Cisco.400-251.v2018-08-20.q120

Exam Code:	400-251
Exam Name:	CCIE Security Written Exam (v5.0)
Certification Provider:	Cisco
Free Question Number:	120
Version:	v2018-08-20
# of views:	1192
# of Questions views:	41391
https://www.freecram.net/torrent/Cisco.400-251.v2018-08-20.q120.html	

NEW QUESTION: 1
Which three transports have been defined for SNMPv3? (Choose three.)
A. IPsec secured tunnel
B. SSL
C. TLS
D. SSH
E. GET
F. DTLS
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 2
What are two features that help to mitigate man-in-the-middle attacks? (Choose two.)
A. ARP spoofing
B. ARP sniffing on specific ports
C. DHCP snooping
D. destination MAC ACLs
E. dynamic ARP inspection
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 3
Which two options are unicast address types for IPv6 addressing? (Choose two.)
A. global
B. established

C. link-local
D. static
E. dynamic
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 4
What are three features that are enabled by generating Change of Authorization (CoA) requests in a push model? (Choose three.)
A. host reauthentication
B. session identification
C. session termination
D. host termination
E. session reauthentication
F. MAC identification
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 5
View the Exhibit.

```
authentication priority dot1x mab
authentication order dot1x mab
authentication event fail action next-method
authentication event server dead action reinitialize vlan 50
authentication host-mode multi-auth
authentication violation restrict
```

Refer to the exhibit. Which two effects of this configuration are true? (Choose two.)
A. If the TACACS+ server is unreachable, the switch places hosts on critical ports in VLAN 50.
B. The device allows multiple authenticated sessions for a single MAC address in the voice domain.
C. If multiple hosts have authenticated to the same port, each can be in their own assigned VLAN.
D. If the authentication priority is changed, the order in which authentication is performed also changes.
E. The switch periodically sends an EAP-Identity-Request to the endpoint supplicant.
F. The port attempts 802.1x authentication first, and then falls back to MAC authentication bypass.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 6
Which three statements about RLDP are true? (Choose three.)

A. It detects rogue access points that are connected to the wired network.
B. It can detect rogue APs operating only on 5 GHz.
C. It can detect rogue APs that use WPA encryption.
D. It can detect rogue APs that use WEP encryption.
E. Active Rogue Containment can be initiated manually against rogue devices detected on the wired network.
F. The AP is unable to serve clients while the RLDP process is active.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 7
Which two statements about ICMP redirect messages are true? (Choose two.)
A. They are generated by the host to inform the router of an alternate route to the destination.
B. The messages contain an ICMP Type 3 and ICMP code 7.
C. Redirects are only punted to the CPU if the packets are also source-routed.
D. By default, configuring HSRP on the interface disables ICMP redirect functionality.
E. They are generated when a packet enters and exists the same router interface.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 8
How would you best describe Jenkins?
A. An orchestration tool
B. Continuous integration and delivery application
C. A REST client
D. Operates in a client/server model
E. Web-based repository hosting service
Answer: (SHOW ANSWER)

NEW QUESTION: 9
View the Exhibit.
%ASA-6-110001: No route to <desr_address> from <source_address>
Refer to the exhibit. Which meaning of this error message on a Cisco ASA is true?
A. The route map redistribution is configured incorrectly.
B. The host is connected directly to the firewall.
C. A packet was denied and dropped by an ACL.
D. The default route is undefined.
Answer: D (LEAVE A REPLY)
Explanation/Reference:

Explanation:

NEW QUESTION: 10

Which statement about SMTP authentication in a Cisco ESA deployment is true?

A. It enables users at remote sites to retrieve their email messages via a secure client.

B. If an authenticating user belongs to more than one LDAP group, each with different user roles, AsyncOS grants permissions in accordance with the least restrictive user role.

C. When SMTP authentication with forwarding is performed by a second SMTP server, the second server also performs the transfer of queued messages.

D. Clients can be authenticated with an LDAP bind or by fetching a passphrase as an attribute.

E. It enables users at remote sites to release email messages from spam quarantine.

F. The LDAP servers used by an ESA must share a single SMTP authentication profile.

Answer: (SHOW ANSWER)

NEW QUESTION: 11

Which statement currently describes Botnet attack?

A. It is launched by a collection of machines to execute DDoS against the attacker.

B. It is a form of a man-in-the-middle attack where the compromised machine is controlled remotely.

C. It is a form of a fragmentation attack to evade an intrusion prevention security device.

D. It is a launched by a single machine controlled by Command and Control system.

E. It is a form a wireless attack where attacker installs an access point to create backdoor to a network.

F. It is launched by a collection of machines controllers by Command and Control system.

Answer: (SHOW ANSWER)

NEW QUESTION: 12

How does Scavenger-class QoS mitigate DoS and worm attacks?

A. It matches traffic from individual hosts against the specific network characteristics of known attack types.

B. It sets a specific intrusion detection mechanism and applies the appropriate ACL when matching traffic is detected.

C. It monitors normal traffic flow and drops burst traffic above the normal rate for a single host.

D. It monitors normal traffic flow and aggressively drops sustained abnormally high traffic streams from multiple hosts.

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Reference: https://www.cisco.com/en/US/technologies/tk543/tk759/technologies_white_paper0900aecd80295ac7.pdf

NEW QUESTION: 13

Witch two statements about ping flood attacks are true? (Choose two.)

