.

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

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

crypto isakmp identity address

crypto isakmp key sharedkeystring address 192.168.1.33

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

crypto isakmp identity address

crypto isakmp key sharedkeystring address 10.0.0.1

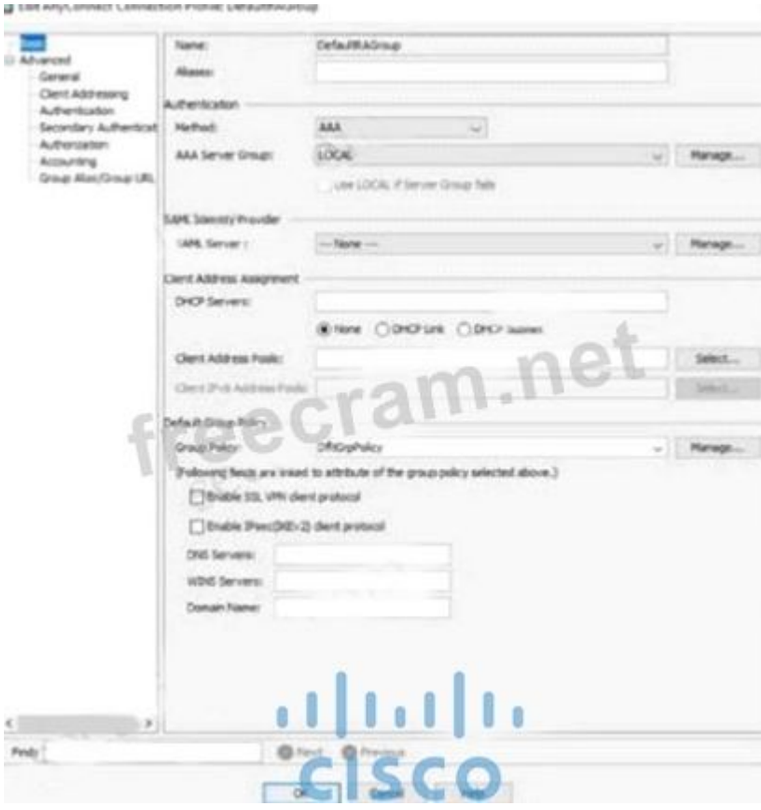
The command "crypto enrollment peer address" is not valid either.

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

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

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

NEW QUESTION: 44
Refer to the exhibit.



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

NEW QUESTION: 45
An organization has a requirement to collect full metadata information about the traffic going through their AWS cloud services They want to use this information for behavior analytics and statistics Which two actions must be taken to implement this requirement? (Choose two.)
A. Send VPC Flow Logs to Cisco Stealthwatch Cloud.

B. Configure Cisco Stealthwatch Cloud to ingest AWS information
C. Configure Cisco Thousand Eyes to ingest AWS information.
D. Configure Cisco ACI to ingest AWS information.
E. Send syslog from AWS to Cisco Stealthwatch Cloud.
Answer: (SHOW ANSWER)

NEW QUESTION: 46
An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems. Why should the organization select either Platform as a Service or Infrastructure as a Service for this environment?
A. Infrastructure as a Service because the customer manages the operating system
B. Platform as a Service because the customer manages the operating system
C. Infrastructure as a Service because the service provider manages the operating system
D. Platform as a Service because the service provider manages the operating system
Answer: (SHOW ANSWER)

NEW QUESTION: 47
A Cisco FTD engineer is creating a new IKEv2 policy called s2s00123456789 for their organization to allow for additional protocols to terminate network devices with. They currently only have one policy established and need the new policy to be a backup in case some devices cannot support the stronger algorithms listed in the primary policy. What should be done in order to support this?
A. Change the integrity algorithms to SHA* to support all SHA algorithms in the primary policy
B. Make the priority for the new policy 5 and the primary policy 1
C. Change the encryption to AES* to support all AES algorithms in the primary policy
D. Make the priority for the primary policy 10 and the new policy 1
Answer: (SHOW ANSWER)
All IKE policies on the device are sent to the remote peer regardless of what is in the selected policy section. The first IKE Policy matched by the remote peer will be selected for the VPN connection. Choose which policy is sent first using the priority field. Priority 1 will be sent first.
All IKE policies on the device are sent to the remote peer regardless of what is in the selected policy section. The first IKE Policy matched by the remote peer will be selected for the VPN connection. Choose which policy is sent first using the priority field. Priority 1 will be sent first.
Reference:

All IKE policies on the device are sent to the remote peer regardless of what is in the selected policy section. The first IKE Policy matched by the remote peer will be selected for the VPN connection. Choose which policy is sent first using the priority field. Priority 1 will be sent first.

NEW QUESTION: 48
What features does Cisco FTDv provide over ASAv?
A. Cisco FTDv runs on VMWare while ASAv does not
B. Cisco FTDv supports URL filtering while ASAv does not
C. Cisco FTDv runs on AWS while ASAv does not
D. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not
Answer: (SHOW ANSWER)

NEW QUESTION: 49
An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?
A. RAT
B. SAT
C. HAT
D. BAT
Answer: (SHOW ANSWER)

NEW QUESTION: 50
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 *.domain.com address in the block list
B. Configure the *.com address in the block list.
C. Configure the *.domain.com address in the block list
D. Configure the domain.com address in the block list
Answer: (SHOW ANSWER)

NEW QUESTION: 51
What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two)
A. data exfiltration
B. command and control communication
C. intelligent proxy
D. snort
E. URL categorization
Answer: (SHOW ANSWER)
Cisco Cognitive Threat Analytics helps you quickly detect and respond to sophisticated, clandestine attacks that are already under way or are attempting to establish a presence within your environment. The solution

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

+ Data exfiltration: Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content
+ Command-and-control (C2) communication: Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPSencoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad range of threats
...

