Cisco.210-260.v2019-08-06.q180

Exam Code:	210-260
Exam Name:	Implementing Cisco Network Security
Certification Provider:	Cisco
Free Question Number:	180
Version:	v2019-08-06
# of views:	1619
# of Questions views:	47365
https://www.freecram.net/torrent/Cisco.210-260.v2019-08-06.q180.html	

NEW QUESTION: 1
Which statement about IOS privilege levels is true?
A. Each privilege level supports the commands at its own level and all levels below it.
B. Each privilege level supports the commands at its own level and all levels above it.
C. Privilege-level commands are set explicitly for each user.
D. Each privilege level is independent of all other privilege levels.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Use either of these commands with the level option to define a password for a specific privilege level. After
you specify the level and set a password, give the password only to users who need to have access at this
level. Use the privilege level configuration command to specify commands accessible at various levels.
Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.html

NEW QUESTION: 2
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: 3
Which IPS mode provides the maximum number of actions?
A. inline
B. promiscuous
C. span
D. failover
E. bypass
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
IPS inline provides maximum number of actions.
Reference: http://www.cisco.com/c/en/us/td/docs/security/ips/5-1/configuration/guide/cli/cliguide/cliEvAct.html

NEW QUESTION: 4
How does the 802.1x supplicant communicate with the authentication server?
A. The supplicant creates RADIUS packets and sends them to the authenticator, which encapsulates
them into EAP and forwards them to the authentication server.
B. The supplicant creates EAP packets and sends them to the authenticator, which encapsulates them
into RADIUS and forwards them to the authentication server.
C. The supplicant creates EAP packets and sends them to the authenticator, which translates them into
RADIUS and forwards them to the authentication server.

D. The supplicant creates RADIUS packets and sends them to the authenticator, which translates them
into EAP and forwards them to the authentication server.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
Which quantifiable item should you consider when your organization adopts new technologies?
A. exploits
B. threats
C. vulnerability
D. risk
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
You have just deployed SNMPv3 in your environment. Your manager asks you to make sure that your
SNMP agents can only talk to the SNMP Manager.
What would you configure on your SNMP agents to satisfy this request?
A. A SNMP View containing the SNMP managers
B. A SNMP Group containing the SNMP managers
C. A standard ACL containing the SNMP managers applied to the SNMP configuration
D. Routing Filter with the SNMP managers in it applied outbound
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which security principle has been violated if data is altered in an unauthorized manner?
A. integrity
B. availability
C. confidentiality
D. accountability
Answer: (SHOW ANSWER)

NEW QUESTION: 8
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: 9
Refer to the exhibit.
What are two effects of the given command? (Choose two.)
A. It configures authentication to use AES 256.
B. It configures authentication to use MD5 HMAC.
C. It configures authorization use AES 256.
D. It configures encryption to use MD5 HMAC.
E. It configures encryption to use AES 256.
Answer: (SHOW ANSWER)
Explanation/Reference:
To define a transform set-an acceptable combination of security protocols and algorithms-use the crypto ipsec transform-set global configuration command. To delete a transform set, use the no form
of the command.
crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]
no crypto ipsec transform-set transform-set-name
Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfipsec.html#wp1017694

NEW QUESTION: 10
What are two reasons to recommend SNMPv3 over SNMPv2? (Choose two.)
A. SNMPv3 is secure because you can configure authentication and privacy
B. SNMPv3 is a Cisco proprietary protocol
C. SNMPv2 is insecure because it sends information in clear text
D. SNMPv2 is secure because you can configure authentication and privacy
E. SNMPv3 is insecure because it sends information in clear text
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Which statement about zone-based firewall configuration is true?
A. The zone must be configured before it can be assigned.
B. Traffic that is destined to or sourced from the Self zone is denied by default.

C. You can assign an interface to more than one zone.
D. Traffic is implicitly denied by default between interfaces in the same zone.
Answer: (SHOW ANSWER)

NEW QUESTION: 12
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: 13
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: 14
What are two major considerations when choosing between a SPAN and a TAP when implementing IPS?
(Choose two.)
A. whether RX and TX signals will use separate ports
B. the way in which dropped packets will be handled
C. the type of analysis the IPS will perform
D. the way in which media errors will be handled
E. the amount of bandwidth available
Answer: (SHOW ANSWER)

NEW QUESTION: 15
What command can you use to verify the binding table status?
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: 16
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: 17
Which path do you follow to enable AAA though the SDM?
A. Configure > Tasks > AAA
B. Configure > Authentication > AAA
C. Configure > AAA
D. Configure > Additional Authentication > AAA
E. Configure > Additional Tasks > AAA

Answer: (SHOW ANSWER)

NEW QUESTION: 18
You are configuring a NAT rule on a Cisco ASA. Which description of a mapped interface is true?
A. It is mandatory for all firewall modes.
B. It is optional in transparent mode.
C. It is optional in routed mode.
D. It is mandatory for identify NAT only.
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config/nat_objects.html

NEW QUESTION: 19
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: 20
Refer to the exhibit.
With which NTP server has the router synchronized?
A. 192.168.10.7
B. 108.61.73.243

C. 209.114.111.1
D. 132.163.4.103
E. 204.2.134.164
F. 241.199.164.101
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
192.168.10.7 is clearly shown in the exhibit. It is NTP server address which is synchronized with router.