A. They attack by sending ping requests to the return address of the network.
B. They use ICMP packets.
C. They attack by sending ping requests to the broadcast address of the network.
D. The attack is intended to overwhelm the CPU of the target victim.
E. They use UDP packets.
F. They use SYN packets.
Answer: B,D (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 14
Which of the following could be an evasion technique used by the attacker?
A. Port access using Dot1x.
B. ACL implementation to drop unwanted traffic.
C. Traffic encryption to bypass IPS detection.
D. TELNET to launch device administrative session.
E. URL filtering to block malicious sites.
F. NAT translations on routers and switches.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
What is the best description of a docker file?
A. Text document used to build an image
B. Software used to manage containers
C. Repository for a docker images
D. Message Daemon files
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which statement is true about a SMURF attack?
A. In order to mitigate the attack you need to enable IP directed broadcast on the router interface.
B. It is used by the attackers to check if destination addresses are alive.
C. The attacker uses spoofed destination address to launch the attack.
D. It sends ICMP Echo Requests to a broadcast address of a subnet.
E. It sends ICMP Echo Replies to known ip addresses in a subnet.
F. it exhausts the victim machine resources with large number of ICMP Echo Requests from a subnet.
Answer: (SHOW ANSWER)

NEW QUESTION: 17

```
control-plane host
    management-interface FastEthernet 0/0 allow ssh snmp
```

Refer to the exhibit. What is the effect of the given command?
A. It enables MPP on the FastEthernet 0/0 interface by enforcing rate-limiting for SSH and SNMO management traffic.
B. It enables MPP on theFastEthernet 0/0 interface for SSH and SNMP management traffic and CoPP for all other protocols.
C. It enables MPP on the FastEthernet 0/0 interface, allowing only SSH and SNMP management traffic.
D. It enables QoS policing on the control plane of the FastEthernet 0/0 interface.
E. It enables CoPP on the FastEthernet 0/0 interface for SSH and SNMP management traffic.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 18
ISE can be integrated with an MDM to ensure that only registered devices are allowed on the network, and use the MDM to push policies to the device. Devices can go in and out of compliance, either due to policy changes on the MDM server, or another reason. For a device that has already authenticated on the network, and stays connected, but fails out of compliance, what can be done to ensure that a non-compliant device is checked periodically and re-assessed before allowing access to the network?
A. FireAMP connector can be used to relay posture information to ISE via FireAMP cloud.
B. The MDM agent will automatically disconnect the device from the network when it is non-compliant.
C. Enable Change of Authorization (CoA) on ISE.
D. Enable Change of Authorization (CoA) on MDM.
E. Enable Period Compliance Checking (PCC) on ISE.
F. The MDM agent periodically sends a packet with compliance info that the Wireless Controller can be used to limit network access.
Answer: (SHOW ANSWER)

NEW QUESTION: 19

Which of the following four traffic should be allowed during an unknown posture state? (Choose four.)

A. Traffic from AnyConnect client, with posture module, to ASA.

B. Traffic to FireAMP cloud for AMP for endpoint scan results.

C. DNS Traffic.

D. Traffic to public search engines.

E. Traffic to ISE PSNs to which Client Provisioning Portal FQDN points.

F. SSH traffic for network device administration.

G. Traffic to remediation servers, if needed.

H. DHCP Traffic.

Answer: (SHOW ANSWER)

NEW QUESTION: 20

You have an ISE deployment with 2 nodes that are configured as PAN and MnT (Primary and Secondary), and 4 Policy Services Nodes. How many additional PSNs can you add to this deployment?

A. 3

B. 4

C. 2

D. 1

E. 0

F. 5

Answer: (SHOW ANSWER)

NEW QUESTION: 21

View the Exhibit.

Switch-A (config)# cgmp leave-processing

Refer to the exhibit. Which two effects of this configuration are true? (Choose two.)

A. It allows the switch to detect IGMPv2leave group messages.

B. It optimizes the use of network bandwidth on the LAN segment.

C. IGMPv2 leave group messages are stored in the switch CAM table for faster processing.

D. Hosts send leave group messages to the Solicited-Node Address multicast address FF02::1:FF00:0000/104.

E. It improves the processing time of CGMP leave messages.

F. Hosts send leave group messages to the all-router multicast address when they want to stop receiving data for that group.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

Reference: ftp://sunsite.icm.edu.pl/site/cisco-ipmulticast/config-notes/cgmp_an.html

NEW QUESTION: 22

Which description of SaaS is true?

A. a service offering that allowing developers to build their own applications
B. a service offering a software environment in which application can be build and deployed
C. a service offering on-demand licensed applications for end users
D. a service offering on-demand software downloads
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference: https://en.wikipedia.org/wiki/Software_as_a_service

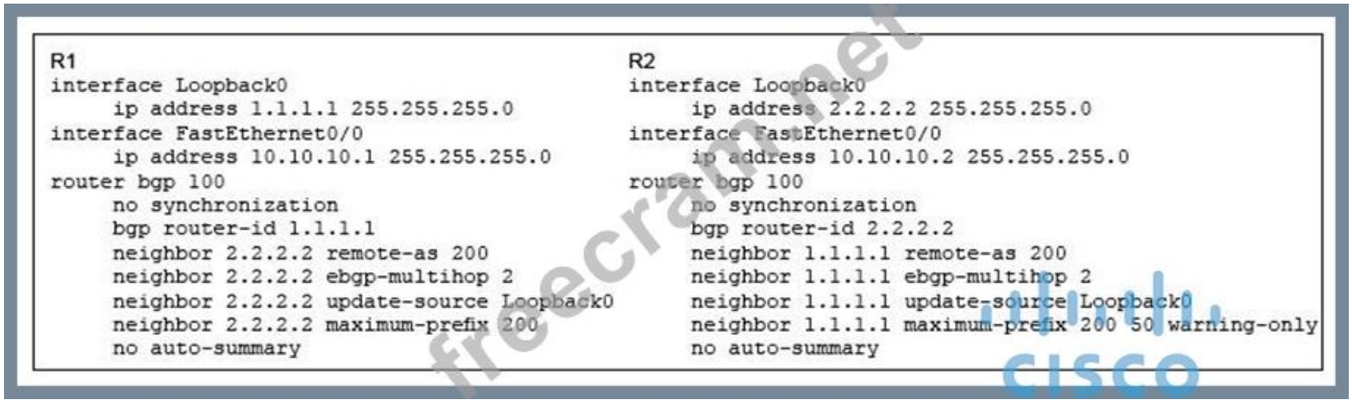
NEW QUESTION: 23
Which of the following is true regarding ASA clustering requirements?
A. Units in the cluster can be in different geographical locations.
B. Only routed mode is allowed in the Single context mode.
C. Units in the cluster can have different amount of flash memory.
D. Units in the cluster can be in different security context modes.
E. Units in the cluster can be running different software version as long as they have identical hardware configuration.
F. Units in the cluster can have different hardware configuration as long as they are running the same software version.
Answer: (SHOW ANSWER)