NEW QUESTION: 52
Which two deployment modes does the Cisco ASA FirePower module support? (Choose two)
A. transparent mode
B. routed mode
C. inline mode
D. active mode
E. passive monitor-only mode
Answer: (SHOW ANSWER)
You can configure your ASA FirePOWER module using one of the following deployment models:
You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment.
You can configure your ASA FirePOWER module using one of the following deployment models:
You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment.
Reference:
modules-sfr.html
You can configure your ASA FirePOWER module using one of the following deployment models:
You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment.
modules-sfr.html

NEW QUESTION: 53
An engineer notices traffic interruption on the network. Upon further investigation, it is learned that broadcast packets have been flooding the network. What must be configured, based on a predefined threshold, to address this issue?
A. Bridge Protocol Data Unit guard
B. embedded event monitoring
C. storm control
D. access control lists
Answer: (SHOW ANSWER)

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.
By using the "storm-control broadcast level [falling-threshold]" we can limit the broadcast traffic on the switch.

NEW QUESTION: 54
An organization has two machines hosting web applications. Machine 1 is vulnerable to SQL injection while machine 2 is vulnerable to buffer overflows. What action would allow the attacker to gain access to machine 1 but not machine 2?
A. sending continuous pings
B. inserting malicious commands into the database
C. sniffing the packets between the two hosts
D. overflowing the buffer's memory
Answer: (SHOW ANSWER)

NEW QUESTION: 55
When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?
A. Security Category Blocking
B. Content Category Blocking
C. File Analysis
D. Application Control
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?
A. File Analysis
B. SafeSearch
C. SSL Decryption
D. Destination Lists
Answer: (SHOW ANSWER)
SSL Decryption is an important part of the Umbrella Intelligent Proxy. he feature allows the Intelligent Proxy to go beyond simply inspecting normal URLs and actually proxy and inspect traffic that's sent over HTTPS. The SSL Decryption feature does require the root certificate be installed.
SSL Decryption is an important part of the Umbrella Intelligent Proxy. he feature allows the Intelligent Proxy to go beyond simply inspecting normal URLs and actually proxy and inspect traffic that's sent over HTTPS. The SSL Decryption feature does require the root certificate be installed.
Reference:

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

NEW QUESTION: 57
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. EPP focuses on network security, and EDR focuses on device security.
C. EDR focuses on network security, and EPP focuses on device security.
D. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.
Answer: (SHOW ANSWER)

NEW QUESTION: 58
An attacker needs to perform reconnaissance on a target system to help gain access to it. The system has weak passwords, no encryption on the VPN links, and software bugs on the system's applications. Which vulnerability allows the attacker to see the passwords being transmitted in clear text?
A. improper file security
B. software bugs on applications
C. weak passwords for authentication
D. unencrypted links for traffic
Answer: (SHOW ANSWER)

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

NEW QUESTION: 60
Cisco SensorBase gaihers threat information from a variety of Cisco products and services and performs analytics to find patterns on threats Which term describes this process?

A. sharing
B. authoring

C. consumption
D. deployment
Answer: (SHOW ANSWER)

NEW QUESTION: 61
Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?
A. TLSv1.2
B. TLSv1.1
C. BJTLSv1
D. DTLSv1
Answer: (SHOW ANSWER)
DTLS is used for delay sensitive applications (voice and video) as its UDP based while TLS is TCP based. Therefore DTLS offers strongest throughput performance. The throughput of DTLS at the time of AnyConnect connection can be expected to have processing performance close to VPN throughput.

NEW QUESTION: 62
What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?
A. Telemetry uses a pull mehod, which makes it more reliable than SNMP
B. Telemetry uses push and pull, which makes it more scalable than SNMP
C. Telemetry uses push and pull which makes it more secure than SNMP
D. Telemetry uses a push method which makes it faster than SNMP
Answer: (SHOW ANSWER)
SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts.
The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data.
Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc.
Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics.
Referfence: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming telemetry SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts.

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

NEW QUESTION: 63
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. ESP
B. AES-192
C. IKEv1
D. AES-256
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
What are two list types within AMP for Endpoints Outbreak Control? (Choose two)
A. blocked ports
B. simple custom detections
C. command and control
D. allowed applications
E. URL
Answer: B,D (LEAVE A REPLY)
Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists.
A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine.
Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to

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

NEW QUESTION: 65
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)
... 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
... we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's Firepower
... 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: 66
Refer to the exhibit.