NEW QUESTION: 21
Which two types of firewalls work at Layer 4 and above? (Choose two.)
A. Application-level firewall
B. Circuit-level gateway
C. Static packet filter
D. Network Address Translation
E. Stateful inspection
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: https://supportforums.cisco.com/t5/security-documents/firewall-and-types/ta-p/3112038

NEW QUESTION: 22
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: 23
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: A,B,C (LEAVE A REPLY)
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: 24
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: 25
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: 26
On an ASA, which maps are used to identify traffic?
A. Route maps
B. Policy maps
C. Service maps
D. Class maps
Answer: D (LEAVE A REPLY)

NEW QUESTION: 27
Referencing the CIA model, in which scenario is a hash-only function most appropriate?
A. securing data in files
B. securing data at rest
C. securing wireless transmissions
D. securing real-time traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 28
In which three cases does the ASA firewall permit inbound HTTP GET requests during normal operations?
(Choose three).
A. when a matching TCP connection is found
B. when the firewall requires strict HTTP inspection
C. when the firewall receives a FIN packet
D. when matching ACL entries are configured
E. when the firewall requires HTTP inspection

F. when matching NAT entries are configured
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
During normal operations, ASA firewall permit inbound HTTP GET requests when a matching TCP
connection is found and a matching ACL entries are configured or when the firewall requires HTTP
inspection.
Reference: https://supportforums.cisco.com/document/69281/asa-using-packet-capture-troubleshoot-asa-
firewall-configuration-and-scenarios

NEW QUESTION: 29
You have been tasked with blocking user access to websites that violate company policy, but the sites use
dynamic IP addresses. What is the best practice for URL filtering to solve the problem?
A. Enable URL filtering and use URL categorization to block the websites that violate company policy.
B. Enable URL filtering and create a blacklist to block the websites that violate company policy.
C. Enable URL filtering and create a whitelist to block the websites that violate company policy.
D. Enable URL filtering and use URL categorization to allow only the websites that company policy allows
users to access.
E. Enable URL filtering and create a whitelist to allow only the websites that company policy allows users
to access.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Enable policy-Enables or disables the individual policy; the global URL Filtering setting overrides the
specifications of an individual policy.
URL Category-Choose a filtering action for the URL categories to which you want to restrict access.
There are over 80 categories segmented in seven logical groups. You can create custom categories
in HTTP > Configuration > Custom Categories.
The following describes the available filtering actions:
- Allow-Connection to the target server is allowed and users can access the Web site.
- Block-Connection to the target server is not established and users are not allowed to access the

Web site. A log entry is also created for this event.
- Block w/Override-Connection to target service is not established unless the user can type a specific password to override the category blocking.
Reference: https://docs.trendmicro.com/all/ent/iwsva/v5.5/en-us/iwsva_5.5_olh/urlf_policy_rule.htm

NEW QUESTION: 30
Which term refers to the electromagnetic interference that can radiate from network cables?
A. multimode distortion
B. Doppler waves
C. Gaussian distributions
D. emanations
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 31
Which IDS/IPS state misidentifies acceptable behavior as an attack?
A. True negative
B. False negative
C. False positives
D. True positive
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which command do you enter to configure your firewall to conceal internal addresses?
A. no ip logging facility
B. no ip inspect
C. no ip directed-broadcast
D. no ip inspect audit-trail
E. no proxy-arp
F. no ip source-route
Answer: (SHOW ANSWER)

NEW QUESTION: 33
In which type of attack does an attacker overwrite an entry in the CAM table to divert traffic destined to a
legitimate host?
A. DHCP spoofing
B. ARP spoofing
C. CAM table overflow
D. MAC spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 34
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
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: 35
Which two ESA services are available for incoming and outgoing mails? (Choose two.)
A. antispam
B. DLP
C. content filter
D. reputation filter
E. anti-DoS
Answer: (SHOW ANSWER)

Explanation/Reference:
Reference : https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_01001.pdf

NEW QUESTION: 36
Which two commands are used to implement Cisco IOS Resilient Configuration? (Choose two.)
A. secure boot-image
B. secure boot-config
C. copy flash:/ios.bin tftp
D. copy running-config stratup-config
E. copy running-config tftp
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: https://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: 37
There are two versions of IKE: IKEv1 and IKEv2. Both IKEv1 and IKEv2 protocols operate in phases.
IKEv1 operates in two phases. IKEv2 operates in how many phases?
A. 5
B. 3
C. 4
D. 2
Answer: D (LEAVE A REPLY)

NEW QUESTION: 38
Which technology can be used to rate data fidelity and to provide an authenticated hash for data?
A. file reputation
B. file analysis
C. signature updates
D. network blocking
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
File analysis rate data fidelity to provide an authenticated hash for data.
Reference:
http://www.cisco.com/c/en/us/td/docs/security/ips/7-1/configuration/guide/idm/idmguide71/idm_collaboration.html