NEW QUESTION: 24
What are three technologies that can be used to trace the source of an attack in a network environment with multiple exit/entry points? (Choose three.)
A. Remotely-triggered destination-based black holing
B. ICMP Unreachable messages
C. Sinkholes
D. A honey pot
E. Traffic scrubbing
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 25
Which four task items need to be performed for an effective risk assessment and to evaluate network posture? (Choose four.)
A. scanning
B. mitigation
C. baselining
D. profiling
E. notification

F. validation
G. discovery
H. escalation
Answer: A,D,F,G (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 26



Refer to the exhibit. Which two effects of this configuration are true? (Choose two.)
A. The BGP neighbor session tears down after R1 receives 100 prefixes from neighbor 1.1.1.1.
B. The BGP neighbor session tears down after R1 receives 200 prefixes from neighbor 2.2.2.2.
C. The BGP neighbor session between R1 and R2 re-establishes after 50 minutes.
D. The BGP neighbor session between R1 and R2 re-establishes after 100 minutes.
E. A warning message is displayed on R2 after it receives 100 prefixes from neighbor 1.1.1.1.
F. A warning message is displayed on R2 after it receives 50 prefixes.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 27
Which of the following correctly describes NVGRE functionality?
A. In NVGRE network the endpoints are not responsible for the NVGRE encapsulation removal.
B. In NVGRE network VSID does not need to be unique.
C. It tunnels Ethernet frames inside an IP packet over a virtual network.
D. It allows to create physical layer-2 topologies on physical layer-3 network.
E. In NVGRE network VSID is used to identify tenant's address space.
F. It tunnels PPP frames inside an IP packet over a physical network.
G. It allows to create physical layer-2 topologies on virtual layer-3 network.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
In which type of multicast does the Cisco ASA forward IGMP messages to the upstream router?

A. multicast group concept
B. PIM multicast routing
C. stub multicastrouting
D. clustering
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/route_multicast.html#pgfId-1099362

NEW QUESTION: 29
Refer to the exhibit. R2 is getting time synchronized from NTP server R1. It has been reported that clock on R2 is not able to associate with the NTP server R1. What could be the possible cause?

```
R1:
ntp authentication-key 12 md5 cisco
ntp authenticate
ntp trusted-key 12
ntp source GigabitEthernet1
ntp master1
!
interface GigabitEthernet1
  ip address 171.1.7.21 255.255.255.0

R2:
ntp authentication-key 12 md5 cisco
ntp authentication-key 102 md5 cisco
ntp authenticate
ntp trusted-key 12
ntp trusted-key 102
ntp server 171.1.7.21 key 102

R2#ping 171.1.7.21
Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 171.1.7.21, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms

R2#sh ntp asso detail
171.1.7.21 configured, ipv4, authenticated, insane, invalid, unsynced,
stratum 16
ref ID INIT, time 00000000.00000000 (17:00:00.000 ccie Wed Dec 31 1899)
```


A. R2 does not support NTP authentication.
B. R2 should not have two trusted keys for the NTP authentication.
C. R2 has incorrect NTP server address.
D. R2 has incorrect trusted key binded with the NTP server.
E. R1 has incorrect NTP source interface defined.

F. R2 has connectivity issue with the NTP server.
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Which three Cisco attributes for LDAP authorization are supported on the ASA? (Choose three.)
A. Authenticated-User-Idle-Timeout
B. Web-VPN-ACL-Filters
C. L2TP-Encryption
D. IPsec-Default-Domain
E. Authorization-Type
F. IPsec-Client-Firewall-Filter-Name
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 31
Which two statements about role-based access control are true? (Choose two.)
A. Server profile administrators have read and write access to all system logs by default.
B. The user profile on an AAA server is configured with the roles that grant user privileges.
C. If the same user name is used for a local user account and a remote user account the roles defined in the remote user account override the local user account.
D. A view is created on the Cisco IOS device to leverage role-based access controls.
E. Network administrators have read and write access to all system logs by default.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