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. authentication key mismatch

B. interesting traffic was not applied

C. hashing algorithm mismatch

D. encryption algorithm mismatch

Answer: (SHOW ANSWER)

NEW QUESTION: 67

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

A. Implement email filtering techniques

B. Define security group memberships

C. Enable browser alerts for fraudulent websites

D. Use antispyware software

E. Revoke expired CRL of the websites

Answer: (SHOW ANSWER)

NEW QUESTION: 68

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

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

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

C. It allows ARP traffic with a single access rule

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

Answer: (SHOW ANSWER)

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

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

NEW QUESTION: 69

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

A. Cisco Umbrella

B. Cisco AMP

C. Cisco Stealthwatch

D. Cisco Tetration

Answer: (SHOW ANSWER)

Micro-segmentation secures applications by expressly allowing particular application traffic and, by default, denying all other traffic. Micro-segmentation is the foundation for implementing a zero-trust security model for application workloads in the data center and cloud.

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

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

Micro-segmentation secures applications by expressly allowing particular application traffic and, by default, denying all other traffic. Micro-segmentation is the foundation for implementing a zero-trust security model for application workloads in the data center and cloud.

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

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

Reference:

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

NEW QUESTION: 70

An engineer wants to automatically assign endpoints that have a specific OUI into a new endpoint group. Which probe must be enabled for this type of profiling to work?

A. NetFlow
B. NMAP
C. SNMP
D. DHCP
Answer: (SHOW ANSWER)
Cisco ISE can determine the type of device or endpoint connecting to the network by performing "profiling." Profiling is done by using DHCP, SNMP, Span, NetFlow, HTTP, RADIUS, DNS, or NMAP scans to collect as much metadata as possible to learn the device fingerprint.
NMAP ("Network Mapper") is a popular network scanner which provides a lot of features. One of them is the OUI (Organizationally Unique Identifier) information. OUI is the first 24 bit or 6 hexadecimal value of the MAC address.
Note: DHCP probe cannot collect OUIs of endpoints. NMAP scan probe can collect these endpoint attributes:
+ EndPointPolicy
+ LastNmapScanCount
+ NmapScanCount
+ OUI
+ Operating-system
Cisco ISE can determine the type of device or endpoint connecting to the network by performing "profiling." Profiling is done by using DHCP, SNMP, Span, NetFlow, HTTP, RADIUS, DNS, or NMAP scans to collect as much metadata as possible to learn the device fingerprint.

NMAP ("Network Mapper") is a popular network scanner which provides a lot of features. One of them is the OUI (Organizationally Unique Identifier) information. OUI is the first 24 bit or 6 hexadecimal value of the MAC address.
Note: DHCP probe cannot collect OUIs of endpoints. NMAP scan probe can collect these endpoint attributes:
+ EndPointPolicy
+ LastNmapScanCount
+ NmapScanCount
+ OUI
+ Operating-system
Reference:
Cisco ISE can determine the type of device or endpoint connecting to the network by performing "profiling." Profiling is done by using DHCP, SNMP, Span, NetFlow, HTTP, RADIUS, DNS, or NMAP scans to collect as much metadata as possible to learn the device fingerprint.
NMAP ("Network Mapper") is a popular network scanner which provides a lot of features. One of them is the OUI (Organizationally Unique Identifier) information. OUI is the first 24 bit or 6 hexadecimal value of the MAC address.
Note: DHCP probe cannot collect OUIs of endpoints. NMAP scan probe can collect these endpoint attributes:
+ EndPointPolicy
+ LastNmapScanCount
+ NmapScanCount
+ OUI
+ Operating-system

NEW QUESTION: 71
An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the endpoint to apply a new or updated policy from ISE. Which CoA type achieves this goal?
A. CoA Session Query
B. CoA Terminate
C. Port Bounce
D. CoA Reauth
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
Which Cisco platform processes behavior baselines, monitors for deviations, and reviews for malicious processes in data center traffic and servers while performing software vulnerability detection?
A. Cisco AMP for Network
B. Cisco ISE?
C. Cisco AnyConnect
D. Cisco Tetration
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Which type of protection encrypts RSA keys when they are exported and imported?
A. NGE
B. passphrase
C. nonexportable
D. file
Answer: (SHOW ANSWER)

NEW QUESTION: 74
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 UDP packets whereas a DDoS attack is where a computer is used to flood a server with TCP packets
C. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where a computer is used to flood multiple servers that are distributed over a LAN
D. A DoS attack is where a computer is used to flood a server with TCP packets whereas a DDoS attack is where a computer is used to flood a server with UDP packets
Answer: (SHOW ANSWER)

NEW QUESTION: 75
An administrator wants to ensure that all endpoints are compliant before users are allowed access on the corporate network. The endpoints must have the corporate antivirus application installed and be running the latest build of Windows 10.
What must the administrator implement to ensure that all devices are compliant before they are allowed on the network?
A. Cisco ASA firewall with Dynamic Access Policies configured
B. Cisco Stealthwatch and Cisco Identity Services Engine integration
C. Cisco Identity Services Engine with PxGrid services enabled
D. Cisco Identity Services Engine and AnyConnect Posture module
Answer: (SHOW ANSWER)

NEW QUESTION: 76
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)

Explanation : Explanation : 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/

Explanation:

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.

Explanation : Explanation : 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: 77
When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?
A. Spero analysis
B. dynamic analysis
C. sandbox analysis
D. malware analysis
Answer: (SHOW ANSWER)
Spero analysis examines structural characteristics such as metadata and header information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware.
Spero analysis examines structural characteristics such as metadata and header information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware.
Reference:
-> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload the whole file. Dynamic analysis sends files to AMP ThreatGrid.
Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco Threat Grid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit.
Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources. -> Malware analysis does not upload files to anywhere, it only checks the files locally.
There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in a virtual machine.
Spero analysis examines structural characteristics such as metadata and header information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware.
-> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload the whole file. Dynamic analysis sends files to AMP ThreatGrid.

Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco Threat Grid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit.
Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources. -> Malware analysis does not upload files to anywhere, it only checks the files locally.
There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in a
-> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload the whole file. Dynamic analysis sends files to AMP ThreatGrid.
Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco Threat Grid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit.
Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources. -> Malware analysis does not upload files to anywhere, it only checks the files locally.
There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in a virtual machine.

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

NEW QUESTION: 79
What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?
A. Activate the Advanced Malware Protection license
B. Enable Intelligent Proxy

C. Activate SSL decryption
D. Enable IP Layer enforcement
Answer: (SHOW ANSWER)

NEW QUESTION: 80
Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?

A. NGFW
B. ESA
C. WSA
D. AMP
Answer: (SHOW ANSWER)

NEW QUESTION: 81
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: (SHOW ANSWER)
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.

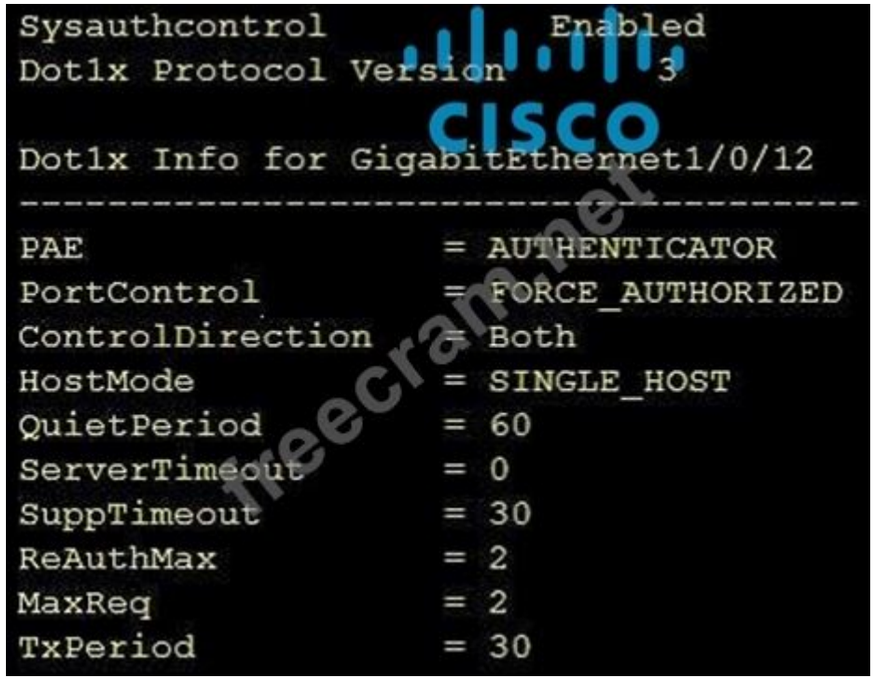
NEW QUESTION: 82
Which risk is created when using an Internet browser to access cloud-based service?
A. insecure implementation of API
B. vulnerabilities within protocol
C. misconfiguration of infrastructure, which allows unauthorized access
D. intermittent connection to the cloud connectors
Answer: (SHOW ANSWER)

NEW QUESTION: 83
When wired 802.1X authentication is implemented, which two components are required? (Choose two.)
A. supplicant: Cisco AnyConnect ISE Posture module
B. authenticator: Cisco Identity Services Engine
C. authentication server: Cisco Prime Infrastructure
D. authentication server: Cisco Identity Service Engine
E. authenticator: Cisco Catalyst switch
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 84
What are two benefits of Flexible NetFlow records? (Choose two)
A. They allow the user to configure flow information to perform customized traffic identification
B. They provide attack prevention by dropping the traffic
C. They provide accounting and billing enhancements
D. They converge multiple accounting technologies into one accounting mechanism
E. They provide monitoring of a wider range of IP packet information from Layer 2 to 4
Answer: (SHOW ANSWER)
NetFlow is typically used for several key customer applications, including the following:
...
Billing and accounting. NetFlow data provides fine-grained metering (for instance, flow data includes details such as IP addresses, packet and byte counts, time stamps, type of service (ToS), and application ports) for highly flexible and detailed resource utilization accounting. Service providers may use the information for billing based on time of day, bandwidth usage, application usage, quality of service, and so on. Enterprise customers may use the information for departmental charge back or cost allocation for resource utilization.
NetFlow is typically used for several key customer applications, including the following:
...

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

NEW QUESTION: 85
Refer to the exhibit.



Which command was used to display this output?

A. show dot1x all summary

B. show dot1x all

C. show dot1x interface gi1/0/12

D. show dot1x

Answer: (SHOW ANSWER)

NEW QUESTION: 86

Refer to the exhibit.

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

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

A. adds a switch to Cisco DNA Center

B. adds authentication to a switch

C. receives information about a switch

Answer: (SHOW ANSWER)

NEW QUESTION: 87

On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed devices?

