Cisco.210-260.v2018-04-02.q137

Exam Code:	210-260
Exam Name:	Implementing Cisco Network Security
Certification Provider:	Cisco
Free Question Number:	137
Version:	v2018-04-02
# of views:	1001
# of Questions views:	54842
https://www.freecram.net/torrent/Cisco.210-260.v2018-04-02.q137.html	

NEW QUESTION: 1
What are two uses of SIEM software? (Choose two.)
A. collecting and archiving syslog data
B. alerting administrators to security events in real time
C. performing automatic network audits
D. configuring firewall and IDS devices
E. scanning email for suspicious attachments
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
SIEM can be used collecting and archiving syslog data and alerting administrators to security events in real time.
Reference: http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-business-architecture/sbaSIEM_deployG.pdf

NEW QUESTION: 2
Which Cisco Security Manager application collects information about device status and uses it to generate notifications and alerts?
A. FlexConfig
B. Device Manager
C. Report Manager
D. Health and Performance Monitor
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Health and Performance Monitor (HPM) periodically polls monitored ASA devices, IPS devices, and ASA-hosted VPN services for key health and performance data, including critical and non-critical issues, such

as memory usage, interface status, dropped packets, tunnel status, and so on. This information is used for alert generation and email notification, and to display trends based on aggregated data, which is available for hourly, daily, and weekly periods.
Reference:
http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-4/user/guide/CSMUserGuide_wrapper/wfplan.html

NEW QUESTION: 3
Which syslog severity level is level number 7?
A. Warning
B. Informational
C. Notification
D. Debugging
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/ configuration/guide/sm_nx_os_cg/sm_5syslog.html

NEW QUESTION: 4
What VPN feature allows traffic to exit the security appliance through the same interface it entered?
A. hairpinning
B. NAT
C. NAT traversal
D. split tunneling
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
This feature is useful for VPN traffic that enters an interface, but is then routed out of that same interface. For example, if you have a hub-and-spoke VPN network where the security appliance is the hub and the remote VPN networks are spokes, in order for one spoke to communicate with another spoke traffic must go to the security appliance and then out again to the other spoke.
Enter the same-security-traffic command in order to allow traffic to enter and exit the same interface.
ciscoasa(config)#same-security-traffic permit intra-interface
Reference: http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html

NEW QUESTION: 5
Which actions can a promiscuous IPS take to mitigate an attack? (Choose three.)
A. Modifying packets
B. Requesting connection blocking

C. Denying packets
D. Resetting the TCP connection
E. Requesting host blocking
F. Denying frames
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The following event actions can be deployed in Promiscuous mode. These actions are in affect for a user-configurable default time of 30 minutes. Because the IPS sensor must send the request to another device or craft a packet, latency is associated with these actions and could allow some attacks to be successful.
Blocking through usage of the Attack Response Controller (ARC) has the potential benefit of being able to perform to the network edge or at multiple places within the network.
Request block host: This event action will send an ARC request to block the host for a specified time frame, preventing any further communication. This is a severe action that is most appropriate when there is minimal chance of a false alarm or spoofing.
Request block connection: This action will send an ARC response to block the specific connection. This action is appropriate when there is potential for false alarms or spoofing.
Reset TCP connection: This action is TCP specific, and in instances where the attack requires several TCP packets, this can be a successful action. However, in some cases where the attack only needs one packet it may not work as well. Additionally, TCP resets are not very effective with protocols such as SMTP that consistently try to establish new connections, nor are they effective if the reset cannot reach the destination host in time.
Reference: http://www.cisco.com/c/en/us/about/security-center/ips-mitigation.html

NEW QUESTION: 6
What features can protect the data plane? (Choose three.)
A. policing
B. ACLs
C. IPS
D. antispoofing
E. QoS
F. DHCP-snooping
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Data plane security can be implemented using the following features:
Access control lists
Access control lists (ACLs) perform packet filtering to control which packets move through the network and where.
Antispoofing
ACLs can be used as an antispoofing mechanism that discards traffic that has an invalid source address.

Layer 2 security features
Cisco Catalyst switches have integrated features to help secure the Layer 2 infrastructure.
Reference: http://www.ciscopress.com/articles/article.asp?p=1924983&seqNum=5

NEW QUESTION: 7
Which command is needed to enable SSH support on a Cisco Router?
A. crypto key lock rsa
B. crypto key generate rsa
C. crypto key zeroize rsa
D. crypto key unlock rsa
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
There are four steps required to enable SSH support on a Cisco IOS router:
1. Configure the hostname command.
2. Configure the DNS domain.
3. Generate the SSH key to be used.
4. Enable SSH transport support for the virtual type terminal (vtys).
If you want to have one device act as an SSH client to the other, you can add SSH to a second device called Reed. These devices are then in a client-server arrangement, where Carter acts as the server, and Reed acts as the client. The Cisco IOS SSH client configuration on Reed is the same as required for the SSH server configuration on Carter.
Reference: http://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html

NEW QUESTION: 8
Refer to the exhibit.
What is the effect of the given command sequence?
A. It defines IPSec policy for traffic sourced from 10.10.10.0/24 with a destination of 10.100.100.0/24.
B. It defines IPSec policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24.
C. It defines IKE policy for traffic sourced from 10.10.10.0/24 with a destination of 10.100.100.0/24.
D. It defines IKE policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Crypto map entry "mymap 30" references the dynamic crypto map set "mydynamicmap," which can be used to process inbound security association negotiation requests that do not match "mymap" entries 10 or
20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in "mydynamicmap," for a flow "permitted" by the access list 103, IPSec will accept the request and set up security associations with the remote peer without previously knowing about the remote peer. If accepted,

the resulting security associations (and temporary crypto map entry) are established according to the settings specified by the remote peer.
Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfipsec.html

NEW QUESTION: 9
Which accounting notices are used to send a failed authentication attempt record to a AAA server? (Choose two.)
A. start-stop
B. stop-record
C. stop-only
D. stop
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Start-stop and stop-only notices are used to send a failed authentication attempt record to AAA server.
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xe-3s/sec-usr-aaa- xe-3s-book/sec-cfg-accountg.html

NEW QUESTION: 10
Which network device does NTP authenticate?
A. Only the time source
B. Only the client device
C. The firewall and the client device
D. The client device and the time source
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
NTP authentication, the device synchronizes to a time source only if the source carries one of the authentication keys specified by the ntp trusted-key command. The device drops any packets that fail the authentication check and prevents them from updating the local clock. NTP authentication is disabled by default.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/ configuration/guide/sm_nx_os_cg/sm_3ntp.html#wp1100303

NEW QUESTION: 11
Refer to the exhibit.
While troubleshooting site-to-site VPN, you issued the show crypto isakmp sa command. What does the given output show?
A. IPSec Phase 1 is established between 10.10.10.2 and 10.1.1.5.
B. IPSec Phase 2 is established between 10.10.10.2 and 10.1.1.5.
C. IPSec Phase 1 is down due to a QM_IDLE state.

D. IPSec Phase 2 is down due to a QM_IDLE state.

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Phase 1 of IPsec is used to establish a secure channel between the two peers that will be used for further data transmission. The ASAs will exchange secret keys, they authenticate each other and will negotiate about the IKE security policies. This is what happens in phase 1:

Authenticate and protect the identities of the IPsec peers.

Negotiate a matching IKE policy between IPsec peers to protect the IKE exchange.

Perform an authenticated Diffie-Hellman exchange to have matching shared secret keys.

Setup a secure tunnel for IKE phase 2.

Reference: https://networklessons.com/security/cisco-asa-site-site-ikev1-ipsec-vpn/

NEW QUESTION: 12

Scenario

In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.

To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

Which four tunneling protocols are enabled in the DfltGrpPolicy group policy? (Choose four)

A. Clientless SSL VPN

B. SSL VPN Client

C. PPTP

D. L2TP/IPsec

E. IPsec IKEv1

F. IPsec IKEv2

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

By clicking one the Configuration-> Remote Access -> Clientless CCL VPN Access-> Group Policies tab you can view the DfltGrpPolicy protocols as shown below:

NEW QUESTION: 13

Which source port does IKE use when NAT has been detected between two VPN gateways?

A. TCP 4500

B. TCP 500

C. UDP 4500

D. UDP 500
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Take the common case of the initiator behind the NAT. The initiator must quickly change to port 4500 once the NAT has been detected to minimize the window of IPsec-aware NAT problems.
Reference: https://tools.ietf.org/html/rfc3947

NEW QUESTION: 14
Which two authentication types does OSPF support? (Choose two.)
A. plaintext
B. MD5
C. HMAC
D. AES 256
E. SHA-1
F. DES
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
These are the three different types of authentication supported by OSPF.
Null Authentication-This is also called Type 0 and it means no authentication information is included in the packet header. It is the default.
Plain Text Authentication-This is also called Type 1 and it uses simple clear-text passwords.
MD5 Authentication-This is also called Type 2 and it uses MD5 cryptographic passwords.
Authentication does not need to be set. However, if it is set, all peer routers on the same segment must have the same password and authentication method. The examples in this document demonstrate configurations for both plain text and MD5 authentication.
Reference: http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13697-25.html

NEW QUESTION: 15
Which Cisco feature can help mitigate spoofing attacks by verifying symmetry of the traffic path?
A. Unidirectional Link Detection
B. Unicast Reverse Path Forwarding
C. TrustSec
D. IP Source Guard
Answer: (SHOW ANSWER)
Explanation/Reference:
The Unicast RPF feature helps to mitigate problems that are caused by malformed or forged IP source addresses that are passing through a router.
Reference:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfrpf.html

NEW QUESTION: 16
You want to allow all of your company's users to access the Internet without allowing other Web servers to collect the IP addresses of individual users. What two solutions can you use? (Choose two).
A. Configure a proxy server to hide users' local IP addresses.
B. Assign unique IP addresses to all users.
C. Assign the same IP address to all users.
D. Install a Web content filter to hide users' local IP addresses.
E. Configure a firewall to use Port Address Translation.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
To restrain servers to collect IP addresses of individual users, you have to configure a proxy server to hide users' local IP addresses and configure a firewall to use port address translation or PAT.

Valid 210-260 Dumps shared by ExamDiscuss.com for Helping Passing 210-260 Exam! ExamDiscuss.com now offer the **newest 210-260 exam dumps**, the ExamDiscuss.com 210-260 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 210-260 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/210-260/premium/ (**515** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 17
Which EAP method uses Protected Access Credentials?
A. EAP-FAST
B. EAP-TLS
C. EAP-PEAP
D. EAP-GTC
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
EAP-FAST is an EAP method that enables secure communication between a client and an authentication server by using Transport Layer Security (TLS) to establish a mutually authenticated tunnel. Within the tunnel, data in the form of type, length, and value (TLV) objects are used to send further authentication-related data between the client and the authentication server.
EAP-FAST supports the TLS extension as defined in RFC 4507 to support the fast re-establishment of the secure tunnel without having to maintain per-session state on the server. EAP-FAST-based mechanisms are defined to provision the credentials for the TLS extension. These credentials are called Protected Access Credentials (PACs).

