Cisco.350-701.v2022-06-21.q171

Exam Code:	350-701
Exam Name:	Implementing and Operating Cisco Security Core Technologies
Certification Provider:	Cisco
Free Question Number:	171
Version:	v2022-06-21
# of views:	3995
# of Questions views:	1710
https://www.freepdfdumps.com/Cisco.350-701.v2022-06-21.q171.html	

NEW QUESTION: 1
What is a feature of NetFlow Secure Event Logging?
A. It delivers data records to NSEL collectors through NetFlow over TCP only.
B. It exports only records that indicate significant events in a flow.
C. It filters NSEL events based on the traffic and event type through RSVP.
D. It supports v5 and v8 templates.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
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: A (LEAVE A REPLY)
SQL injection usually occurs when you ask a user for input, like their username/userid, but the user gives ("injects") you an SQL statement that you will unknowingly run on your database. For example:
Look at the following example, which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
If user enter something like this: "100 OR 1=1" then the SzQL statement will look like this:
SELECT * FROM Users WHERE UserId = 100 OR 1=1;
The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE. A hacker might get access to all the user names and passwords in this database.

NEW QUESTION: 3

Refer to the exhibit.

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

A. set the IP address of an interface

B. complete no configurations

C. complete all configurations

D. add subinterfaces

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 4

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 TCP/53 packet header

C. as part of the DNS response packet

D. as part of the UDP'53 packet payload

Answer: A (LEAVE A REPLY)

NEW QUESTION: 5

What is a difference between DMVPN and sVTI?

A. DMVPN supports static tunnel establishment, whereas sVTI does not.

B. DMVPN supports tunnel encryption, whereas sVTI does not.

C. DMVPN provides interoperability with other vendors, whereas sVTI does not.

D. DMVPN supports dynamic tunnel establishment, whereas sVTI does not.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 6

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

A. Orchestration

B. CI/CD pipeline

C. Container
D. Security
Answer: B (LEAVE A REPLY)
Unlike the traditional software life cycle, the CI/CD implementation process gives a weekly or daily update instead of monthly or quarterly. The fun part is customers won't even realize the update is in their applications, as they happen on the fly. Reference: https://devops.com/how-to-implement-an-effective-ci-cd-pipeline/
instead of monthly or quarterly. The fun part is customers won't even realize the update is in their applications, as they happen on the fly.
Unlike the traditional software life cycle, the CI/CD implementation process gives a weekly or daily update instead of monthly or quarterly. The fun part is customers won't even realize the update is in their applications, as they happen on the fly. Reference: https://devops.com/how-to-implement-an-effective-ci-cd-pipeline/

NEW QUESTION: 7
A large organization wants to deploy a security appliance in the public cloud to form a site-to-site VPN and link the public cloud environment to the private cloud in the headquarters data center. Which Cisco security appliance meets these requirements?
A. Cisco Cloud Orchestrator
B. Cisco WSAV
C. Cisco Stealthwatch Cloud
D. Cisco ASAV
Answer: D (LEAVE A REPLY)

NEW QUESTION: 8
An engineer is configuring Cisco WSA and needs to enable a separated email transfer flow from the Internet and from the LAN. Which deployment mode must be used to accomplish this goal?
A. multi-context
B. transparent
C. two-interface
D. single interface
Answer: C (LEAVE A REPLY)

NEW QUESTION: 9
Which solution should be leveraged for secure access of a CI/CD pipeline?
A. remote access client
B. Duo Network Gateway
C. Cisco FTD network gateway
D. SSL WebVPN
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Why would a user choose an on-premises ESA versus the CES solution?

A. Demand is unpredictable.
B. Sensitive data must remain onsite.
C. The server team wants to outsource this service.
D. ESA is deployed inline.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
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. Enable insecure protocols within Cisco ISE in the allowed protocols configuration.
B. Configure authentication event fail retry 2 action authorize vlan 41 on the interface
C. Change the default policy in Cisco ISE to allow all devices not using machine authentication .
D. Add mab to the interface configuration.
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which two components do southbound APIs use to communicate with downstream devices? (Choose two.)
A. services running over the network
B. OpFlex
C. applications running over the network
D. OpenFlow
E. external application APIs
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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

A. displays client ID

B. HTTP authorization

C. HTTP authentication

D. Imports requests

Answer: (SHOW ANSWER)

NEW QUESTION: 14

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

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

B. Configure a common administrator account

C. Configure a common DNS server

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

Answer: D (LEAVE A REPLY)

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

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

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

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

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

NEW QUESTION: 15
After a recent breach, an organization determined that phishing was used to gain initial access to the network before regaining persistence. The information gained from the phishing attack was a result of users visiting known malicious websites. What must be done in order to prevent this from happening in the future?
A. Modify an access policy
B. Modify identification profiles
C. Modify outbound malware scanning policies
D. Modify web proxy settings
Answer: A (LEAVE A REPLY)
URL conditions in access control rules allow you to limit the websites that users on your network can access. This feature is called URL filtering. There are two ways you can use access control to specify URLs you want to block (or, conversely, allow): - With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic. - With a URL Filtering license, you can also control access to websites based on the URL's general classification, or category, and risk level, or reputation. The system displays this category and reputation data in connection logs, intrusion events, and application details. Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies. Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html
- With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic.
- With a URL Filtering license, you can also control access to websites based on the URL's general classification, or category, and risk level, or reputation. The system displays this category and reputation data in connection logs, intrusion events, and application details.

Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies.
URL conditions in access control rules allow you to limit the websites that users on your network can access. This feature is called URL filtering. There are two ways you can use access control to specify URLs you want to block (or, conversely, allow): - With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic. - With a URL Filtering license, you can also control access to websites based on the URL's general classification, or category, and risk level, or reputation. The system displays this category and reputation data in connection logs, intrusion events, and application details. Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies. Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access_Control_Rules__URL_Filtering.html

NEW QUESTION: 16
Refer to the exhibit. All servers are in the same VLAN/Subnet. DNS Server-1 and DNS Server-2 must communicate with each other, and communicate with default gateway multilayer switch. Which type of private VLAN ports should be configured to prevent communication and the file server?
A. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as isolated port, and GigabitEthernet0/3 and GigabitEthernet... ports.
B. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as promiscuous port, GigabitEthernet0/3 and GigabitEthernet...0/
C. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as community port, and GigabitEthernet0/3 and GigabitEthen... ports.
D. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as isolated port, and GigabitEthernet0/3 and GigabitEthernet...OA ports.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 17
What is the primary role of the Cisco Email Security Appliance?
A. Mail Submission Agent
B. Mail Transfer Agent
C. Mail Delivery Agent
D. Mail User Agent
Answer: B (LEAVE A REPLY)
Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay. Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/Cisco_SBA_BN_EmailSecurityUsingCiscoESADeploymentGuide-Feb2013.pdf by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay.
Reference:
Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay. Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/Cisco_SBA_BN_EmailSecurityUsingCiscoESADeploymentGuide-Feb2013.pdf

NEW QUESTION: 18
Which Cisco security solution protects remote users against phishing attacks when they are not connected to the VPN?
A. Cisco Stealthwatch
B. Cisco Umbrella
C. Cisco Firepower
D. NGIPS
Answer: B (LEAVE A REPLY)
Cisco Umbrella protects users from accessing malicious domains by proactively analyzing and blocking unsafe destinations - before a connection is ever made. Thus it can protect from phishing attacks by blocking suspicious domains when users click on the given links that an attacker sent. Cisco Umbrella roaming protects your employees even when they are off the VPN.

NEW QUESTION: 19

Refer to the exhibit.

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

What does the number 15 represent in this configuration?

A. privilege level for an authorized user to this router

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

C. interval in seconds between SNMPv3 authentication attempts

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

Answer: B (LEAVE A REPLY)

The syntax of this command is shown below:

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

NEW QUESTION: 20

An administrator enables Cisco Threat Intelligence Director on a Cisco FMC. Which process uses STIX and allows uploads and downloads of block lists?

A. authoring

B. sharing

C. consumption

D. editing

Answer: D (LEAVE A REPLY)

NEW QUESTION: 21

An MDM provides which two advantages to an organization with regards to device management? (Choose two)

A. allowed application management

B. Active Directory group policy management

C. network device management

D. asset inventory management

E. critical device management

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 22

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

A. SDN controller and the network elements
B. management console and the SDN controller
C. management console and the cloud
D. SDN controller and the cloud
Answer: A (LEAVE A REPLY)
The Southbound API is used to communicate between Controllers and network devices

NEW QUESTION: 23
When a next-generation endpoint security solution is selected for a company, what are two key deliverables that help justify the implementation? (Choose two.)
A. continuous monitoring of all files that are located on connected endpoints
B. signature-based endpoint protection on company endpoints
C. macro-based protection to keep connected endpoints safe
D. email integration to protect endpoints from malicious content that is located in email
E. real-time feeds from global threat intelligence centers
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 24
How is Cisco Umbrella configured to log only security events?
A. per policy
B. in the Reporting settings
C. in the Security Settings section
D. per network in the Deployments section
Answer: A (LEAVE A REPLY)
The logging of your identities' activities is set per-policy when you first create a policy. By default, logging is on and set to log all requests an identity makes to reach destinations. At any time after you create a policy, you can change what level of identity activity Umbrella logs. From the Policy wizard, log settings are: Log All Requests-For full logging, whether for content, security or otherwise Log Only Security Events-For security logging only, which gives your users more privacy-a good setting for people with the roaming client installed on personal devices Don't Log Any Requests-Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on. Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management From the Policy wizard, log settings are:
Log All Requests-For full logging, whether for content, security or otherwise Log Only Security Events-For security logging only, which gives your users more privacy-a good setting for people with the roaming client installed on personal devices Don't Log Any Requests-Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on.
The logging of your identities' activities is set per-policy when you first create a policy. By default, logging is on and set to log all requests an identity makes to reach destinations. At any time after you create a policy, you can change what level of identity activity Umbrella logs. From the Policy wizard, log settings are: Log All Requests-For full logging, whether for content, security or otherwise Log Only Security Events-For security

logging only, which gives your users more privacy-a good setting for people with the roaming client installed on personal devices Don't Log Any Requests-Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on. Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management

NEW QUESTION: 25
What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?
A. It alerts users when the WSA decrypts their traffic.
B. It decrypts HTTPS application traffic for unauthenticated users.
C. It decrypts HTTPS application traffic for authenticated users.
D. It provides enhanced HTTPS application detection for AsyncOS.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 26
A user has a device in the network that is receiving too many connection requests from multiple machines. Which type of attack is the device undergoing?
A. phishing
B. pharming
C. SYN flood
D. slowloris
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
Which option is the main function of Cisco Firepower impact flags?
A. They alert administrators when critical events occur.
B. They identify data that the ASA sends to the Firepower module.
C. They correlate data about intrusions and vulnerability.
D. They highlight known and suspected malicious IP addresses in reports.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?
A. SIEM
B. CASB
C. Adaptive MFA
D. Cisco Cloudlock
Answer: (SHOW ANSWER)
+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy. + Cloudlock is API-based. + Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy

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

NEW QUESTION: 29
What is a feature of the open platform capabilities of Cisco DNA Center?
A. application adapters
B. automation adapters
C. domain integration
D. intent-based APIs
Answer: D (LEAVE A REPLY)

NEW QUESTION: 30
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: A,B (LEAVE A REPLY)