NEW QUESTION: 39
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: 40
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM
then answer the four 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: (SHOW ANSWER)
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: 41
Which command successfully creates an administrative user with a password of "cisco" on a Cisco router?
A. username Operator privilege 1 password cisco
B. username Operator privilege 7 password cisco
C. username Operator privilege 15 password cisco
D. username Operator password cisco privilege 15
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which two options are the primary deployment models for mobile device management? (Choose two.)
A. multisite
B. hybrid cloud-based
C. single-site
D. on-premises
E. cloud-based
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_MDMs.html

NEW QUESTION: 43
Which NAT type allows only objects or groups to reference an IP address?
A. dynamic NAT
B. dynamic PAT
C. static NAT
D. identity NAT
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Dynamic PAT translates multiple real addresses to a single mapped IP address by translating the real
source address and source port to the mapped address and unique mapped port. Each connection
requires a separate translation session because the source port differs for each connection.
Reference: http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-
firewalls/111842-asa-dynamic-pat-00.html

NEW QUESTION: 44

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: 45

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: 46
Which feature prevents loops by moving a nontrunking port into an errdisable state when a BPDU is
received on that port?
A. DHCP snooping
B. BPDU filter
C. BPDU guard
D. PortFast
Answer: (SHOW ANSWER)

NEW QUESTION: 47
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: 48
What is the maximum number of methods that a single method list can contain?
A. 5
B. 4

C. 3
D. 2
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which command do you enter to enable authentication for OSPF on an interface?
A. router(config-router)#area 0 authentication message-digest
B. router(config-router)#ip ospf authentication-key CISCOPASS
C. router(config-if)#ip ospf message-digest-key 1 md5 CISCOPASS
D. router(config-if)#ip ospf authentication message-digest
Answer: (SHOW ANSWER)

NEW QUESTION: 50
When setting up a site-to-site VPN with PSK authentication on a Cisco router, which two elements must be
configured under crypto map? (Choose two.)

A. nat
B. peer
C. pfs
D. reverse-route
E. transform-set
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html#wp1036915

NEW QUESTION: 51
Which two types of VLANs using PVLANs are valid? (Choose two.)
A. isolated
B. secondary
C. backup
D. community
E. promiscuous
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which product can be used to provide application layer protection for TCP port 25 traffic?
A. ESA
B. ASA
C. WSA
D. CWS

Answer: A (LEAVE A REPLY)

NEW QUESTION: 53
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: 54
Which two characteristics of a PVLAN are true? (Choose two.)
A. Isolated ports cannot communicate with other ports on the same VLAN.
B. Community ports have to be a part of the trunk.
C. They require VTP to be enabled in server mode.
D. PVLAN ports can be configured as EtherChannel ports.
E. Promiscuous ports can communicate with PVLAN ports.
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Which command do you enter to verify the status and settings of an IKE Phase 1 tunnel?
A. show crypto ipsec transform-set
B. show crypto isakmp policy
C. show crypto isakmp sa
D. show crypto ipsec as output
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
Which two SNMPv3 services support its capabilities as a secure network management protocol? (Choose
two.)
A. the shared secret key
B. access control
C. authentication
D. authorization
E. accounting
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
SNMPv3 includes three important services: authentication, privacy, and access control.
Reference: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-20/snmpv3.html

NEW QUESTION: 57
When an administrator initiates a device wipe command from the ISE, what is the immediate effect?
A. It requests the administrator to choose between erasing all device data or only managed corporate
data.
B. It requests the administrator to enter the device PIN or password before proceeding with the operation.
C. It notifies the device user and proceeds with the erase operation.
D. It immediately erases all data on the device.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
In this case, ISE will ask the admin to chose between erasing all device data or only managed corporate
data.

NEW QUESTION: 58
What mechanism does asymmetric cryptography use to secure data?
A. a public/private key pair
B. shared secret keys
C. an RSA nonce
D. an MD5 hash
Answer: (SHOW ANSWER)

Explanation/Reference:
Explanation:
Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt
and decrypt data. The keys are simply large numbers that have been paired together but are not identical
(asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in
the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the
opposite key from the one used to encrypt the message is used for decryption.
Reference: http://searchsecurity.techtarget.com/definition/asymmetric-cryptography

NEW QUESTION: 59
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: 60
Which EAP method authenticates a client against Active Directory without the use of client-side 802.1X certificates?