Reference: http://www.cisco.com/c/en/us/td/docs/wireless/wlan_adapter/cb21ag/user/vista/1-0/configuration/guide/cb21ag10vistaconfigguide/eap_types.html

NEW QUESTION: 18
Which option describes information that must be considered when you apply an access list to a physical interface?
A. Protocol used for filtering
B. Direction of the access class
C. Direction of the access group
D. Direction of the access list
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
You use direction of the access group when you apply an access list to a physical interface.
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book/sec-create-ip-apply.html

NEW QUESTION: 19
Which Sourcefire logging action should you choose to record the most detail about a connection?
A. Enable logging at the end of the session.
B. Enable logging at the beginning of the session.
C. Enable alerts via SNMP to log events off-box.
D. Enable eStreamer to log events off-box.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
When the system detects a connection, in most cases you can log it at its beginning or its end. However, because blocked traffic is immediately denied without further inspection, in most cases you can log only beginning-of-connection events for blocked or blacklisted traffic; there is no unique end of connection to log. An exception occurs when you block encrypted traffic. When you enable connection logging in an SSL policy, the system logs end-of-connection rather than beginning-of-connection events. This is because the system cannot determine if a connection is encrypted using the first packet in the session, and thus cannot immediately block encrypted sessions.
Reference: http://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/AC-Connection-Logging.html#pgfId-1604681

NEW QUESTION: 20
A. Policy-based IPS
B. Anomaly-based IPS
C. Reputation-based IPS
D. Signature-based IPS

Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Cisco's best-in-class anomaly detection feature detects worms by learning the "normal" traffic patterns of the network, and then scanning for anomalous behavior. Fast-propagating network worms scan the network in order to infect other hosts. For each protocol or service, the anomaly detection program studies what is normal scanning activity, and accumulates this information in a threshold histogram and an absolute scanner threshold. The scanner threshold specifies the absolute scanning rate above which any source is considered malicious.
Reference: http://www.cisco.com/c/en/us/products/collateral/security/ips-4200-series-sensors/prod_brochure0900aecd805baea7.html

NEW QUESTION: 21
Which two services define cloud networks? (Choose two.)
A. Infrastructure as a Service
B. Platform as a Service
C. Security as a Service
D. Compute as a Service
E. Tenancy as a Service
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The diagram below depicts the Cloud Computing stack - it shows three distinct categories within Cloud Computing: Software as a Service, Platform as a Service and Infrastructure as a Service.
A simplified way of differentiating these flavors of Cloud Computing is as follows; SaaS applications are designed for end-users, delivered over the web
PaaS is the set of tools and services designed to make coding and deploying those applications quick and efficient
IaaS is the hardware and software that powers it all - servers, storage, networks, operating systems
Reference: https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/

NEW QUESTION: 22
Which components does HMAC use to determine the authenticity and integrity of a message? (Choose two.)
A. The password
B. The hash
C. The key
D. The transform set
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:
An HMAC is a MAC which is based on a hash function. The basic idea is to concatenate the key and the message, and hash them together. Since it is impossible, given a cryptographic hash, to find out what it is the hash of, knowing the hash (or even a collection of such hashes) does not make it possible to find the key. The basic idea doesn't quite work out, in part because of length extension attacks, so the actual HMAC construction is a little more complicated.
Reference: http://security.stackexchange.com/questions/20129/how-and-when-do-i-use-hmac/20301

NEW QUESTION: 23
Which three statements about host-based IPS are true? (Choose three.)
A. It can view encrypted files.
B. It can have more restrictive policies than network-based IPS.
C. It can generate alerts based on behavior at the desktop level.
D. It can be deployed at the perimeter.
E. It uses signature-based policies.
F. It works with deployed firewalls.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Cisco Host based IPS can generate alerts based on behavior at desktop level. They can also be more restrictive in policies than network based IPS. And you can view encrypted files using Host-based IPS solution.
Reference: http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3

NEW QUESTION: 24
Your security team has discovered a malicious program that has been harvesting the CEO's email messages and the company's user database for the last 6 months. What type of attack did your team discover?
A. advanced persistent threat
B. targeted malware
C. drive-by spyware
D. social activism
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Phishing attempts most often take the form of an email that seemingly comes from a company the recipient knows or does business with. The most recognized type of phishing attack is similar to the bank example described above, where the email asks the recipient to enter his account credentials on a website.
Reference: https://digitalguardian.com/blog/what-phishing-attack-defining-and-identifying-different-types-phishing-attacks

NEW QUESTION: 25
By which kind of threat is the victim tricked into entering username and password information at a disguised website?
A. Spoofing
B. Malware
C. Spam
D. Phishing
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.
Reference: https://en.wikipedia.org/wiki/Phishing

NEW QUESTION: 26
Which type of secure connectivity does an extranet provide?
A. other company networks to your company network
B. remote branch offices to your company network
C. your company network to the Internet
D. new networks to your company network
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Extranet or external network provides secure connectivity to other company networks from your own company's network.
Reference: http://searchenterprisewan.techtarget.com/definition/extranet

NEW QUESTION: 27
What is one requirement for locking a wired or wireless device from ISE?
A. The ISE agent must be installed on the device.
B. The device must be connected to the network when the lock command is executed.
C. The user must approve the locking action.
D. The organization must implement an acceptable use policy allowing device locking.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
To lock a wired or wireless device from ISE, you need to install ISE agent on that device first. The agent will assist in locking the device promptly.

NEW QUESTION: 28
If the native VLAN on a trunk is different on each end of the link, what is a potential consequence?
A. The interface on both switches may shut down
B. STP loops may occur
C. The switch with the higher native VLAN may shut down
D. The interface with the lower native VLAN may shut down
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
If the native VLAN on a trunk is different on each end of the link, STP loops may occur.
Reference: https://supportforums.cisco.com/discussion/12477986/using-different-native-vlans-different-ports-switch-configured-trunks

NEW QUESTION: 29
What is an advantage of placing an IPS on the inside of a network?
A. It can provide higher throughput.
B. It receives traffic that has already been filtered.
C. It receives every inbound packet.
D. It can provide greater security.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: Your IPS will generally be placed at an edge of the network, such as immediately inside an Internet firewall, or in front of a server farm. Position the IPS where it will see the bare minimum of traffic it needs to, in order to keep performance issues under tight control.
Reference: http://www.pcworld.com/article/144634/guide_network_intrusion_prevention_systems.html

NEW QUESTION: 30
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
To access ASDM, click the ASA icon in the topology diagram.
Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

When users login to the Clientless SSLVPN using https://209.165.201.2/test, which group policy will be applied?
A. test
B. clientless

C. Sales
D. DfltGrpPolicy
E. DefaultRAGroup
F. DefaultWEBVPNGroup
Answer: (SHOW ANSWER)
Explanation/Reference:
First navigate to the Connection Profiles tab as shown below, highlight the one with the test alias:
Then hit the "edit" button and you can clearly see the Sales Group Policy being applied.

NEW QUESTION: 31
Which statement about communication over failover interfaces is true?
A. All information that is sent over the failover and stateful failover interfaces is sent as clear text by default.
B. All information that is sent over the failover interface is sent as clear text, but the stateful failover link is encrypted by default.
C. All information that is sent over the failover and stateful failover interfaces is encrypted by default.
D. User names, passwords, and preshared keys are encrypted by default when they are sent over the failover and stateful failover interfaces, but other information is sent as clear text.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.
Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/configuration/guide/conf_gd/failover.html

Valid 210-260 Dumps shared by ExamDiscuss.com for Helping Passing 210-260 Exam!
ExamDiscuss.com now offer the **newest 210-260 exam dumps**, the ExamDiscuss.com 210-260 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 210-260 dumps with Test Engine here:
https://www.examdiscuss.com/Cisco/exam/210-260/premium/ (**515** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 32
Which option is the most effective placement of an IPS device within the infrastructure?

A. Inline, behind the internet router and firewall
B. Inline, before the internet router and firewall
C. Promiscuously, after the Internet router and before the firewall
D. Promiscuously, before the Internet router and the firewall
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet-inspection-based feature that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. While it is common practice to defend against attacks by inspecting traffic at the data centers and corporate headquarters, it is also critical to distribute the network-level defense to stop malicious traffic close to its entry point at the branch or telecommuter offices.
Reference: http://www.cisco.com/c/en/us/products/collateral/security/ios-intrusion-prevention-system-ips/prod_white_paper0900aecd8062acfb.html

NEW QUESTION: 33
Which statement about a PVLAN isolated port configured on a switch is true?
A. The isolated port can communicate only with the promiscuous port.
B. The isolated port can communicate with other isolated ports and the promiscuous port.
C. The isolated port can communicate only with community ports.
D. The isolated port can communicate only with other isolated ports.
Answer: (SHOW ANSWER)
Explanation/Reference:
A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.
Reference: http://www.cisco.com/c/en/us/tech/lan-switching/private-vlans-pvlans-promiscuous-isolated-community/index.html

NEW QUESTION: 34
Which statement about extended access lists is true?
A. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the destination
B. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the source
C. Extended access lists perform filtering that is based on destination and are most effective when applied to the source
D. Extended access lists perform filtering that is based on source and are most effective when applied to the destination
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

An extended ACL gives you much more power than just a standard ACL. Extended IP ACLs check both the source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters, which allow administrators more flexibility and control.
Reference: http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/access-control-list.html

NEW QUESTION: 35
Which two next-generation encryption algorithms does Cisco recommend? (Choose two.)
A. AES
B. 3DES
C. DES
D. MD5
E. DH-1024
F. SHA-384
G. Explanation/Reference:
Answer: (SHOW ANSWER)
The following table shows the relative security level provided by the recommended and NGE algorithms. The security level is the relative strength of an algorithm. An algorithm with a security level of x bits is stronger than one of y bits if x > y. If an algorithm has a security level of x bits, the relative effort it would take to "beat" the algorithm is of the same magnitude of breaking a secure x-bit symmetric key algorithm (without reduction or other attacks). The 128-bit security level is for sensitive information and the 192-bit level is for information of higher importance.
Reference: http://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

NEW QUESTION: 36
Which TACACS+ server-authentication protocols are supported on Cisco ASA firewalls? (Choose three.)
A. EAP
B. ASCII
C. PAP
D. PEAP
E. MS-CHAPv1
F. MS-CHAPv2
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The ASA supports TACACS+ server authentication with the following protocols: ASCII, PAP, CHAP, and MS-CHAPv1.
Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/general/asa-general-asdm/aaa-tacacs.html