NEW QUESTION: 31

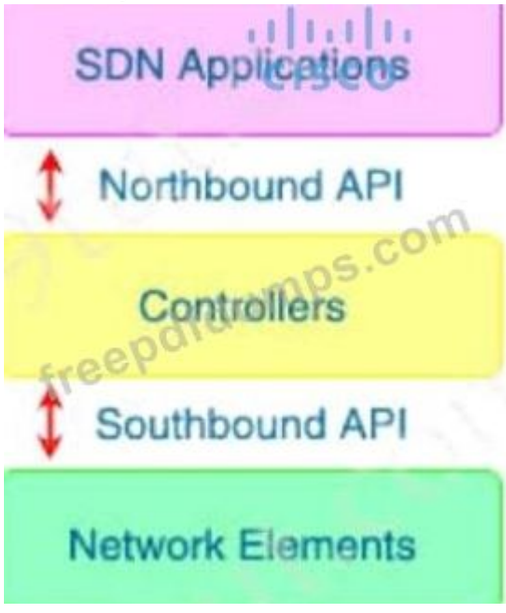
What is the difference between Cross-site Scripting and SQL Injection, attacks?
A. Cross-site Scripting is an attack where code is injected into a database, whereas SQL Injection is an attack where code is injected into a browser.
B. Cross-site Scripting is a brute force attack targeting remote sites, 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: A (LEAVE A REPLY)
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: 32
Which direction do attackers encode data in DNS requests during exfiltration using DNS tunneling?
A. north-south
B. outbound
C. east-west
D. inbound
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
Which function is the primary function of Cisco AMP threat Grid?
A. automated email encryption
B. monitoring network traffic
C. automated malware analysis
D. applying a real-time URI blacklist
Answer: C (LEAVE A REPLY)

NEW QUESTION: 34
When planning a VPN deployment, for which reason does an engineer opt for an active/active FlexVPN configuration as opposed to DMVPN?
A. Multiple routers or VRFs are required.
B. Floating static routes are required.
C. HSRP is used for faliover.
D. Traffic is distributed statically by default.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
Which type of API is being used when a controller within a software-defined network architecture dynamically makes configuration changes on switches within the network?
A. westbound AP
B. southbound API
C. northbound API
D. eastbound API
Answer: B (LEAVE A REPLY)
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs.



NEW QUESTION: 36
Which industry standard is used to integrate Cisco ISE and pxGrid to each other and with other interoperable security platforms?
A. ANSI
B. NIST
C. IEEE
D. IETF
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37
An engineer is implementing NTP authentication within their network and has configured both the client and server devices with the command ntp authentication-key 1 md5 Cisc392368270. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however it is unable to do so. Which command is required to enable the client to accept the server's authentication key?
A. ntp peer 1.1.1.1 key 1
B. ntp server 1.1.1.1 key 1
C. ntp server 1.1.1.2 key 1
D. ntp peer 1.1.1.2 key 1
Answer: B (LEAVE A REPLY)
To configure an NTP enabled router to require authentication when other devices connect to it, use the following commands:
NTP_Server(config)#ntp authentication-key 2 md5 securitytut
NTP_Server(config)#ntp authenticate
NTP_Server(config)#ntp trusted-key 2
Then you must configure the same authentication-key on the client router:
NTP_Client(config)#ntp authentication-key 2 md5 securitytut
NTP_Client(config)#ntp authenticate
NTP_Client(config)#ntp trusted-key 2
NTP_Client(config)#ntp server 10.10.10.1 key 2
Note: To configure a Cisco device as a NTP client, use the command ntp server <IP address>. For example: Router(config)#ntp server 10.10.10.1. This command will instruct the router to query 10.10.10.1 for the time.

NEW QUESTION: 38
An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?
A. Cisco Umbrella
B. Cisco Cloud Email Security
C. Cisco NGFW
D. Cisco Cloudlock

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

NEW QUESTION: 39
What are two differences between a Cisco WSA that is running in transparent mode and one running in explicit mode? (Choose two)
A. When the Cisco WSA is running in transparent mode, it uses the WSA's own IP address as the HTTP request destination.
B. The Cisco WSA responds with its own IP address only if it is running in explicit mode.
C. The Cisco WSA is configured in a web browser only if it is running in transparent mode.
D. The Cisco WSA uses a Layer 3 device to redirect traffic only if it is running in transparent mode.
E. The Cisco WSA responds with its own IP address only if it is running in transparent mode.
Answer: (SHOW ANSWER)
The Cisco Web Security Appliance (WSA) includes a web proxy, a threat analytics engine, antimalware engine, policy management, and reporting in a single physical or virtual appliance. The main use of the Cisco WSA is to protect users from accessing malicious websites and being infected by malware.
You can deploy the Cisco WSA in two different modes:
- Explicit forward mode
- Transparent mode
In explicit forward mode, the client is configured to explicitly use the proxy, subsequently sending all web traffic to the proxy. Because the client knows there is a proxy and sends all traffic to the proxy in explicit forward mode, the client does not perform a DNS lookup of the domain before requesting the URL. The Cisco WSA is responsible for DNS resolution, as well.
When you configure the Cisco WSA in explicit mode, you do not need to configure any other network infrastructure devices to redirect client requests to the Cisco WSA. However, you must configure each client to send traffic to the Cisco WSA. -> Therefore in explicit mode, WSA only checks the traffic between client & web server. WSA does not use its own IP address to request -> Answer B is not correct. When the Cisco WSA is in transparent mode, clients do not know there is a proxy deployed. Network infrastructure devices are configured to forward traffic to the Cisco WSA. In transparent mode deployments, network infrastructure devices redirect web traffic to the proxy. Web traffic redirection can be done using policybased routing (PBR)-available on many routers -or using Cisco's Web Cache Communication Protocol (WCCP) on Cisco ASA, Cisco routers, or switches. The Web Cache Communication Protocol (WCCP), developed by Cisco Systems, specifies interactions between one or more switches) and one or more web-caches. The purpose of the interaction is to establish and maintain the transparent redirectio of traffic flowing through a group of routers.
Reference: https://www.cisco.com/c/en/us/tech/content-networking/web-cache-communications-protocol-

wccp/index.html ->Therefore answer D is correct as redirection can be done on Layer 3 device only. In transparent mode, the client is unaware its traffic is being sent to a proxy (Cisco WSA) and, as a result, the client uses DNS to resolve the domain name in the URL and send the web request destined for the web server (not the proxy). When you configure the Cisco WSA in transparent mode, you need to identify a network choke point with a redirection device (a Cisco ASA) to redirect traffic to the proxy.
infrastructure devices to redirect client requests to the Cisco WSA. However, you must configure each client to send traffic to the Cisco WSA.
-> Therefore in explicit mode, WSA only checks the traffic between client & web server. WSA does not use its own IP address to request -> Answer B is not correct.
When the Cisco WSA is in transparent mode, clients do not know there is a proxy deployed. Network infrastructure devices are configured to forward traffic to the Cisco WSA. In transparent mode deployments, network infrastructure devices redirect web traffic to the proxy. Web traffic redirection can be done using policybased routing (PBR)-available on many routers -or using Cisco's Web Cache Communication Protocol (WCCP) on Cisco ASA, Cisco routers, or switches.
The Web Cache Communication Protocol (WCCP), developed by Cisco Systems, specifies interactions between one or more switches) and one or more web-caches. The purpose of the interaction is to establish and maintain the transparent redirectio of traffic flowing through a group of routers.
Reference:
->Therefore answer D is correct as redirection can be done on Layer 3 device only.
When you configure the Cisco WSA in explicit mode, you do not need to configure any other network infrastructure devices to redirect client requests to the Cisco WSA. However, you must configure each client to send traffic to the Cisco WSA. -> Therefore in explicit mode, WSA only checks the traffic between client & web server. WSA does not use its own IP address to request -> Answer B is not correct. When the Cisco WSA is in transparent mode, clients do not know there is a proxy deployed. Network infrastructure devices are configured to forward traffic to the Cisco WSA. In transparent mode deployments, network infrastructure devices redirect web traffic to the proxy. Web traffic redirection can be done using policybased routing (PBR)-available on many routers -or using Cisco's Web Cache Communication Protocol (WCCP) on Cisco ASA, Cisco routers, or switches. The Web Cache Communication Protocol (WCCP), developed by Cisco Systems, specifies interactions between one or more switches) and one or more web-caches. The purpose of the interaction is to establish and maintain the transparent redirectio of traffic flowing through a group of routers.
Reference: https://www.cisco.com/c/en/us/tech/content-networking/web-cache-communications-protocol-wccp/index.html ->Therefore answer D is correct as redirection can be done on Layer 3 device only. In transparent mode, the client is unaware its traffic is being sent to a proxy (Cisco WSA) and, as a result, the client uses DNS to resolve the domain name in the URL and send the web request destined for the web server (not the proxy). When you configure the Cisco WSA in transparent mode, you need to identify a network choke point with a redirection device (a Cisco ASA) to redirect traffic to the proxy.
WSA in Transparent mode
-> Therefore in Transparent mode, WSA uses its own IP address to initiate a new connection the Web Server (in step 4 above) -> Answer E is correct.
Answer C is surely not correct as WSA cannot be configured in a web browser in either mode.

Answer A seems to be correct but it is not. This answer is correct if it states "When the Cisco WSA is running in transparent mode, it uses the WSA's own IP address as the HTTP request source" (not destination).

NEW QUESTION: 40
Which solution is made from a collection of secure development practices and guidelines that developers must follow to build secure applications?
A. OWASP
B. Fuzzing Framework
C. Radamsa
D. AFL
Answer: (SHOW ANSWER)

NEW QUESTION: 41
What features does Cisco FTDv provide over ASAv?
A. Cisco FTDv runs on VMWare while ASAv does not
B. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not
C. Cisco FTDv supports URL filtering while ASAv does not
D. Cisco FTDv runs on AWS while ASAv does not
Answer: C (LEAVE A REPLY)

NEW QUESTION: 42
Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?
A. OpenC2
B. OpenIOC
C. CybOX
D. STIX
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
Which technology must be used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?
A. DMVPN
B. FlexVPN
C. IPsec DVTI
D. GET VPN
Answer: D (LEAVE A REPLY)
Cisco's Group Encrypted Transport VPN (GETVPN) introduces the concept of a trusted group to eliminate point-to-point tunnels and their associated overlay routing. All group members (GMs) share a common security association (SA), also known as a group SA. This enables GMs to decrypt traffic that was encrypted by any other GM. GETVPN provides instantaneous large-scale any-to-any IP connectivity using a group IPsec

security paradigm. Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/ GETVPN_DIG_version_2_0_External.pdf

NEW QUESTION: 44
Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?
A. Contiv
B. Docker
C. Lambda
D. SDLC
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or Microsoft vSwitch?
A. inter-VLAN security
B. intra-EPG isolation
C. placement in separate EPGs
D. inter-EPG isolation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
Which RADIUS attribute can you use to filter MAB requests in an 802.1 x deployment?
A. 1
B. 2
C. 6
D. 31
Answer: C (LEAVE A REPLY)
Because MAB uses the MAC address as a username and password, you should make sure that the RADIUS server can differentiate MAB requests from other types of requests for network access. This precaution will prevent other clients from attempting to use a MAC address as a valid credential. Cisco switches uniquely identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB Access-Request message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server. Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networkingservices/config_guide_c17-663759.html identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB Access-Request message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server.
Because MAB uses the MAC address as a username and password, you should make sure that the RADIUS server can differentiate MAB requests from other types of requests for network access. This precaution will prevent other clients from attempting to use a MAC address as a valid credential. Cisco switches uniquely

identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB Access-Request message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server. Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networkingservices/config_guide_c17-663759.html