A. EAP-PEAP
B. EAP-MSCHAPv2
C. EAP-GTC
D. EAP-TLS
Answer: (SHOW ANSWER)

NEW QUESTION: 61
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: (SHOW ANSWER)
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: 62
Which IPSec mode is used to encrypt traffic directly between a client and a server VPN endpoint?
A. aggressive mode
B. quick mode
C. tunnel mode
D. transport mode
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Which technology could be used on top of an MPLS VPN to add confidentiality?
A. SSL
B. 3DES
C. IPsec
D. AES
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Which statement about an ASA in transparent mode is true?
A. It allows the use of dynamic NAT.
B. It requires an IP address for each interface.
C. It requires a management IP address.
D. It supports OSPF.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
For IPv4, a management IP address is required for both management traffic and for traffic to pass through
the adaptive security appliance. For multiple context mode, an IP address is required for each context.
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa83/configuration/guide/config/fwmode.html

NEW QUESTION: 65
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: 66
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: 67
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: 68
Which firewall configuration must you perform to allow traffic to flow in both directions between two zones?
A. You must configure two zone pairs, one for each direction.
B. You can configure a single zone pair that allows bidirectional traffic flows for any zone.
C. You can configure a single zone pair that allows bidirectional traffic flows for any zone except the self
zone.
D. You can configure a single zone pair that allows bidirectional traffic flows only if the source zone is the
less secure zone.
Answer: (SHOW ANSWER)

Explanation/Reference:
Explanation:
f there are two zones and you require policies for traffic going in both directions (from Z1 to Z2 and Z2 to
Z1), you must configure two zone pairs (one for each direction).
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book/sec-zone-pol-fw.html#GUID-16FD9685-CB43-45AF-9D24-F6E2E6467FF3

NEW QUESTION: 69
What configuration allows AnyConnect to automatically establish a VPN session when a user logs in to the
computer?
A. always-on
B. proxy
C. transparent mode
D. Trusted Network Detection
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
You can configure AnyConnect to establish a VPN session automatically after the user logs in to a
computer. The VPN session remains open until the user logs out of the computer, or the session timer or
idle session timer expires. The group policy assigned to the session specifies these timer values. If
AnyConnect loses the connection with the ASA, the ASA and the client retain the resources assigned to
the session until one of these timers expire. AnyConnect continually attempts to reestablish the connection
to reactivate the session if it is still open; otherwise, it continually attempts to establish a new VPN session.
Reference: http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/anyconnectadmin30/ac03vpn.html

NEW QUESTION: 70
Which two attack types can be prevented with the implementation of a Cisco IPS solution? (Choose two.)

A. man-in-the-middle
B. worms
C. DDoS

D. VLAN hopping
E. ARP spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 71
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: 72
Which option is the default value for the Diffie-Hellman group when configuring a site-to-site VPN on an
ASA device?
A. Group 1
B. Group 5
C. Group 2
D. Group 7
Answer: (SHOW ANSWER)

NEW QUESTION: 73
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: 74
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: (SHOW ANSWER)
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: 75
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: 76
Which two configurations can prevent VLAN hopping attack from attackers at VLAN 10? (Choose two.)
A. using switchport mode access command on all host ports
B. creating VLAN 99 and using switchport trunk native vlan 99 command on trunk ports
C. applying ACL between VLANs
D. using switchport nonegotiate command on dynamic desirable ports
E. using switchport trunk native vlan 10 command on trunk ports
F. enabling BPDU guard on all access ports
Answer: (SHOW ANSWER)

NEW QUESTION: 77
What are two challenges of using a network-based IPS? (Choose two.)
A. As the network expands, it requires you to add more sensors
B. It is unable to detect attacks across the entire network
C. It is unable to determine whether a detected attack was successful
D. It must support multiple operating systems
E. It requires additional storage and processor capacity on syslog servers
Answer: (SHOW ANSWER)

NEW QUESTION: 78
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: 79
What is an advantage of split tunneling?
A. It allows users with a VPN connection to a corporate network to access the Internet by using the VPN
for security.
B. It enables the VPN server to filter traffic more efficiently.
C. It allows users with a VPN connection to a corporate network to access the Internet without sending
traffic across the corporate network.
D. It protects traffic on the private network from users on the public network.
Answer: (SHOW ANSWER)

NEW QUESTION: 80
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: (SHOW ANSWER)
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: 81
Which feature can help a router or switch maintain packet forwarding and protocol states despite an attack
or heavy traffic load on the router or switch?
A. Cisco Express Forwarding
B. Service Policy
C. Policy Map
D. Control Plane Policing
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/15-mt/qos-plcshp-
15-mt-book/qos-plcshp-ctrl-pln-plc.html

NEW QUESTION: 82
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM
then answer the four 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: 83
Which technology can you implement to centrally mitigate potential threats when users on your network
download files that might be malicious?
A. Verify that the company IPS blocks all known malicious websites.
B. Enable file-reputation services to inspect all files that traverse the company network and block files with
low reputation scores.
C. Implement URL filtering on the perimeter firewall.
D. Verify that antivirus software is installed and up to date for all users on your network.
Answer: (SHOW ANSWER)

NEW QUESTION: 84
What does the DH group refer to?
A. length of key for encryption
B. length of key for authentication
C. length of key for key exchange
D. tunnel lifetime key
E. length of key for hashing
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Which type of IPS can identify worms that are propagating in a network?
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: 86
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: 87
Which two actions can a zone-based firewall take when looking at traffic? (Choose two.)
A. inspect
B. forward
C. drop
D. filter
E. broadcast
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Traffic cannot flow between a zone member interface and any interface that is not a zone member. Pass,
inspect, and drop actions can only be applied between two zones.
Reference: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html

NEW QUESTION: 88
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: 89
Which IPS detection method examines network traffic for preconfigured patterns?
A. Anomaly-based detection
B. Policy-based detection
C. Honey-pot detection
D. Signature-based detection
Answer: (SHOW ANSWER)

NEW QUESTION: 90

Which command do you enter to verify the Phase 1 status of a VPN connection?