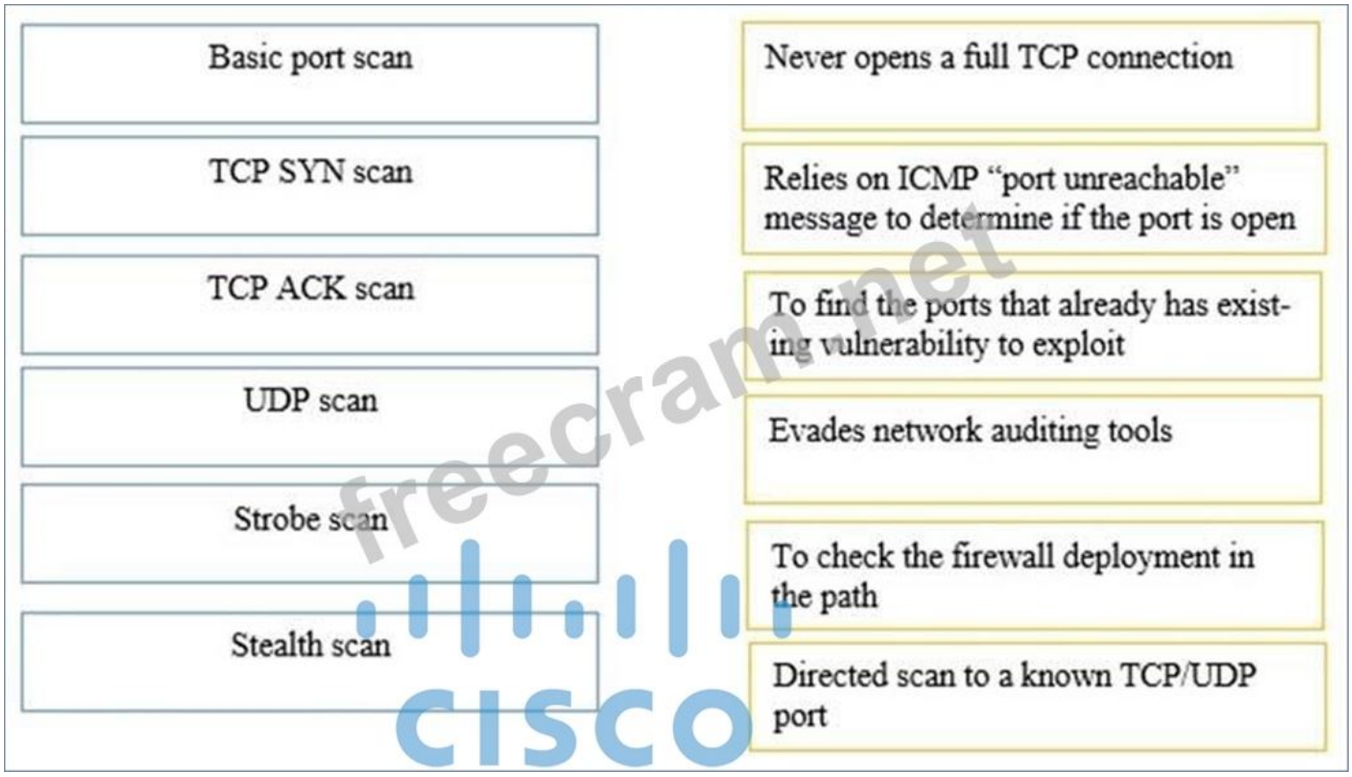
NEW QUESTION: 32
Which three statements about PKI on Cisco IOS Software are true? (Choose three.)
A. The match certificate and allow expired-certificate commands are ignored unless the router clock is set.
B. OCSP enables a PKI to use a CRL without time limitations.

C. Different OCSP servers can be configured for different groups of client certificates.
D. OCSPis well-suited for enterprise PKIs in which CRLs expire frequently.
E. Certificate-based ACLs can be configured to allow expired certificates if the peer is otherwise valid.
F. If a certificate-based ACL specifies more than one field, any one successful field-to-value test is treated as a match.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

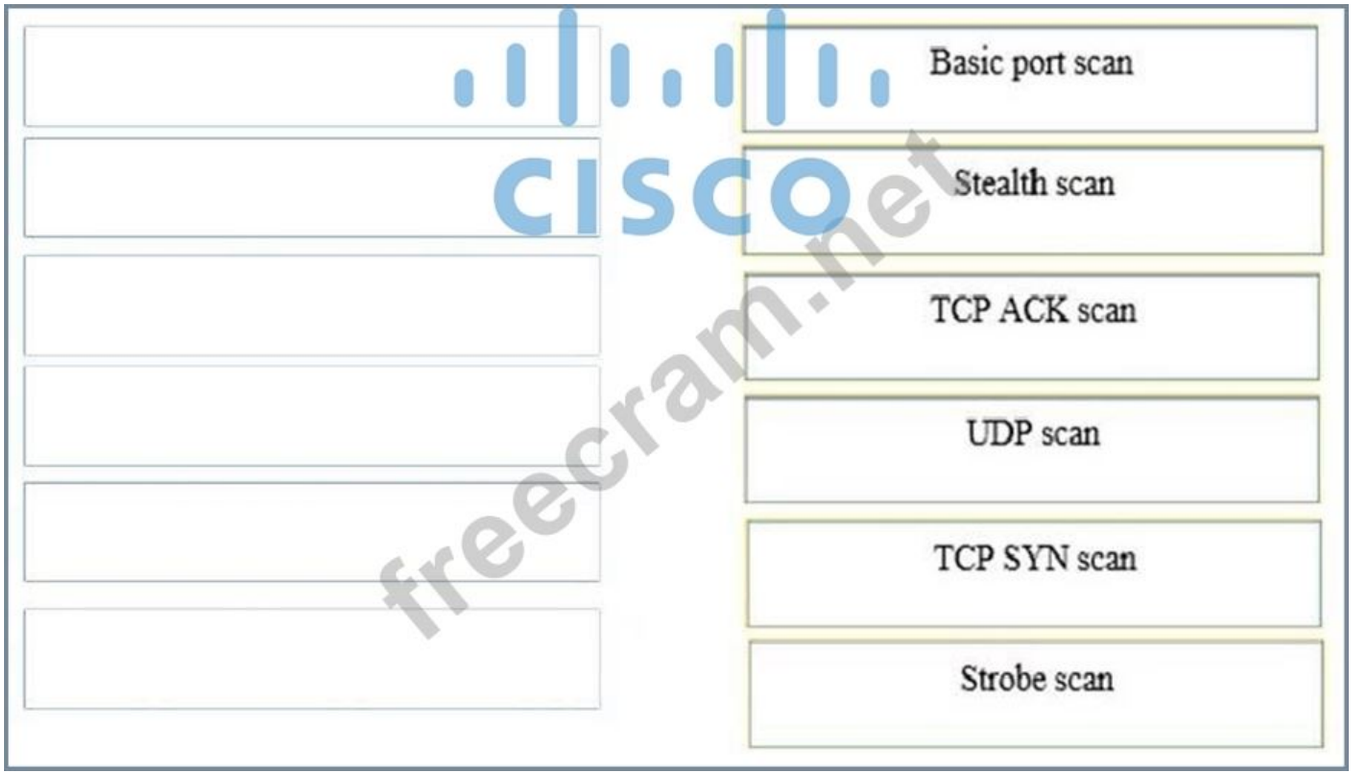
NEW QUESTION: 33
What are the three scanning engines that the Cisco IronPort dynamic vectoring and streaming engine can use to protect against malware? (Choose three.)
A. Symantec
B. McAfee
C. F-Secure
D. TrendMicro
E. Sophos
F. Webroot
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 34
Which two options are benefits of the Cisco ASA Identity Firewall? (Choose two.)
A. It can identify threats quickly based on their URLs.
B. It can operate completely independently of other services.
C. It supports an AD server module to verify identity data.
D. It decouples security from the network topology.
E. It can apply security policies on an individual user or user-group basis.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/configuration/general/asa-general-cli/ aaa-idfw.html

