Cisco.350-701.v2022-10-06.q199

Exam Code:	350-701
Exam Name:	Implementing and Operating Cisco Security Core Technologies
Certification Provider:	Cisco
Free Question Number:	199
Version:	v2022-10-06
# of views:	497
# of Questions views:	20914
https://www.freecram.net/torrent/Cisco.350-701.v2022-10-06.q199.html	

NEW QUESTION: 1
When configuring ISAKMP for IKEv1 Phase1 on a Cisco IOS router, an administrator needs to input the command crypto isakmp key cisco address 0.0.0.0. The administrator is not sure what the IP addressing in this command issued for. What would be the effect of changing the IP address from 0.0.0.0 to 1.2.3.4?
A. The key server that is managing the keys for the connection will be at 1.2.3.4
B. The remote connection will only be allowed from 1.2.3.4
C. The address that will be used as the crypto validation authority
D. All IP addresses other than 1.2.3.4 will be allowed
Answer: (SHOW ANSWER)
The command crypto isakmp key cisco address 1.2.3.4 authenticates the IP address of the 1.2.3.4 peer by using the key cisco. The address of "0.0.0.0" will authenticate any address with this key

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

node.com/blog/2016/1/2/ise-20-profiling Profiling is done by using DHCP, SNMP, Span, NetFlow, HTTP, RADIUS, DNS, or NMAP scans to collect as much metadata as possible to learn the device fingerprint.
NMAP ("Network Mapper") is a popular network scanner which provides a lot of features. One of them is the OUI (Organizationally Unique Identifier) information. OUI is the first 24 bit or 6 hexadecimal value of the MAC address.
Note: DHCP probe cannot collect OUIs of endpoints. NMAP scan probe can collect these endpoint attributes:
+ EndPointPolicy
+ LastNmapScanCount
+ NmapScanCount
+ OUI
+ Operating-system
Cisco ISE can determine the type of device or endpoint connecting to the network by performing "profiling." Profiling is done by using DHCP, SNMP, Span, NetFlow, HTTP, RADIUS, DNS, or NMAP scans to collect as much metadata as possible to learn the device fingerprint. NMAP ("Network Mapper") is a popular network scanner which provides a lot of features. One of them is the OUI (Organizationally Unique Identifier) information. OUI is the first 24 bit or 6 hexadecimal value of the MAC address. Note: DHCP probe cannot collect OUIs of endpoints. NMAP scan probe can collect these endpoint attributes: + EndPointPolicy + LastNmapScanCount + NmapScanCount + OUI + Operating-system Reference: http://www.network-node.com/blog/2016/1/2/ise-20-profiling

NEW QUESTION: 3
Refer to the exhibit.
What will happen when the Python script is executed?
A. The script will translate the IP address to FODN and print it
B. The hostname will be translated to an IP address and printed.
C. The hostname will be printed for the client in the client ID field.
D. The script will pull all computer hostnames and print them.
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Email security has become a high priority task for a security engineer at a large multi-national organization due to ongoing phishing campaigns. To help control this, the engineer has deployed an Incoming Content Filter with a URL reputation of (-10 00 to -6 00) on the Cisco ESA Which action will the system perform to disable any links in messages that match the filter?
A. Defang
B. FilterAction
C. Quarantine
D. ScreenAction
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?
A. Group Policy

B. Access Control Policy
C. Device Management Policy
D. Platform Service Policy
Answer: (SHOW ANSWER)
Cisco Firepower deployments can take advantage of platform settings policies. A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. Examples of these platform settings policies are time and date settings, external authentication, and other common administrative features. A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device. For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/platform_settings_policies_for_managed_devices.html Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best answer here so we have to choose it.
administrative features.
A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device.
For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.
Reference:
Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best Cisco Firepower deployments can take advantage of platform settings policies. A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. Examples of these platform settings policies are time and date settings, external authentication, and other common administrative features. A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device. For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/platform_settings_policies_for_managed_devices.html Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best answer here so we have to choose it.

NEW QUESTION: 6
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: 7
Which RADIUS attribute can you use to filter MAB requests in an 802.1 x deployment?
A. 1
B. 2
C. 6
D. 31
Answer: (SHOW ANSWER)
Because MAB uses the MAC address as a username and password, you should make sure that the RADIUS server can differentiate MAB requests from other types of requests for network access. This precaution will prevent other clients from attempting to use a MAC address as a valid credential. Cisco switches uniquely identify MAB requests by setting Attribute 6 (Service-Type) to 10 (Call-Check) in a MAB Access-Request message. Therefore, you can use Attribute 6 to filter MAB requests at the RADIUS server. 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: 8
Which type of algorithm provides the highest level of protection against brute-force attacks?
A. PFS
B. HMAC
C. SHA
D. MD5
Answer: C (LEAVE A REPLY)

NEW QUESTION: 9
An organization has two systems in their DMZ that have an unencrypted link between them for communication.

The organization does not have a defined password policy and uses several default accounts on the systems.
The application used on those systems also have not gone through stringent code reviews. Which vulnerability would help an attacker brute force their way into the systems?

A. weak passwords
B. lack of input validation
C. missing encryption
D. lack of file permission

Answer: (SHOW ANSWER)

The version 9 export format uses templates to provide access to observations of IP packet flows in a flexible and extensible manner. A template defines a collection of fields, with corresponding descriptions of structure and semantics. Reference: https://tools.ietf.org/html/rfc3954 The version 9 export format uses templates to provide access to observations of IP packet flows in a flexible and extensible manner. A template defines a collection of fields, with corresponding descriptions of structure and semantics. Reference: https://tools.ietf.org/html/rfc3954

NEW QUESTION: 10

Refer to the exhibit.
What does the number 15 represent in this configuration?

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 11

Which public cloud provider supports the Cisco Next Generation Firewall Virtual?

A. Google Cloud Platform
B. Red Hat Enterprise Visualization
C. VMware ESXi
D. Amazon Web Services

Answer: (SHOW ANSWER)

Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco's Firepower next generation firewall. The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not

available in Azure. In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet. In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions. Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/ white-paper-c11-740505.html The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure.
In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet.
In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions.
Cisco Firepower NGFW Virtual (NGFWv) is the virtualized version of Cisco's Firepower next generation firewall. The Cisco NGFW virtual appliance is available in the AWS and Azure marketplaces. In AWS, it can be deployed in routed and passive modes. Passive mode design requires ERSPAN, the Encapsulated Remote Switched Port Analyzer, which is currently not available in Azure. In passive mode, NGFWv inspects packets like an Intrusion Detection System (IDS) appliance, but no action can be taken on the packet. In routed mode NGFWv acts as a next hop for workloads. It can inspect packets and also take action on the packet based on rule and policy definitions. Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/ white-paper-c11-740505.html

NEW QUESTION: 12
What is the purpose of the My Devices Portal in a Cisco ISE environment?
A. to register new laptops and mobile devices
B. to request a newly provisioned mobile device
C. to provision userless and agentless systems
D. to manage and deploy antivirus definitions and patches on systems owned by the end user
Answer: (SHOW ANSWER)
Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html
Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html

NEW QUESTION: 13
An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users.
A. Upload the organization root CA to the Umbrella admin portal
B. Restrict access to only websites with trusted third-party signed certificates.
C. Modify the user's browser settings to suppress errors from Umbrella.
D. Import the Umbrella root CA into the trusted root store on the user's device.