A. correlation policy

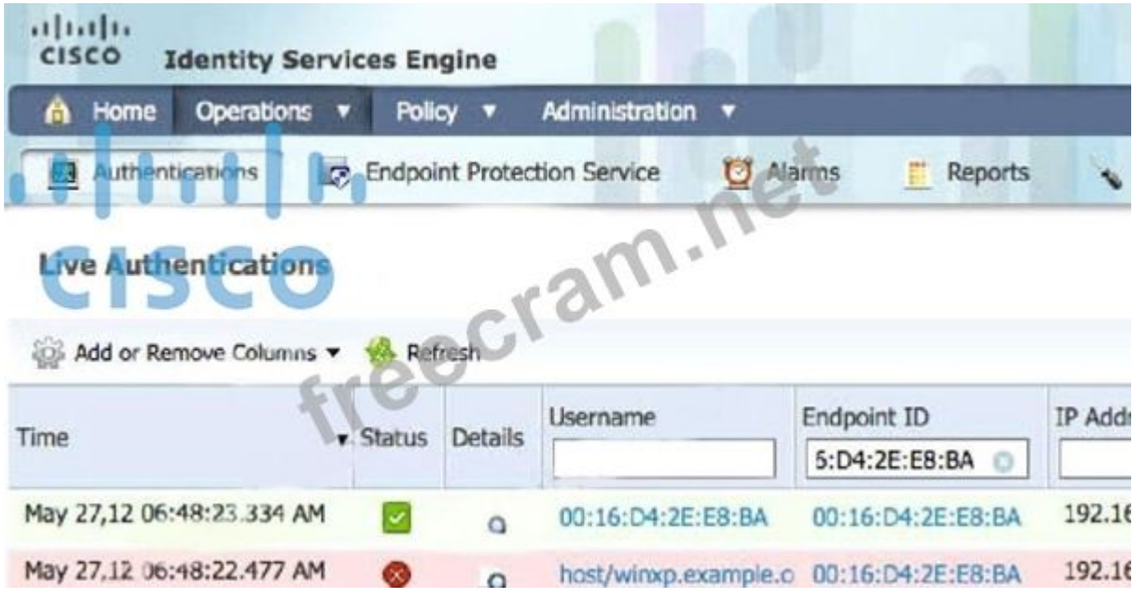
B. health awareness policy

C. access control policy

D. health policy
E. system policy
Answer: (SHOW ANSWER)

NEW QUESTION: 88
What is a difference between DMVPN and sVTI?
A. DMVPN supports static tunnel establishment, whereas sVTI does not.
B. DMVPN supports dynamic tunnel establishment, whereas sVTI does not.
C. DMVPN supports tunnel encryption, whereas sVTI does not.
D. DMVPN provides interoperability with other vendors, whereas sVTI does not.
Answer: (SHOW ANSWER)

NEW QUESTION: 89
A network administrator is configuring a switch to use Cisco ISE for 802.1X. An endpoint is failing authentication and is unable to access the network. Where should the administrator begin troubleshooting to verify the authentication details?
A. Adaptive Network Control Policy List
B. Context Visibility
C. Accounting Reports
D. RADIUS Live Logs
Answer: (SHOW ANSWER)
How To Troubleshoot ISE Failed Authentications & Authorizations
Check the ISE Live Logs
Login to the primary ISE Policy Administration Node (PAN).
Go to Operations > RADIUS > Live Logs
(Optional) If the event is not present in the RADIUS Live Logs, go to Operations > Reports > Reports > Endpoints and Users > RADIUS Authentications Check for Any Failed Authentication Attempts in the Log



NEW QUESTION: 90

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

NEW QUESTION: 91
Which VPN technology can support a multivendor environment and secure traffic between sites?
A. SSL VPN
B. GET VPN
C. FlexVPN
D. DMVPN
Answer: C (LEAVE A REPLY)
Explanation: FlexVPN is an IKEv2-based VPN technology that provides several benefits beyond traditional site-to-site VPN implementations. FlexVPN is a standards-based solution that can interoperate with non-Cisco IKEv2 implementations. Therefore FlexVPN can support a multivendor environment. All of the three VPN technologies support traffic between sites (site-to-site or spoke-to-spoke).

NEW QUESTION: 92
How does Cisco Workload Optimization Manager help mitigate application performance issues?
A. It deploys an AWS Lambda system
B. It automates resource resizing
C. It optimizes a flow path
D. It sets up a workload forensic score
Answer: (SHOW ANSWER)

Cisco Workload Optimization Manager provides specific real-time actions that ensure workloads get the resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software). Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software). Cisco Workload Optimization Manager provides specific real-time actions that ensure workloads get the resources they need when they need them, enabling continuous placement, resizing, and capacity decisions that can be automated, driving continuous health in the environment. You can automate the software's decisions according to your level of comfort: recommend (view only), manual (select and apply), or automated (executed in real time by software). Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-overview-c22-739078.pdf

NEW QUESTION: 93
Which service allows a user export application usage and performance statistics with Cisco Application Visibility and control?
A. SNORT
B. NetFlow
C. SNMP
D. 802.1X
Answer: (SHOW ANSWER)
Application Visibility and control (AVC) supports NetFlow to export application usage and performance statistics. This data can be used for analytics, billing, and security policies.