NEW QUESTION: 37

Which of the following statements about access lists are true? (Choose three.)
A. Extended access lists should be placed as near as possible to the destination
B. Extended access lists should be placed as near as possible to the source
C. Standard access lists should be placed as near as possible to the destination
D. Standard access lists should be placed as near as possible to the source
E. Standard access lists filter on the source address
F. Standard access lists filter on the destination address
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Standard ACLs
A standard IP ACL is simple; it filters based on source address only. You can filter a source network or a source host, but you cannot filter based on the destination of a packet, the particular protocol being used such as the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP), or on the port number. You can permit or deny only source traffic.
Extended ACLs:
An extended ACL gives you much more power than just a standard ACL. Extended IP ACLs check both the source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters, which allow administrators more flexibility and control.
Named ACLs
One of the disadvantages of using IP standard and IP extended ACLs is that you reference them by number, which is not too descriptive of its use. With a named ACL, this is not the case because you can name your ACL with a descriptive name. The ACL named DenyMike is a lot more meaningful than an ACL simply numbered 1. There are both IP standard and IP extended named ACLs.
Another advantage to named ACLs is that they allow you to remove individual lines out of an ACL. With numbered ACLs, you cannot delete individual statements. Instead, you will need to delete your existing access list and re-create the entire list.
Reference: http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/access-control-list.html

NEW QUESTION: 38
Which of the following are features of IPsec transport mode? (Choose three.)
A. IPsec transport mode is used between end stations
B. IPsec transport mode is used between gateways
C. IPsec transport mode supports multicast
D. IPsec transport mode supports unicast
E. IPsec transport mode encrypts only the payload
F. IPsec transport mode encrypts the entire packet
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

IPSec can be run in either tunnel mode or transport mode. Each of these modes has its own particular uses and care should be taken to ensure that the correct one is selected for the solution:
Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.
Transport mode is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host-for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.
Reference: http://www.ciscopress.com/articles/article.asp?p=25477

NEW QUESTION: 39
When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?
A. Deny the connection inline.
B. Perform a Layer 6 reset.
C. Deploy an antimalware system.
D. Enable bypass mode.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
This action prevents the attacker from communicating with the victim on any port. However, the attacker could communicate with other hosts, making this action better suited for exploits that target a specific host.
This event action is appropriate when the likelihood of a false alarm or spoofing is minimal.
Reference: http://www.cisco.com/c/en/us/about/security-center/ips-mitigation.html

NEW QUESTION: 40
A. CCPr
B. Parser views
C. Access control lists
D. Port security
E. CoPP
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Starting with Cisco IOS Software release 12.4(4)T, Control Plane Protection (CPPr) can be used to restrict and/or police control plane traffic destined to the route processor of the Cisco IOS device. Although it is similar to Control Plane Policing (CoPP), CPPr has the ability to restrict/police traffic using finer granularity than that used by CoPP. CPPr divides the aggregate control plane into three separate control plane categories, known as subinterfaces: (1) host, (2) transit, and (3) CEF-exception. In addition, CPPr includes the following additional control plane protection features:
The port-filtering feature provides for policing/dropping of packets going to closed or nonlistening TCP/UDP ports

Queue thresholding limits the number of packets for a specified protocol that will be allowed in the control plane IP input queue
Reference: http://www.cisco.com/c/en/us/about/security-center/understanding-cppr.html

NEW QUESTION: 41
What is a possible reason for the error message?Router(config)#aaa server?% Unrecognized command
A. The command syntax requires a space after the word "server"
B. The command is invalid on the target device
C. The router is already running the latest operating system
D. The router is a new device on which the aaa new-model command must be applied before continuing
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
It means that the router is a new device on which aaa new model command must be applied before inducting it into the system.
Reference: http://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html

NEW QUESTION: 42
Refer to the exhibit.
What type of firewall would use the given configuration line?
A. a stateful firewall
B. a personal firewall
C. a proxy firewall
D. an application firewall
E. a stateless firewall
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: stateful firewalls, a type of firewall that attempts to track the state of network connections when filtering packets. The stateful firewall's capabilities are somewhat of a cross between the functions of a packet filter and the additional application-level protocol intelligence of a proxy.
Reference: http://www.informit.com/articles/article.aspx?p=373120

NEW QUESTION: 43
Which sensor mode can deny attackers inline?
A. IPS
B. fail-close
C. IDS
D. fail-open
Answer: A (LEAVE A REPLY)
Explanation/Reference:

Explanation:
You can configure certain aspects of the deny attackers inline event action. You can configure the number of seconds you want to deny attackers inline and you can limit the number of attackers you want denied in the system at any one time.
Reference: http://www.cisco.com/c/en/us/td/docs/security/ips/5-1/configuration/guide/cli/cliguide/cliEvAct.html

NEW QUESTION: 44
What is the default timeout interval during which a router waits for responses from a TACACS server before declaring a timeout failure?
A. 5 seconds
B. 10 seconds
C. 15 seconds
D. 20 seconds
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
You can set a global timeout interval for all TACACS+ servers. The timeout interval determines how long the Cisco CG-OS router waits for responses from TACACS+ servers before declaring a timeout failure.
Reference: http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/security/security_Book/sec_tacacspl_cgr1000.html

NEW QUESTION: 45
What is the only permitted operation for processing multicast traffic on zone-based firewalls?
A. Only control plane policing can protect the control plane against multicast traffic.
B. Stateful inspection of multicast traffic is supported only for the self-zone.
C. Stateful inspection for multicast traffic is supported only between the self-zone and the internal zone.
D. Stateful inspection of multicast traffic is supported only for the internal zone.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: stateful inspection support for multicast traffic is not supported between any zones, including the self zone. Use Control Plane Policing for the protection of the control plane against multicast traffic.
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/sec-zone-pol-fw.html

NEW QUESTION: 46
Which type of security control is defense in depth?
A. Threat mitigation
B. Risk analysis
C. Botnet mitigation
D. Overt and covert channels

Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Defense in-depth is a technique that uses many layers of network defense to secure a network and all devices connected to that network. The theory behind defense in-depth is to deploy different layers of security in key parts of the network to detect, contain and ultimately stop an attack.
Reference: http://security2b.blogspot.com/2006/12/what-is-defense-in-depth-and-why-is-it.html

Valid 210-260 Dumps shared by ExamDiscuss.com for Helping Passing 210-260 Exam!
ExamDiscuss.com now offer the **newest 210-260 exam dumps**, the ExamDiscuss.com 210-260 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 210-260 dumps with Test Engine here:
https://www.examdiscuss.com/Cisco/exam/210-260/premium/ (**515** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 47
A clientless SSL VPN user who is connecting on a Windows Vista computer is missing the menu option for Remote Desktop Protocol on the portal web page. Which action should you take to begin troubleshooting?
A. Ensure that the RDP2 plug-in is installed on the VPN gateway
B. Reboot the VPN gateway
C. Instruct the user to reconnect to the VPN gateway
D. Ensure that the RDP plug-in is installed on the VPN gateway
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The RDP plug-in is only one of the plug-ins available to users, along with others such as Secure Shell (SSH), Virtual Network Computing (VNC), and Citrix. The RDP plug-in is one of the most frequently used plug-ins in this collection. This document provides more details about the deployment and troubleshoot procedures for this plug-in.
Reference: http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113600-technote-product-00.html

NEW QUESTION: 48
Refer to the exhibit.
How many times was a read-only string used to attempt a write operation?
A. 9
B. 6
C. 4

D. 3
E. 2
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The read-only string attempted a write operation nine times as seen in the exhibit. It says, 9 illegal operations to community name supplied which means the read-only string attempted 9 write operations.
Reference: http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

NEW QUESTION: 49
An attacker installs a rogue switch that sends superior BPDUs on your network. What is a possible result of this activity?
A. The switch could offer fake DHCP addresses.
B. The switch could become the root bridge.
C. The switch could be allowed to join the VTP domain.
D. The switch could become a transparent bridge.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The BPDU guard feature is designed to allow network designers to keep the active network topology predictable. BPDU guard is used to protect the switched network from the problems that may be caused by the receipt of BPDUs on ports that should not be receiving them. The receipt of unexpected BPDUs may be accidental or may be part of an unauthorized attempt to add a switch to the network. BPDU guard is best deployed toward user-facing ports to prevent rogue switch network extensions by an attacker.

NEW QUESTION: 50
A. The user will be prompted to authenticate using the enable password
B. Authentication attempts to the router will be denied
C. Authentication will use the router`s local database
D. Authentication attempts will be sent to the TACACS+ server
Answer: A,B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern would continue through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated.

It is important to remember that a FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.
Suppose the system administrator wants to apply a method list only to a particular interface or set of interfaces. In this case, the system administrator creates a named method list and then applies this named list to the applicable interfaces.
Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathen.html

NEW QUESTION: 51
If a switch receives a superior BPDU and goes directly into a blocked state, what mechanism must be in use?
A. root guard
B. EtherChannel guard
C. loop guard
D. BPDU guard
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The root guard feature protects the network against such issues.
The configuration of root guard is on a per-port basis. Root guard does not allow the port to become an STP root port, so the port is always STP-designated. If a better BPDU arrives on this port, root guard does not take the BPDU into account and elect a new STP root. Instead, root guard puts the port into the root- inconsistent STP state. You must enable root guard on all ports where the root bridge should not appear.
In a way, you can configure a perimeter around the part of the network where the STP root is able to be located.
In the following figure, enable root guard on the Switch C port that connects to Switch D.
Switch C in figure below blocks the port that connects to Switch D, after the switch receives a superior BPDU. Root guard puts the port in the root-inconsistent STP state. No traffic passes through the port in this state. After device D ceases to send superior BPDUs, the port is unblocked again. Via STP, the port goes from the listening state to the learning state, and eventually transitions to the forwarding state. Recovery is automatic; no human intervention is necessary.
This message appears after root guard blocks a port:
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
Moved to root-inconsistent state
Reference: http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html

NEW QUESTION: 52
Which command verifies phase 1 of an IPsec VPN on a Cisco router?
A. show crypto map
B. show crypto ipsec sa
C. show crypto isakmp sa
D. show crypto engine connection active
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
When a problem exist with the connectivity, even phase 1 of VPN does not come up. On the ASA, if connectivity fails, the SA output is similar to this example, which indicates possibly an incorrect crypto peer configuration and/or incorrect ISAKMP proposal configuration:
Router#show crypto isakmp sa
1 IKE Peer: XX.XX.XX.XX
Type : L2L Role : initiator
Rekey : no State : MM_WAIT_MSG2
Reference: http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html

NEW QUESTION: 53
Which type of firewall can act on the behalf of the end device?
A. Stateful packet
B. Application
C. Packet
D. Proxy
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Local session termination allows routers to act as proxies for remote systems that represent session endpoints. (A proxy is a device that acts on behalf of another device.) Reference: http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_--_Internetworking_Design_Basics