Answer: (SHOW ANSWER)

NEW QUESTION: 14
What are two characteristics of Cisco DNA Center APIs? (Choose two)
A. They view the overall health of the network
B. They are Cisco proprietary.
C. They quickly provision new devices.
D. Postman is required to utilize Cisco DNA Center API calls.
E. They do not support Python scripts.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
An organization is trying to implement micro-segmentation on the network and wants to be able to gain visibility on the applications within the network. The solution must be able to maintain and force compliance. Which product should be used to meet these requirements?
A. Cisco Umbrella
B. Cisco AMP
C. Cisco Stealthwatch
D. Cisco Tetration
Answer: (SHOW ANSWER)
Micro-segmentation secures applications by expressly allowing particular application traffic and, by default, denying all other traffic. Micro-segmentation is the foundation for implementing a zero-trust security model for application workloads in the data center and cloud. Cisco Tetration is an application workload security platform designed to secure your compute instances across any infrastructure and any cloud. To achieve this, it uses behavior and attribute-driven microsegmentation policy generation and enforcement. It enables trusted access through automated, exhaustive context from various systems to automatically adapt security policies. To generate accurate microsegmentation policy, Cisco Tetration performs application dependency mapping to discover the relationships between different application tiers and infrastructure services. In addition, the platform supports "what-if" policy analysis using real-time data or historical data to assist in the validation and risk assessment of policy application pre-enforcement to ensure ongoing application availability. The normalized microsegmentation policy can be enforced through the application workload itself for a consistent approach to workload microsegmentation across any environment, including virtualized, bare-metal, and container workloads running in any public cloud or any data center. Once the microsegmentation policy is enforced, Cisco Tetration continues to monitor for compliance deviations, ensuring the segmentation policy is up to date as the application behavior change. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22-739268.pdf denying all other traffic. Micro-segmentation is the foundation for implementing a zero-trust security model for application workloads in the data center and cloud.
Cisco Tetration is an application workload security platform designed to secure your compute instances across any infrastructure and any cloud. To achieve this, it uses behavior and attribute-driven microsegmentation policy generation and enforcement. It enables trusted access through automated, exhaustive context from various systems to automatically adapt security policies.
To generate accurate microsegmentation policy, Cisco Tetration performs application dependency mapping to discover the relationships between different application tiers and infrastructure services. In addition, the platform supports "what-if" policy analysis using real-time data or historical data to assist in the validation and risk assessment of policy application pre-

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

NEW QUESTION: 16
Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.
Answer:

NEW QUESTION: 17
What is a benefit of using Cisco Tetration?
A. It collects near-real time data from servers and inventories the software packages that exist on servers.
B. It collects policy compliance data and process details.
C. It collects enforcement data from servers and collects interpacket variation.
D. It collects telemetry data from servers and then uses software sensors to analyze flow information.
Answer: (SHOW ANSWER)

NEW QUESTION: 18

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

NEW QUESTION: 19
An engineer configured a new network identity in Cisco Umbrella but must verify that traffic is being routed through the Cisco Umbrella network. Which action tests the routing?
A. Browse to http://welcome.umbrella.com/ to validate that the new identity is working.
B. Enable the Intelligent Proxy to validate that traffic is being routed correctly.
C. Add the public IP address that the client computers are behind to a Core Identity.
D. Ensure that the client computers are pointing to the on-premises DNS servers.
Answer: (SHOW ANSWER)

NEW QUESTION: 20
When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, which name is used?

A. Common Security Exploits
B. Common Vulnerabilities and Exposures
C. Common Exploits and Vulnerabilities
D. Common Vulnerabilities, Exploits and Threats
Answer: B (LEAVE A REPLY)
CVE is an industry-wide standard. CVE is sponsored by US-CERT, the office of Cybersecurity and Communications at the U.S. Department of Homeland Security.
The goal of CVE is to make it's easier to share data across tools, vulnerability repositories, and security services.

NEW QUESTION: 21
An organization wants to use Cisco FTD or Cisco ASA devices. Specific URLs must be blocked from being accessed via the firewall which requires that the administrator input the bad URL categories that the organization wants blocked into the access policy. Which solution should be used to meet this requirement?
A. Cisco ASA because it includes URL filtering in the access control policy capabilities, whereas Cisco FTD does not
B. Cisco ASA because it enables URL filtering and blocks malicious URLs by default, whereas Cisco FTD does not
C. Cisco FTD because it includes URL filtering in the access control policy capabilities, whereas Cisco ASA does not
D. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22

An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1 1 11 using the flow record Stea!thwatch406397954 command Which additional command is required to complete the flow record?

A. match ipv4 ttl

B. destination 1.1.1.1

C. transport udp 2055

D. cache timeout active 60

Answer: (SHOW ANSWER)

NEW QUESTION: 23

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 service provider manages the operating system

B. Platform as a Service because the customer manages the operating system

C. Infrastructure as a Service because the service provider manages the operating system

D. Infrastructure as a Service because the customer manages the operating system

Answer: (SHOW ANSWER)

NEW QUESTION: 24

Which two parameters are used for device compliance checks? (Choose two.)

A. endpoint protection software version

B. DHCP snooping checks

C. Windows registry values

D. device operating system version

E. DNS integrity checks

Answer: (SHOW ANSWER)

NEW QUESTION: 25

Refer to the exhibit.

A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced What is the cause of this issue?

A. The key was configured in plain text.

B. The hashing algorithm that was used was MD5. which is unsupported.

C. The router was not rebooted after the NTP configuration updated.

D. NTP authentication is not enabled.

Answer: (SHOW ANSWER)

NEW QUESTION: 26

What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?

A. STIX

B. XMPP

C. pxGrid

D. SMTP
Answer: A (LEAVE A REPLY)
TAXII (Trusted Automated Exchange of Indicator Information) is a standard that provides a transport

NEW QUESTION: 27
What is the purpose of the Cisco Endpoint IoC feature?
A. It provides stealth threat prevention.
B. It is a signature-based engine. W
C. It is an incident response tool 6W
D. It provides precompromise detection.
Answer: C (LEAVE A REPLY)
https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Secure_Managed_Endpoint.pdf

NEW QUESTION: 28
Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?
A. WSA
B. AMP
C. ESA
D. NGFW
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which method of attack is used by a hacker to send malicious code through a web application to an unsuspecting user to request that the victim's web browser executes the code?
A. buffer overflow
B. cross-site scripting
C. SQL injection
D. browser WGET
Answer: (SHOW ANSWER)

NEW QUESTION: 30
When a transparent authentication fails on the Web Security Appliance, which type of access does the end user get?

A. guest
B. limited Internet
C. blocked
D. full Internet
Answer: (SHOW ANSWER)

NEW QUESTION: 31

What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.)

A. The eDirectory client must be installed on each client workstation.

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

C. Deploy a separate eDirectory server; the dent IP address is recorded in this server.

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 32

Which feature within Cisco ISE verifies the compliance of an endpoint before providing access to the network?

A. pxGrid

B. Profiling

C. Posture

D. MAB

Answer: (SHOW ANSWER)

NEW QUESTION: 33

Which attack is commonly associated with C and C++ programming languages?

A. cross-site scripting

B. water holing

C. DDoS

D. buffer overflow

Answer: (SHOW ANSWER)

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's alloted memory space. This happens quite frequently in the case of arrays.

NEW QUESTION: 34

An organization has a requirement to collect full metadata information about the traffic going through their AWS cloud services They want to use this information for behavior analytics and statistics Which two actions must be taken to implement this requirement? (Choose two.)

A. Configure Cisco ACI to ingest AWS information.

B. Configure Cisco Thousand Eyes to ingest AWS information.

C. Configure Cisco Stealthwatch Cloud to ingest AWS information

D. Send VPC Flow Logs to Cisco Stealthwatch Cloud.

E. Send syslog from AWS to Cisco Stealthwatch Cloud.

Answer: (SHOW ANSWER)

NEW QUESTION: 35

How is ICMP used an exfiltration technique?

A. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host

B. by overwhelming a targeted host with ICMP echo-request packets

C. by flooding the destination host with unreachable packets

D. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address

Answer: (SHOW ANSWER)

NEW QUESTION: 36

For Cisco IOS PKI, which two types of Servers are used as a distribution point for CRLs? (Choose two)

A. SDP

B. LDAP

C. subordinate CA

D. SCP

E. HTTP

Answer: (SHOW ANSWER)

Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI. A PKI is composed of the following entities: ... - A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs) Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mtbook/sec-pki-overview.html A PKI is composed of the following entities: ...

- A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs) Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI. A PKI is composed of the following entities: ... - A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs) Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mtbook/sec-pki-overview.html

NEW QUESTION: 37

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

A. data exfiltration
B. command and control communication
C. intelligent proxy
D. snort
E. URL categorization
Answer: (SHOW ANSWER)
Cisco Cognitive Threat Analytics helps you quickly detect and respond to sophisticated, clandestine attacks that are already under way or are attempting to establish a presence within your environment. The solution automatically identifies and investigates suspicious or malicious web-based traffic. It identifies both potential and confirmed threats, allowing you to quickly remediate the infection and reduce the scope and damage of an attack, whether it's a known threat campaign that has spread across multiple organizations or a unique threat you've never seen before. Detection and analytics features provided in Cognitive Threat Analytics are shown below: + Data exfiltration: Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content + Command-and-control (C2) communication: Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPSencoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad range of threats ... Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-aglance-c45-736555.pdf Detection and analytics features provided in Cognitive Threat Analytics are shown below:
+ Data exfiltration: Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content
+ Command-and-control (C2) communication: Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPSencoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad range of threats
...
Cisco Cognitive Threat Analytics helps you quickly detect and respond to sophisticated, clandestine attacks that are already under way or are attempting to establish a presence within your environment. The solution automatically identifies and investigates suspicious or malicious web-based traffic. It identifies both potential and confirmed threats, allowing you to quickly remediate the infection and reduce the scope and damage of an attack, whether it's a known threat campaign that has spread across multiple organizations or a unique threat you've never seen before. Detection and analytics features provided in Cognitive Threat Analytics are shown below: + Data exfiltration: Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content + Command-and-control (C2) communication: Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPSencoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad range of

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

NEW QUESTION: 38
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: 39
A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address Error! Hyperlink reference not valid. IP>/capure/CAPI/pcap/test.pcap, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?
A. Disable the HTTPS server and use HTTP instead
B. Disable the proxy setting on the browser
C. Use the Cisco FTD IP address as the proxy server setting on the browser
D. Enable the HTTPS server for the device platform policy
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?