A. sh crypto isakmp sa

B. sh crypto ipsec sa

C. debug crypto isakmp

D. sh crypto session

Answer: (SHOW ANSWER)

Explanation/Reference:

Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html#anc25

NEW QUESTION: 91

What are two advanced features of the Cisco AMP solution for endpoints? (Choose two.)

A. foresight

B. contemplation

C. reputation

D. reflection

E. sandboxing

Answer: (SHOW ANSWER)

NEW QUESTION: 92

Which Sourcefire event action should you choose if you want to block only malicious traffic from a particular end user?

A. Allow with inspection

B. Allow without inspection

C. Block

D. Trust

E. Monitor

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

Choose allow with inspection to block only malicious traffic from a specific end user.

Reference: https://popravak.wordpress.com/2015/05/20/sourcefire-access-control-policies-part-two/

NEW QUESTION: 93
Which attack involves large numbers of ICMP packets with a spoofed source IP address?
A. Teardrop attack
B. Smurf attack
C. SYN Flood attack
D. Nuke attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
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: (SHOW ANSWER)
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: 95
Which type of encryption technology has the broadest platform support to protect operating systems?
A. software
B. hardware
C. middleware
D. file-level
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Software encryption has the broadest platform support to protect operating systems
Reference: https://marketplace.cisco.com/catalog/companies/vormetric/products/vormetric-data-security

NEW QUESTION: 96
What are two direct-to-tower methods for redirecting web traffic to Cisco Cloud Web Security? (Choose
two.)
A. third-party proxies
B. Cisco Catalyst platforms
C. hosted PAC files
D. Cisco NAC Agent
E. Cisco ISE
Answer: (SHOW ANSWER)

NEW QUESTION: 97
In which type of attack does the attacker attempt to overload the CAM table on a switch so that the switch
acts as a hub?
A. MAC spoofing
B. gratuitous ARP
C. MAC flooding

D. DoS
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
MAC flooding is the act of attempting to overload the switches content addressable memory (CAM) table.
By sending a large stream of packets with random addresses, the CAM table of the switch will evenly fill up
and the switch can hold no more entries; some switches might divert to a "fail open" state. This means that
all frames start flooding out all ports of the switch.
Reference: http://howdoesinternetwork.com/2011/mac-address-flooding

NEW QUESTION: 98
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: 99
Which statement provides the best definition of malware?
A. Malware is unwanted software that is harmful or destructive.
B. Malware is software used by nation states to commit cyber crimes.
C. Malware is a collection of worms, viruses, and Trojan horses that is distributed as a single package.
D. Malware is tools and applications that remove unwanted programs.
Answer: (SHOW ANSWER)

Explanation/Reference:
Explanation:
Malware" is short for malicious software and used as a single term to refer to virus, spy ware, worm etc.
Malware is designed to cause damage to a stand alone computer or a networked pc. So wherever a
malware term is used it means a program, which is designed to damage your computer it may be a virus,
worm, or Trojan.
Reference: http://www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookies-
and-what-differentiates-them

NEW QUESTION: 100
Which two 802.1x features can you enable by running the IOS authentication priority command? (Choose two.)

A. forced authorized port state
B. Telnet authentication
C. automatic selection
D. Web authentication
E. MAC authentication bypass
Answer: D,E (LEAVE A REPLY)
Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/
sec-user-8021x-xe-3se-3850-book/sec-ieee-802x-fa.html

NEW QUESTION: 101
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: (SHOW ANSWER)
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: 102
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: 103
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: 104

When using the Adaptive Security Device Manager (ASDM), which two methods are available to add a
new root certificate? (Choose two.)
A. Use HTTPS
B. Install from a file
C. Use LDAP
D. Install from SFTP server
E. Use SCEP
Answer: (SHOW ANSWER)

NEW QUESTION: 105
What is a potential drawback to leaving VLAN 1 as the native VLAN?
A. It may be susceptible to a VLAN hoping attack.
B. Gratuitous ARPs might be able to conduct a man-in-the-middle attack.
C. The CAM might be overloaded, effectively turning the switch into a hub.
D. VLAN 1 might be vulnerable to IP address spoofing.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
If you leave VLAN 1 as native, your network might be susceptible to a VLAN hoping attack.
Reference: http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=3

NEW QUESTION: 106
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: 107
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: (SHOW ANSWER)
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

NEW QUESTION: 108
Which two are the default settings for port security? (Choose two.)
A. Violation is Protect

B. Maximum number of MAC addresses is 1
C. Violation is Restrict
D. Violation is Shutdown
E. Maximum number of MAC addresses is 2
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html

NEW QUESTION: 109
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: (SHOW ANSWER)
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: 110

Which two models of ASA tend to be used in a data center? (Choose two.)