NEW QUESTION: 54
What type of security support is provided by the Open Web Application Security Project?
A. Education about common Web site vulnerabilities.
B. A Web site security framework.
C. A security discussion forum for Web site developers.
D. Scoring of common vulnerabilities and exposures.
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:
OWASP seeks to educate developers, designers, architects and business owners about the risks associated with the most common Web application security vulnerabilities. OWASP, which supports both open source and commercial security products, has become known as a forum in which information technology professionals can network and build expertise. The organization publishes a popular Top Ten list that explains the most dangerous Web application security flaws and provides recommendations for dealing with those flaws.
Reference: http://searchsoftwarequality.techtarget.com/definition/OWASP

NEW QUESTION: 55
In a security context, which action can you take to address compliance?
A. Implement rules to prevent a vulnerability.
B. Correct or counteract a vulnerability.
C. Reduce the severity of a vulnerability.
D. Follow directions from the security appliance manufacturer to remediate a vulnerability.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Addressing compliance is an integral part of security context. It implement rules to prevent vulnerability.
Reference: http://www.cisco.com/security/

NEW QUESTION: 56
Which type of mirroring does SPAN technology perform?
A. Remote mirroring over Layer 2
B. Remote mirroring over Layer 3
C. Local mirroring over Layer 2
D. Local mirroring over Layer 3
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The traffic for each RSPAN session is carried as Layer 2 nonroutable traffic over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. All participating switches must be trunk-connected at Layer 2.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/span.html

NEW QUESTION: 57
Which protocol provides security to Secure Copy?
A. IPsec
B. SSH
C. HTTPS

D. ESP
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The Secure Copy (SCP) feature provides a secure and authenticated method for copying device configurations or device image files. SCP relies on Secure Shell (SSH), an application and protocol that provide a secure replacement for the Berkeley r-tools suite (Berkeley university's own set of networking applications).
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-s/sec-usr-ssh-15-s-book/sec-secure-copy.html

NEW QUESTION: 58
In which type of attack does an attacker send email messages that ask the recipient to click a link such as https://www.cisco.net.cc/securelogon?
A. phishing
B. secure transaction
C. solicitation
D. pharming
Answer: (SHOW ANSWER)

NEW QUESTION: 59
Refer to the exhibit.
What is the effect of the given command sequence?
A. It configures IKE Phase 1.
B. It configures a site-to-site VPN tunnel.
C. It configures a crypto policy with a key size of 14400.
D. It configures IPSec Phase 2.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
To create an IKE policy, enter the crypto ikev1 | ikev2 policy command from global configuration mode. The prompt displays IKE policy configuration mode. For example:
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
After creating the policy, you can specify the settings for the policy.
Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/vpn_ike.html

NEW QUESTION: 60
A. Every time a new update is available.
B. When the local scanner has detected a new virus.

C. When a new virus is discovered in the wild.
D. When the system detects a browser hook.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
You can automatically check for Anti-Virus signature updates from Cisco's signature server every 24 hours or to manually check for Anti-Virus signature updates at any time by clicking Update. When a newer signature file is available on the server, the new signature file will be downloaded to your device.
Reference: https://www.cisco.com/assets/sol/sb/isa500_emulator/help/guide/af1321261.html

NEW QUESTION: 61
What three actions are limitations when running IPS in promiscuous mode? (Choose three.)
A. deny attacker
B. deny packet
C. modify packet
D. request block connection
E. request block host
F. reset TCP connection
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The following actions require the device to be deployed in Inline mode and are in affect for a user-configurable default time of 3600 seconds (60 minutes).
Deny attacker inline: This action is the most severe and effectively blocks all communication from the attacking host that passes through the IPS for a specified period of time. Because this event action is severe, administrators are advised to use this only when the probability of false alarms or spoofing is minimal.
Deny attacker service pair inline: This action prevents communication between the attacker IP address and the protected network on the port in which the event was detected. However, the attacker would be able to communicate on another port that has hosts on the protected network. This event action works well for worms that attack many hosts on the same service port. If an attack occurred on the same host but on another port, this communication would be allowed. This event action is appropriate when the likelihood of a false alarm or spoofing is minimal.
Deny attacker victim pair inline: This action prevents the attacker from communicating with the victim on any port. However, the attacker could communicate with other hosts, making this action better suited for exploits that target a specific host. This event action is appropriate when the likelihood of a false alarm or spoofing is minimal.
Deny connection inline: This action prevents further communication for the specific TCP flow. This action is appropriate when there is the potential for a false alarm or spoofing and when an administrator wants to prevent the action but not deny further communication.

Deny packet inline: This action prevents the specific offending packet from reaching its intended destination. Other communication between the attacker and victim or victim network may still exist. This action is appropriate when there is the potential for a false alarm or spoofing. Note that for this action, the default time has no effect.
Modify packet inline: This action enables the IPS device to modify the offending part of the packet. However, it forwards the modified packet to the destination. This action is appropriate for packet normalization and other anomalies, such as TCP segmentation and IP fragmentation re-ordering.
Reference: http://www.cisco.com/c/en/us/about/security-center/ips-mitigation.html

Valid 210-260 Dumps shared by ExamDiscuss.com for Helping Passing 210-260 Exam! ExamDiscuss.com now offer the **newest 210-260 exam dumps**, the ExamDiscuss.com 210-260 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 210-260 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/210-260/premium/ (**515** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 62
A specific URL has been identified as containing malware. What action can you take to block users from accidentally visiting the URL and becoming infected with malware.
A. Enable URL filtering on the perimeter router and add the URLs you want to block to the router's local URL list.
B. Enable URL filtering on the perimeter firewall and add the URLs you want to allow to the router's local URL list.
C. Enable URL filtering on the perimeter router and add the URLs you want to allow to the firewall's local URL list.
D. Create a blacklist that contains the URL you want to block and activate the blacklist on the perimeter router.
E. Create a whitelist that contains the URLs you want to allow and activate the whitelist on the perimeter router.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
URL filtering window displays the global settings for URL filtering on the router. You can maintain the local URL list and the URL filter server list in the Additional Tasks screens or in the Application Security windows. The Global settings for URL filtering can only be maintained from this Additional Tasks window. Use the Edit Global Settings button to change these values.
Reference: http://www.cisco.com/c/en/us/td/docs/routers/access/cisco_router_and_security_device_manager/24/software/user/guide/URLftr.html

NEW QUESTION: 63
Which statements about smart tunnels on a Cisco firewall are true? (Choose two.)
A. Smart tunnels can be used by clients that do not have administrator privileges
B. Smart tunnels support all operating systems
C. Smart tunnels offer better performance than port forwarding
D. Smart tunnels require the client to have the application installed locally
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Tunnel offers better performance than browser plug-ins.
Port forwarding is the legacy technology for supporting TCP-based applications over a Clientless SSL VPN connection. Unlike port forwarding, Smart Tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.
Smart Tunnel does not require users to have administrator privileges.
Smart Tunnel does not require the administrator to know application port numbers in advance.
Reference: http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/tunnel.pdf

NEW QUESTION: 64
Which statements about reflexive access lists are true? (Choose three.)
A. Reflexive access lists create a permanent ACE
B. Reflexive access lists approximate session filtering using the established keyword
C. Reflexive access lists can be attached to standard named IP ACLs
D. Reflexive access lists support UDP sessions
E. Reflexive access lists can be attached to extended named IP ACLs
F. Reflexive access lists support TCP sessions
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reflexive access lists allow IP packets to be filtered based on upper-layer session information. You can use reflexive access lists to permit IP traffic for sessions originating from within your network but to deny IP traffic for sessions originating from outside your network. This is accomplished by reflexive filtering, a kind of session filtering.
Reflexive access lists can be defined with extended named IP access lists only. You cannot define reflexive access lists with numbered or standard named IP access lists or with other protocol access lists.
Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfreflx.html

NEW QUESTION: 65
What is the purpose of a honeypot IPS?
A. To create customized policies

B. To detect unknown attacks
C. To normalize streams
D. To collect information about attacks
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Honeypot systems use a dummy server to attract attacks. The purpose of the honeypot approach is to distract attacks away from real network devices. By staging different types of vulnerabilities in the honeypot server, you can analyze incoming types of attacks and malicious traffic patterns. You can use this analysis to tune your sensor signatures to detect new types of malicious network traffic.
Honeypot systems are used in production environments, typically by large organizations that come across as interesting targets for hackers, such as financial enterprises, governmental agencies, and so on. Also, antivirus and other security vendors tend to use them for research.
Reference: http://www.ciscopress.com/articles/article.asp?p=1336425

NEW QUESTION: 66
Which RADIUS server authentication protocols are supported on Cisco ASA firewalls? (Choose three.)
A. EAP
B. ASCII
C. PAP
D. PEAP
E. MS-CHAPv1
F. MS-CHAPv2
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The ASA supports the following authentication methods with RADIUS servers:
PAP-For all connection types.
CHAP and MS-CHAPv1-For L2TP-over-IPsec connections.
MS-CHAPv2-For L2TP-over-IPsec connections, and for regular IPsec remote access connections when the password management feature is enabled. You can also use MS-CHAPv2 with clientless connections.
Authentication Proxy modes-For RADIUS-to Active-Directory, RADIUS-to-RSA/SDI, RADIUS- to-Token server, and RSA/SDI-to-RADIUS connections,
Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/aaa_radius.html#pgfId-1211697

NEW QUESTION: 67
Which three statements describe DHCP spoofing attacks? (Choose three.)
A. They can modify traffic in transit.
B. They are used to perform man-in-the-middle attacks.

C. They use ARP poisoning.
D. They can access most network devices.
E. They protect the identity of the attacker by masking the DHCP address.
F. They can physically modify the network gateway.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
DHCP spoofing attacks modify traffic in transit and they use man-in-the-middle attacks along with ARP poisoning.
Reference: https://learningnetwork.cisco.com/thread/67229

NEW QUESTION: 68
How does a zone-based firewall implementation handle traffic between interfaces in the same zone?
A. Traffic between two interfaces in the same zone is allowed by default.
B. Traffic between interfaces in the same zone is blocked unless you configure the same-security permit command.
C. Traffic between interfaces in the same zone is always blocked.
D. Traffic between interfaces in the same zone is blocked unless you apply a service policy to the zone pair.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: By default, the traffic between interfaces in the same zone is not subject to any policy and passes freely. Firewall zones are used for security features.
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/sec-zone-pol-fw.html

NEW QUESTION: 69
What can the SMTP preprocessor in FirePOWER normalize?
A. It can extract and decode email attachments in client to server traffic.
B. It can look up the email sender.
C. It compares known threats to the email sender.
D. It can forward the SMTP traffic to an email filter server.
E. It uses the Traffic Anomaly Detector.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Transport and network layer preprocessors detect attacks that exploit IP fragmentation, checksum validation, and TCP and UDP session preprocessing. Before packets are sent to preprocessors, the packet decoder converts packet headers and payloads into a format that can be easily used by the preprocessors and the intrusion rules engine and detects various anomalous behaviors in packet headers.