NEW QUESTION: 94
Which exfiltration method does an attacker use to hide and encode data inside DNS requests and queries?
A. DNS tunneling
B. DNSCrypt
C. DNS security
D. DNSSEC
Answer: (SHOW ANSWER)
DNS Tunneling is a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses. DNS tunneling often includes data payloads that can be added to an attacked DNS server and used to control a remote server and applications.

NEW QUESTION: 95
An engineer needs to add protection for data in transit and have headers in the email message Which configuration is needed to accomplish this goal?

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

NEW QUESTION: 96
Which command enables 802.1X globally on a Cisco switch?
A. dot1x system-auth-control
B. authentication port-control aut
C. dot1x pae authenticator
D. aaa new-model
Answer: (SHOW ANSWER)

NEW QUESTION: 97
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: (SHOW ANSWER)
The syntax of this command is shown below:
snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]}] [read read-view] [write write-view] [notify notify-view] [access access-list] The command above restricts which IP source addresses are allowed to access SNMP functions on the router. You could restrict SNMP access by simply applying an interface ACL to block incoming SNMP packets that don't come from trusted servers. However, this would not be as effective as using the global SNMP commands shown in this recipe. Because you can apply this method once for the whole router, it is much simpler than applying ACLs to block SNMP on all interfaces separately. Also, using interface ACLs would block not only SNMP packets intended for this router, but also may stop SNMP packets that just happened to be passing through on their way to some other destination device.

NEW QUESTION: 98
Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?
A. user input validation in a web page or web application
B. Linux and Windows operating systems
C. database
D. web page images

Answer: (SHOW ANSWER)

SQL injection usually occurs when you ask a user for input, like their username/userid, but the user gives ("injects") you an SQL statement that you will unknowingly run on your database. For example:
Look at the following example, which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
If user enter something like this: "100 OR 1=1" then the SQL statement will look like this:
SELECT * FROM Users WHERE UserId = 100 OR 1=1;
The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE. A hacker might get access to all the user names and passwords in this database.

NEW QUESTION: 99

What is a key difference between Cisco Firepower and Cisco ASA?

A. Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not.

B. Cisco Firepower provides identity-based access control while Cisco ASA does not.

C. Cisco ASA provides access control while Cisco Firepower does not.

D. Cisco ASA provides SSL inspection while Cisco Firepower does not.

Answer: (SHOW ANSWER)

NEW QUESTION: 100

Which SNMPv3 configuration must be used to support the strongest security possible?

A. 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

B. 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

C. asa-host(config)#snmp-server group myv3 v3 noauth
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

D. asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

Answer: (SHOW ANSWER)

NEW QUESTION: 101

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

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

B. Configure a common administrator account

C. Configure a common DNS server

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

Answer: (SHOW ANSWER)

The following are the prerequisites to integrate Active Directory with Cisco ISE.

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

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

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

The following are the prerequisites to integrate Active Directory with Cisco ISE.

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

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

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

Reference:

b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F The following are the prerequisites to integrate Active Directory with Cisco ISE.

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

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

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

b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F

NEW QUESTION: 102

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 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 used as the identity when matching an IKEv2 authorization policy.
D. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER
Answer: (SHOW ANSWER)

NEW QUESTION: 103
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: 104
Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two)
A. accounting
B. assurance
C. automation
D. authentication
E. encryption
Answer: (SHOW ANSWER)
What Cisco DNA Center enables you to do

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

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

NEW QUESTION: 105
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 hashing algorithm that was used was MD5. which is unsupported.
C. The router was not rebooted after the NTP configuration updated.
D. The key was configured in plain text.
Answer: (SHOW ANSWER)

NEW QUESTION: 106
How is ICMP used an exfiltration technique?
A. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host
B. by flooding the destination host with unreachable packets
C. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address
D. by overwhelming a targeted host with ICMP echo-request packets

Answer: (SHOW ANSWER)

NEW QUESTION: 107
Which two key and block sizes are valid for AES? (Choose two)
A. 64-bit block size, 112-bit key length
B. 64-bit block size, 168-bit key length
C. 128-bit block size, 192-bit key length
D. 128-bit block size, 256-bit key length
E. 192-bit block size, 256-bit key length
Answer: C,D (LEAVE A REPLY)
The AES encryption algorithm encrypts and decrypts data in blocks of 128 bits (block size). It can do this using 128-bit, 192-bit, or 256-bit keys

NEW QUESTION: 108
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. because human error or insider threats will still exist
C. to expose the endpoint to more threats
D. to prevent theft of the endpoints
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Which two request of REST API are valid on the Cisco ASA Platform? (Choose two)
A. put
B. options
C. get
D. push
E. connect
Answer: (SHOW ANSWER)
The ASA REST API gives you programmatic access to managing individual ASAs through a Representational State Transfer (REST) API. The API allows external clients to perform CRUD (Create, Read, Update, Delete) operations on ASA resources; it is based on the HTTPS protocol and REST methodology.

All API requests are sent over HTTPS to the ASA, and a response is returned.
Request Structure
Available request methods are:
GET - Retrieves data from the specified object.
PUT - Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist.
POST - Creates the object with the supplied information.
DELETE - Deletes the specified object
PATCH - Applies partial modifications to the specified object. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html PATCH - Applies partial modifications to the specified object. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html

NEW QUESTION: 110

A network engineer is trying to figure out whether FlexVPN or DMVPN would fit better in their environment.
They have a requirement for more stringent security multiple security associations for the connections, more efficient VPN establishment as well consuming less bandwidth. Which solution would be best for this and why?