A. Cisco Umbrella
B. Cisco AMP for Endpoints
C. Cisco ISE
D. Cisco Stealthwatch
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Why is it important to have logical security controls on endpoints even though the users are trained to spot security threats and the network devices already help prevent them?
A. because defense-in-depth stops at the network
B. because human error or insider threats will still exist
C. to prevent theft of the endpoints
D. to expose the endpoint to more threats
Answer: (SHOW ANSWER)

NEW QUESTION: 42
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 WSAV
B. Cisco Cloud Orchestrator
C. Cisco ASAV
D. Cisco Stealthwatch Cloud
Answer: (SHOW ANSWER)

NEW QUESTION: 43

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

NEW QUESTION: 44
Which deployment model is the most secure when considering risks to cloud adoption?
A. Public Cloud
B. Private Cloud
C. Hybrid Cloud
D. Community Cloud
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which Cisco cloud security software centrally manages policies on multiple platforms such as Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS?
A. Cisco Defense Orchestrator
B. Cisco DNAC
C. Cisco Secureworks
D. Cisco Configuration Professional
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?
A. Advanced Malware Protection
B. Platform Exchange Grid
C. Multifactor Platform Integration
D. Firepower Threat Defense
Answer: (SHOW ANSWER)
With Cisco pxGrid (Platform Exchange Grid), your multiple security products can now share data and work together. This open, scalable, and IETF standards-driven platform helps you automate security to get answers and contain threats faster.

NEW QUESTION: 47
Drag and drop the deployment models from the left onto the explanations on the right.
Answer:

NEW QUESTION: 48
An engineer notices traffic interruption on the network. Upon further investigation, it is learned that broadcast packets have been flooding the network. What must be configured, based on a predefined threshold, to address this issue?
A. Bridge Protocol Data Unit guard
B. embedded event monitoring
C. storm control
D. access control lists
Answer: C (LEAVE A REPLY)
Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.
By using the "storm-control broadcast level [falling-threshold]" we can limit the broadcast traffic on the switch.

NEW QUESTION: 49
Which Cisco ISE service checks the compliance of endpoints before allowing the endpoints to connect to the network?
A. profiler
B. Cisco TrustSec
C. posture
D. Threat Centric NAC
Answer: (SHOW ANSWER)

NEW QUESTION: 50
What is the function of the Context Directory Agent?
A. maintains users' group memberships
B. relays user authentication requests from Web Security Appliance to Active Directory
C. reads the Active Directory logs to map IP addresses to usernames
D. accepts user authentication requests on behalf of Web Security Appliance for user identification
Answer: (SHOW ANSWER)
Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to). CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest

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

NEW QUESTION: 51
Which Cisco ASA Platform mode disables the threat detection features except for Advanced Threat Statistics?
A. cluster
B. transparent
C. routed
D. multiple context
Answer: (SHOW ANSWER)

NEW QUESTION: 52
How does Cisco AMP for Endpoints provide next-generation protection?
A. It integrates with Cisco FTD devices.
B. It encrypts data on user endpoints to protect against ransomware.
C. It leverages an endpoint protection platform and endpoint detection and response.
D. It utilizes Cisco pxGrid, which allows Cisco AMP to pull threat feeds from threat intelligence centers.
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Which two descriptions of AES encryption are true? (Choose two)
A. AES encrypts and decrypts a key three times in sequence.
B. AES is less secure than 3DES.
C. AES is more secure than 3DES.
D. AES can use a 256-bit key for encryption.
E. AES can use a 168-bit key for encryption.
Answer: (SHOW ANSWER)

NEW QUESTION: 54
An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically.
What must be configured to accomplish this?
A. Configure the Cisco WSA to modify policies based on the traffic seen
B. Configure the Cisco ESA to receive real-time updates from Talos
C. Configure the Cisco WSA to receive real-time updates from Talos
D. Configure the Cisco ESA to modify policies based on the traffic seen
Answer: (SHOW ANSWER)
The Mail Policies menu is where almost all of the controls related to email filtering happens. All the security and content filtering policies are set here, so it's likely that, as an ESA administrator, the pages on this menu are where you are likely to spend most of your time.

NEW QUESTION: 55
Refer to the exhibit.
Which command was used to display this output?
A. show dot1x all summary
B. show dot1x
C. show dot1x all
D. show dot1x interface gi1/0/12
Answer: (SHOW ANSWER)

NEW QUESTION: 56
An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the endpoint to apply a new or updated policy from ISE. Which CoA type achieves this goal?
A. CoA Session Query
B. Port Bounce
C. CoA Reauth
D. CoA Terminate
Answer: (SHOW ANSWER)

NEW QUESTION: 57
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. single interface
B. multi-context
C. transparent
D. two-interface
Answer: (SHOW ANSWER)

NEW QUESTION: 58

Which cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group?

A. Hybrid

B. Community

C. Private

D. Public

Answer: B (LEAVE A REPLY)

Community Cloud allows system and services to be accessible by group of organizations. It shares the infrastructure between several organizations from a specific community. It may be managed internally by organizations or by the third-party.

NEW QUESTION: 59

In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?

A. LDAP injection

B. cross-site scripting

C. insecure API

D. man-in-the-middle

Answer: (SHOW ANSWER)

NEW QUESTION: 60

Refer to the exhibit.

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

A. HTTP authorization

B. plays dent ID

C. imports requests

D. HTTP authentication

Answer: (SHOW ANSWER)

NEW QUESTION: 61

Which API is used for Content Security?

A. NX-OS API

B. AsyncOS API

C. IOS XR API

D. OpenVuln API

Answer: (SHOW ANSWER)

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

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

NEW QUESTION: 63
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: 64
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: (SHOW ANSWER)
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: 65
An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users. Which action accomplishes this goal?
A. Modify the user's browser settings to suppress errors from Cisco Umbrella.
B. Upload the organization root CA to Cisco Umbrella.
C. Restrict access to only websites with trusted third-party signed certificates.
D. Install the Cisco Umbrella root CA onto the user's device.
Answer: (SHOW ANSWER)

NEW QUESTION: 66
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: (SHOW ANSWER)
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs.

NEW QUESTION: 67
What is the difference between EPP and EDR?
A. Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior.
B. EPP focuses primarily on threats that have evaded front-line defenses that entered the environment.

C. Having an EPP solution allows an engineer to detect, investigate, and remediate modern threats.
D. EDR focuses solely on prevention at the perimeter.
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Which RADIUS feature provides a mechanism to change the AAA attributes of a session after it is authenticated?
A. Authorization
B. CoA
C. Accounting
D. Authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 69
What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?
A. Indicators of Compromise
B. The Exploit Database
C. trusted automated exchange
D. threat intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 70
What provides the ability to program and monitor networks from somewhere other than the DNAC GUI?
A. ASDM
B. desktop client
C. API
D. NetFlow
Answer: (SHOW ANSWER)

NEW QUESTION: 71
What is a characteristic of Firepower NGIPS inline deployment mode?
A. It is out-of-band from traffic.
B. It must have inline interface pairs configured.
C. ASA with Firepower module cannot be deployed.
D. It cannot take actions such as blocking traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 72
What is the difference between a vulnerability and an exploit?
A. A vulnerability is a weakness that can be exploited by an attacker
B. An exploit is a hypothetical event that causes a vulnerability in the network

C. An exploit is a weakness that can cause a vulnerability in the network
D. A vulnerability is a hypothetical event for an attacker to exploit
Answer: (SHOW ANSWER)

NEW QUESTION: 73
An engineer needs to add protection for data in transit and have headers in the email message Which configuration is needed to accomplish this goal?
A. Enable flagged message handling
B. Deploy an encryption appliance.
C. Map sender !P addresses to a host interface.
D. Provision the email appliance
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Refer to the exhibit.
Which statement about the authentication protocol used in the configuration is true?
A. The authentication request contains only a password
B. The authentication request contains only a username
C. The authentication and authorization requests are grouped in a single packet
D. There are separate authentication and authorization request packets
Answer: (SHOW ANSWER)
This command uses RADIUS which combines authentication and authorization in one function (packet).