After packet decoding and before sending packets to other preprocessors, the inline normalization preprocessor normalizes traffic for inline deployments.
Reference: http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/NAP-Transport-Network-Layer.html

NEW QUESTION: 70
A. when multiple management applications need concurrent access to the device
B. when you require administrator access from multiple locations
C. when a network device fails to forward packets
D. when you require ROMMON access
E. when the control plane fails to respond
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
In-band management can be used when management applications need concurrent access to the device.
In-band management can also be used to gain administrator access from multiple locations.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/hubs/fhub316c_t/bmm/install_config/guide/bmmicg/bmminbn.pdf

NEW QUESTION: 71
If you change the native VLAN on the trunk port to an unused VLAN, what happens if an attacker attempts a double-tagging attack?
A. The trunk port would go into an error-disabled state.
B. A VLAN hopping attack would be successful.
C. A VLAN hopping attack would be prevented.
D. The attacked VLAN will be pruned.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The key feature of a double tagging attack is exploiting the native VLAN. Since VLAN 1 is the default VLAN for access ports and the default native VLAN on trunks, it's an easy target. The first countermeasure is to remove access ports from the default VLAN 1 since the attacker's port must match that of the switch's native VLAN.
Reference: https://www.nlogic.co/understanding-vlan-hopping-attacks/

NEW QUESTION: 72
What are the three layers of a hierarchical network design? (Choose three.)
A. access
B. core
C. distribution
D. user

E. server
F. Internet
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Hierarchical network design has access, core and distribution layers.
Reference: http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

NEW QUESTION: 73
Which tool can an attacker use to attempt a DDoS attack?
A. botnet
B. Trojan horse
C. virus
D. adware
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Attackers build networks of infected computers, known as 'botnets', by spreading malicious software through emails, websites and social media. Once infected, these machines can be controlled remotely, without their owners' knowledge, and used like an army to launch an attack against any target. Some botnets are millions of machines strong.
Reference: http://www.digitalattackmap.com/understanding-ddos/

NEW QUESTION: 74
How many crypto map sets can you apply to a router interface?
A. 3
B. 2
C. 4
D. 1
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
These commands apply the crypto map to the interface. You can assign only one crypto map set to an interface. If multiple crypto map entries have the same map-name but a different seq-num, they are part of the same set and are all applied to the interface. The security appliance evaluates the crypto map entry with the lowest seq-num first.
dt3-45a(config)#interface e0
dt3-45a(config-if)#crypto map armadillo
Reference: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/16439- IPSECpart8.html

NEW QUESTION: 75
A data breach has occurred and your company database has been copied. Which security principle has been violated?
A. confidentiality
B. availability
C. access
D. control
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
IF the data breach is occurred within the company and the database has been copied, the confidentiality has been breached.
An employee may steal valuable trade secret information as seen at DuPont. However, not every business has these types of trade secrets. The type of information an employee is most likely to steal is the information needed to do his or her specific job, usually information that is readily available to them. To maintain a competitive advantage, the electronic information an employee uses everyday must be protected. Everyday employees have access to a wide variety of electronic information which range from important (email lists and non-financial business information), to confidential (customer information), to private (employee records), through the most sensitive and potentially damaging data: financial records, databases with enormous company history, trade secrets and intellectual property.
Reference: https://www.nowsecure.com/blog/2010/08/31/departing-employees-and-data-theft/

NEW QUESTION: 76
For what reason would you configure multiple security contexts on the ASA firewall?
A. To separate different departments and business units.
B. To enable the use of VRFs on routers that are adjacently connected.
C. To provide redundancy and high availability within the organization.
D. To enable the use of multicast routing and QoS through the firewall.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: You administer a large enterprise with different departmental groups, and each department wants to implement its own security policies.
Reference: http://www.ciscopress.com/articles/article.asp?p=426641

Valid 210-260 Dumps shared by ExamDiscuss.com for Helping Passing 210-260 Exam! ExamDiscuss.com now offer the **newest 210-260 exam dumps**, the ExamDiscuss.com 210-260 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 210-260 dumps with Test Engine here:

https://www.examdiscuss.com/Cisco/exam/210-260/premium/ (**515** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
What hash type does Cisco use to validate the integrity of downloaded images?
A. Sha1
B. Sha2
C. Md5
D. Md1
Answer: (SHOW ANSWER)
Explanation/Reference:
The MD5 File Validation feature allows you to generate the MD5 checksum for the Cisco IOS image stored on your router and compare it to the value posted on Cisco.com to verify that the image on your router is not corrupted.
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sys-image-mgmt/configuration/15-s/sysimgmgmt-15-s-book/sysimgmgmt-md5.html#GUID-9E5A6790-5E81-442B-8F6F-54271B25A9F8

NEW QUESTION: 78
How can the administrator enable permanent client installation in a Cisco AnyConnect VPN firewall configuration?
A. Issue the command anyconnect keep-installer under the group policy or username webvpn mode
B. Issue the command anyconnect keep-installer installed in the global configuration
C. Issue the command anyconnect keep-installer installed under the group policy or username webvpn mode
D. Issue the command anyconnect keep-installer installer under the group policy or username webvpn mode
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
To enable permanent client installation for a specific group or user, use the anyconnect keep- installer command from group-policy or username webvpn modes:
anyconnect keep-installer installer
The default is that permanent installation of the client is enabled. The client remains on the remote computer at the end of the session. The following example configures the existing group-policy sales to remove the client on the remote computer at the end of the session:
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect keep-installer installed none Reference:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/vpn_anyconnect.html

NEW QUESTION: 79
What are two ways to prevent eavesdropping when you perform device-management tasks? (Choose two.)
A. Use an SSH connection.
B. Use SNMPv3.
C. Use out-of-band management.
D. Use SNMPv2.
E. Use in-band management.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
To prevent eavesdropping during device management tasks, you can use SSH and SNMPv3 to get info on eavesdropping if any.
Reference: https://www.ietf.org/rfc/rfc5592.txt

NEW QUESTION: 80
A. show ip dhcp snooping database
B. show ip dhcp snooping binding
C. show ip dhcp snooping statistics
D. show ip dhcp pool
E. show ip dhcp source binding
F. show ip dhcp snooping
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
To retain the bindings across reloads, you must use the DHCP snooping database agent. Without this agent, the bindings established by DHCP snooping are lost upon reload, and connectivity is lost as well. The database agent stores the bindings in a file at a configured location. Upon reload, the switch reads the file to build the database for the bindings. The switch keeps the file current by writing to the file as the database changes.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html#wp1090624

NEW QUESTION: 81
Which tasks is the session management path responsible for? (Choose three.)
A. Verifying IP checksums
B. Performing route lookup
C. Performing session lookup
D. Allocating NAT translations
E. Checking TCP sequence numbers
F. Checking packets against the access list

Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The session management path is responsible for the following tasks:
- Performing the access list checks
- Performing route lookups
- Allocating NAT translations (xlates)
- Establishing sessions in the "fast path"
Reference: http://www.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/intro_f.html

NEW QUESTION: 82
In which three ways does the TACACS protocol differ from RADIUS? (Choose three.)
A. TACACS uses TCP to communicate with the NAS.
B. TACACS can encrypt the entire packet that is sent to the NAS.
C. TACACS supports per-command authorization.
D. TACACS authenticates and authorizes simultaneously, causing fewer packets to be transmitted.
E. TACACS uses UDP to communicate with the NAS.
F. TACACS encrypts only the password field in an authentication packet.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
TACACS+ uses Transmission Control Protocol (TCP) port 49 to communicate between the TACACS+ client and the TACACS+ server. An example is a Cisco switch authenticating and authorizing administrative access to the switch's IOS CLI. The switch is the TACACS+ client, and Cisco Secure ACS is the server.
TACACS+ communication between the client and server uses different message types depending on the function. In other words, different messages may be used for authentication than are used for authorization and accounting. Another very interesting point to know is that TACACS+ communication will encrypt the entire packet.
Reference: http://www.networkworld.com/article/2838882/radius-versus-tacacs.html

NEW QUESTION: 83
What is the effect of the send-lifetime local 23:59:00 31 December 31 2013 infinite command?
A. It configures the device to begin transmitting the authentication key to other devices at 00:00:00 local time on January 1, 2014 and continue using the key indefinitely.
B. It configures the device to begin transmitting the authentication key to other devices at 23:59:00 local time on December 31, 2013 and continue using the key indefinitely.
C. It configures the device to begin accepting the authentication key from other devices immediately and stop accepting the key at 23:59:00 local time on December 31, 2013.
D. It configures the device to generate a new authentication key and transmit it to other devices at

23:59:00 local time on December 31, 2013.
E. It configures the device to begin accepting the authentication key from other devices at 23:59:00 local time on December 31, 2013 and continue accepting the key indefinitely.
F. It configures the device to begin accepting the authentication key from other devices at 00:00:00 local time on January 1, 2014 and continue accepting the key indefinitely.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Send-lifetime infinite command configures the device to begin transmitting the authentication key to other devices at 23:59:00 local time on December 31, 2013 and continue using the key indefinitely

NEW QUESTION: 84
What are the primary attack methods of VLAN hopping? (Choose two.)
A. VoIP hopping
B. Switch spoofing
C. CAM-table overflow
D. Double tagging
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
VLAN hopping is a computer security exploit, a method of attacking networked resources on a Virtual LAN (VLAN). The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging. Both attack vectors can be easily mitigated with proper switchport configuration.
Reference: https://en.wikipedia.org/wiki/VLAN_hopping

NEW QUESTION: 85
In which stage of an attack does the attacker discover devices on a target network?
A. Reconnaissance
B. Covering tracks
C. Gaining access
D. Maintaining access
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Knowledge is power goes the old and equally wise saying. This axiom is applicable to the arena of network attacks as well. The reconnaissance attack is one where the main purpose of the attacker is to find out information about the vulnerable points of the network which is being targeted.
Reference: https://www.certificationkits.com/cisco-certification/ccna-security-certification-topics/ccna-security-describe-security-threats/ccna-security-common-network-attacks/

NEW QUESTION: 86
How does the Cisco ASA use Active Directory to authorize VPN users?
A. It queries the Active Directory server for a specific attribute for the specified user.
B. It sends the username and password to retrieve an ACCEPT or REJECT message from the Active Directory server.
C. It downloads and stores the Active Directory database to query for future authorization requests.
D. It redirects requests to the Active Directory server defined for the VPN group.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
When user LDAP authentication for VPN access has succeeded, the ASA queries the LDAP server, which returns LDAP, attributes. These attributes generally include authorization data that applies to the VPN session. Thus, using LDAP accomplishes authentication and authorization in a single step.
Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/access_aaa.html

NEW QUESTION: 87
What is the most common Cisco Discovery Protocol version 1 attack?
A. Denial of Service
B. MAC-address spoofing
C. CAM-table overflow
D. VLAN hopping
Answer: (SHOW ANSWER)
Explanation/Reference:
The older version of CDP v1 are vulnerable to DoS attacks, such that an attacker could flood the network segment with large CDP frames containing random device ID's causing Cisco devices running this version to crash. Targeting a vulnerable router using this attack could allow the attacker to send spoofed CDP frames with new route information with a higher priority so that traffic is rerouted to an unauthorised device.
Although this form of DoS only affects older versions of the protocol many older platforms cannot upgrade to newer releases due to flash ROM size constraints, so I'm sure there are many devices still at risk to this exploit.
Reference: http://packetbuddha.blogspot.com/2009/12/cdp-attacks.html

NEW QUESTION: 88
You have implemented a Sourcefire IPS and configured it to block certain addresses utilizing Security Intelligence IP Address Reputation. A user calls and is not able to access a certain IP address. What action can you take to allow the user access to the IP address?
A. Create a whitelist and add the appropriate IP address to allow the traffic.
B. Create a custom blacklist to allow the traffic.