NEW QUESTION: 35
DRAG DROP
Drag the network scan type on the left to its definition on the right.
Select and Place:



Answer:



NEW QUESTION: 36

Which of the following is used by WSA to extract session information from ISE and use that in access policies?

A. SXP

B. Proprietary protocol over TCP/8302

C. RPC
D. pxGrid
E. RADIUS
F. EAP
Answer: (SHOW ANSWER)

NEW QUESTION: 37
In OpenStack, which two statements about the NOVA component are true? (Choose two.)
A. It is considered the cloud computing fabric controller.
B. It provides the authentication and authorization services.
C. It tracks cloud usage statistics for billing purposes.
D. It launches virtual machine instances.
E. It provides persistent block storage to running instances of virtual machines.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 38
View the Exhibit.

```
aaa-server AuthAutho protocol radius
merge-dacl after-avpair
```

Refer to the exhibit. Which effect of this configuration is true?
A. A downloadable ACL is applied after an AV pair ACL.
B. For all users, entries in a downloadable ACL are given priority over entries in an AV pair ACL.
C. The downloadable ACL and the AV pair ACL entries are merged together, one ACE at a time.
D. The downloadable ACL and AV pair ACL entries are merged immediately when the RADIUS server is activated.
E. The downloadable ACL and AV pair ACL entries are merged after three connection attempts are made to the RADIUS server.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 39
Which two statements about Cisco AMP for Web Security are true? (Choose two.)
A. It can detect and block malware and other anomalous traffic before it passes through the Web gateway.
B. It can identify anomalous traffic passing through the Web gateway by comparing it to an established baseline of expected activity.

C. It can perform file analysis by sandboxing known malware and comparing unknown files to a local repository of threats.
D. It continues monitoring files after they pass the Web gateway.
E. It can prevent malicious data exfiltration by blocking critical files from exiting through the Web gateway.
F. It can perform reputation-based evaluation and blocking by uploading the fingerprint of incoming files to a cloud-based threat intelligence network.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 40
Which three statements about WCCP are true? (Choose three.)
A. The minimum WCCP-Fast Timers message interval is 500 ms.
B. If a specific capability is missing from the Capabilities Info Component, the router is assumed to support the default capability.
C. If the packet return method is missing from a packet return method advertisement, the web cache uses the Layer 2 rewrite method.
D. The router must receive a valid receive ID before it negotiates capabilities.
E. The assignment method supports GRE encapsulation for sending traffic.
F. The web cache transmits its capabilities as soon as it receives a receive ID from a router.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference: https://tools.ietf.org/id/draft-wilson-wrec-wccp-v2-01.txt

NEW QUESTION: 41
Which statement is true about Remote Triggered Black Hole Filtering feature (RTBH)?
A. It works in conjunction with QoS to drop the traffic that has a less priority.
B. In RTBH filtering the trigger device is always an ISP edge router.
C. It helps mitigate DDoS attack based only on source address.
D. The Null0 interface used for filtering able to receive the traffic but never forwards it.
E. It drops malicious traffic at the customer edge router by forwarding it to a NullO interface.
F. In RTBH filtering the trigger device redistributes static route to the iBGP peers.
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which two options are normal functionalities for ICMP? (Choose two.)
A. packet filtering
B. host detection
C. relaying traffic statistics to applications
D. path MTU discovery

E. router discovery
F. port scanning
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 43
Which two statements about uRPF are true? (Choose two.)
A. The administrator can configure the allow-default command to force the routing table to use only the default route.
B. In strict mode, only one routing path can be available to reach network devices on a subnet.
C. The administrator can use the show cef interface command to determine whether uRPF is enabled.
D. The administrator can configure the ip verify unicast source reachable-via any command to enable the RPF check to work through HSRP routing groups.
E. It is not supported on the Cisco ASA security appliance.
Answer: B,C (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 44
View the Exhibit.
monitor session 1 source interface gigabitEthernet 0/1
monitor session 1 destination interface gigabitEthernet 0/20 encapsulation dot1q ingress vlan 3 Refer to the exhibit. What are two functionalities of this configuration? (Choose two.)
A. The encapsulation command is used to do deep scan on dot1q encapsulated traffic
B. Traffic will not be able to pass on gigabitEthernet 0/1
C. The ingress command is used for an IDS to send a reset on vlan 3 only
D. Traffic will only be sent to gigabitEthernet 0/20
E. The source interface should always be a VLAN
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 45
A server with IP address 209.165.202.150 is protected behind the inside interface of a Cisco ASA and the Internet on the outside interface. Users on the Internet need to access the server at any time, but the firewall administrator does not want to apply NAT to the address of the server because it is currently a public address. Which three of the following commands can be used to accomplish this? (Choose three.)
A. static (outside, inside) 209.165.202.150 209.165.202.150 netmask 255.255.255.255
B. access-list no-nat permit ip host 209.165.202.150 anynat (inside) 0 access-list no-nat
C. static (inside, outside) 209.165.202.150 209.165.202.150 netmask 255.255.255.255