NEW QUESTION: 75
An email administrator is setting up a new Cisco ESA.
The administrator wants to enable the blocking of greymail for the end user. Which feature must the administrator enable first?
A. IP Reputation Filtering
B. Anti-Virus Filtering
C. Intelligent Multi-Scan
D. File Analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Refer to the exhibit.
What will happen when this Python script is run?
A. The compromised computers and malware trajectories will be received from Cisco AMP
B. The list of computers and their current vulnerabilities will be received from Cisco AMP
C. The compromised computers and what compromised them will be received from Cisco AMP
D. The list of computers, policies, and connector statuses will be received from Cisco AMP
Answer: (SHOW ANSWER)

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

NEW QUESTION: 77
Why should organizations migrate to an MFA strategy for authentication?
A. Single methods of authentication can be compromised more easily than MFA.
B. Biometrics authentication leads to the need for MFA due to its ability to be hacked easily.
C. MFA does not require any piece of evidence for an authentication mechanism.
D. MFA methods of authentication are never compromised.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
What are two benefits of using an MDM solution? (Choose two.)
A. encrypts data that is stored on endpoints
B. provides simple and streamlined login experience for multiple applications and users
C. native integration that helps secure applications across multiple cloud platforms or on-premises environments
D. grants administrators a way to remotely wipe a lost or stolen device
E. allows for centralized management of endpoint device applications and configurations
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 79
What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?
A. It tracks flow-create, flow-teardown, and flow-denied events.
B. It provides stateless IP flow tracking that exports all records of a specific flow.
C. It tracks the flow continuously and provides updates every 10 seconds.
D. Its events match all traffic classes in parallel.
Answer: (SHOW ANSWER)

The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs). Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.html The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs).
The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs). Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.html

NEW QUESTION: 80

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

A. sharing
B. authoring
C. consumption
D. deployment
Answer: (SHOW ANSWER)

NEW QUESTION: 81

A network engineer has configured a NTP server on a Cisco ASA.
The Cisco ASA has IP reachability to the NTP server and is not filtering any traffic.
The show ntp association detail command indicates that the configured NTP server is unsynchronized and has a stratum of 16.
What is the cause of this issue?
A. An access list entry for UDP port 123 on the inside interface is missing.
B. NTP is not configured to use a working server.
C. An access list entry for UDP port 123 on the outside interface is missing.
D. Resynchronization of NTP is not forced
Answer: (SHOW ANSWER)

NEW QUESTION: 82

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: 83

An engineer needs behavioral analysis to detect malicious activity on the hosts, and is configuring the organization's public cloud to send telemetry using the cloud provider's mechanisms to a security device. Which mechanism should the engineer configure to accomplish this goal?

A. mirror port

B. NetFlow

C. VPC flow logs

D. Flow

Answer: (SHOW ANSWER)

NEW QUESTION: 84

A network administrator is configuring a switch to use Cisco ISE for 802.1X. An endpoint is failing authentication and is unable to access the network. Where should the administrator begin troubleshooting to verify the authentication details?

A. Adaptive Network Control Policy List

B. Context Visibility

C. Accounting Reports

D. RADIUS Live Logs

Answer: (SHOW ANSWER)

How To Troubleshoot ISE Failed Authentications & Authorizations

Check the ISE Live Logs

Login to the primary ISE Policy Administration Node (PAN).

Go to Operations > RADIUS > Live Logs

(Optional) If the event is not present in the RADIUS Live Logs, go to Operations > Reports > Reports > Endpoints and Users > RADIUS Authentications Check for Any Failed Authentication Attempts in the Log

NEW QUESTION: 85

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: 86
Which two kinds of attacks are prevented by multifactor authentication? (Choose two)
A. teardrop
B. man-in-the-middle
C. DDOS
D. phishing
E. brute force
Answer: (SHOW ANSWER)

NEW QUESTION: 87
What are two ways that Cisco Container Platform provides value to customers who utilize cloud service providers? (Choose two.)
A. manages Docker containers
B. Allows developers to create code once and deploy to multiple clouds
C. manages Kubernetes clusters
D. helps maintain source code for cloud deployments
E. Creates complex tasks for managing code
Answer: (SHOW ANSWER)

NEW QUESTION: 88
What are two benefits of using Cisco Duo as an MFA solution? (Choose two.)
A. grants administrators a way to remotely wipe a lost or stolen device
B. allows for centralized management of endpoint device applications and configurations
C. encrypts data that is stored on endpoints
D. provides simple and streamlined login experience for multiple applications and users
E. native integration that helps secure applications across multiple cloud platforms or on-premises environments
Answer: (SHOW ANSWER)

NEW QUESTION: 89
Refer to the exhibit.
What is the result of this Python script of the Cisco DNA Center API?

A. receives information about a switch
B. adds authentication to a switch
C. adds a switch to Cisco DNA Center
Answer: (SHOW ANSWER)

NEW QUESTION: 90
What are two security benefits of an MDM deployment? (Choose two.)
A. on-device content management
B. distributed dashboard
C. distributed software upgrade
D. robust security policy enforcement
E. privacy control checks
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 91
Which security solution uses NetFlow to provide visibility across the network, data center, branch offices, and cloud?
A. Cisco Umbrella
B. Cisco CTA
C. Cisco Stealthwatch
D. Cisco Encrypted Traffic Analytics
Answer: (SHOW ANSWER)

NEW QUESTION: 92
What is the process of performing automated static and dynamic analysis of files against preloaded behavioral indicators for threat analysis?
A. deep visibility scan
B. point-in-time checks
C. advanced scanning
D. advanced sandboxing
Answer: (SHOW ANSWER)

NEW QUESTION: 93
What is a benefit of using Cisco FMC over Cisco ASDM?

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

NEW QUESTION: 94
What is provided by the Secure Hash Algorithm in a VPN?
A. integrity
B. key exchange
C. encryption
D. authentication
Answer: (SHOW ANSWER)
The HMAC-SHA-1-96 (also known as HMAC-SHA-1) encryption technique is used by IPSec to ensure that a message has not been altered. (-> Therefore answer "integrity" is the best choice). HMAC-SHA-1 uses the SHA-1 specified in FIPS-190-1, combined with HMAC (as per RFC 2104), and is described in RFC 2404. Reference: https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=4 The HMAC-SHA-1-96 (also known as HMAC-SHA-1) encryption technique is used by IPSec to ensure that a message has not been altered. (-> Therefore answer "integrity" is the

best choice). HMAC-SHA-1 uses the SHA-1 specified in FIPS-190-1, combined with HMAC (as per RFC 2104), and is described in RFC 2404. Reference: https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=4

NEW QUESTION: 95
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. GRE over IPsec cannot be used as a standalone protocol, and L2TP can.
B. L2TP is an IP packet encapsulation protocol, and GRE over IPsec is a tunneling protocol.
C. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701.
D. GRE over IPsec adds its own header, and L2TP does not.
Answer: (SHOW ANSWER)

NEW QUESTION: 96
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: 97
Which statement about IOS zone-based firewalls is true?
A. Only one interface can be assigned to a zone.
B. An unassigned interface can communicate with assigned interfaces
C. An interface can be assigned to multiple zones.
D. An interface can be assigned only to one zone.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
A network engineer entered the snmp-server user asmith myv7 auth sha cisco priv aes 256 cisc0xxxxxxxxx command and needs to send SNMP information to a host at 10.255.255.1. Which command achieves this goal?
A. snmp-server host inside 10.255.255.1 snmpv3 asmith
B. snmp-server host inside 10.255.255.1 version 3 myv7
C. snmp-server host inside 10.255.255.1 snmpv3 myv7
D. snmp-server host inside 10.255.255.1 version 3 asmith
Answer: (SHOW ANSWER)

NEW QUESTION: 99
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: 100
Which Cisco security solution stops exfiltration using HTTPS?
A. Cisco FTD
B. Cisco AnyConnect
C. Cisco CTA
D. Cisco ASA
Answer: (SHOW ANSWER)
https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf

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

NEW QUESTION: 102
Drag and drop the NetFlow export formats from the left onto the descriptions on the right.
Answer:

NEW QUESTION: 103
What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?
A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX

B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX
Answer: (SHOW ANSWER)
The syntax of above command is: crypto isakmp key enc-type-digit keystring {address peer-address [mask] | ipv6 ipv6-address/ ipv6-prefix | hostname hostname} [no-xauth] The peer-address argument specifies the IP or IPv6 address of the remote peer. Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp6039879000 crypto isakmp key enc-type-digit keystring {address peer-address [mask] | ipv6 ipv6-address/ ipv6-prefix | hostname hostname} [no-xauth] The peer-address argument specifies the IP or IPv6 address of the remote peer.
The syntax of above command is: crypto isakmp key enc-type-digit keystring {address peer-address [mask] | ipv6 ipv6-address/ ipv6-prefix | hostname hostname} [no-xauth] The peer-address argument specifies the IP or IPv6 address of the remote peer. Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp6039879000

NEW QUESTION: 104
What is the primary role of the Cisco Email Security Appliance?
A. Mail Submission Agent
B. Mail Transfer Agent
C. Mail Delivery Agent
D. Mail User Agent
Answer: (SHOW ANSWER)
Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay. Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/ Cisco_SBA_BN_EmailSecurityUsingCiscoESADeploymentGuide-Feb2013.pdf by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay.
Reference:
Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay. Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/ Cisco_SBA_BN_EmailSecurityUsingCiscoESADeploymentGuide-Feb2013.pdf

NEW QUESTION: 105
A network administrator is configuring a rule in an access control policy to block certain URLs and selects the "Chat and Instant Messaging" category. Which reputation score should be selected to accomplish this goal?
A. 1
B. 3
C. 5
D. 10

Answer: (SHOW ANSWER)
We choose "Chat and Instant Messaging" category in "URL Category":
To block certain URLs we need to choose URL Reputation from 6 to 10.

NEW QUESTION: 106
Which two components do southbound APIs use to communicate with downstream devices? (Choose two.)
A. external application APIs
B. applications running over the network
C. OpenFlow
D. OpFlex
E. services running over the network
Answer: (SHOW ANSWER)

NEW QUESTION: 107
Which two mechanisms are used to control phishing attacks? (Choose two)
A. Use antispyware software.
B. Revoke expired CRL of the websites.
C. Define security group memberships.
D. Implement email filtering techniques.
E. Enable browser alerts for fraudulent websites.
Answer: (SHOW ANSWER)

NEW QUESTION: 108
Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?
A. network address translations
B. intrusion policy
C. quality of service
D. time synchronization
Answer: (SHOW ANSWER)

NEW QUESTION: 109
What Cisco command shows you the status of an 802.1X connection on interface gi0/1?
A. show authorization status

B. show connection status gi0/1
C. show authen sess int gi0/1
D. show ver gi0/1
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two)

A. sFlow
B. DHCP
C. SMTP
D. RADIUS
E. TACACS+
Answer: (SHOW ANSWER)

NEW QUESTION: 111
A network engineer is deciding whether to use stateful or stateless failover when configuring two ASAs for high availability. What is the connection status in both cases?
A. need to be reestablished with both stateful and stateless failover
B. preserved with both stateful and stateless failover
C. need to be reestablished with stateful failover and preserved with stateless failover
D. preserved with stateful failover and need to be reestablished with stateless failover
Answer: (SHOW ANSWER)

NEW QUESTION: 112
An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?
A. TCP 6514
B. UDP 1700
C. TCP 49
D. UDP 1812
Answer: (SHOW ANSWER)
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: 113
Which algorithm provides asymmetric encryption?
A. AES
B. RC4
C. RSA
D. 3DES

Answer: (SHOW ANSWER)

NEW QUESTION: 114
How does Cisco Workload Optimization portion of the network do EPP solutions solely performance issues?
A. It automates resource resizing
B. It sets up a workload forensic score
C. It deploys an AWS Lambda system
D. It optimizes a flow path
Answer: (SHOW ANSWER)

NEW QUESTION: 115
What is a capability of Cisco ASA Netflow?
A. It filters NSEL events based on traffic
B. It logs all event types only to the same collector
C. It generates NSEL events even if the MPF is not configured
D. It sends NetFlow data records from active and standby ASAs in an active standby failover pair
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
Which baseline form of telemetry is recommended for network infrastructure devices?
A. SNMP
B. passive taps
C. SDNS
D. NetFlow
Answer: (SHOW ANSWER)

NEW QUESTION: 117
What is the intent of a basic SYN flood attack?
A. to flush the register stack to re-initiate the buffers
B. to solicit DNS responses
C. to exceed the threshold limit of the connection queue
D. to cause the buffer to overflow
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Drag and drop the capabilities from the left onto the correct technologies on the right.
Answer:

NEW QUESTION: 119
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: 120

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

A. SNMP

B. SMTP

C. syslog

D. model-driven telemetry

Answer: (SHOW ANSWER)

The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data. Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc. Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming. Reference: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming.

The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data. Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc. Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming. Reference: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide

NEW QUESTION: 121
An engineer needs to configure an access control policy rule to always send traffic for inspection without using the default action.
Which action should be configured for this rule?
A. allow
B. monitor
C. trust
D. block
Answer: (SHOW ANSWER)

NEW QUESTION: 122
How is DNS tunneling used to exfiltrate data out of a corporate network?
A. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.
B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.
C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network.
D. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.
Answer: (SHOW ANSWER)
Domain name system (DNS) is the protocol that translates human-friendly URLs, such as securitytut.com, into IP addresses, such as 183.33.24.13. Because DNS messages are only used as the beginning of each communication and they are not intended for data transfer, many organizations do not monitor their DNS traffic for malicious activity. As a result, DNS-based attacks can be effective if launched against their networks. DNS tunneling is one such attack.
An example of DNS Tunneling is shown below:
The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNS nameserver (NS) and malicious payload.
2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. attackerdomain.com) is registered or reused. The registrar informs the top-level domain (.com) nameservers to refer requests for attackerdomain.com to ns.attackerdomain.com, which has a DNS record mapped to 1.2.3.4
3. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, P028X977W,...).
4. The payload initiates thousands of unique DNS record requests to the attacker's domain with each string as a part of the domain name (e.g. 3KJ242AIE9.attackerdomain.com). Depending on the attacker's patience and stealth, requests can be spaced out over days or months to avoid suspicious network activity. 5. The requests are forwarded to a recursive DNS resolver.

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

NEW QUESTION: 123
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: (SHOW ANSWER)
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: 124
Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks? (Choose two.)
A. uses a static algorithm to determine malicious
B. provides a defense for on-premises email deployments
C. blocks malicious websites and adds them to a block list
D. determines if the email messages are malicious
E. does a real-time user web browsing behavior analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 125
Which two activities can be done using Cisco DNA Center? (Choose two)
A. DHCP
B. Design
C. Accounting
D. DNS
E. Provision
Answer: (SHOW ANSWER)
Cisco DNA Center has four general sections aligned to IT workflows: Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site. Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center

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

Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task.

The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups.

Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work.

The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks.

Cisco DNA Center has four general sections aligned to IT workflows: Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure

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

NEW QUESTION: 126
Which MDM configuration provides scalability?
A. automatic device classification with level 7 fingerprinting
B. BYOD support without extra appliance or licenses
C. pushing WPA2-Enterprise settings automatically to devices
D. enabling use of device features such as camera use
Answer: (SHOW ANSWER)

NEW QUESTION: 127
Refer to the exhibit.
How does Cisco Umbrella manage traffic that is directed toward risky domains?
A. Traffic is managed by the security settings and blocked.
B. Traffic is proximed through the intelligent proxy.
C. Traffic is allowed but logged.
D. Traffic is managed by the application settings, unhandled and allowed.
Answer: (SHOW ANSWER)

NEW QUESTION: 128

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: 129
Which CLI command is used to enable URL filtering support for shortened URLs on the Cisco ESA?
A. webadvancedconfig
B. outbreakconfig
C. websecurity advancedconfig
D. websecurity config
Answer: (SHOW ANSWER)

NEW QUESTION: 130
An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco Firepower. Which feature should be used to accomplish this?