C. Create a user based access control rule to allow the traffic.
D. Create a network based access control rule to allow the traffic.
E. Create a rule to bypass inspection to allow the traffic.
Answer: (SHOW ANSWER)
Explanation/Reference:
When a blacklist is too broad in scope, or incorrectly blocks traffic that you want to allow (for example, to vital resources), you can override a blacklist with a custom whitelist.
Reference: http://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/AC-Secint-Blacklisting.html

NEW QUESTION: 89
Which command causes a Layer 2 switch interface to operate as a Layer 3 interface?
A. no switchport nonnegotiate
B. switchport
C. no switchport mode dynamic auto
D. no switchport
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Configure routed ports by putting the interface into Layer 3 mode with the no switchport interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the ip routing and router protocol global configuration commands.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swint.html

NEW QUESTION: 90
Refer to the exhibit.
While troubleshooting site-to-site VPN, you issued the show crypto ipsec sa command. What does the given output show?
A. IPSec Phase 2 is established between 10.1.1.1 and 10.1.1.5.
B. ISAKMP security associations are established between 10.1.1.5 and 10.1.1.1.
C. IKE version 2 security associations are established between 10.1.1.1 and 10.1.1.5.
D. IPSec Phase 2 is down due to a mismatch between encrypted and decrypted packets.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Once the secure tunnel from phase 1 has been established, we will start phase 2. In this phase the two firewalls will negotiate about the IPsec security parameters that will be used to protect the traffic within the tunnel. In short, this is what happens in phase 2:
Negotiate IPsec security parameters through the secure tunnel from phase 1.
Establish IPsec security associations.

Periodically renegotiates IPsec security associations for security.
Reference: https://networklessons.com/security/cisco-asa-site-site-ikev1-ipsec-vpn/

NEW QUESTION: 91
What type of attack was the Stuxnet virus?
A. cyber warfare
B. hacktivism
C. botnet
D. social engineering
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Stuxnet virus is part of cyber warfare unleashed by governments to hinder their opponents computer systems and steal vital information.
Reference: https://en.wikipedia.org/wiki/Stuxnet

Valid 210-260 Dumps shared by ExamDiscuss.com for Helping Passing 210-260 Exam! ExamDiscuss.com now offer the **newest 210-260 exam dumps**, the ExamDiscuss.com 210-260 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 210-260 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/210-260/premium/ (**515** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 92
Which type of address translation should be used when a Cisco ASA is in transparent mode?
A. Static NAT
B. Dynamic NAT
C. Overload
D. Dynamic PAT
Answer: (SHOW ANSWER)
Explanation/Reference:
Using NAT on a security appliance operating in transparent mode eliminates the need for upstream or downstream routers to perform NAT for their networks.
Reference:
http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-1/user/guide/CSMUserGuide_wrapper/NATchap.html#51621

NEW QUESTION: 93
Which two features do CoPP and CPPr use to protect the control plane? (Choose two.)

A. access lists
B. policy maps
C. QoS
D. class maps
E. traffic classification
F. Cisco Express Forwarding
Answer: (SHOW ANSWER)

NEW QUESTION: 94
Which Cisco product can help mitigate web-based attacks within a network?
A. Adaptive Security Appliance
B. Web Security Appliance
C. Email Security Appliance
D. Identity Services Engine
Answer: (SHOW ANSWER)
Explanation/Reference:
To protect against the growing breadth and diversity of threats in today's business climate, you need a modern approach. That means a variety of protections that can block hidden malware from both suspicious and legitimate sites before it reaches you. We think the best Web security solutions today should be backed by the best real-time security intelligence available to help you stay abreast of this changing threat landscape and prevent the latest exploits from turning into issues. And modern Web security should be able to support policies that give employees access to the sites they need to use to do their jobs while selectively denying the use of undesired sites and features like web-based file-sharing. You get all of those features and more with the Cisco® Web Security Appliance (WSA), Figure 1. Cisco WSA safeguards businesses through broad threat intelligence, multiple layers of malware defense, and vital data loss prevention (DLP) capabilities across the attack continuum. It's an all-in-one web gateway that brings you broad protection, extensive controls, and investment value. It also offers an array of competitive web security deployment options, each of which includes Cisco's market-leading global threat intelligence infrastructure.
Reference: http://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/solution-overview-c22-732948.html

NEW QUESTION: 95
What are purposes of the Internet Key Exchange in an IPsec VPN? (Choose two.)
A. The Internet Key Exchange protocol establishes security associations
B. The Internet Key Exchange protocol provides data confidentiality
C. The Internet Key Exchange protocol provides replay detection
D. The Internet Key Exchange protocol is responsible for mutual authentication
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

Using the channel created in phase 1, this phase establishes IPSec security associations and negotiates information needed for the IPSec tunnel. This phase can be seen in the above figure as "IPsec-SA established." Note that two phase 2 events are shown, this is because a separate SA is used for each subnet configured to traverse the VPN.
Reference: https://documentation.meraki.com/zGeneral_Administration/Tools_and_Troubleshooting/Networking_Fundamentals%3A_IPSec_and_IKEv

NEW QUESTION: 96
Which two statements about stateless firewalls are true? (Choose two.)
A. They compare the 5-tuple of each incoming packet against configurable rules.
B. They cannot track connections.
C. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS.
D. Cisco IOS cannot implement them because the platform is stateful by nature.
E. The Cisco ASA is implicitly stateless because it blocks all traffic by default.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
However, since iptables and Netfilter were introduced and connection tracking in particular, this option was gotten rid of. The reason for this is that connection tracking can not work properly without defragmenting packets, and hence defragmenting has been incorporated into conntrack and is carried out automatically. It can not be turned off, except by turning off connection tracking. Defragmentation is always carried out if connection tracking is turned on.
Reference: http://www.iptables.info/en/connection-state.html

NEW QUESTION: 97
In which three ways does the RADIUS protocol differ from TACACS? (Choose three.)
A. RADIUS uses UDP to communicate with the NAS.
B. RADIUS encrypts only the password field in an authentication packet.
C. RADIUS authenticates and authorizes simultaneously, causing fewer packets to be transmitted.
D. RADIUS uses TCP to communicate with the NAS.
E. RADIUS can encrypt the entire packet that is sent to the NAS.
F. RADIUS supports per-command authorization.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Two prominent security protocols used to control access into networks are Cisco TACACS+ and RADIUS.
The RADIUS specification is described in RFC 2865 leavingcisco.com, which obsoletes RFC 2138 leavingcisco.com. Cisco is committed to supporting both protocols with the best of class offerings. It is not the intention of Cisco to compete with RADIUS or influence users to use TACACS+. You should choose the solution that best meets your needs.

Reference: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

NEW QUESTION: 98
What is an advantage of implementing a Trusted Platform Module for disk encryption?
A. It provides hardware authentication.
B. It allows the hard disk to be transferred to another device without requiring re-encryption.dis
C. It supports a more complex encryption algorithm than other disk-encryption technologies.
D. It can protect against single points of failure.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A Trusted Platform Module (TPM) is a specialized chip on an endpoint device that stores RSA encryption keys specific to the host system for hardware authentication.
Each TPM chip contains an RSA key pair called the Endorsement Key (EK). The pair is maintained inside the chip and cannot be accessed by software. The Storage Root Key (SRK) is created when a user or administrator takes ownership of the system. This key pair is generated by the TPM based on the Endorsement Key and an owner-specified password.
Reference: http://whatis.techtarget.com/definition/trusted-platform-module-TPM

NEW QUESTION: 99
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
To access ASDM, click the ASA icon in the topology diagram.
Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

Which user authentication method is used when users login to the Clientless SSLVPN portal using https://209.165.201.2/test?
A. AAA with LOCAL database
B. AAA with RADIUS server
C. Certificate
D. Both Certificate and AAA with LOCAL database
E. Both Certificate and AAA with RADIUS server
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:

This can be seen from the Connection Profiles Tab of the Remote Access VPN configuration, where the alias of test is being used,

NEW QUESTION: 100

A. Port security
B. DHCP snooping
C. IP source guard
D. Dynamic ARP inspection
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The best measure is to enable DHCP snooping and dynamic ARP inspection for ARP spoofing attacks.
Reference: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html

NEW QUESTION: 101

When a switch has multiple links connected to a downstream switch, what is the first step that STP takes to prevent loops?
A. STP elects the root bridge
B. STP selects the root port
C. STP selects the designated port
D. STP blocks one of the ports
Answer: (SHOW ANSWER)
Explanation/Reference:
To prevent loops when a switch has multiple links connected to a downstream switch, STP will elect Root Bridge to prevent loops in the process.
Reference: http://networkengineering.stackexchange.com/questions/114/how-is-the-stp-root-bridge-and-path-to-the-root-bridge-determined

NEW QUESTION: 102

Which protocols use encryption to protect the confidentiality of data transmitted between two parties? (Choose two.)
A. FTP
B. SSH
C. Telnet
D. AAA
E. HTTPS
F. HTTP
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

An encrypted connection becomes useless if you've unknowingly connected to a bogus server or a malicious client. While SSH and SSL use symmetric cryptography to preserve the confidentiality of transmitted data, they use another form of encryption for authentication. Authentication allows one party to verify whether the other party is really who it claims it is.
Reference: http://www.jscape.com/blog/ssl-vs-ssh-simplified