NEW QUESTION: 47
Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two)
A. DHCP
B. sFlow
C. RADIUS
D. SMTP
E. TACACS+
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?
A. Dynamic ARP Inspection
B. fingerprinting
C. RADIUS-based REAP
D. multifactor authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 49
An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation. What must be un solution?
A. L2TP is an IP packet encapsulation protocol, and GRE over IPsec is a tunneling protocol.
B. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701.
C. GRE over IPsec cannot be used as a standalone protocol, and L2TP can.
D. GRE over IPsec adds its own header, and L2TP does not.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?
A. network address translations
B. time synchronization
C. quality of service
D. intrusion policy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
An organization is implementing URL blocking using Cisco Umbrell
a. The users are able to go to some sites
but other sites are not accessible due to an error. Why is the error occurring?
A. Client computers do not have the Cisco Umbrella Root CA certificate installed.
B. IP-Layer Enforcement is not configured.
C. Client computers do not have an SSL certificate deployed from an internal CA server.
D. Intelligent proxy and SSL decryption is disabled in the policy
Answer: A (LEAVE A REPLY)
Other features are dependent on SSL Decryption functionality, which requires the Cisco Umbrella root certificate. Having the SSL Decryption feature improves: Custom URL Blocking-Required to block the HTTPS version of a URL. ... Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed. Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you may wish to prevent it from appearing. To avoid these error pages, install the Cisco Umbrella root certificate into your browser or the browsers of your users-if you're a network admin. Reference: https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information certificate. Having the SSL Decryption feature improves:
Custom URL Blocking-Required to block the HTTPS version of a URL.
...
Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed. Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you may wish to prevent it from appearing.
To avoid these error pages, install the Cisco Umbrella root certificate into your browser or the browsers of your users-if you're a network admin.

Other features are dependent on SSL Decryption functionality, which requires the Cisco Umbrella root certificate. Having the SSL Decryption feature improves: Custom URL Blocking-Required to block the HTTPS version of a URL. ... Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed. Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you may wish to prevent it from appearing. To avoid these error pages, install the Cisco Umbrella root certificate into your browser or the browsers of your users-if you're a network admin. Reference: https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information

NEW QUESTION: 52
Which type of protection encrypts RSA keys when they are exported and imported?
A. passphrase
B. NGE
C. nonexportable
D. file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 53
Which feature within Cisco ISE verifies the compliance of an endpoint before providing access to the network?
A. Profiling
B. Posture
C. MAB
D. pxGrid
Answer: (SHOW ANSWER)

NEW QUESTION: 54
What is managed by Cisco Security Manager?
A. access point
B. WSA
C. ASA
D. ESA
Answer: C (LEAVE A REPLY)
Cisco Security Manager provides a comprehensive management solution for: - Cisco ASA 5500 Series Adaptive Security Appliances - Cisco intrusion prevention systems 4200 and 4500 Series Sensors - Cisco AnyConnect Secure Mobility Client Reference: https://www.cisco.com/c/en/us/products/security/security-manager/index.html
- Cisco ASA 5500 Series Adaptive Security Appliances

- Cisco intrusion prevention systems 4200 and 4500 Series Sensors
- Cisco AnyConnect Secure Mobility Client
Cisco Security Manager provides a comprehensive management solution for: - Cisco ASA 5500 Series Adaptive Security Appliances - Cisco intrusion prevention systems 4200 and 4500 Series Sensors - Cisco AnyConnect Secure Mobility Client Reference: https://www.cisco.com/c/en/us/products/security/security-manager/index.html

NEW QUESTION: 55
What does Cisco AMP for Endpoints use to help an organization detect different families of malware?
A. Ethos Engine to perform fuzzy fingerprinting
B. Tetra Engine to detect malware when me endpoint is connected to the cloud
C. Clam AV Engine to perform email scanning
D. Spero Engine with machine learning to perform dynamic analysis
Answer: A (LEAVE A REPLY)
ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected.
Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf ETHOS = Fuzzy Fingerprinting using static/passive heuristics a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected.
Reference:
ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected.
Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf ETHOS = Fuzzy Fingerprinting using static/passive heuristics

NEW QUESTION: 56
Which two capabilities does TAXII support? (Choose two)
A. Exchange
B. Pull messaging
C. Binding
D. Correlation
E. Mitigating
Answer: (SHOW ANSWER)
The Trusted Automated eXchangeof Indicator Information (TAXII) specifies mechanisms for exchanging structured cyber threat information between parties over the network.
TAXII exists to provide specific capabilities to those interested in sharing structured cyber threat information.
TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilities that this version of TAXII supports: push messaging, pull messaging, and discovery.
Although there is no "binding" capability in the list but it is the best answer here.

NEW QUESTION: 57

Where are individual sites specified to be blacklisted in Cisco Umbrella?

A. application settings

B. content categories

C. security settings

D. destination lists

Answer: D (LEAVE A REPLY)

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

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

NEW QUESTION: 58

An organization wants to provide visibility and to identify active threats in its network using a VM. The organization wants to extract metadata from network packet flow while ensuring that payloads are not retained or transferred outside the network. Which solution meets these requirements?

A. Cisco Umbrella Cloud

B. Cisco Stealthwatch Cloud PNM

C. Cisco Stealthwatch Cloud PCM

D. Cisco Umbrella On-Premises

Answer: B (LEAVE A REPLY)

Private Network Monitoring (PNM) provides visibility and threat detection for the on-premises network, delivered from the cloud as a SaaS solution. It is the perfect solution for organizations who prefer SaaS products and desire better awareness and security in their on-premises environments while reducing capital expenditure and operational overhead. It works by deploying lightweight software in a virtual machine or server that can consume a variety of native sources of telemetry or extract metadata from network packet flow. It encrypts this metadata and sends it to the Stealthwatch Cloud analytics platform for analysis. Stealthwatch Cloud consumes metadata only. The packet payloads are never retained or transferred outside the network. This lab focuses on how to configure a Stealthwatch Cloud Private Network Monitoring (PNM) Sensor, in order to provide visibility and effectively identify active threats, and monitors user and device behavior within onpremises networks. The Stealthwatch Cloud PNM Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on

hardware running a number of different Linux-based operating systems. Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf operational overhead. It works by deploying lightweight software in a virtual machine or server that can consume a variety of native sources of telemetry or extract metadata from network packet flow. It encrypts this metadata and sends it to the Stealthwatch Cloud analytics platform for analysis. Stealthwatch Cloud consumes metadata only. The packet payloads are never retained or transferred outside the network.
This lab focuses on how to configure a Stealthwatch Cloud Private Network Monitoring (PNM) Sensor, in order to provide visibility and effectively identify active threats, and monitors user and device behavior within onpremises networks.
The Stealthwatch Cloud PNM Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.
Private Network Monitoring (PNM) provides visibility and threat detection for the on-premises network, delivered from the cloud as a SaaS solution. It is the perfect solution for organizations who prefer SaaS products and desire better awareness and security in their on-premises environments while reducing capital expenditure and operational overhead. It works by deploying lightweight software in a virtual machine or server that can consume a variety of native sources of telemetry or extract metadata from network packet flow. It encrypts this metadata and sends it to the Stealthwatch Cloud analytics platform for analysis. Stealthwatch Cloud consumes metadata only. The packet payloads are never retained or transferred outside the network.
This lab focuses on how to configure a Stealthwatch Cloud Private Network Monitoring (PNM) Sensor, in order to provide visibility and effectively identify active threats, and monitors user and device behavior within onpremises networks. The Stealthwatch Cloud PNM Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems. Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf

NEW QUESTION: 59
What is a commonality between DMVPN and FlexVPN technologies?
A. FlexVPN and DMVPN use IS-IS routing protocol to communicate with spokes
B. FlexVPN and DMVPN use the new key management protocol
C. FlexVPN and DMVPN use the same hashing algorithms
D. IOS routers run the same NHRP code for DMVPN and FlexVPN
Answer: (SHOW ANSWER)
In its essence, FlexVPN is the same as DMVPN. Connections between devices are still point-to-point GRE tunnels, spoke-to-spoke connectivity is still achieved with NHRP redirect message, IOS routers even run the same NHRP code for both DMVPN and FlexVPN, which also means that both are Cisco's proprietary technologies. Reference: https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/ In its essence, FlexVPN is the same as DMVPN. Connections between devices are still point-to-point GRE tunnels, spoke-to-spoke connectivity is still achieved with NHRP redirect message, IOS routers even run the same NHRP code

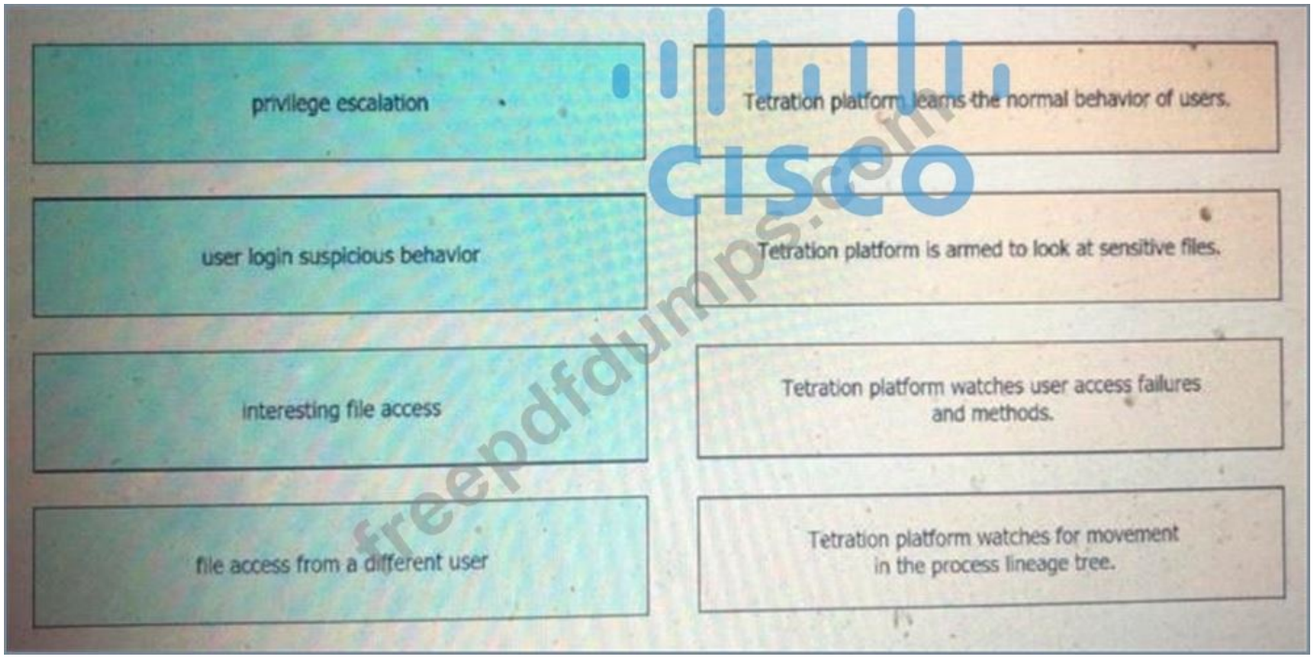
for both DMVPN and FlexVPN, which also means that both are Cisco's proprietary technologies. Reference: https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/

NEW QUESTION: 60
Which two mechanisms are used to control phishing attacks? (Choose two)
A. Enable browser alerts for fraudulent websites.
B. Revoke expired CRL of the websites.
C. Define security group memberships.
D. Use antispyware software.
E. Implement email filtering techniques.
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 61
Which encryption algorithm provides highly secure VPN communications?
A. DES
B. 3DES
C. AES 128
D. AES 256
Answer: D (LEAVE A REPLY)

NEW QUESTION: 62
Which CLI command is used to register a Cisco FirePower sensor to Firepower Management Center?
A. configure system add <host><key>
B. configure manager delete
C. configure manager add <host><key
D. configure manager <key> add host
Answer: C (LEAVE A REPLY)

NEW QUESTION: 63
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.