D. nat (inside) 1 209.165.202.150 255.255.255.255
E. no nat-control
F. nat (inside) 0 209.165.202.150 255.255.255.255
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 46
AMP for Endpoints is supported on which of these platforms?
A. Windows, ANDROID, LINUX (REDHAT, CentOS), MAC
B. Windows, MAC, ANDROID
C. Windows, MAC, LINUX (SuSE, UBUNTU), ANDROID
D. Windows, ANDROID, LINUX (SuSE, REDHAT)
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:http://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html

NEW QUESTION: 47
A new computer is not getting its IPv6 address assigned by the router. While running WireShark to try to troubleshoot the problem, you find a lot of data that is not helpful to nail down the problem.
What two filters would you apply to WireShark to filter the data that you are looking for? (Choose two.)
A. icmpv6.type = =136
B. icmpv6.type = =135
C. icmpv5type = =135
D. icmpv6type = =136
E. icmpv6type = =135
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 48

View the Exhibit.

```
asal (config) #crypto ikevl policy 1
asal (config-ikevl-policy) #authentication pre-share
asal (config-ikevl-policy) #encryption 3des
asal (config-ikevl-policy) #hash md5
asal (config-ikevl-policy) #group 2
asal (config-ikevl-policy) #lifetime 86400
```

Refer to the exhibit. Which level of encryption is set by this configuration?

A. 56-bit

B. 168-bit

C. 1024-bit

D. 192-bit

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 49

Which of the following is AMP Endpoints office engine for windows?

A. ClamAV

B. ClamAMP

C. TETRA

D. TETRAAMP

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 50

```
Router(config)#crypto key zeroize pubkey-chain
```

Refer to the exhibit. Which effect of this command is true?

A. The current public key of the router is deleted from the cache when the router reboots, and the router generates a new one.

B. The CA revokes the public key certificate of the router.

C. The router sends a request to the CA to delete the router certificate from its configuration.

D. The router immediately deletes its current public key from the cache and generates a new one.

E. The public key of the remote peer is deleted from the router cache.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 51
Which statement is correct regarding Cisco VSG functionality?
A. It allows Active-Active failover operation mode when deployed as HA pair.
B. It applies security profile only after VM instantiation.
C. It allows third-party orchestration tool to interact with XML APIs for its provisioning.
D. It does not allow to extend Zone-Based firewall capabilities to VMs on VXLAN.
E. It allows administrative segregation due to which Security administrator can author and manage port profiles.
F. It does not provide trusted access to VMs in an enterprise data center.
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which two characteristics of DTLS are true? (Choose two.)
A. It includes a retransmission method because it uses an unreliable datagram transport.
B. It cannot be used if NAT exists along the path.
C. It completes key negotiation and bulk data transfer over a single channel.
D. It includes a congestion control mechanism.
E. It supports long data transfers and connectionless data transfers.
F. It is used mostly by applications that use application layer object-security protocols.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 53
View the Exhibit.

```
ASA (config)# class default
ASA (config-class)# limit-resource conns 10%
ASA (config-class)# limit-resource vpn other 10
ASA (config-class)# limit-resource vpn burst other 5
```

Refer to the exhibit. What is the maximum number of site-to-site VPNs allowed by this configuration?
A. 10
B. 15
C. unlimited
D. 5
E. 0
F. 1
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ha_contexts.html#pgfId-1142960

NEW QUESTION: 54
Which two statements about Cisco VSG are true? (Choose two.)
A. It uses IP-to-virtual machine mappings to simplify management of virtual machines.
B. According to Cisco best practices, the VSG should use the same VLAN for VSM-VEM control traffic and management traffic.
C. It has built-in intelligence for redirecting traffic and fast-path offload.
D. Because it is deployed at Layer 2, it can be inserted without significant reengineering of the network.
E. It can be integrated with VMware vCenter to provide transparent provisioning of policies and profiles.
F. It uses the Cisco VSG user agent to register with the Cisco Prime Network Services Controller
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 55
Refer to the exhibit.

R9 is running FLEXVPN with peer R10 at 20.1.4.10 using a pre-shared key "ccier10". The IPSec tunnel is sourced from 172.16.2.0/24 network and is included in EIGRP routing process.

BGP nexthop is in AS 345 with address 20.1.3.12. It has been reported that FLEXVPN is down. What could be the issue?

A. Incorrect IKEv2 profile configuration.

B. Incorrect keyring configuration.

C. Incorrect IPSec profile configuration.

D. Incorrect tunnel source for the tunnel interface.

E. Incorrect local network address in BGP routing process.

F. Incorrect tunnel network address in EIGRP routing process.

Answer: (SHOW ANSWER)

NEW QUESTION: 56

Which two statements about SCEP are true? (Choose two.)