A. 5555X
B. 5540
C. ASA service module
D. 5520
E. 5512X
F. 5585X
Answer: C,F (LEAVE A REPLY)

NEW QUESTION: 111
How can you detect a false negative on an IPS?
A. View the alert on the IPS.
B. Review the IPS log.
C. Review the IPS console.
D. Use a third-party system to perform penetration testing.
E. Use a third-party to audit the next-generation firewall rules.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
You need a third party system to perform penetration testing to identify false negative on IPS.
Reference: http://airccse.org/journal/ijsptm/papers/4115ijsptm04.pdf

NEW QUESTION: 112
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: 113
Refer to the exhibit.
Which area represents the data center?
A. A
B. D

C. B
D. C
Answer: (SHOW ANSWER)

NEW QUESTION: 114
Which statement represents a difference between an access list on an ASA versus an access list on a
router?
A. The ASA does not support standard access lists
B. The ASA does not ever use a wildcard mask
C. The ASA does not support numbered access lists
D. The ASA does not support extended access lists
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reference: http://www.ciscopress.com/articles/article.asp?p=2104953

NEW QUESTION: 115
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: 116
Which two are characteristics of RADIUS? (Choose two.)

A. Uses TCP port 49
B. Uses TCP ports 1812/1813
C. Encrypts only the password between user and server
D. Uses UDP ports 1812/1813
E. Uses UDP port 49
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 117
What improvement does EAP-FASTv2 provide over EAP-FAST?
A. It allows multiple credentials to be passed in a single EAP exchange.
B. It supports more secure encryption protocols.
C. It allows faster authentication by using fewer packets.
D. It addresses security vulnerabilities found in the original protocol.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The one improvement EAP-FASTv2 provides is that it allows multiple credentials to be passed in a single
EAP exchange. EAP-FAST was unable to do that in a single EAP exchange.
Reference: https://tools.ietf.org/html/draft-zhou-emu-eap-fastv2-00

NEW QUESTION: 118
What are two default behaviors of the traffic on a zone-based firewall? (Choose two.)
A. Communication is blocked between interfaces that are members of the same zone
B. The CBAC rules that are configured on router interfaces apply to zone interfaces
C. All traffic between zone is implicitly blocked
D. Traffic within the self-zone uses an implicit deny all
E. Communication is allowed between interfaces that are members of the same zone
Answer: (SHOW ANSWER)

NEW QUESTION: 119
Which IOS command do you enter to test authentication against a AAA server?
A. test aaa-server authentication dialergroup username <user> password <password>
B. ppp authentication chap pap test
C. aaa authentication enable default test group tacacs+
D. dialer aaa suffix <suffix> password <password>
Answer: (SHOW ANSWER)

NEW QUESTION: 120
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: 121
Which two actions can a zone-based firewall apply to a packet as it transits a zone pair? (Choose two.)
A. drop
B. queue
C. inspect
D. block
E. quarantine
Answer: (SHOW ANSWER)

NEW QUESTION: 122
In which form of fraud does an attacker try to learn information such as login credentials or account
information by masquerading as a reputable entity or person in email, IM or other communication channels?
A. Phishing

B. Identity Spoofing
C. Smurfing
D. Hacking
Answer: A (LEAVE A REPLY)

NEW QUESTION: 123
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: 124
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: 125
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: 126
What type of packet creates and performs network operations on a network device?
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: 127
What is true about the Cisco IOS Resilient Configuration feature?
A. There is additional space required to secure the primary Cisco IOS image file.
B. The feature can be disabled through a remote session.
C. Remote storage is used for securing files.
D. The feature automatically detects image or configuration version mismatch.
Answer: (SHOW ANSWER)

NEW QUESTION: 128
How can you prevent NAT rules from sending traffic to incorrect interfaces?
A. Use packet-tracer rules to reroute misrouted NAT entries
B. Configure twice NAT instead of object NAT
C. Add the no-proxy-arp command to the nat line
D. Assign the output interface in the NAT statement
Answer: (SHOW ANSWER)

NEW QUESTION: 129
What are two challenges when deploying host-level IPS? (Choose two.)
A. It is unable to determine the outcome of every attack that it detects.
B. It is unable to provide a complete network picture of an attack.
C. The deployment must support multiple operating systems.
D. It does not provide protection for offsite computers.
E. It is unable to detect fragmentation attacks.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Advantages of HIPS: The success or failure of an attack can be readily determined. A network IPS sends
an alarm upon the presence of intrusive activity but cannot always ascertain the success or failure of such
an attack. HIPS does not have to worry about fragmentation attacks or variable Time to Live (TTL) attacks
because the host stack takes care of these issues. If the network traffic stream is encrypted, HIPS has

access to the traffic in unencrypted form.
Limitations of HIPS:
There are two major drawbacks to HIPS:
+ HIPS does not provide a complete network picture: Because HIPS examines information only at the local
host level, HIPS has difficulty constructing an accurate network picture or coordinating the events happening across the entire network. + HIPS has a requirement to support multiple operating systems:
HIPS needs to run on every system in the network. This requires verifying support for all the different
operating systems used in your network.
Reference: http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3