Answer:

NEW QUESTION: 64

An engineer is configuring web filtering for a network using Cisco Umbrella Secure Internet Gateway. The requirement is that all traffic needs to be filtered. Using the SSL decryption feature, which type of certificate should be presented to the end-user to accomplish this goal?

A. SubCA

B. self-signed

C. third-party

D. organization owned root

Answer: D (LEAVE A REPLY)

NEW QUESTION: 65

Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

url = 'https://api.amp.cisco.com/v1/computers'

response = requests.get(url, auth=(client_id, api_key))

response_json = response.json()

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

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

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

B. create an SNMP pull mechanism for managing AMP

C. gather network telemetry information from AMP for endpoints

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

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 66

How does a cloud access security broker function?

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

NEW QUESTION: 67
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: 68
How many interfaces per bridge group does an ASA bridge group deployment support?
A. up to 2
B. up to 4
C. up to 8
D. up to 16
Answer: B (LEAVE A REPLY)
Each of the ASAs interfaces need to be grouped into one or more bridge groups. Each of these groups acts as an independent transparent firewall. It is not possible for one bridge group to communicate with another bridge group without assistance from an external router.
As of 8.4(1) upto 8 bridge groups are supported with 2-4 interface in each group. Prior to this only one bridge group was supported and only 2 interfaces.
Up to 4 interfaces are permitted per bridge-group (inside, outside, DMZ1, DMZ2)

NEW QUESTION: 69
Refer to the exhibit.

An administrator is adding a new Cisco FTD device to their network and wants to manage it with Cisco FMC. The Cisco FTD is not behind a NAT device. Which command is needed to enable this on the Cisco FTD?

A. configure manager add DONTRESOLVE kregistration key>

B. configure manager add <FMC IP address> <registration key> 16

C. configure manager add DONTRESOLVE <registration key> FTD123

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

Answer: D (LEAVE A REPLY)

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

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

NEW QUESTION: 70

How does a WCCP-configured router identify if the Cisco WSA is functional?

A. The WSA sends a Here-I-Am message every 10 seconds, and the router acknowledges with an ISee-You message.

B. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the WSA.

C. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the router.

D. The router sends a Here-I-Am message every 10 seconds, and the WSA acknowledges with an ISee-You message.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 71
Which algorithm provides asymmetric encryption?
A. 3DES
B. RC4
C. RSA
D. AES
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72
Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?
A. File Analysis
B. SafeSearch
C. SSL Decryption
D. Destination Lists
Answer: C (LEAVE A REPLY)
SSL Decryption is an important part of the Umbrella Intelligent Proxy. he feature allows the Intelligent Proxy to go beyond simply inspecting normal URLs and actually proxy and inspect traffic that's sent over HTTPS. The SSL Decryption feature does require the root certificate be installed. Reference: https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-IntelligentProxy SSL Decryption is an important part of the Umbrella Intelligent Proxy. he feature allows the Intelligent Proxy to go beyond simply inspecting normal URLs and actually proxy and inspect traffic that's sent over HTTPS. The SSL Decryption feature does require the root certificate be installed. Reference: https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-IntelligentProxy

NEW QUESTION: 73
Which deployment model is the most secure when considering risks to cloud adoption?
A. Hybrid Cloud
B. Private Cloud
C. Community Cloud
D. Public Cloud
Answer: (SHOW ANSWER)

NEW QUESTION: 74
What are two security benefits of an MDM deployment? (Choose two.)
A. privacy control checks
B. distributed dashboard
C. on-device content management
D. distributed software upgrade
E. robust security policy enforcement

Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 75

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

A. insecure implementation of API

B. vulnerabilities within protocol

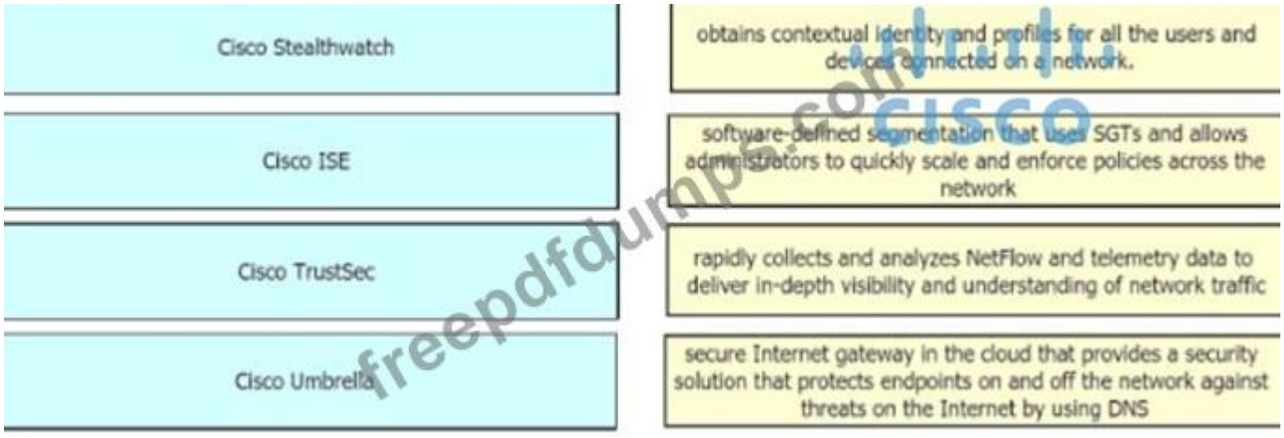
C. intermittent connection to the cloud connectors

D. misconfiguration of infrastructure, which allows unauthorized access

Answer: B (LEAVE A REPLY)

NEW QUESTION: 76

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



Answer:

NEW QUESTION: 77
Which Cisco AMP feature allows an engineer to look back to trace past activities, such as file and process activity on an endpoint?
A. endpoint isolation
B. advanced search
C. retrospective security
D. advanced investigation
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Which Cisco ISE service checks the compliance of endpoints before allowing the endpoints to connect to the network?
A. Threat Centric NAC
B. Cisco TrustSec
C. posture
D. profiler
Answer: C (LEAVE A REPLY)

NEW QUESTION: 79
Which IETF attribute is supported for the RADIUS CoA feature?
A. 30 Calling-Station-ID
B. 81 Message-Authenticator
C. 24 State
D. 42 Acct-Session-ID
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
Which feature is leveraged by advanced antimalware capabilities to be an effective endpomt protection platform?
A. sandboxing
B. big data
C. storm centers
D. blocklisting
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two)
A. packet decoder
B. SIP
C. modbus

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

NEW QUESTION: 82
Which benefit does DMVPN provide over GETVPN?
A. DMVPN supports non-IP protocols, and GETVPN supports only IP protocols.
B. DMVPN is a tunnel-less VPN, and GETVPN is tunnel-based.
C. DMVPN can be used over the public Internet, and GETVPN requires a private network.
D. DMVPN supports QoS, multicast, and routing, and GETVPN supports only QoS.
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Which Cisco AMP file disposition valid?
A. pristine
B. dirty
C. malware
D. non malicious
Answer: C (LEAVE A REPLY)

NEW QUESTION: 84
What is the difference between deceptive phishing and spear phishing?
A. Deceptive phishing is an attacked aimed at a specific user in the organization who holds a C-level role.
B. A spear phishing campaign is aimed at a specific person versus a group of people.
C. Spear phishing is when the attack is aimed at the C-level executives of an organization.
D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.
Answer: B (LEAVE A REPLY)
In deceptive phishing, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.
Spear phishing is carefully designed to get a single recipient to respond. Criminals select an individual target within an organization, using social media and other public information - and craft a fake email tailored for that person.

NEW QUESTION: 85
What are two things to consider when using PAC files with the Cisco WSA? (Choose two.)
A. The WSA hosts PAC files on port 9001 by default.
B. By default, they direct traffic through a proxy when the PC and the host are on the same subnet.
C. PAC files use if-else statements to determine whether to use a proxy or a direct connection for traffic between the PC and the host.
D. The WSA hosts PAC files on port 6001 by default.
E. If the WSA host port is changed, the default port redirects web traffic to the correct port automatically.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 86
An organization is receiving SPAM emails from a known malicious domain. What must be configured in order to prevent the session during the initial TCP communication?
A. Configure the Cisco ESA to drop the malicious emails
B. Configure the Cisco ESA to reset the TCP connection
C. Configure policies to stop and reject communication
D. Configure policies to quarantine malicious emails
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
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 Terminate
B. CoA Reauth
C. Port Bounce
D. CoA Session Query

Answer: B (LEAVE A REPLY)

NEW QUESTION: 88
Refer to the exhibit. What does this Python script accomplish?
A. It authenticates to a Cisco ISE server using the username of ersad
B. It authenticates to a Cisco ISE with an SSH connection.
C. It allows authentication with TLSv1 SSL protocol
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
What are two ways that Cisco Container Platform provides value to customers who utilize cloud service providers? (Choose two.)
A. manages Kubernetes clusters
B. Allows developers to create code once and deploy to multiple clouds
C. manages Docker containers
D. helps maintain source code for cloud deployments
E. Creates complex tasks for managing code
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 90
Why should organizations migrate to an MFA strategy for authentication?
A. Biometrics authentication leads to the need for MFA due to its ability to be hacked easily.
B. Single methods of authentication can be compromised more easily than MFA.
C. MFA methods of authentication are never compromised.
D. MFA does not require any piece of evidence for an authentication mechanism.
Answer: (SHOW ANSWER)

NEW QUESTION: 91
What must be used to share data between multiple security products?
A. Cisco Rapid Threat Containment
B. Cisco Advanced Malware Protection
C. Cisco Platform Exchange Grid
D. Cisco Stealthwatch Cloud
Answer: C (LEAVE A REPLY)

NEW QUESTION: 92
What is an attribute of the DevSecOps process?
A. mandated security controls and check lists
B. security scanning and theoretical vulnerabilities
C. development security
D. isolated security team
Answer: C (LEAVE A REPLY)
DevSecOps (development, security, and operations) is a concept used in recent years to describe how to move security activities to the start of the development life cycle and have built-in security practices in the continuous integration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer to IT and business objectives.
Three key things make a real DevSecOps environment:
+ Security testing is done by the development team.
+ Issues found during that testing is managed by the development team.
+ Fixing those issues stays within the development team.