A. DMVPN because it supports IKEv2 and FlexVPN does not
B. FlexVPN because it supports IKEv2 and DMVPN does not
C. FlexVPN because it uses multiple SAs and DMVPN does not
D. DMVPN because it uses multiple SAs and FlexVPN does not
Answer: (SHOW ANSWER)
FlexVPN supports IKEv2 -> Answer A is not correct.
DMVPN supports both IKEv1 & IKEv2 -> Answer B is not correct.
FlexVPN support multiple SAs -> Answer D is not correct.

NEW QUESTION: 111
What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?
A. STIX
B. XMPP
C. pxGrid
D. SMTP
Answer: (SHOW ANSWER)
TAXII (Trusted Automated Exchange of Indicator Information) is a standard that provides a transport

NEW QUESTION: 112
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: (SHOW ANSWER)
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: 113
When choosing an algorithm to us, what should be considered about Diffie Hellman and RSA for key establishment?
A. RSA is an asymmetric key establishment algorithm intended to output symmetric keys
B. RSA is a symmetric key establishment algorithm intended to output asymmetric keys
C. DH is a symmetric key establishment algorithm intended to output asymmetric keys
D. DH is on asymmetric key establishment algorithm intended to output symmetric keys
Answer: D (LEAVE A REPLY)
Diffie Hellman (DH) uses a private-public key pair to establish a shared secret, typically a symmetric key. DH is not a symmetric algorithm - it is an asymmetric algorithm used to establish a shared secret for a symmetric key algorithm.

NEW QUESTION: 114
Which API is used for Content Security?
A. AsyncOS API
B. OpenVuln API
C. IOS XR API
D. NX-OS API
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?
A. Group Policy
B. Access Control Policy
C. Device Management Policy
D. Platform Service Policy

Answer: (SHOW ANSWER)

Cisco Firepower deployments can take advantage of platform settings policies. A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. Examples of these platform settings policies are time and date settings, external authentication, and other common administrative features.

A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device.

For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.

Cisco Firepower deployments can take advantage of platform settings policies. A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. Examples of these platform settings policies are time and date settings, external authentication, and other common administrative features.

A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device.

For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.

Reference:

Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best answer here so we have to choose it.

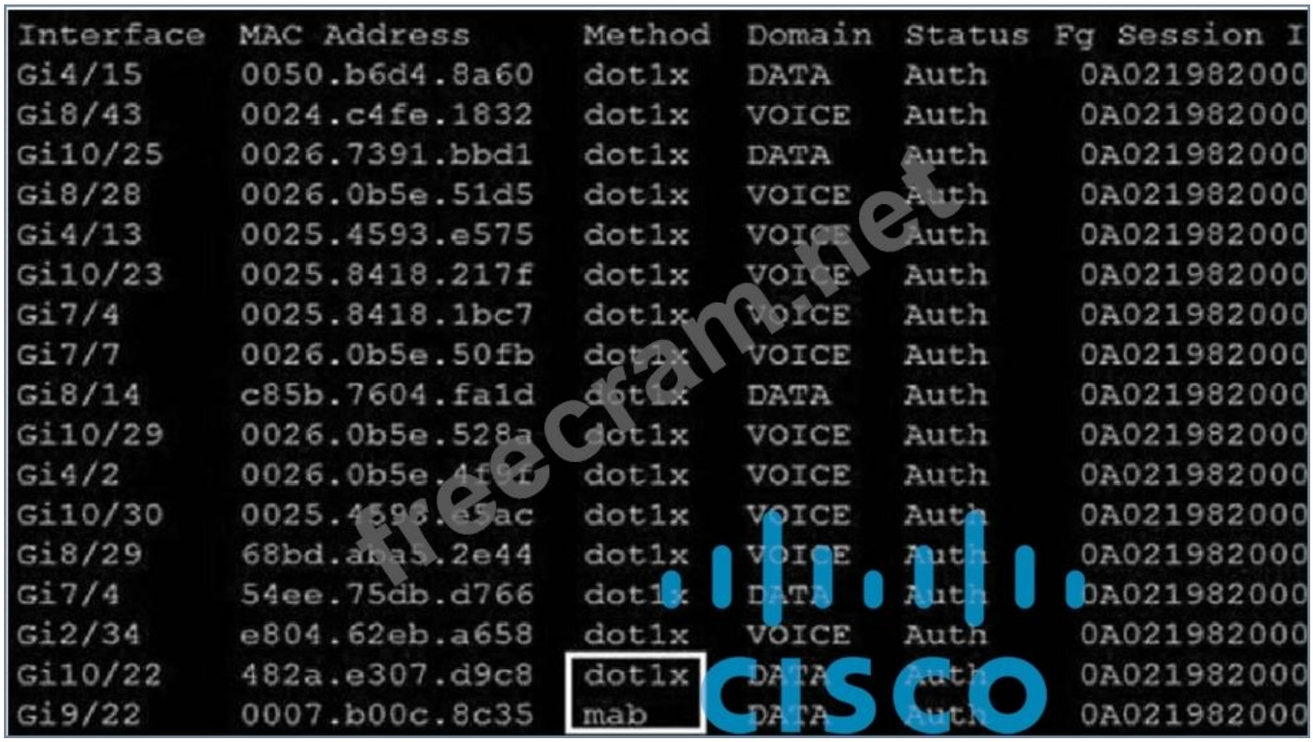
Cisco Firepower deployments can take advantage of platform settings policies. A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. Examples of these platform settings policies are time and date settings, external authentication, and other common administrative features.