NEW QUESTION: 130

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: 131
Which type of malicious software can create a back-door into a device or network?
A. Bot
B. Virus
C. Worm
D. Trojan
Answer: (SHOW ANSWER)

NEW QUESTION: 132
Which security measures can protect the control plane of a Cisco router? (Choose two.)
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: 133
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: 134
Which network topology describes multiple LANs in a geographically limited area?
A. SOHO
B. CAN
C. MAN
D. PAN
Answer: (SHOW ANSWER)

NEW QUESTION: 135
What is a limitation of network-based IPS?
A. Large installations require numerous sensors to fully protect the network.
B. It is unable to monitor attacks across the entire network.
C. It is most effective at the individual host level.
D. It must be individually configured to support every operating system on the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 136
What is the effect of the ip scp server enable command?
A. It references an access list that allows specific SCP servers.
B. It allows the router to become an SCP server.
C. It adds SCP to the list of allowed copy functions.
D. It allows the router to initiate requests to an SCP server.
Answer: (SHOW ANSWER)

NEW QUESTION: 137

Which three descriptions of RADIUS are true? (Choose three.)

A. It supports multiple transport protocols.

B. It separates authentication, authorization, and accounting.

C. It uses UDP as its transport protocol.

D. It uses TCP as its transport protocol.

E. Only the password is encrypted.

F. It combines authentication and authorization.

Answer: (SHOW ANSWER)

NEW QUESTION: 138

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: 139

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

NEW QUESTION: 140

Which statement about the native VLAN is true?

A. It is most secure when it is assigned to VLAN 1.

B. It is the Cisco recommended VLAN for switch-management traffic.

C. It is susceptible to VLAN hopping attacks.

D. It is the Cisco-recommended VLAN for user traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 141
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: 142
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: 143
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

NEW QUESTION: 144
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

NEW QUESTION: 145
Which IDS/IPS solution can monitor system processes and resources?

A. IDS
B. HIPS
C. IPS
D. PROXY
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
HIPS audits host log files, host file systems, and resources. A significant advantage of HIPS is that it can
monitor operating system processes and protect critical system resources, including files that may exist
only on that specific host.

NEW QUESTION: 146
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: 147
What are two features of transparent firewall mode? (Choose two.)
A. It conceals the presence of the firewall from attackers.
B. It acts as a routed hop in the network.
C. It enables the ASA to perform as a router.
D. It allows some traffic that is blocked in routed mode.
E. It is configured by default.
Answer: (SHOW ANSWER)

NEW QUESTION: 148
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: 149
Refer to the exhibit. What is the effect of the given configuration?
A. The two devices are able to pass the message digest to one another
B. It enables authentication
C. The two routers receive normal updates from one another
D. It prevents keychain authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 150
Which two characteristics of an application layer firewall are true? (Choose two.)
A. provides stateful firewall functionality
B. provides reverse proxy services
C. provides protection for multiple applications
D. has low processor usage
E. is immune to URL manipulation
Answer: (SHOW ANSWER)

NEW QUESTION: 151
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: 152
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: 153
Which type of attack can exploit design flaws in the implementation of an application without going
noticed?
A. DHCP starvation attacks
B. application DDoS flood attacks

C. volume-based DDoS attacks
D. low-rate DoS attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 154
Which two primary security concerns can you mitigate with a BYOD solution? (Choose two.)
A. schedule for patching the device
B. connections to public Wi-Fi networks
C. device tagging and inventory
D. securing access to a trusted corporate network
E. compliance with applicable policies
Answer: (SHOW ANSWER)

NEW QUESTION: 155
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

NEW QUESTION: 156
Which two are considered basic security principles? (Choose two.)
A. Confidentiality
B. High Availability
C. Accountability
D. Integrity
E. Redundancy
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 157
Which command should be used to enable AAA authentication to determine if a user can access the

privilege command level?
A. aaa authentication enable method default
B. aaa authentication enable default local
C. aaa authentication enable local
D. aaa authentication enable level
Answer: (SHOW ANSWER)

NEW QUESTION: 158
Which feature allows a dynamic PAT pool to select the next address in the PAT pool instead of the next
port of an existing address?
A. next IP
B. round robin
C. dynamic rotation
D. NAT address rotation
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Check the Round Robin check box to assign addresses/ports in a round-robin fashion. By default without
round robin, all ports for a PAT address will be allocated before the next PAT address is used. The round-
robin method assigns one address/port from each PAT address in the pool before returning to use the first
address again, and then the second address, and so on.
Reference:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/asdm65/configuration_guide/asa_cfg_asdm_65/nat_objects.html