NEW QUESTION: 93
How does Cisco Advanced Phishing Protection protect users?
A. It validates the sender by using DKIM.
B. It determines which identities are perceived by the sender
C. It utilizes sensors that send messages securely.
D. It uses machine learning and real-time behavior analytics.
Answer: (SHOW ANSWER)
Cisco Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to protect against identity deception-based threats. Reference: https://docs.ces.cisco.com/docs/advanced-phishing-protection Cisco Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advanced machine learning techniques, real-time behavior analytics, relationship modeling, and telemetry to protect against identity deception-based threats. Reference: https://docs.ces.cisco.com/docs/advanced-phishing-protection

NEW QUESTION: 94
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 Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp3880782430

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

identity {address | hostname}. The following example uses preshared keys at two peers and sets both their ISAKMP identities to the IP address.

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

crypto isakmp identity address

crypto isakmp key sharedkeystring address 192.168.1.33

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

crypto isakmp identity address

crypto isakmp key sharedkeystring address 10.0.0.1

Reference:

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

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

The command "crypto isakmp identity address 172.19.20.24" is not valid. We can only use "crypto isakmp identity {address | hostname}. The following example uses preshared keys at two peers and sets both their ISAKMP identities to the IP address. At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified: crypto isakmp identity address crypto isakmp key sharedkeystring address 192.168.1.33 At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified: crypto isakmp identity address crypto isakmp key sharedkeystring address 10.0.0.1 Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp3880782430

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

NEW QUESTION: 95

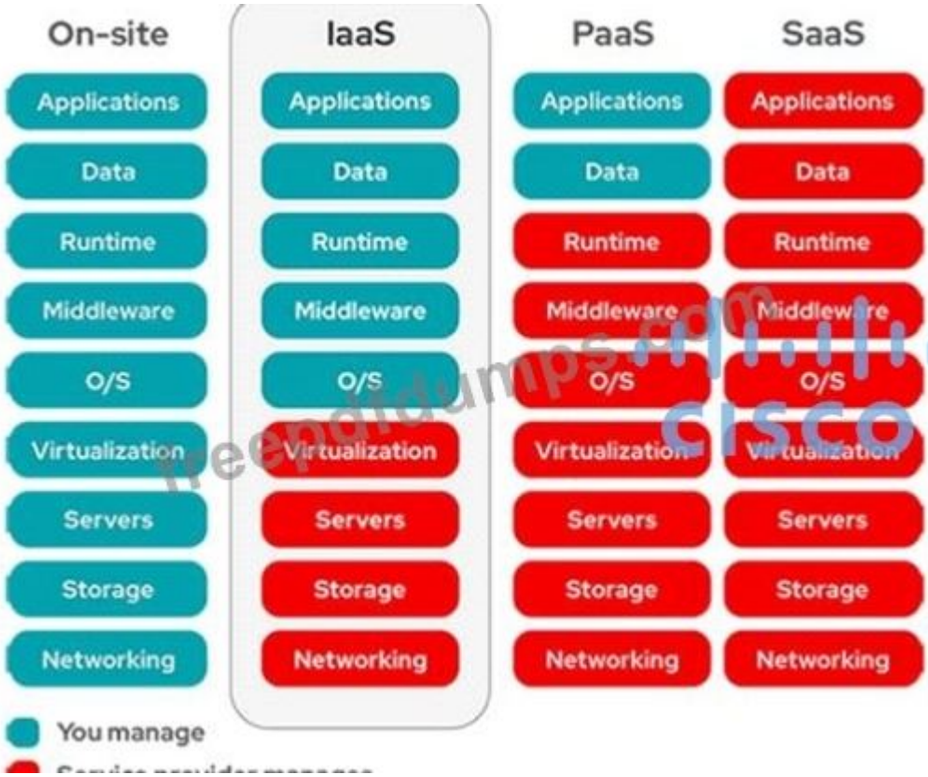
Refer to the exhibit. Which configuration item makes it possible to have the AAA session on the network?

A. aaa authentication login console ise

B. aaa authorization network default group ise
C. aaa authentication enable default enable
D. aaa authorization exec default ise
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?
A. Advanced Malware Protection
B. Platform Exchange Grid
C. Multifactor Platform Integration
D. Firepower Threat Defense
Answer: B (LEAVE A REPLY)
With Cisco pxGrid (Platform Exchange Grid), your multiple security products can now share data and work together. This open, scalable, and IETF standards-driven platform helps you automate security to get answers and contain threats faster.

NEW QUESTION: 97
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two)
A. virtualization
B. middleware
C. operating systems
D. applications
E. data
Answer: (SHOW ANSWER)
Customers must manage applications and data in PaaS.



NEW QUESTION: 98
An organization wants to secure users, data, and applications in the cloud. The solution must be API-based and operate as a cloud-native CASB. Which solution must be used for this implementation?
A. Cisco Cloudlock
B. Cisco Cloud Email Security
C. Cisco Firepower Next-Generation Firewall
D. Cisco Umbrella
Answer: A (LEAVE A REPLY)
Cisco Cloudlock: Secure your cloud users, data, and applications with the cloud-native Cloud Access Security Broker (CASB) and cloud cybersecurity platform. Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45-738565.pdf 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. Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45-738565.pdf

NEW QUESTION: 99
Which Cisco platform processes behavior baselines, monitors for deviations, and reviews for malicious processes in data center traffic and servers while performing software vulnerability detection?
A. Cisco AnyConnect
B. Cisco AMP for Network

C. Cisco Tetration
D. Cisco ISE?
Answer: B (LEAVE A REPLY)

NEW QUESTION: 100
Refer to the exhibit. When creating an access rule for URL filtering, a network engineer adds certain categories and individual URLs to block. What is the result of the configuration?
A. Only URLs for botnets with reputation scores of 3-5 will be blocked.
B. Only URLs for botnets with reputation scores of 1-3 will be blocked.
C. Only URLs for botnets with a reputation score of 3 will be blocked.
D. Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked.
Answer: (SHOW ANSWER)

NEW QUESTION: 101
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: 102
In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?
A. Smurf
B. distributed denial of service
C. cross-site scripting
D. rootkit exploit
Answer: C (LEAVE A REPLY)
Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.
Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on.
For example the code below is written in hex: <a

href=javascript:alert&#
x28'XSS')>Click Here
is equivalent to:
Click Here
Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form.

NEW QUESTION: 103
An engineer is implementing Cisco CES in an existing Microsoft Office 365 environment and must route inbound email to Cisco CE.. record must be modified to accomplish this task?
A. CNAME
B. MX
C. DKIM
D. SPF
Answer: (SHOW ANSWER)

NEW QUESTION: 104
A network engineer must monitor user and device behavior within the on-premises network. This data must be sent to the Cisco Stealthwatch Cloud analytics platform for analysis. What must be done to meet this requirement using the Ubuntu-based VM appliance deployed in a VMware-based hypervisor?
A. Configure a Cisco FMC to send syslogs to Cisco Stealthwatch Cloud
B. Deploy the Cisco Stealthwatch Cloud PNM sensor that sends data to Cisco Stealthwatch Cloud
C. Deploy a Cisco FTD sensor to send network events to Cisco Stealthwatch Cloud
D. Configure a Cisco FMC to send NetFlow to Cisco Stealthwatch Cloud
Answer: B (LEAVE A REPLY)
The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems. Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems.
The Stealthwatch Cloud Private Network Monitoring (PNM) Sensor is an extremely flexible piece of technology, capable of being utilized in a number of different deployment scenarios. It can be deployed as a complete Ubuntu based virtual appliance on different hypervisors (e.g. -VMware, VirtualBox). It can be deployed on hardware running a number of different Linux-based operating systems. Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf

NEW QUESTION: 105
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. deployment
B. consumption
C. authoring
D. sharing
Answer: A (LEAVE A REPLY)

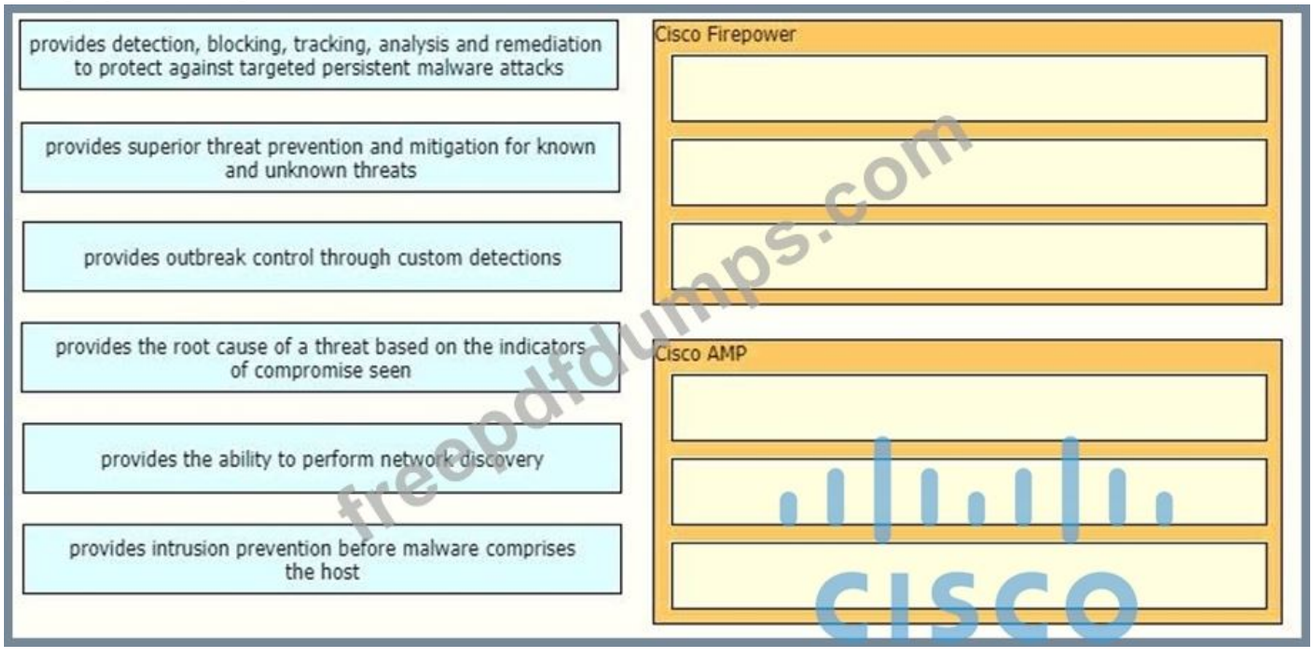
NEW QUESTION: 106
Which benefit does endpoint security provide the overall security posture of an organization?
A. It allows the organization to detect and respond to threats at the edge of the network.
B. It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.
C. It streamlines the incident response process to automatically perform digital forensics on the endpoint.
D. It allows the organization to mitigate web-based attacks as long as the user is active in the domain.
Answer: (SHOW ANSWER)

NEW QUESTION: 107
Which type of algorithm provides the highest level of protection against brute-force attacks?
A. MD5
B. SHA
C. HMAC
D. PFS
Answer: (SHOW ANSWER)