A. NetFlow
B. Packet Tracer
C. Network Discovery
D. Access Control
Answer: (SHOW ANSWER)
NetFlow is a network protocol developed by Cisco for the collection and monitoring of network traffic flow data generated by NetFlow-enabled routers and switches. The flows do not contain actual packet data, but rather the metadata for communications. It is a standard form of session data that details who, what, when, and where of network traffic -> Answer A is not correct. Reference: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper-c11-736595.html generated by NetFlow-enabled routers and switches. The flows do not contain actual packet data, but rather the metadata for communications. It is a standard form of session data that details who, what, when, and where of network traffic -> Answer A is not correct.
Reference:
NetFlow is a network protocol developed by Cisco for the collection and monitoring of network traffic flow data generated by NetFlow-enabled routers and switches. The flows do not contain actual packet data, but rather the metadata for

communications. It is a standard form of session data that details who, what, when, and where of network traffic -> Answer A is not correct. Reference: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper-c11-736595.html

NEW QUESTION: 131
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: (SHOW ANSWER)
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: 132
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 ISE?
B. Cisco Tetration
C. Cisco AMP for Network
D. Cisco AnyConnect
Answer: (SHOW ANSWER)

NEW QUESTION: 133
Refer to the exhibit.
An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained. Which command should be configured on the switch interface in order to provide the user with network connectivity?
A. ip dhcp snooping verify mac-address
B. ip dhcp snooping limit 41
C. ip dhcp snooping vlan 41
D. ip dhcp snooping trust
Answer: (SHOW ANSWER)
To understand DHCP snooping we need to learn about DHCP spoofing attack first.
DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle".

The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.
DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.
Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.
The port connected to a DHCP server should be configured as trusted port with the "ip dhcp snooping trust" command. Other ports connecting to hosts are untrusted ports by default.
In this question, we need to configure the uplink to "trust" (under interface Gi1/0/1) as shown below.

NEW QUESTION: 134
Drag and drop the cloud security assessment components from the left onto the definitions on the right.
Answer:

NEW QUESTION: 135
Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?
A. file access from a different user
B. interesting file access
C. user login suspicious behavior
D. privilege escalation
Answer: (SHOW ANSWER)
The various suspicious patterns for which the Cisco Tetration platform looks in the current release are: + Shell code execution: Looks for the patterns used by shell code. + Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree. + Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these, it can detect Meltdown, Spectre, and other cache-timing attacks. + Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping). + User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods. + Interesting file access: Cisco Tetration platform can be armed to look at sensitive files. + File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user. + Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html
+ Shell code execution: Looks for the patterns used by shell code.
+ Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.
+ Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts.
Using these, it can detect Meltdown, Spectre, and other cache-timing attacks.
+ Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping).
+ User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods.
+ Interesting file access: Cisco Tetration platform can be armed to look at sensitive files.
+ File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user.

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

NEW QUESTION: 136
With which components does a southbound API within a software-defined network architecture communicate?
A. controllers within the network
B. applications
C. appliances
D. devices such as routers and switches
Answer: (SHOW ANSWER)
The Southbound API is used to communicate between Controllers and network devices.

NEW QUESTION: 137
Refer to the exhibit.
What does the API key do while working with https://api.amp.cisco.com/v1/computers?
A. displays client ID
B. Imports requests
C. HTTP authentication
D. HTTP authorization
Answer: (SHOW ANSWER)

NEW QUESTION: 138

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

A. Cisco Cloudlock

B. Cisco Umbrella

C. Cisco AMP

D. Cisco App Dynamics

Answer: (SHOW ANSWER)

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

NEW QUESTION: 139

A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to ensure that bandwidth is available for VPN users needing access to corporate resources on the10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the network?

A. Configure VPN load balancing to send non-corporate traffic straight to the internet.

B. Use split tunneling to tunnel all traffic except for the 10.0.0.0/24 network.

C. Use split tunneling to tunnel traffic for the 10.0.0.0/24 network only.

D. Configure VPN load balancing to distribute traffic for the 10.0.0.0/24 network,

Answer: (SHOW ANSWER)

NEW QUESTION: 140

What is the function of Cisco Cloudlock for data security?

A. data loss prevention

B. controls malicious cloud apps

C. detects anomalies

D. user and entity behavior analytics

Answer: A (LEAVE A REPLY)

NEW QUESTION: 141

Which statement describes a serverless application?

A. The application runs from an ephemeral, event-triggered, and stateless container that is fully managed by a cloud provider.

B. The application delivery controller in front of the server farm designates on which server the application runs each time.

C. The application is installed on network equipment and not on physical servers.

D. The application runs from a containerized environment that is managed by Kubernetes or Docker Swarm.

Answer: (SHOW ANSWER)

NEW QUESTION: 142

What is the most common type of data exfiltration that organizations currently experience?

A. encrypted SMTP

B. HTTPS file upload site

C. Microsoft Windows network shares
D. SQL database injections
Answer: (SHOW ANSWER)

NEW QUESTION: 143
Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)
A. Cisco ISE
B. Cisco Duo Security
C. Cisco TrustSec
D. Cisco Umbrella
E. Cisco DNA Center
Answer: (SHOW ANSWER)

NEW QUESTION: 144
In which two ways does the Cisco Advanced Phishing Protection solution protect users? (Choose two.)
A. It prevents use of compromised accounts and social engineering.
B. It automatically removes malicious emails from users' inbox.
C. It prevents trojan horse malware using sensors.
D. It prevents all zero-day attacks coming from the Internet.
E. It secures all passwords that are shared in video conferences.
Answer: (SHOW ANSWER)

NEW QUESTION: 145
Which command enables 802.1X globally on a Cisco switch?
A. aaa new-model
B. dot1x pae authenticator
C. authentication port-control aut
D. dot1x system-auth-control
Answer: (SHOW ANSWER)

NEW QUESTION: 146
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. If the WSA host port is changed, the default port redirects web traffic to the correct port automatically.
D. PAC files use if-else statements to determine whether to use a proxy or a direct connection for traffic between the PC and the host.
E. The WSA hosts PAC files on port 6001 by default.
Answer: (SHOW ANSWER)

NEW QUESTION: 147

What provides total management for mobile and PC including managing inventory and device tracking, remote view, and live troubleshooting using the included native remote desktop support?

A. mobile device management

B. mobile content management

C. mobile application management

D. mobile access management

Answer: (SHOW ANSWER)

NEW QUESTION: 148

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

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

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

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

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

E. Cisco FTDv configured in routed mode and IPv6 configured

Answer: (SHOW ANSWER)

NEW QUESTION: 149

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. real-time feeds from global threat intelligence centers

C. signature-based endpoint protection on company endpoints

D. email integration to protect endpoints from malicious content that is located in email

E. macro-based protection to keep connected endpoints safe

Answer: (SHOW ANSWER)

NEW QUESTION: 150

Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)

A. It must reside in the trusted store of the WSA.

B. it must contain a SAN.

C. It must have been signed by an internal CA.

D. It must reside in the trusted store of the endpoint.

E. It must include the current date.

Answer: (SHOW ANSWER)

NEW QUESTION: 151

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

A. RAT

B. Sophos engine
C. white list
D. DLP
E. outbreak filters
Answer: (SHOW ANSWER)

NEW QUESTION: 152
Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?
A. IP Blacklist Center
B. IP and Domain Reputation Center
C. File Reputation Center
D. AMP Reputation Center
Answer: (SHOW ANSWER)

NEW QUESTION: 153
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: 154
What is a prerequisite when integrating a Cisco ISE server and an AD domain?
A. Place the Cisco ISE server and the AD server in the same subnet
B. Configure a common administrator account
C. Configure a common DNS server
D. Synchronize the clocks of the Cisco ISE server and the AD server
Answer: (SHOW ANSWER)
The following are the prerequisites to integrate Active Directory with Cisco ISE. + Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI. + If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that trust

relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation. + You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE. 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: 155
What are two features of NetFlow flow monitoring? (Choose two)
A. Can track ingress and egress information
B. Include the flow record and the flow importer
C. Copies all ingress flow information to an interface
D. Does not required packet sampling on interfaces
E. Can be used to track multicast, MPLS, or bridged traffic
Answer: (SHOW ANSWER)
The following are restrictions for Flexible NetFlow: + Traditional NetFlow (TNF) accounting is not supported. + Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported. + Both ingress and egress NetFlow accounting is supported. + Microflow policing feature shares the NetFlow hardware resource with FNF. + Only one flow monitor per interface and per direction is supported. Reference: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html When configuring NetFlow, follow these guidelines and restrictions: + Except in PFC3A mode, NetFlow supports bridged IP traffic. PFC3A mode does not support NetFlow bridged IP traffic. + NetFlow supports multicast IP traffic. Reference:
https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.html The Flexible NetFlow - MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching

(MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow.html
+ Traditional NetFlow (TNF) accounting is not supported.
+ Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported.
+ Both ingress and egress NetFlow accounting is supported.
+ Microflow policing feature shares the NetFlow hardware resource with FNF.
+ Only one flow monitor per interface and per direction is supported.
Reference:
consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html
When configuring NetFlow, follow these guidelines and restrictions:
+ Except in PFC3A mode, NetFlow supports bridged IP traffic. PFC3A mode does not support NetFlow bridged IP traffic.
+ NetFlow supports multicast IP traffic.
The Flexible NetFlow - MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN The following are restrictions for Flexible NetFlow: + Traditional NetFlow (TNF) accounting is not supported. + Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported. + Both ingress and egress NetFlow accounting is supported. + Microflow policing feature shares the NetFlow hardware resource with FNF. + Only one flow monitor per interface and per direction is supported. Reference:
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/
consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html When configuring NetFlow, follow these guidelines and restrictions: + Except in PFC3A mode, NetFlow supports bridged IP traffic. PFC3A mode does not support NetFlow bridged IP traffic. + NetFlow supports multicast IP traffic. Reference:
https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.html The Flexible NetFlow - MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgmpls-netflow.html

NEW QUESTION: 156
What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?
A. It decrypts HTTPS application traffic for unauthenticated users.
B. It alerts users when the WSA decrypts their traffic.
C. It provides enhanced HTTPS application detection for AsyncOS.
D. It decrypts HTTPS application traffic for authenticated users.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 157
Which solution supports high availability in routed or transparent mode as well as in northbound and southbound deployments?
A. Cisco Firepower NGFW physical appliance with Cisco. FMC

B. Cisco Firepower NGFW Virtual appliance with Cisco FMC
C. Cisco FTD with Cisco ASDM
D. Cisco FTD with Cisco FMC
Answer: (SHOW ANSWER)

NEW QUESTION: 158
A network administrator is configuring SNMPv3 on a new router. The users have already been created; however, an additional configuration is needed to facilitate access to the SNMP views. What must the administrator do to accomplish this?
A. map SNMPv3 users to SNMP views
B. specify the UDP port used by SNMP
C. set the password to be used for SNMPv3 authentication
D. define the encryption algorithm to be used by SNMPv3
Answer: (SHOW ANSWER)

NEW QUESTION: 159
What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?
A. Cisco Umbrella
B. External Threat Feeds
C. Cisco Threat Grid
D. Cisco Stealthwatch
Answer: (SHOW ANSWER)
Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector Cisco Threat Intelligence Director (CTID) can be integrated with existing Threat Intelligence Platforms deployed by your organization to ingest threat intelligence automatically. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector

NEW QUESTION: 160
In a PaaS model, which layer is the tenant responsible for maintaining and patching?
A. hypervisor
B. virtual machine
C. application
D. network
Answer: (SHOW ANSWER)

NEW QUESTION: 161
Drag and drop the security solutions from the left onto the benefits they provide on the right.
Answer:

NEW QUESTION: 162

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

A. Forward file

B. PAC file

C. Transparent mode

D. Bridge mode

Answer: (SHOW ANSWER)

NEW QUESTION: 163

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

A. editing

B. authoring

C. consumption

D. sharing

Answer: (SHOW ANSWER)

NEW QUESTION: 164

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

A. Virtual routing and forwarding

B. Microsegmentation

C. Access control policy

D. Virtual LAN

Answer: (SHOW ANSWER)

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

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

NEW QUESTION: 165

Refer to the exhibit.

Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

A. show authentication registrations

B. show authentication method

C. show dot1x all

D. show authentication sessions
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137 Displaying the Summary of All Auth Manager Sessions on the Switch Enter the following:
Switch# show authentication sessions
Interface MAC Address Method Domain Status Session ID
Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58 Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

NEW QUESTION: 166
Refer to the exhibit. What does this Python script accomplish?
A. It allows authentication with TLSv1 SSL protocol
B. It authenticates to a Cisco ISE with an SSH connection.
C. It authenticates to a Cisco ISE server using the username of ersad
Answer: (SHOW ANSWER)

NEW QUESTION: 167
What are two list types within AMP for Endpoints Outbreak Control? (Choose two)
A. blocked ports
B. simple custom detections
C. command and control
D. allowed applications
E. URL
Answer: (SHOW ANSWER)
Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists. A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine. Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine.
Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced

Custom Detections, and IP Blocked and Allowed Lists. A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine. Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf

NEW QUESTION: 168
Which component of Cisco umbrella architecture increases reliability of the service?
A. AMP Threat grid
B. Cisco Talos
C. BGP route reflector
D. Anycast IP
Answer: (SHOW ANSWER)

NEW QUESTION: 169
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. organization owned root
C. self-signed
D. third-party
Answer: (SHOW ANSWER)

NEW QUESTION: 170
Refer to the exhibit.
What are two indications of the Cisco Firepower Services Module configuration?
(Choose two.)
A. The module is operating in IDS mode.
B. Traffic is blocked if the module fails.
C. Traffic continues to flow if the module fails.
D. The module fails to receive redirected traffic
E. The module is operating in IPS mode.
Answer: (SHOW ANSWER)

NEW QUESTION: 171
What is a difference between FlexVPN and DMVPN?
A. DMVPN uses only IKEv1 FlexVPN uses only IKEv2
B. FlexVPN uses IKEv2, DMVPN uses IKEv1 or IKEv2
C. DMVPN uses IKEv1 or IKEv2, FlexVPN only uses IKEv1
D. FlexVPN uses IKEv1 or IKEv2, DMVPN uses only IKEv2
Answer: (SHOW ANSWER)

NEW QUESTION: 172
An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?
A. SIEM
B. CASB
C. Adaptive MFA
D. Cisco Cloudlock
Answer: D (LEAVE A REPLY)
+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy. + Cloudlock is API-based. + Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file). 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: 173
Which capability is provided by application visibility and control?
A. deep packet inspection
B. reputation filtering
C. data obfuscation
D. data encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 174
An administrator needs to configure the Cisco ASA via ASDM such that the network management system can actively monitor the host using SNMPv3. Which two tasks must be performed for this configuration?
(Choose two.)
A. Specify the SNMP manager and UDP port.
B. Specify a community string.
C. Add an SNMP host access entry
D. Specify an SNMP user group
E. Add an SNMP USM entry
Answer: (SHOW ANSWER)

NEW QUESTION: 175
Which security solution protects users leveraging DNS-layer security?
A. Cisco ASA
B. Cisco Umbrella
C. Cisco ISE
D. Cisco FTD
Answer: (SHOW ANSWER)

NEW QUESTION: 176
A network administrator is using the Cisco ESA with AMP to upload files to the cloud for analysis. The network is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?
A. AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.
B. The file is queued for upload when connectivity is restored.
C. The file upload is abandoned.
D. The ESA immediately makes another attempt to upload the file.
Answer: (SHOW ANSWER)
The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more. Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technoteesa-00.html In this question, it stated "the network is congested" (not the file analysis server was overloaded) so the appliance will not try to upload the file again.
connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.
Reference:
In this question, it stated "the network is congested" (not the file analysis server was overloaded) so the The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more. Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technoteesa-00.html In this question, it stated "the network is congested" (not the file analysis server was overloaded) so the appliance will not try to upload the file again.

NEW QUESTION: 177
Refer to the exhibit.
Which type of authentication is in use?
A. LDAP authentication for Microsoft Outlook
B. POP3 authentication
C. SMTP relay server authentication
D. external user and relay mail authentication
Answer: (SHOW ANSWER)
The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection. Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118844-technoteesa-00.html The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.
messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.
Reference:
The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection. Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118844-technoteesa-00.html The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

NEW QUESTION: 178
An engineer is configuring Cisco Umbrella and has an identity that references two different policies. Which action ensures that the..... use takes precedence over the second one?
A. Configure the default policy to redirect the requests to the correct policy.
B. Make the correct policy first in the policy order.
C. Configure only the policy with the most recently changed timestamp.
D. Place the policy with the most-specific configuration last in the policy order.
Answer: (SHOW ANSWER)

NEW QUESTION: 179
Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?
A. SDLC
B. Lambda
C. Docker
D. Contiv

Answer: (SHOW ANSWER)

NEW QUESTION: 180

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

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

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

C. It allows ARP traffic with a single access rule

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

Answer: (SHOW ANSWER)

A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place. Each bridge group includes a Bridge Virtual Interface (BVI). The ASA uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported. You can include multiple interfaces per bridge group. If you use more than 2 interfaces per bridge group, you can control communication between multiple segments on the same network, and not just between inside and outside. For example, if you have three inside segments that you do not want to communicate with each other, you can put each segment on a separate interface, and only allow them to communicate with the outside interface. Or you can customize the access rules between interfaces to allow only as much access as desired. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.html Note: BVI interface is not used for management purpose. But we can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA.

supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place.