NEW QUESTION: 103
Which alert protocol is used with Cisco IPS Manager Express to support up to 10 sensors?
A. SDEE
B. Syslog
C. SNMP
D. CSM
Answer: (SHOW ANSWER)
Explanation/Reference:
Cisco's IPS sensors support event retrieval using the Security Device Event Exchange (SDEE) protocol. SDEE is an industry standard protocol and there are several open-source libraries available for using in the creation of an event collection and storage solution.
Reference: https://supportforums.cisco.com/discussion/10988211/how-monitor-cisco-ids-4215-v60

NEW QUESTION: 104
After reloading a router, you issue the dir command to verify the installation and observe that the image file appears to be missing. For what reason could the image file fail to appear in the dir output?
A. The secure boot-image command is configured.
B. The secure boot-comfit command is configured.
C. The confreg 0x24 command is configured.
D. The reload command was issued from ROMMON.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Secured files will not appear on the output of a dir command issued from an executive shell because the IFS prevents secure files in a directory from being listed. ROM monitor (ROMMON) mode does not have any such restriction and can be used to list and boot secured files.
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-mt/sec-usr-cfg-15-mt-book/sec-resil-config.html

NEW QUESTION: 105
What are two default Cisco IOS privilege levels? (Choose two.)
A. 0
B. 1
C. 5
D. 7

E. 10
F. 15
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
By default, the Cisco IOS software command-line interface (CLI) has two levels of access to commands: user EXEC mode (level 1) and privileged EXEC mode (level 15). However, you can configure additional levels of access to commands, called privilege levels, to meet the needs of your users while protecting the system from unauthorized access. Up to 16 privilege levels can be configured, from level 0, which is the most restricted level, to level 15, which is the least restricted level.
Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.html#wp1001016

NEW QUESTION: 106
If a packet matches more than one class map in an individual feature type's policy map, how does the ASA handle the packet?
A. The ASA will apply the actions from only the first matching class map it finds for the feature type.
B. The ASA will apply the actions from only the most specific matching class map it finds for the feature type.
C. The ASA will apply the actions from all matching class maps it finds for the feature type.
D. The ASA will apply the actions from only the last matching class map it finds for the feature type.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: When the packet matches a class map for a feature type, the ASA does not attempt to match it to any subsequent class maps for that feature type.
Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/mpf_service_policy.html

Valid 210-260 Dumps shared by ExamDiscuss.com for Helping Passing 210-260 Exam! ExamDiscuss.com now offer the **newest 210-260 exam dumps**, the ExamDiscuss.com 210-260 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 210-260 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/210-260/premium/ (**515** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 107
Refer to the exhibit.
If a supplicant supplies incorrect credentials for all authentication methods configured on the switch, how will the switch respond?

A. The supplicant will fail to advance beyond the webauth method.
B. The switch will cycle through the configured authentication methods indefinitely.
C. The authentication attempt will time out and the switch will place the port into the unauthorized state.
D. The authentication attempt will time out and the switch will place the port into VLAN 101.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Incorrect credentials supplied will result in failure to advance beyond webauth method. The authentication needs correct credentials as seen in the exhibit.

NEW QUESTION: 108
Which statement correctly describes the function of a private VLAN?
A. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains
B. A private VLAN partitions the Layer 3 broadcast domain of a VLAN into subdomains
C. A private VLAN enables the creation of multiple VLANs using one broadcast domain
D. A private VLAN combines the Layer 2 broadcast domains of many VLANs into one major broadcast domain
Answer: (SHOW ANSWER)
Explanation/Reference:
A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing you to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.pdf

NEW QUESTION: 109
Which statement about Cisco ACS authentication and authorization is true?
A. ACS servers can be clustered to provide scalability.
B. ACS can query multiple Active Directory domains.
C. ACS uses TACACS to proxy other authentication servers.
D. ACS can use only one authorization profile to allow or deny requests.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The ACS console server provides the scalability, reliability and security a company requires to control and manage servers and other networked devices.
Reference: http://www.uk.insight.com/content/dam/insight/EMEA/uk/shop/emerson/advanced-console-server.pdf (page 2)

NEW QUESTION: 110
A. Minimizing risk

B. Minimizing total cost of ownership
C. Minimizing liability
D. Maximizing compliance
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A security policy is used to minimize risk by allocating company's resources to eliminate risk and focus on growth and revenues.
Reference: http://searchsecurity.techtarget.com/definition/security-policy

NEW QUESTION: 111
What is the purpose of the Integrity component of the CIA triad?
A. to ensure that only authorized parties can modify data
B. to determine whether data is relevant
C. to create a process for accessing data
D. to ensure that only authorized parties can view data
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The I in CIA stands for Integrity - specifically, data integrity. The key to this component of the CIA Triad is protecting data from modification or deletion by unauthorized parties, and ensuring that when authorized people make changes that shouldn't have been made the damage can be undone.
Reference: http://www.techrepublic.com/blog/it-security/the-cia-triad/

NEW QUESTION: 112
What is the Cisco preferred countermeasure to mitigate CAM overflows?
A. Port security
B. Dynamic port security
C. IP source guard
D. Root guard
Answer: (SHOW ANSWER)
Explanation/Reference:
Port Security on a Cisco switch enables you to control how the switch port handles the learning and storing of MAC addresses on a per-interface basis. The main use of this command is to set a limit to the maximum number of concurrent MAC addresses that can be learned and allocated to the individual switch port.
Reference: http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=2

NEW QUESTION: 113
Which FirePOWER preprocessor engine is used to prevent SYN attacks?
A. Rate-Based Prevention

B. Portscan Detection
C. IP Defragmentation
D. Inline Normalization
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The detection_filter keyword and the thresholding and suppression features provide other ways to filter either the traffic itself or the events that the system generates. You can use rate-based attack prevention alone or in any combination with thresholding, suppression, or the detection_filter keyword to prevent SYN attacks.
Reference: http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Threat-Detection.html#10682

NEW QUESTION: 114
What is the transition order of STP states on a Layer 2 switch interface?
A. listening, learning, blocking, forwarding, disabled
B. listening, blocking, learning, forwarding, disabled
C. blocking, listening, learning, forwarding, disabled
D. forwarding, listening, learning, blocking, disabled
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Each interface on a access point using spanning tree exists in one of these states:
Blocking-The interface does not participate in frame forwarding.
Listening-The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.
Learning-The interface prepares to participate in frame forwarding.
Forwarding-The interface forwards frames.
Disabled-The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.
Reference: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-3_7_JA/configuration/guide/i1237sc/s37span.html#wp1040509

NEW QUESTION: 115
Which options are filtering options used to display SDEE message types? (Choose two.)
A. stop
B. none
C. error
D. all
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:
Secure Device Event Exchange (SDEE) messages report on the progress of Cisco IOS IPS initialization and operation. Click to display the Edit IPS: SDEE Messages window, where you can review SDEE messages and filter them to display only error, status, or alert messages.
Reference: http://www.cisco.com/c/en/us/td/docs/routers/access/cisco_router_and_security_device_manager/24/software/user/guide/IPS.html

NEW QUESTION: 116
Which security zone is automatically defined by the system?
A. The source zone
B. The self zone
C. The destination zone
D. The inside zone
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The self zone is a system-defined zone which does not have any interfaces as members. A zone pair that includes the self zone, along with the associated policy, applies to traffic directed to the device or traffic generated by the device. It does not apply to traffic through the device.
The most common usage of firewall is to apply them to traffic through a device, so you need at least two zones (that is, you cannot use the self zone).
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-2mt/sec-zone- pol-fw.html

NEW QUESTION: 117
Which address block is reserved for locally assigned unique local addresses?
A. 2002::/16
B. FD00::/8
C. 2001::/32
D. FB00::/8
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Using one of the common Unique Local IPv6 global prefix generators, the Acme corporate network was assigned the global prefix of 6D8D64AF0C; when pushed together with the common unique local locally assigned prefix (FD00::/8) the prefix expands to FD6D:8D64:AF0C::/48; this leaves Acme with an additional 16 bits of space to use for subnetting across their sites.
Reference: http://www.ciscopress.com/articles/article.asp?p=2154678&seqNum=2

NEW QUESTION: 118

According to Cisco best practices, which three protocols should the default ACL allow on an access port to enable wired BYOD devices to supply valid credentials and connect to the network? (Choose three.)
A. BOOTP
B. TFTP
C. DNS
D. MAB
E. HTTP
F. 802.1x
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
ACL-DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.
Reference: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_Wired.html

NEW QUESTION: 119
Refer to the exhibit.
The Admin user is unable to enter configuration mode on a device with the given configuration. What change can you make to the configuration to correct the problem?
A. Remove the autocommand keyword and arguments from the Username Admin privilege line.
B. Change the Privilege exec level value to 15.
C. Remove the two Username Admin lines.
D. Remove the Privilege exec line.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The autocommand causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and contain embedded spaces, commands using the autocommand keyword must be the last option on the line.
Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/fsecur_r/srfpass.html#wp1030793

NEW QUESTION: 120
A. AAA Summary
B. AAA Servers and Groups
C. Authentication Policies
D. Authorization Policies
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

AAA summary screen is used to enable AAA authentication.
Reference: https://books.google.com.pk/books?id=V8kmEemJPlkC&pg=PA81&lpg=PA81&dq=enable+AAA+AAA+summary+screen&source=bl&ots=Yw_-pFKTbZ&sig=GxQD3FnhFotUeDenrA4Ssg4oQxg&hl=en&sa=X&ved=0ahUKEwjdlaCcoKPNAhUK6xQKHa9OAV0Q6AEIMjAE#v=onepage&q=enable%20AAA%20AAA%20summary%20screen&f=false

NEW QUESTION: 121
What is the FirePOWER impact flag used for?
A. A value that indicates the potential severity of an attack.
B. A value that the administrator assigns to each signature.
C. A value that sets the priority of a signature.
D. A value that measures the application awareness.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The impact level in this field indicates the correlation between intrusion data, network discovery data, and vulnerability information.
Reference: http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/ViewingEvents.html

Valid 210-260 Dumps shared by ExamDiscuss.com for Helping Passing 210-260 Exam! ExamDiscuss.com now offer the **newest 210-260 exam dumps**, the ExamDiscuss.com 210-260 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 210-260 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/210-260/premium/ (**515** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 122
SIMULATION
Scenario
Given the new additional connectivity requirements and the topology diagram, use ASDM to accomplish the required ASA configurations to meet the requirements.
New additional connectivity requirements:
Currently, the ASA configurations only allow on the Inside and DMZ networks to access any hosts on the Outside. Your task is to use ASDM to configure the ASA to also allow any host only on the Outside to HTTP to the DMZ server. The hosts on the Outside will need to use the 209.165.201.30 public IP address when HTTPing to the DMZ server.
Currently, hosts on the ASA higher security level interfaces are not able to ping any hosts on the lower

security level interfaces. Your task in this simulation is to use ASDM to enable the ASA to dynamically allow the echo-reply responses back through the ASA.
Once the correct ASA configurations have been configured:
You can test the connectivity to http://209.165.201.30 from the Outside PC browser.
You can test the pings to the Outside (www.cisco.com) by opening the inside PC command prompt window. In this simulation, only testing pings to www.cisco.com will work.
To access ASDM, click the ASA icon in the topology diagram.
To access the Firefox Browser on the Outside PC, click the Outside PC icon in the topology diagram.
To access the Command prompt on the Inside PC, click the Inside PC icon in the topology diagram.
Note:
After you make the configuration changes in ASDM, remember to click Apply to apply the configuration changes.
Not all ASDM screens are enabled in this simulation, if some screen is not enabled, try to use different methods to configure the ASA to meet the requirements.
In this simulation, some of the ASDM screens may not look and function exactly like the real ASDM.