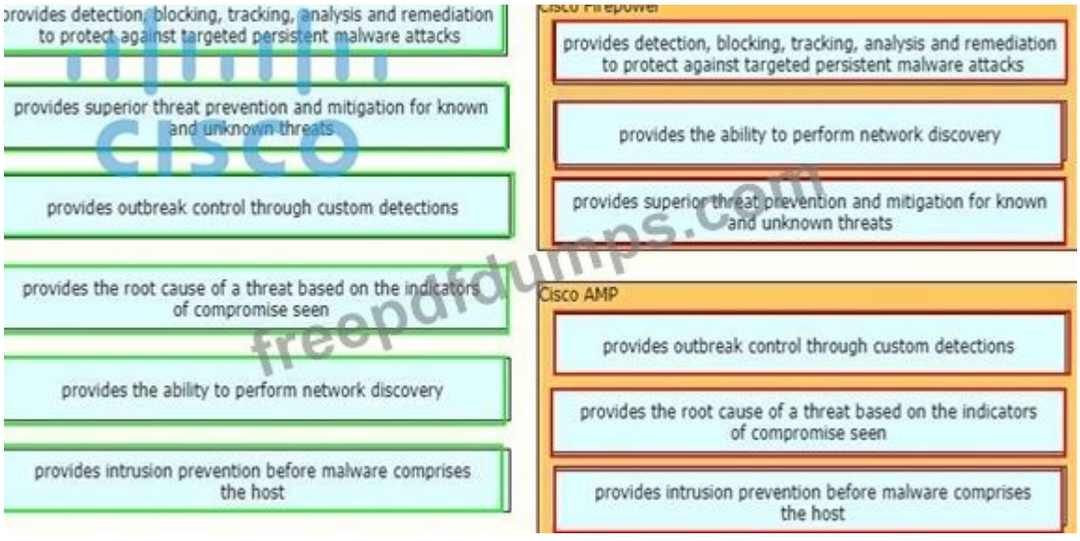
NEW QUESTION: 108
A network engineer is tasked with configuring a Cisco ISE server to implement external authentication against Active Directory. What must be considered about the authentication requirements? (Choose two.)
A. Active Directory supports user and machine authentication by using MSCHAPv2.
B. Active Directory only supports user authentication by using MSCHAPv2.
C. LDAP communication must be permitted between the ISE server and the domain controller.
D. The ISE account must be a domain administrator in Active Directory to perform JOIN operations.
E. RADIUS communication must be permitted between the ISE server and the domain controller.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 109

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



Answer:



NEW QUESTION: 110

What are two benefits of Flexible NetFlow records? (Choose two)

A. They allow the user to configure flow information to perform customized traffic identification

B. They provide attack prevention by dropping the traffic

C. They provide accounting and billing enhancements

D. They converge multiple accounting technologies into one accounting mechanism

E. They provide monitoring of a wider range of IP packet information from Layer 2 to 4

Answer: (SHOW ANSWER)

NetFlow is typically used for several key customer applications, including the following: ... Billing and accounting. NetFlow data provides fine-grained metering (for instance, flow data includes details such as IP addresses, packet and byte counts, time stamps, type of service (ToS), and application ports) for highly

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

NEW QUESTION: 111
What are two characteristics of Cisco DNA Center APIs? (Choose two)
A. They are Cisco proprietary.

B. They quickly provision new devices.
C. Postman is required to utilize Cisco DNA Center API calls.
D. They view the overall health of the network
E. They do not support Python scripts.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 112
The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the ASA be added on the Cisco UC Manager platform?
A. Enterprise Proxy Service
B. Certificate Trust List
C. Secured Collaboration Proxy
D. Endpoint Trust List
Answer: B (LEAVE A REPLY)

NEW QUESTION: 113
A network administrator is configuring a role in an access control policy to block certain URLs and selects the "Chat and instant Messaging" category. which reputation score should be selected to accomplish this goal?
A. 5
B. 3
C. 10
D. 1
Answer: (SHOW ANSWER)

NEW QUESTION: 114
Which function is included when Cisco AMP is added to web security?
A. threat prevention on an infected endpoint
B. phishing detection on emails
C. detailed analytics of the unknown file's behavior
D. multifactor, authentication-based user identity
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Refer to the exhibit.

How does Cisco Umbrella manage traffic that is directed toward risky domains?

A. Traffic is allowed but logged.

B. Traffic is proximed through the intelligent proxy.

C. Traffic is managed by the security settings and blocked.

D. Traffic is managed by the application settings, unhandled and allowed.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 116

On which part of the IT environment does DevSecOps focus?

A. perimeter network

B. application development

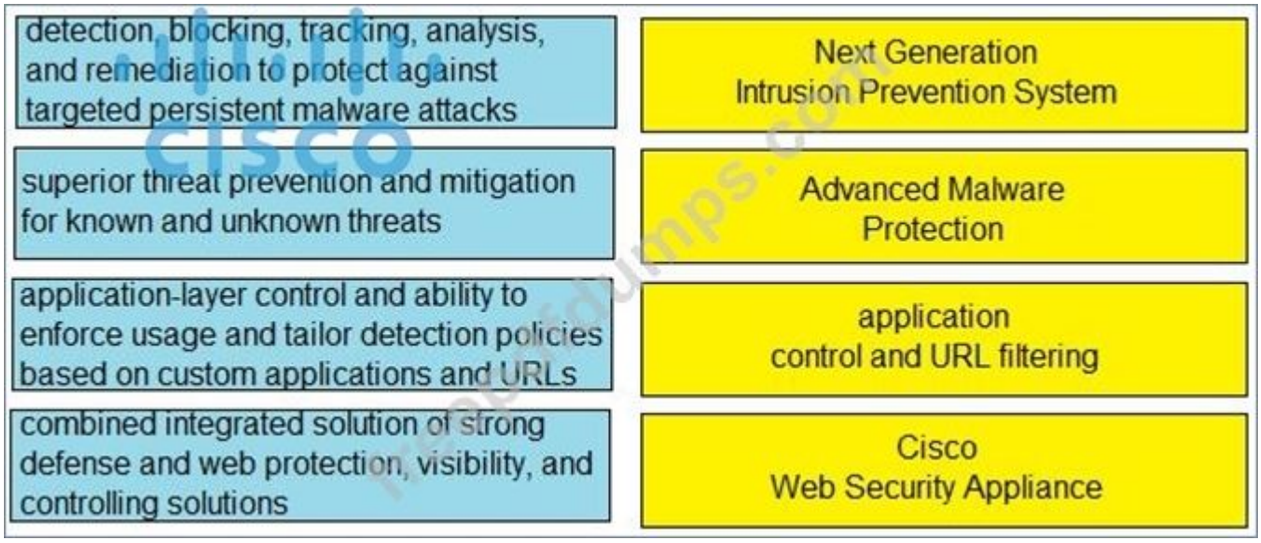
C. data center

D. wireless network

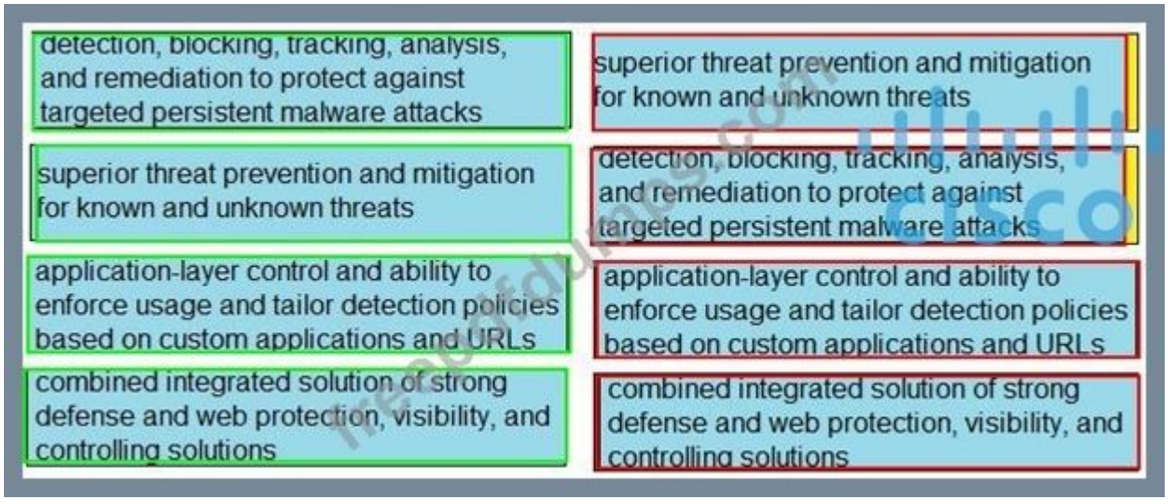
Answer: (SHOW ANSWER)

NEW QUESTION: 117

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



Answer:



NEW QUESTION: 118

Which two Cisco ISE components must be configured for BYOD? (Choose two.)

A. null WebAuth

B. local WebAuth

C. dual

D. guest

E. central WebAuth

Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 119

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 and AnyConnect Posture module
D. Cisco Identity Services Engine with PxGrid services enabled
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Which two methods must be used to add switches into the fabric so that administrators can control how switches are added into DCNM for private cloud management? (Choose two.)
A. CDP AutoDiscovery
B. Seed IP
C. PowerOn Auto Provisioning
D. Cisco Prime Infrastructure
E. Cisco Cloud Director
Answer: (SHOW ANSWER)

NEW QUESTION: 121
What is the function of the crypto is a kmp key cisc406397954 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel?
A. It configures the local address for the VPN server.
B. It prevents all IP addresses from connecting to the VPN server.
C. It configures the pre-shared authentication key
D. It defines what data is going to be encrypted via the VPN
Answer: (SHOW ANSWER)

NEW QUESTION: 122
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: 123
Which technology provides a combination of endpoint protection endpoint detection, and response?
A. Cisco AMP
B. Cisco Umbrella
C. Cisco Threat Grid
D. Cisco Talos
Answer: (SHOW ANSWER)

NEW QUESTION: 124
Which ASA deployment mode can provide separation of management on a shared appliance?
A. routed mode
B. multiple context mode
C. DMZ multiple zone mode
D. transparent firewall mode
Answer: B (LEAVE A REPLY)

NEW QUESTION: 125
What is the purpose of CA in a PKI?
A. To issue and revoke digital certificates
B. To validate the authenticity of a digital certificate
C. To create the private key for a digital certificate
D. To certify the ownership of a public key by the named subject
Answer: (SHOW ANSWER)
A trusted CA is the only entity that can issue trusted digital certificates. This is extremely important because while PKI manages more of the encryption side of these certificates, authentication is vital to understanding which entities own what keys. Without a trusted CA, anyone can issue their own keys, authentication goes out the window and chaos ensues. Reference: https://cheapsslsecurity.com/blog/understanding-the-role-of-certificate-authorities-in-pki/ A trusted CA is the only entity that can issue trusted digital certificates. This is extremely important because while PKI manages more of the encryption side of these certificates, authentication is vital to understanding which entities own what keys. Without a trusted CA, anyone can issue their own keys, authentication goes out the window and chaos ensues. Reference: https://cheapsslsecurity.com/blog/understanding-the-role-of-certificate-authorities-in-pki/

NEW QUESTION: 126
What is the role of an endpoint in protecting a user from a phishing attack?
A. Ensure that antivirus and anti malware software is up to date
B. Use machine learning models to help identify anomalies and determine expected sending behavior.
C. Utilize 802.1X network security to ensure unauthorized access to resources.