Each bridge group includes a Bridge Virtual Interface (BVI). The ASA uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.

You can include multiple interfaces per bridge group. If you use more than 2 interfaces per bridge group, you can control communication between multiple segments on the same network, and not just between inside and outside. For example, if you have three inside segments that you do not want to communicate with each other, you can put each segment on a separate interface, and only allow them to communicate with the outside interface. Or you can customize the access rules between interfaces to allow only as much access as desired.

Reference:

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

a separate interface, and only allow them to communicate with the outside interface. Or you can customize the access rules between interfaces to allow only as much access as desired. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.html Note: BVI interface is not used for management purpose. But we can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA.

NEW QUESTION: 181
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. westbound AP
B. eastbound API
C. southbound API
D. northbound API
Answer: (SHOW ANSWER)

NEW QUESTION: 182
Elliptic curve cryptography is a stronger more efficient cryptography method meant to replace which current encryption technology?
A. 3DES
B. RSA
C. DES
D. AES
Answer: (SHOW ANSWER)
Compared to RSA, the prevalent public-key cryptography of the Internet today, Elliptic Curve Cryptography (ECC) offers smaller key sizes, faster computation,as well as memory, energy and bandwidth savings and is thus better suited forsmall devices.

NEW QUESTION: 183
Which type of data does the Cisco Stealthwatch system collect and analyze from routers, switches, and firewalls?
A. NetFlow
B. SNMP
C. NTP
D. syslog
Answer: (SHOW ANSWER)

NEW QUESTION: 184
How does a WCCP-configured router identify if the Cisco WSA is functional?
A. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the router.
B. The WSA sends a Here-I-Am message every 10 seconds, and the router acknowledges with an ISee-You message.
C. The router sends a Here-I-Am message every 10 seconds, and the WSA acknowledges with an ISee-You message.
D. If an ICMP ping fails three consecutive times between a router and the WSA, traffic is no longer transmitted to the WSA.
Answer: (SHOW ANSWER)

NEW QUESTION: 185
Which solution stops unauthorized access to the system if a user's password is compromised?
A. VPN
B. MFA
C. AMP
D. SSL
Answer: (SHOW ANSWER)

NEW QUESTION: 186
What is a functional difference between Cisco AMP for Endpoints and Cisco Umbrella Roaming Client?
A. AMP for Endpoints stops and tracks malicious activity on hosts, and the Umbrella Roaming Client tracks only URL-based threats.
B. The Umbrella Roaming client stops and tracks malicious activity on hosts, and AMP for Endpoints tracks only URL-based threats.
C. The Umbrella Roaming Client authenticates users and provides segmentation, and AMP for Endpoints allows only for VPN connectivity
D. AMP for Endpoints authenticates users and provides segmentation, and the Umbrella Roaming Client allows only for VPN connectivity.
Answer: (SHOW ANSWER)

NEW QUESTION: 187
Which method is used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources?
A. BYOD on boarding
B. Simple Certificate Enrollment Protocol
C. Client provisioning
D. MAC authentication bypass
Answer: (SHOW ANSWER)
When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network. Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices

portal. Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/ m_ise_devices_byod.html data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network.
Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal.
Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices.
Reference:
When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network. Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal. Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/ m_ise_devices_byod.html

NEW QUESTION: 188
An organization deploys multiple Cisco FTD appliances and wants to manage them using one centralized solution. The organization does not have a local VM but does have existing Cisco ASAs that must migrate over to Cisco FTDs. Which solution meets the needs of the organization?
A. Cisco FDM
B. Cisco FMC
C. CDO
D. CSM
Answer: (SHOW ANSWER)

NEW QUESTION: 189
Which two cryptographic algorithms are used with IPsec? (Choose two)
A. AES-BAC
B. AES-ABC
C. HMAC-SHA1/SHA2
D. Triple AMC-CBC
E. AES-CBC
Answer: (SHOW ANSWER)
Cryptographic algorithms defined for use with IPsec include:
+ HMAC-SHA1/SHA2 for integrity protection and authenticity.
+ TripleDES-CBC for confidentiality
+ AES-CBC and AES-CTR for confidentiality.
+ AES-GCM and ChaCha20-Poly1305 providing confidentiality and authentication together efficiently.

NEW QUESTION: 190
Which standard is used to automate exchanging cyber threat information?
A. STIX
B. TAXIL
C. IoC
D. MITRE
Answer: (SHOW ANSWER)

NEW QUESTION: 191
What are two functions of TAXII in threat intelligence sharing? (Choose two.)
A. allows users to describe threat motivations and abilities
B. exchanges trusted anomaly intelligence information
C. determines how threat intelligence information is relayed
D. determines the "what" of threat intelligence
E. Supports STIX information
Answer: (SHOW ANSWER)

NEW QUESTION: 192
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. overflowing the buffer's memory
B. sniffing the packets between the two hosts
C. inserting malicious commands into the database
D. sending continuous pings
Answer: C (LEAVE A REPLY)

NEW QUESTION: 193
Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?
A. Cisco Talos Intelligence
B. Cognitive Threat Analytics
C. Threat Intelligence Director
D. Encrypted Traffic Analytics
Answer: (SHOW ANSWER)

NEW QUESTION: 194
Which attack type attempts to shut down a machine or network so that users are not able to access it?
A. smurf
B. bluesnarfing
C. MAC spoofing
D. IP spoofing

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

NEW QUESTION: 195
An engineer is deploying Cisco Advanced Malware Protection (AMP) for Endpoints and wants to create a policy that prevents users from executing file named abc424952615.exe without quarantining that file What type of Outbreak Control list must the SHA.-256 hash value for the file be added to in order to accomplish this?
A. Blocked Application
B. Advanced Custom Detection
C. Isolation
D. Simple Custom Detection
Answer: (SHOW ANSWER)

NEW QUESTION: 196
A network engineer must configure a Cisco ESA to prompt users to enter two forms of information before gaining access The Cisco ESA must also join a cluster machine using preshared keys What must be configured to meet these requirements?
A. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA GUI
B. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA CLI.
C. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA GUI.
D. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA CLI
Answer: (SHOW ANSWER)

NEW QUESTION: 197
What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?
A. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not
B. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA
C. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA
D. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA.
Answer: (SHOW ANSWER)

NEW QUESTION: 198

A network engineer has entered the snmp-server user andy myv3 auth sha cisco priv aes 256 cisc0380739941 command and needs to send SNMP information to a host at 10.255.254.1. Which command achieves this goal?

A. snmp-server host inside 10.255.254.1 version 3 andy

B. snmp-server host inside 10.255.254.1 version 3 myv3

C. snmp-server host inside 10.255.254.1 snmpv3 andy

D. snmp-server host inside 10.255.254.1 snmpv3 myv3

Answer: (SHOW ANSWER)

The command "snmp-server user user-name group-name [remote ip-address [udp-port port]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]" adds a new user (in this case "andy") to an SNMPv3 group (in this case group name "myv3") and configures a password for the user.

In the "snmp-server host" command, we need to:

+ Specify the SNMP version with key word "version {1 | 2 | 3}"

+ Specify the username ("andy"), not group name ("myv3").

Note: In "snmp-server host inside ..." command, "inside" is the interface name of the ASA interface through which the NMS (located at 10.255.254.1) can be reached.

NEW QUESTION: 199

What is a functional difference between a Cisco ASA and a Cisco IOS router with Zone-based policy firewall?

A. The Cisco IOS router with Zone-Based Policy Firewall denies all traffic by default, whereas the Cisco ASA starts out by allowing all traffic until rules are added

B. The Cisco IOS router with Zone-Based Policy Firewall can be configured for high availability, whereas the Cisco ASA cannot

C. The Cisco ASA can be configured for high availability whereas the Cisco IOS router with Zone-Based Policy Firewall cannot

D. The Cisco ASA denies all traffic by default whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces

Answer: (SHOW ANSWER)