Answer:
Follow the explanation part to get answer on this sim question.
Explanation/Reference:
Explanation:
First, for the HTTP access we need to creat a NAT object. Here I called it HTTP but it can be given any name.
Then, create the firewall rules to allow the HTTP access:
You can verify using the outside PC to HTTP into 209.165.201.30.
For step two, to be able to ping hosts on the outside, we edit the last service policy shown below:
And then check the ICMP box only as shown below, then hit Apply.
After that is done, we can ping www.cisco.com again to verify:

NEW QUESTION: 123
Which wildcard mask is associated with a subnet mask of /27?
A. 0.0.0.31
B. 0.0.027
C. 0.0.0.224
D. 0.0.0.255
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
On Cisco router, wildcard subnet mask is used in the following occasion
* Defining subnet in ACL

* Defining subnet member in OSPF area
Reference: http://www.dslreports.com/faq/15216

NEW QUESTION: 124
In what type of attack does an attacker virtually change a device's burned-in address in an attempt to circumvent access lists and mask the device's true identity?
A. gratuitous ARP
B. ARP poisoning
C. IP spoofing
D. MAC spoofing
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
If your original MAC address is revealed, an hacker can use it to impersonate you! On many networks (wired or wireless) access is restricted based on MAC address to avoid access to unauthorized devices on the network. So, when you go offline, someone can use your machine's MAC address and access the network as 'you'.
Reference: http://blog.technitium.com/2011/06/why-you-need-to-change-mac-address.html

NEW QUESTION: 125
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
To access ASDM, click the ASA icon in the topology diagram.
Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

Which two statements regarding the ASA VPN configurations are correct? (Choose two)
A. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM_TrustPoint1.
B. The DefaultWEBVPNGroup Connection Profile is using the AAA with RADIUS server method.
C. The Inside-SRV bookmark references the https://192.168.1.2 URL
D. Only Clientless SSL VPN access is allowed with the Sales group policy
E. AnyConnect, IPSec IKEv1, and IPSec IKEv2 VPN access is enabled on the outside interface
F. The Inside-SRV bookmark has not been applied to the Sales group policy
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

For B:
For C, Navigate to the Bookmarks tab:
Then hit "edit" and you will see this:
Not A, as this is listed under the Identity Certificates, not the CA certificates:
Note E:

NEW QUESTION: 126
Which statement about application blocking is true?
A. It blocks access to specific programs.
B. It blocks access to files with specific extensions.
C. It blocks access to specific network addresses.
D. It blocks access to specific network services.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Application filters allow you to quickly create application conditions for access control rules. They simplify policy creation and administration, and grant you assurance that the system will control web traffic as expected. For example, you could create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the session is blocked.
Reference: http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/AC-Rules-App-URL-Reputation.html#pgfId-1576835

NEW QUESTION: 127
Which command initializes a lawful intercept view?
A. username cisco1 view lawful-intercept password cisco
B. parser view cisco li-view
C. li-view cisco user cisco1 password cisco
D. parser view li-view inclusive
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Parser view cisco li-view is the command that initializes lawful intercept view.
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xe-3s/sec-usr-cfg-xe-3s-book/sec-role-base-cli.html#GUID-682CE43D-C9FC-4F47-848E-0DBC84ED6F32

NEW QUESTION: 128
In which two situations should you use out-of-band management? (Choose two.)
A. when a network device fails to forward packets
B. when you require ROMMON access
C. when management applications need concurrent access to the device

D. when you require administrator access from multiple locations
E. when the control plane fails to respond
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Out-of-band refers to an interface that allows only management protocol traffic to be forwarded or processed. An out-of-band management interface is defined by the network operator to specifically receive network management traffic. The advantage isthat forwarding (or customer) traffic cannot interfere with the management of the router, which significantly reduces the possibility of denial-of-service attacks.
Out-of-band interfaces forward traffic only between out-of-band interfaces or terminate management packets that are destined to the router. In addition, the out-of-band interfaces can participate in dynamic routing protocols. The service provider connects to the router's out-of-band interfaces and builds an independent overlay management network, with all the routing and policy tools that the router can provide.
Reference: http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-0/security/configuration/guide/b_sc40asr9kbook/b_sc40asr9kbook_chapter_0101.pdf

NEW QUESTION: 129
What VPN feature allows Internet traffic and local LAN/WAN traffic to use the same network connection?
A. split tunneling
B. hairpinning
C. tunnel mode
D. transparent mode
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
When split tunneling is enabled, Internet traffic goes directly from your computer to the Internet and back without involving the VPN at all. Split tunneling also allows you to access other systems on your local network which is impossible if all traffic has go to the corporate network first, although this can be mitigated in some configurations.
Reference: http://www.tripwire.com/state-of-security/security-data-protection/36th-article-vpn-split-tunneling/

NEW QUESTION: 130
A. control plane packets
B. data plane packets
C. management plane packets
D. services plane packets
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:
Under normal network operating conditions, the vast majority of packets handled by network devices are data plane packets. These packets are handled in the fast path. Network devices are optimized to handle these fast path packets efficiently. Typically, considerably fewer control and management plane packets are required to create and operate IP networks. Thus, the punt path and route processor are significantly less capable of handling the kinds of packets rates experienced in the fast path since they are never directly involved in the forwarding of data plane packets
Reference: http://www.cisco.com/c/en/us/about/security-center/copp-best-practices.html

NEW QUESTION: 131
What type of algorithm uses the same key to encrypt and decrypt data?
A. a symmetric algorithm
B. an asymmetric algorithm
C. a Public Key Infrastructure algorithm
D. an IP security algorithm
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Symmetric encryption (or pre-shared key encryption) uses a single key to both encrypt and decrypt data. Both the sender and the receiver need the same key to communicate.
Reference: https://www.digicert.com/ssl-cryptography.htm

NEW QUESTION: 132
What is a reason for an organization to deploy a personal firewall?
A. To protect endpoints such as desktops from malicious activity.
B. To protect one virtual network segment from another.
C. To determine whether a host meets minimum security posture requirements.
D. To create a separate, non-persistent virtual environment that can be destroyed after a session.
E. To protect the network from DoS and syn-flood attacks.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The sole purpose of firewall is to protect endpoints (workstations, and other devices) from malicious activity and network connections with nefarious purposes.
Reference: http://searchmidmarketsecurity.techtarget.com/definition/personal-firewall

NEW QUESTION: 133
Which two statements about Telnet access to the ASA are true? (Choose two).
A. You may VPN to the lowest security interface to telnet to an inside interface.
B. You must configure an AAA server to enable Telnet.
C. You can access all interfaces on an ASA using Telnet.

D. You must use the command virtual telnet to enable Telnet.
E. Best practice is to disable Telnet and use SSH.
Answer: A,E (LEAVE A REPLY)
Explanation/Reference:
Explanation: If SSH is not enabled, the Java applet uses Telnet. But as soon as the SSH service is enabled on the switch, the Java applet will stop using Telnet and use SSH instead.
Reference: https://www.alliedtelesis.com/sites/default/files/alliedwareplus-best-practice-guide_reva.pdf

NEW QUESTION: 134
Which statement about personal firewalls is true?
A. They can protect a system by denying probing requests.
B. They are resilient against kernel attacks.
C. They can protect email messages and private documents in a similar way to a VPN.
D. They can protect the network against attacks.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Drop or ignore any probing requests sent to certain service ports on your system. This can mask the presence of the computer from the attacker who is fooled into thinking that no machine is there.
Reference: https://www.polyu.edu.hk/~ags/itsnews0604/security.html

NEW QUESTION: 135
Which command will configure a Cisco ASA firewall to authenticate users when they enter the enable syntax using the local database with no fallback method?
A. aaa authentication enable console LOCAL SERVER_GROUP
B. aaa authentication enable console SERVER_GROUP LOCAL
C. aaa authentication enable console local
D. aaa authentication enable console LOCAL
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The CONSOLE list overrides the default method list default on line con 0. You need to enter the password
"cisco" (configured on line con 0) to get console access. The default list is still used on tty, vty and aux.
Note: To have console access authenticated by a local username and password, use:
Router(config)# aaa authentication login CONSOLE local
Reference: http://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html#login_auth

NEW QUESTION: 136
Which three ESP fields can be encrypted during transmission? (Choose three.)

A. Security Parameter Index
B. Sequence Number
C. MAC Address
D. Padding
E. Pad Length
F. Next Header
Answer: D,E,F (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The remaining four parts of the ESP are all encrypted during transmission across the network. Those parts are as follows:
The Payload Data is the actual data that is carried by the packet.
The Padding, from 0 to 255 bytes of data, allows certain types of encryption algorithms to require the data to be a multiple of a certain number of bytes. The padding also ensures that the text of a message terminates ona four-byte boundary (an architectural requirement within IP).
The Pad Length field specifies how much of the payload is padding rather than data.
The Next Header field, like a standard IP Next Header field, identifies the type of data carried and the protocol.
Reference: http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html

Valid 210-260 Dumps shared by ExamDiscuss.com for Helping Passing 210-260 Exam!
ExamDiscuss.com now offer the **newest 210-260 exam dumps**, the ExamDiscuss.com 210-260 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 210-260 dumps with Test Engine here:
https://www.examdiscuss.com/Cisco/exam/210-260/premium/ (**515** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 137
Refer to the exhibit.
Which statement about the device time is true?
A. The time is authoritative, but the NTP process has lost contact with its servers.
B. The time is authoritative because the clock is in sync.
C. The clock is out of sync.
D. NTP is configured incorrectly.
E. The time is not authoritative.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

The read-only string attempted a write operation nine times as seen in the exhibit. It says, 9 illegal operations to community name supplied which means the read-only string attempted 9 write operations.
Reference: http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Valid 210-260 Dumps shared by ExamDiscuss.com for Helping Passing 210-260 Exam! ExamDiscuss.com now offer the **newest 210-260 exam dumps**, the ExamDiscuss.com 210-260 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 210-260 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/210-260/premium/ (**515** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)