D. Use Cisco Stealthwatch and Cisco ISE Integration.
Answer: (SHOW ANSWER)

NEW QUESTION: 127
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. Content Category Blocking
B. File Analysis
C. Application Control
D. Security Category Blocking
Answer: (SHOW ANSWER)

NEW QUESTION: 128
Which two preventive measures are used to control cross-site scripting? (Choose two)
A. Disable cookie inspection in the HTML inspection engine.
B. Enable client-side scripts on a per-domain basis.
C. Incorporate contextual output encoding/escaping.
D. Same Site cookie attribute should not be used.
E. Run untrusted HTML input through an HTML sanitization engine.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 129
A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?
A. Use MAB with profiling
B. Use MAB with posture assessment.
C. Use 802.1X with posture assessment.
D. Use 802.1X with profiling.
Answer: (SHOW ANSWER)
As the new device does not have a supplicant, we cannot use 802.1X. MAC Authentication Bypass (MAB) is a fallback option for devices that don't support 802.1x. It is virtually always used in deployments in some way shape or form. MAB works by having the authenticator take the connecting device's MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or Access-Reject just like it would with 802.1x. Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers,

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

access when accessing the network from their personal iPhone. Reference:
https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456

NEW QUESTION: 130
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. sniffing the packets between the two hosts
B. overflowing the buffer's memory
C. inserting malicious commands into the database
D. sending continuous pings
Answer: C (LEAVE A REPLY)

NEW QUESTION: 131
Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?
A. RSA SecureID
B. LDAP
C. Internal Database
D. Active Directory
Answer: D (LEAVE A REPLY)

NEW QUESTION: 132
An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?
A. TCP 6514
B. UDP 1700
C. TCP 49
D. UDP 1812
Answer: B (LEAVE A REPLY)
CoA Messages are sent on two different udp ports depending on the platform. Cisco standardizes on UDP port
1700, while the actual RFC calls out using UDP port 3799.

NEW QUESTION: 133
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: 134
An engineer needs a solution for TACACS+ authentication and authorization for device administration.
The engineer also wants to enhance wired and wireless network security by requiring users and endpoints to use 802.1X, MAB, or WebAuth. Which product meets all of these requirements?
A. Cisco Prime Infrastructure
B. Cisco Stealthwatch
C. Cisco Identity Services Engine
D. Cisco AMP for Endpoints
Answer: C (LEAVE A REPLY)

NEW QUESTION: 135
Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?
A. aaa new-model
B. ip device-tracking
C. aaa server radius dynamic-author
D. auth-type all
Answer: (SHOW ANSWER)

NEW QUESTION: 136
How does Cisco Stealthwatch Cloud provide security for cloud environments?
A. It delivers visibility and threat detection.
B. It prevents exfiltration of sensitive data.
C. It assigns Internet-based DNS protection for clients and servers.
D. It facilitates secure connectivity between public and private networks.
Answer: (SHOW ANSWER)
Cisco Stealthwatch Cloud: Available as an SaaS product offer to provide visibility and threat detection within public cloud infrastructures such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

NEW QUESTION: 137
Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two)
A. accounting
B. assurance
C. automation
D. authentication
E. encryption
Answer: B,C (LEAVE A REPLY)
What Cisco DNA Center enables you to do Automate: Save time by using a single dashboard to manage and automate your network. Quickly scale your business with intuitive workflows and reusable templates. Configure and provision thousands of network devices across your enterprise in minutes, not hours. Secure policy: Deploy group-based secure access and network segmentation based on business needs. With Cisco DNA Center, you apply policy to users and applications instead of to your network devices. Automation reduces manual operations and the costs associated with human errors, resulting in more uptime and improved security. Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent. Assurance: Monitor, identify, and react in real time to changing network and wireless conditions. Cisco DNA Center uses your network's wired and wireless devices to create sensors everywhere, providing real-time feedback based on actual network conditions. The Cisco DNA Assurance engine correlates network sensor insights with streaming telemetry and compares this with the current context of these data sources. With a quick check of the health scores on the Cisco DNA Center dashboard, you can see where there is a performance issue and identify the most likely cause in minutes. Extend ecosystem: With the new Cisco DNA Center platform, IT can now integrate Cisco solutions and thirdparty technologies into a single network operation for streamlining IT workflows and increasing business value and innovation. Cisco DNA Center allows you to run the network with open interfaces with IT and business applications, integrates across IT operations and technology domains, and can manage heterogeneous network devices. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- cisco-dna-center-aag-cte-en.html Automate: Save time by using a single dashboard to manage and automate your network. Quickly scale your business with intuitive workflows and reusable templates. Configure and provision thousands of network devices across your enterprise in minutes, not hours.
Secure policy: Deploy group-based secure access and network segmentation based on business needs. With Cisco DNA Center, you apply policy to users and applications instead of to your network devices. Automation reduces manual operations and the costs associated with human errors, resulting in more uptime and improved security. Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent.
Assurance: Monitor, identify, and react in real time to changing network and wireless conditions. Cisco DNA Center uses your network's wired and wireless devices to create sensors everywhere, providing real-time feedback based on actual network conditions. The Cisco DNA Assurance engine correlates network sensor insights with streaming telemetry and compares this with the current context of these data sources. With a quick check of the health scores on the Cisco DNA Center dashboard, you can see where there is a performance issue and identify the most likely cause in minutes.

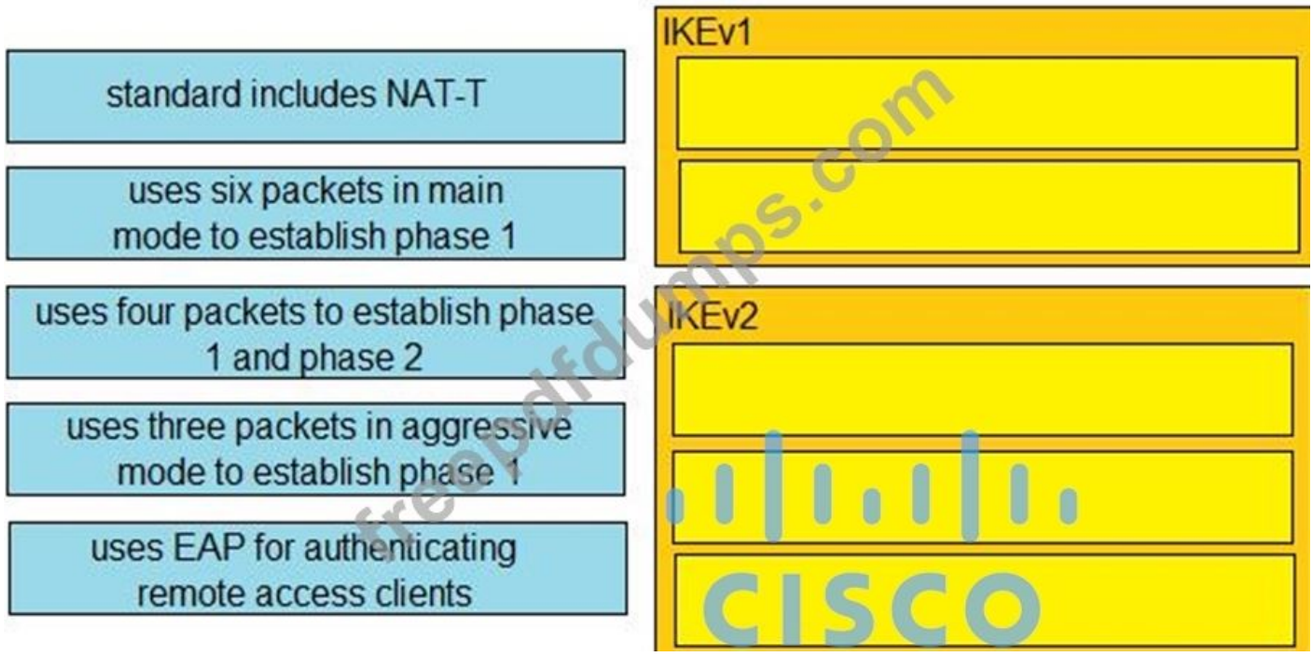
Extend ecosystem: With the new Cisco DNA Center platform, IT can now integrate Cisco solutions and thirdparty technologies into a single network operation for streamlining IT workflows and increasing business value and innovation. Cisco DNA Center allows you to run the network with open interfaces with IT and business applications, integrates across IT operations and technology domains, and can manage heterogeneous network devices.
What Cisco DNA Center enables you to do Automate: Save time by using a single dashboard to manage and automate your network. Quickly scale your business with intuitive workflows and reusable templates. Configure and provision thousands of network devices across your enterprise in minutes, not hours. Secure policy: Deploy group-based secure access and network segmentation based on business needs. With Cisco DNA Center, you apply policy to users and applications instead of to your network devices. Automation reduces manual operations and the costs associated with human errors, resulting in more uptime and improved security. Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent. Assurance: Monitor, identify, and react in real time to changing network and wireless conditions. Cisco DNA Center uses your network's wired and wireless devices to create sensors everywhere, providing real-time feedback based on actual network conditions. The Cisco DNA Assurance engine correlates network sensor insights with streaming telemetry and compares this with the current context of these data sources. With a quick check of the health scores on the Cisco DNA Center dashboard, you can see where there is a performance issue and identify the most likely cause in minutes. Extend ecosystem: With the new Cisco DNA Center platform, IT can now integrate Cisco solutions and thirdparty technologies into a single network operation for streamlining IT workflows and increasing business value and innovation. Cisco DNA Center allows you to run the network with open interfaces with IT and business applications, integrates across IT operations and technology domains, and can manage heterogeneous network devices. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- cisco-dna-center-aag-cte-en.html

NEW QUESTION: 138
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

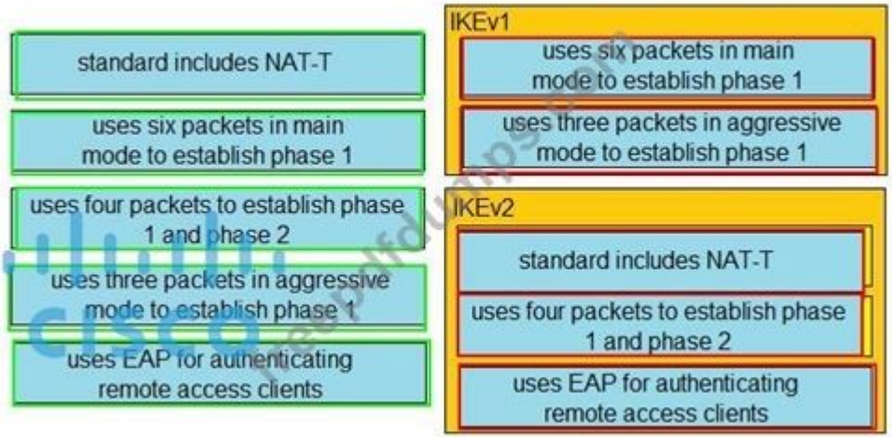
interfaces (APIs), website portals, or gateway software. These solutions tend to be proprietary, which can cause problems if the customer moves away from the provider's platform.
+ Software as a Service (SaaS): SaaS is designed to provide a complete packaged solution. The software is rented out to the 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: 139
What is a description of microsegmentation?
A. Environments deploy a container orchestration platform, such as Kubernetes, to manage the application delivery
B. Environments implement private VLAN segmentation to group servers with similar applications.
C. Environments deploy centrally managed host-based firewall rules on each server or container
D. Environments apply a zero-trust model and specify how applications on different servers or containers can communicate
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
Drag and drop the descriptions from the left onto the correct protocol versions on the right.