NEW QUESTION: 159
In which configuration mode do you configure the ip ospf authentication-key 1 command?
A. routing process
B. interface
C. privileged
D. global
Answer: (SHOW ANSWER)

NEW QUESTION: 160
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: 161
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

NEW QUESTION: 162
Which address block is reserved for locally assigned unique local addresses?
A. 2002::/16
B. FD00::/8

C. 2001::/32
D. FB00::/8
Answer: B (LEAVE A REPLY)
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: 163
Why does ISE require its own certificate issued by a trusted CA?
A. It requests certificates for guest devices from the CA server based on its own certificate.
B. ISE's certificate allows guest devices to validate it as a trusted network device.
C. It generates certificates for guest devices based on its own certificate.
D. ISE's certificate allows it to join the network security framework.
Answer: (SHOW ANSWER)

NEW QUESTION: 164
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: 165
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: 166

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: A (LEAVE A REPLY)
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: 167
How can FirePOWER block malicious email attachments?
A. It forwards email requests to an external signature engine.
B. It scans inbound email messages for known bad URLs.
C. It sends the traffic through a file policy.
D. It sends an alert to the administrator to verify suspicious email messages.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Malicious software, or malware, can enter your organization's network via multiple routes. To help you
identify and mitigate the effects of malware, the ASA FirePOWER module's file control and advanced

malware protection components can detect, track, store, analyze, and optionally block the transmission of
malware and other types of files in network traffic.
You configure the system to perform malware protection and file control as part of your overall access
control configuration. File policies that you create and associate with access control rules handle network
traffic that matches the rules.
Reference: http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-
firepower-module-user-guide-v541/AMP-Config.html

NEW QUESTION: 168
Which two advantages does the on-premise model for MDM deployment have over the cloud-based
model? (Choose two.)
A. The on-premise model is easier and faster to deploy than the cloud-based model
B. The on-premise model is more scalable than the cloud-based model
C. The on-premise model is generally less expensive than the cloud-based model
D. The on-premise model provides more control of the MDM solution than the cloud-based model
E. The on-premise model generally has less latency than the cloud-based model
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_MDMs.html

NEW QUESTION: 169
Which action does standard antivirus software perform as part of the file-analysis process?
A. create a backup copy of the file
B. execute the file in a simulated environment to examine its behavior
C. examine the execution instructions in the file
D. flag the unexamined file as a potential threat
Answer: (SHOW ANSWER)

NEW QUESTION: 170
Which sensor mode can deny attackers inline?
A. IPS
B. fail-close
C. IDS
D. fail-open
Answer: (SHOW ANSWER)

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: 171
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

NEW QUESTION: 172
How can you protect CDP from reconnaissance attacks?
A. Disable CDP on ports connected to endpoints.
B. Enable dynamic ARP inspection on all untrusted ports.
C. Enable dot1x on all ports that are connected to other switches.
D. Disable CDP on trunk ports.
Answer: (SHOW ANSWER)

NEW QUESTION: 173
Which countermeasures can mitigate ARP spoofing attacks? (Choose two.)
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: 174
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: 175
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: 176

What is the best way to confirm that AAA authentication is working properly?
A. Use the test aaa command.
B. Ping the NAS to confirm connectivity.
C. Use the Cisco-recommended configuration for AAA authentication.
D. Log into and out of the router, and then check the NAS authentication log.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
To associate a dialed number identification service (DNIS) or calling line identification (CLID) user profile
with the record that is sent to the RADIUS server or to manually test load-balancing server status, use the
test aaa group command in privileged EXEC mode.
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-
s1-xe-3se-3850-cr-book_chapter_0101.html#wp1375904793

NEW QUESTION: 177
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. IKE Phase 1 main mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.
B. IKE Phase 1 main mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.
C. IKE Phase 1 aggressive mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.
D. IKE Phase 1 aggressive mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The IKE phase 1 main mode was created on 10.1.1.5 but it failed to negotiate with 10.10.10.2.
Reference: http://www.juniper.net/techpubs/software/screenos/screenos6.3.0/630_ce_VPN.pdf

NEW QUESTION: 178
In the router ospf 200 command, what does the value 200 stand for?
A. process ID
B. area ID
C. administrative distance value
D. ABR ID
Answer: A (LEAVE A REPLY)
Explanation/Reference:

This command performs the same function as the distance command used with an access list. However,
the distance ospf command allows you to set a distance for an entire group of routes, rather than a specific
route that passes an access list.
A common reason to use the distance ospf command is when you have multiple OSPF processes with
mutual redistribution, and you want to prefer internal routes from one over external routes from the other.
Reference:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfospf.html

NEW QUESTION: 179
Which feature of the Cisco Email Security Appliance can mitigate the impact of snowshoe spam and
sophisticated phishing attacks?
A. contextual analysis
B. signature-based IPS
C. graymail management and filtering
D. reputation based filtering
Answer: (SHOW ANSWER)

NEW QUESTION: 180
Which type of social-engineering attack uses normal telephone service as the attack vector?
A. smishing
B. phishing
C. war dialing
D. vishing
Answer: (SHOW ANSWER)