A. The GetCACaps response message supports DES encryption and the SHA-128 hashing algorithm.
B. CA servers must support GetCACaps response message in order to implement extended functionality.
C. The GetCert exchange is signed and encrypted only in the response direction.
D. It is vulnerable to downgrade attacks on its cryptographic
E. The GetCRL exchange is signed and encrypted only in the response direction.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:http://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/116167-technote-scep-00.html#anc21

NEW QUESTION: 57
Which effect of the ip nhrp map multicast dynamic command is true?
A. It configures a hub router to reflect the routes it learns from a spoke back to other spokes through the same interface.
B. It enables a GRE tunnel to dynamically update the routing tables on the devices at each end of the tunnel.
C. It configures a hub router to automatically add spoke routers to the multicast replication list of the hub.
D. It enables a GRE tunnel to operate without the IPsec peer or crypto ACLs.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 58
Which two statements about 802.1X components are true? (Choose two.)
A. The certificates that are used in the client-server authentication process are stored on the access switch.
B. The access layer switch is the policy enforcement point.
C. The RADIUS server is the policy enforcement point.
D. The RADIUS server is the policy information point.
E. The RADIUS server is the policy decision point.
F. An LDAP server can serve as the policy enforcement point.
Answer: C,E (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 59
Which statement is true regarding the wireless security technologies?
A. WPA2-ENT mode does not require RADIUS for authentication.
B. WPA2-PSK mode allows passphrase to store locally on the device.
C. WPA2 is more secure than WPA because it uses TKIP for encryption.

D. WEP is more secure than WPA2 because it uses AES for encryption.
E. WPA provides message integrity using AES.
F. WPA2-PSK mode provides better security by having same passphrase across the network.
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 60
Which three authorization technologies does Cisco TrustSec support? (Choose three.)
A. SGT
B. SGAGL
C. MAB
D. 802.1x
E. DACL
F. VLAN
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 61
View the Exhibit.

```
class Partner-Class
   limit-resource routes 50
   limit-resource ASDM 4
   limit-resource VPN Other 400
   limit-resource xlates 18000
```

Refer to the exhibit. Which effect of this configuration is true?
A. It creates a default class.
B. It creates a resource class.
C. It oversubscribes VPN sessions for the given class.
D. It allows each context to use all available resources.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 62
Which effect of the crypto pki authenticate command is true?
A. It sets the certificate enrollment method.
B. It retrieves and authenticates a CA certificate.
C. It displays the current CA certificate.
D. It configures a CA trustpoint.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:https://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c5.pdf

NEW QUESTION: 63
What IOS feature can prevent header attacks by using packet-header information to classify traffic?
A. LLQ
B. TOS
C. FPM
D. CAR
E. TTL
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 64
Which option is a data modeling language used to model configuration and state data of network elements?
A. NETCONF
B. RESTCONF
C. YANG
D. SNMPv4
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference:https://www.ietf.org/proceedings/92/slides/slides-92-netmod-10.pdf

NEW QUESTION: 65
Which two events can cause a failover event on an active/standby setup? (Choose two.)
A. The stateful failover link fails.
B. The failover link fails.

C. The active unit experiences interface failure above the threshold.
D. The active unit fails.
E. The unit that was previously active recovers.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 66
In an effort to secure your enterprise campus network, any endpoint that connects to the network should authenticate before being access. For all corporate-owned endpoints, such as laptops, mobile phones and tablets, you would like to enable 802.1x, and once authenticated allow full access to the network. For all employee owned personal devices, you would like to use web authentication, and only allow limited access to the network. Which two authentication methods can ensure that an employee on a personal device can't use his or her Active Directory credentials to log on to the network by simply reconfiguring their supplicant, to use 802.1x and getting unfettered access? (Choose two.)
A. Use PEAP-EAP-MSCHAPv2
B. Use PEAP-EAP-TLS
C. Use EAP-MSCHAPv2
D. Use EAP-TLS or EAP-TTLS
E. Use EAP-FAST
F. Use PAP-CHAP-MSCHAP
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which two options are benefits of network summarization? (Choose two.)
A. It can summarize discontiguous IP addresses.
B. It can easily be added to existing networks.
C. It prevents unnecessary routing updates at the summarization boundary if one of the routes in the summary is unstable.
D. It reduces the number of routes.
E. It can increase the convergence of the network.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 68
Refer to the exhibit. ASA2 is configured for the Clientless SSL VPN connection with DNS server at 150.1.7.200 that is reachable only from the Management0/0 interface. The incoming VPN session will be received on outside interface with authentication credentials. Username: ccie, Password: ccie.

ASA2 is configured for the Self-Signed certificate with trustpoint "ccietrust" enabled for the outside interface. It has been reported that resources accessibility is timing out after the VPN connection establishment. What could be the reason?