Answer:



NEW QUESTION: 141
Which category includes DoS Attacks?
A. Trojan attacks
B. Virus attacks
C. Flood attacks
D. Phishing attacks
Answer: C (LEAVE A REPLY)

NEW QUESTION: 142
Which two descriptions of AES encryption are true? (Choose two)
A. AES can use a 168-bit key for encryption.
B. AES encrypts and decrypts a key three times in sequence.
C. AES is less secure than 3DES.
D. AES is more secure than 3DES.
E. AES can use a 256-bit key for encryption.
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 143
What Cisco command shows you the status of an 802.1X connection on interface gi0/1?
A. show connection status gi0/1
B. show ver gi0/1
C. show authorization status
D. show authen sess int gi0/1
Answer: D (LEAVE A REPLY)

NEW QUESTION: 144
When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?
A. Spero analysis
B. dynamic analysis

C. sandbox analysis
D. malware analysis
Answer: B (LEAVE A REPLY)
Spero analysis examines structural characteristics such as metadata and header information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Reference_a_wrapper_Chapter_topic_here.html -> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload the whole file. Dynamic analysis sends files to AMP ThreatGrid. Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco Threat Grid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit. Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources. -> Malware analysis does not upload files to anywhere, it only checks the files locally. There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in a virtual machine.
files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware.
Reference:
-> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload the whole file. Dynamic analysis sends files to AMP ThreatGrid.
Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco Threat Grid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit.
Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources. -> Malware analysis does not upload files to anywhere, it only checks the files locally.
There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in a
Spero analysis examines structural characteristics such as metadata and header information in executable

files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Reference_a_wrapper_Chapter_topic_here.html -> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload the whole file. Dynamic analysis sends files to AMP ThreatGrid. Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco Threat Grid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit. Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Cisco Talos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources. -> Malware analysis does not upload files to anywhere, it only checks the files locally. There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in a virtual machine.

NEW QUESTION: 145
What is the benefit of installing Cisco AMP for Endpoints on a network?
A. It provides operating system patches on the endpoints for security.
B. It enables behavioral analysis to be used for the endpoints.
C. It protects endpoint systems through application control and real-time scanning
D. It provides flow-based visibility for the endpoints network connections.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 146
What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?
A. Enable Intelligent Proxy.
B. Activate SSL decryption.
C. Enable IP Layer enforcement.
D. Activate the Advanced Malware Protection license
Answer: A (LEAVE A REPLY)

NEW QUESTION: 147
An organization recently installed a Cisco WSA and would like to take advantage of the AVC engine to allow the organization to create a policy to control application specific activity. After enabling the AVC engine, what must be done to implement this?
A. Use security services to configure the traffic monitor, .
B. Use URL categorization to prevent the application traffic.

C. Use an access policy group to configure application control settings.
D. Use web security reporting to validate engine functionality
Answer: C (LEAVE A REPLY)
The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or allow applications individually or according to application type. You can also apply controls to particular application types.

NEW QUESTION: 148
Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?
A. Firepower
B. Stealthwatch
C. Nexus
D. Tetration
Answer: D (LEAVE A REPLY)

NEW QUESTION: 149
An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems. Why should the organization select either Platform as a Service or Infrastructure as a Service for this environment?
A. Platform as a Service because the customer manages the operating system
B. Infrastructure as a Service because the service provider manages the operating system
C. Platform as a Service because the service provider manages the operating system
D. Infrastructure as a Service because the customer manages the operating system
Answer: (SHOW ANSWER)

NEW QUESTION: 150
What is a difference between GETVPN and IPsec?
A. GETVPN is used to build a VPN network with multiple sites without having to statically configure all devices
B. GETVPN reduces latency and provides encryption over MPLS without the use of a central hub
C. GETVPN provides key management and security association management
D. GETVPN is based on IKEv2 and does not support IKEv1
Answer: B (LEAVE A REPLY)

NEW QUESTION: 151
Which VPN technology can support a multivendor environment and secure traffic between sites?
A. SSL VPN
B. GET VPN
C. FlexVPN
D. DMVPN
Answer: (SHOW ANSWER)

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: 152
A customer has various external HTTP resources available including Intranet. Extranet, and Internet, with a proxy configuration running in explicit mode Which method allows the client desktop browsers to be configured to select when to connect direct or when to use the proxy?
A. PAC file
B. Bridge mode
C. Forward file
D. Transparent mode
Answer: A (LEAVE A REPLY)

NEW QUESTION: 153
An administrator is adding a new switch onto the network and has configured AAA for network access control. When testing the configuration, the RADIUS authenticates to Cisco ISE but is being rejected. Why is the ip radius source-interface command needed for this configuration?
A. RADIUS requests are generated only by a router if a RADIUS source interface is defined.
B. Only requests that originate from a configured NAS IP are accepted by a RADIUS server
C. Encrypted RADIUS authentication requires the RADIUS source interface be defined
D. The RADIUS authentication key is transmitted only from the defined RADIUS source interface
Answer: (SHOW ANSWER)

NEW QUESTION: 154
Which Cisco platform provides an agentless solution to provide visibility across the network including encrypted traffic analytics to detect malware in encrypted traffic without the need for decryption?
A. Cisco Advanced Malware Protection
B. Cisco AnyConnect
C. Cisco Stealthwatch
D. Cisco Identity Services Engine
Answer: (SHOW ANSWER)

NEW QUESTION: 155
Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?
A. Cognitive Threat Analytics
B. Threat Intelligence Director
C. Cisco Talos Intelligence
D. Encrypted Traffic Analytics
Answer: B (LEAVE A REPLY)

NEW QUESTION: 156
Using Cisco Cognitive Threat Analytics, which platform automatically blocks risky sites, and test unknown sites for hidden advanced threats before allowing users to click them?
A. Cisco Advanced Stealthwatch Appliance
B. Cisco Enterprise Security Appliance
C. Cisco Web Security Appliance
D. Cisco Identity Services Engine
Answer: (SHOW ANSWER)

NEW QUESTION: 157
What provides visibility and awareness into what is currently occurring on the network?
A. CMX
B. WMI
C. Prime Infrastructure
D. Telemetry
Answer: D (LEAVE A REPLY)
Telemetry - Information and/or data that provides awareness and visibility into what is occurring on the network at any given time from networking devices, appliances, applications or servers in which the core function of the device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks. Reference: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/activethreat-analytics-premier.pdf at any given time from networking devices, appliances, applications or servers in which the core function of the device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks.
Telemetry - Information and/or data that provides awareness and visibility into what is occurring on the network at any given time from networking devices, appliances, applications or servers in which the core function of the device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks. Reference: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/activethreat-analytics-premier.pdf

NEW QUESTION: 158

Which two parameters are used for device compliance checks? (Choose two.)
A. Windows registry values
B. DHCP snooping checks
C. endpoint protection software version
D. DNS integrity checks
E. device operating system version
Answer: (SHOW ANSWER)

NEW QUESTION: 159
Which technology provides the benefit of Layer 3 through Layer 7 innovative deep packet inspection, enabling the platform to identify and output various applications within the network traffic flows?
A. Account on Resolution
B. Cisco NBAR2
C. Cisco Prime Infrastructure
D. Cisco ASAV
Answer: B (LEAVE A REPLY)

NEW QUESTION: 160
A network administrator needs to find out what assets currently exist on the network. Third-party systems need to be able to feed host data into Cisco Firepower. What must be configured to accomplish this?
A. a Network Discovery policy to receive data from the host
B. a Threat Intelligence policy to download the data from the host
C. a File Analysis policy to send file data into Cisco Firepower
D. a Network Analysis policy to receive NetFlow data from the host
Answer: A (LEAVE A REPLY)
You can configure discovery rules to tailor the discovery of host and application data to your needs.
The Firepower System can use data from NetFlow exporters to generate connection and discovery events, and to add host and application data to the network map.
A network analysis policy governs how traffic is decoded and preprocessed so it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt -> Answer D is not correct.

NEW QUESTION: 161
What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?
A. Cisco Cloudlock
B. Cisco Umbrella
C. Cisco AMP
D. Cisco App Dynamics
Answer: A (LEAVE A REPLY)
Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely.

It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

NEW QUESTION: 162
Which two fields are defined in the NetFlow flow? (Choose two)
A. type of service byte
B. class of service bits
C. Layer 4 protocol type
D. destination port
E. output logical interface
Answer: A,D (LEAVE A REPLY)
Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share seven values which define a unique key for the flow:
+ Ingress interface (SNMP ifIndex)
+ Source IP address
+ Destination IP address
+ IP protocol
+ Source port for UDP or TCP, 0 for other protocols
+ Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
+ IP Type of Service
Note: A flow is a unidirectional series of packets between a given source and destination.

NEW QUESTION: 163
What are two facts about WSA HTTP proxy configuration with a PAC file? (Choose two.)
A. It is defined as a Bridge proxy deployment.
B. The PAC file, which references the proxy, is deployed to the client web browser.
C. In a dual-NIC configuration, the PAC file directs traffic through the two NICs to the proxy.
D. It is defined as an Explicit proxy deployment.
E. It is defined as a Transparent proxy deployment.
Answer: (SHOW ANSWER)

NEW QUESTION: 164
Which type of attack is MFA an effective deterrent for?
A. teardrop
B. phishing
C. ping of death
D. syn flood
Answer: B (LEAVE A REPLY)

NEW QUESTION: 165

A network engineer must migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vMotion. What is a requirement for both physical hosts?

A. The hosts must use a different datastore than the virtual appliance.

B. The hosts must run different versions of Cisco AsyncOS.

C. The hosts must have access to the same defined network.

D. The hosts must run Cisco AsyncOS 10.0 or greater.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 166

What limits communication between applications or containers on the same node?

A. microservicing

B. Software-Defined Access

C. container orchestration

D. microsegmentation

Answer: (SHOW ANSWER)

NEW QUESTION: 167

Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps.

Which two actions must be taken to ensure that interfaces are put back into service? (Choose two)

A. Have Cisco Prime Infrastructure issue an SNMP set command to re-enable the ports after the pre configured interval.

B. Use EEM to have the ports return to service automatically in less than 300 seconds.

C. Enter the shutdown and no shutdown commands on the interfaces.

D. Enable the snmp-server enable traps command and wait 300 seconds

E. Ensure that interfaces are configured with the error-disable detection and recovery feature

Answer: (SHOW ANSWER)

You can also bring up the port by using these commands:

+ The "shutdown" interface configuration command followed by the "no shutdown" interface configuration command restarts the disabled port.

+ The "errdisable recovery cause ..." global configuration command enables the timer to automatically recover error-disabled state, and the "errdisable recovery interval interval" global configuration command specifies the time to recover error-disabled state.

NEW QUESTION: 168
What is a characteristic of traffic storm control behavior?
A. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
B. Traffic storm control cannot 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 uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 169
What is a function of 3DES in reference to cryptography?
A. It encrypts traffic.
B. It creates one-time use passwords.
C. It generates private keys.
D. It hashes files.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 170
Which portion of the network do EPP solutions solely focus on and EDR solutions do not?
A. East-West gateways
B. server farm
C. perimeter
D. core
Answer: C (LEAVE A REPLY)

NEW QUESTION: 171
Which technology reduces data loss by identifying sensitive information stored in public computing environments?
A. Cisco Firepower
B. Cisco HyperFlex
C. Cisco Cloudlock
D. Cisco SDA
Answer: C (LEAVE A REPLY)