A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device.

For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.

Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best
Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best
answer here so we have to choose it.

NEW QUESTION: 116
Refer to the exhibit.



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

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

NEW QUESTION: 117
An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?
A. Cisco Umbrella
B. Cisco Cloud Email Security
C. Cisco NGFW
D. Cisco Cloudlock
Answer: (SHOW ANSWER)

Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform.
Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform.
Reference:
Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform.

NEW QUESTION: 118
What is the benefit of integrating Cisco ISE with a MDM solution?
A. It provides compliance checks for access to the network
B. It provides the ability to update other applications on the mobile device
C. It provides the ability to add applications to the mobile device through Cisco ISE
D. It provides network device administration access
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperability_mdm.html
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/
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: 119
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: B (LEAVE A REPLY)
Cisco's DNA Center is the only centralized network management system to bring all of this functionality into a single pane of glass.
Cisco's DNA Center is the only centralized network management system to bring all of this functionality into a single pane of glass.
Reference:
Cisco's DNA Center is the only centralized network management system to bring all of this functionality into a single pane of glass.

NEW QUESTION: 120
Which compliance status is shown when a configured posture policy requirement is not met?
A. compliant
B. unknown
C. authorized

D. noncompliant

Answer: (SHOW ANSWER)

Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies.

A posture policy is a collection of posture requirements that are associated with one or more identity groups and operating systems.

Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies.

+ If a mandatory requirement fails, the user will be moved to Non-Compliant state

+ If an optional requirement fails, the user is allowed to skip the specified optional requirements and the user is moved to Compliant state This Qdid not clearly specify the type of posture policy requirement (mandatory or optional) is not met so the user can be in Non-compliant or compliant state. But "noncompliant" is the best answer here.

Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies.

A posture policy is a collection of posture requirements that are associated with one or more identity groups and operating systems.

Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies.

+ If a mandatory requirement fails, the user will be moved to Non-Compliant state

+ If an optional requirement fails, the user is allowed to skip the specified optional requirements and the user is moved to Compliant state This Qdid not clearly specify the type of posture policy requirement (mandatory or optional) is not met so the user can be in Non-compliant or compliant state. But "noncompliant" is the best answer here.

Reference:

b_ise_admin_guide_sample_chapter_010111.html

Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies.

A posture policy is a collection of posture requirements that are associated with one or more identity groups and operating systems.

Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies.

+ If a mandatory requirement fails, the user will be moved to Non-Compliant state

+ If an optional requirement fails, the user is allowed to skip the specified optional requirements and the user is moved to Compliant state This Qdid not clearly specify the type of posture policy requirement (mandatory or optional) is not met so the user can be in Non-compliant or compliant state. But "noncompliant" is the best answer here.

b_ise_admin_guide_sample_chapter_010111.html

NEW QUESTION: 121

Which attack type attempts to shut down a machine or network so that users are not able to access it?

A. smurf
B. bluesnarfing
C. MAC spoofing
D. IP spoofing
Answer: (SHOW ANSWER)
Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to its intended users.
The Smurf attack is a DDoS attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.

NEW QUESTION: 122
What are the two types of managed Intercloud Fabric deployment models? (Choose two)
A. Service Provider managed
B. Public managed
C. Hybrid managed
D. User managed
E. Enterprise managed
Answer: (SHOW ANSWER)
Explanation Explanation Many enterprises prefer to deploy development workloads in the public cloud, primarily for convenience and faster deployment. This approach can cause concern for IT administrators, who must control the flow of IT traffic and spending and help ensure the security of data and intellectual property. Without the proper controls, data and intellectual property can escape this oversight. The Cisco Intercloud Fabric solution helps control this shadow IT, discovering resources deployed in the public cloud outside IT control and placing these resources under Cisco Intercloud Fabric control. Cisco Intercloud Fabric addresses the cloud deployment requirements appropriate for two hybrid cloud deployment models: Enterprise Managed (an enterprise manages its own cloud environments) and Service Provider Managed (the service provider administers and controls all cloud resources). Reference: https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric.pdf The Cisco Intercloud Fabric architecture provides two product configurations to address the following two consumption models: + Cisco Intercloud Fabric for Business + Cisco Intercloud Fabric for Providers Reference: https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric/Intercloud_Fabric_2.html

NEW QUESTION: 123
A company discovered an attack propagating through their network via a file. A custom file policy was created in order to track this in the future and ensure no other endpoints execute the infected file. In addition, it was discovered during testing that the scans are not detecting the file as an indicator of compromise. What must be done in order to ensure that the created is functioning as it should?
A. Create an IP block list for the website from which the file was downloaded
B. Upload the hash for the file into the policy
C. Block the application that the file was using to open
D. Send the file to Cisco Threat Grid for dynamic analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 124
What are two functions of secret key cryptography? (Choose two.)
A. utilization of less memory
B. utilization of different keys for encryption and decryption
C. key selection without integer factorization
D. provides the capability to only know the key on one side
E. utilization of large prime number iterations
Answer: (SHOW ANSWER)