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 20.1.2.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.1.22.1 255.255.255.0
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 100
ip address 150.1.7.55 255.255.0.0
!
access-list ccieacls webtype permit url http://server.cisco.com.8o log
default
!
crypto ca trustpoint ccietrust
 enrollment self
 subject-name CN=ASA2
 serial-number
 keypair cciekey
 crl configure
!
ssl trust-point ccietrust outside
!
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 150 2.7.200
 domain-name cisco.com
!
group-policy cciegroup internal
group-policy cciegroup attributes
 banner value CCIE Written!
 vpn-tunnel-protocol ssl-clientless
 webvpn
 url-list value servers
 filter value ccieacls
!
tunnel-group ccietunnel type remote-access
tunnel-group ccietunnel general-attributes
 default-group-policy cciegroup
!
webvpn
 enable outside
 tunnel-group-list enable
!
crypto ikev2 remote-access trustpoint ccietrust
dynamic-access-policy-record DfltAccessPolicy
username ccie password mflDmeWbPXQtCAxZ encrypted
username ccie attributes
 service-type remote-access
```

A. Incorrect banner value in the group policy.

B. The "ccieacl" should be configured for port 443.

C. Webvpn needs to be enabled on the management interface.

D. Management interface has incorrect security level configured.

E. The tunnel group is tied up with the incorrect group policy.

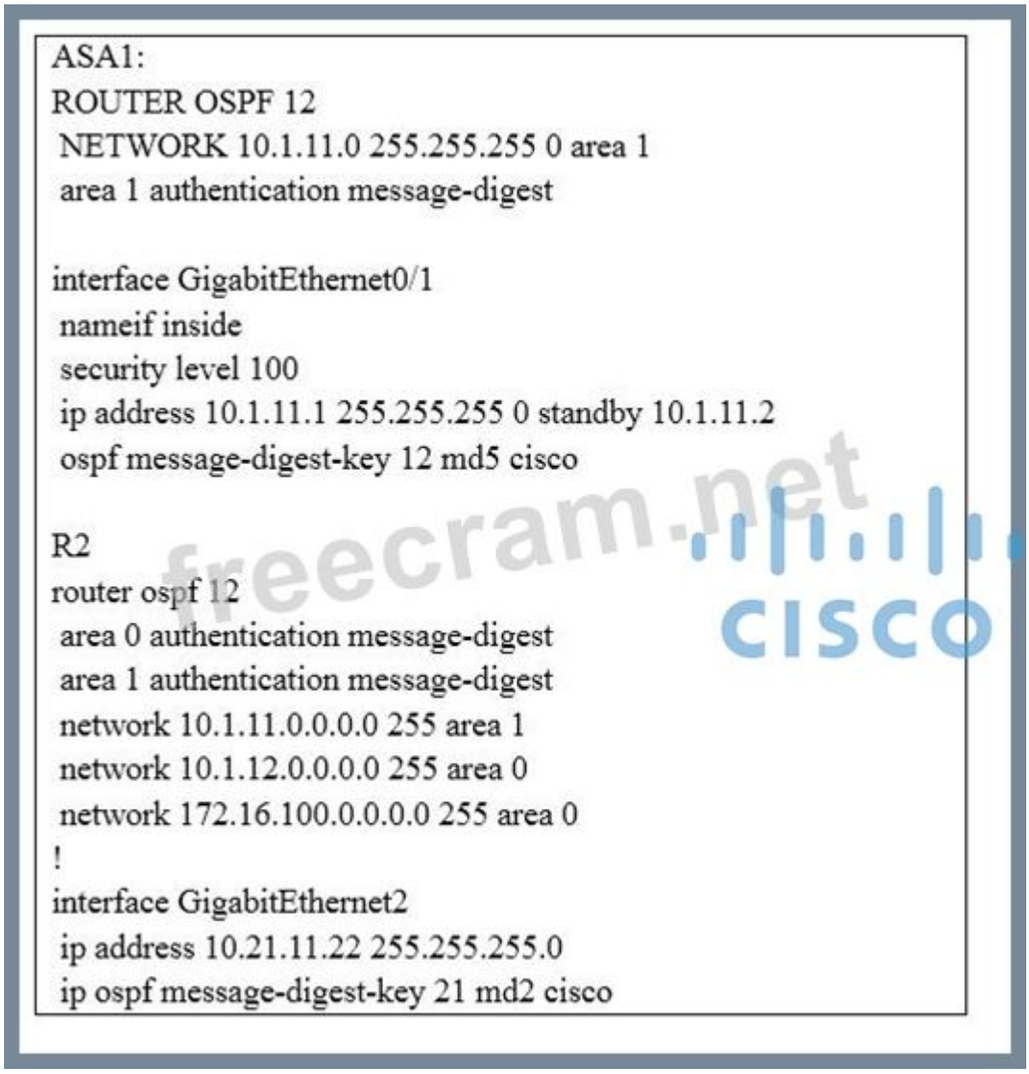
F. The domain-lookup should be performed from management interface.

G. The CA trustpoint "ccietrust" has incorrect keypair.

Answer: (SHOW ANSWER)

NEW QUESTION: 69

Refer to the exhibit.



Firewall ASA1 and router R2 are running OSPF routing process in area 1 connected via 10.1.11.0/24 subnet in the inside zone. It has been reported that ASA1 is unable to see any OSPF learned routes, what could be the reason?

A. On ASA1 Incorrect subnet mask on Gi0/1 interface.

B. On R2 Incorrect subnet defined for the Gi2 interface.

C. On ASA1 Gi0/1 interface should have security level at "0".

D. On ASA1 standby interface need to be disabled on Gi0/1 interface.

E. On R2 10.1.11.0/24 subnet should be in area "0" in OSPF routing process.

F. The R2 has mismatched message-digest key id.

Answer: (SHOW ANSWER)

NEW QUESTION: 70

Nexus 9000 platform supports the following configuration management tools?

A. Ansible

B. Chef
C. Puppet
D. Jenkins
E. Salt
Answer: (SHOW ANSWER)

NEW QUESTION: 71
Which type of header attack is detected by Cisco ASA basic threat detector?
A. failed application inspection
B. connection limit exceeded
C. bad packet format
D. denial by access list
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Using basic threat detection statistics, the ASA monitors the rate of dropped packets and security events due to the following reasons:
* Denial by access lists
* Bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length)
* Connection limits exceeded (both system-wide resource limits, and limits set in the configuration)
* DoS attack detected (such as an invalid SPI, Stateful Firewall check failure)
* Basic firewall checks failed (This option is a combined rate that includes all firewall-related packet drops in this bulleted list. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.)
* Suspicious ICMP packets detected
* Packets failed application inspection
* Interface overload
Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/conns_threat.html#wp1067533

NEW QUESTION: 72
Which two statements about the TTL value in an IPv4 header are true? (Choose two.)
A. It is a 4-bit value.
B. Its maximum value is 128.
C. It is a 16-bit value.
D. It can be used for traceroute operations.
E. When it reaches 0, the router sends an ICMP Type 11 message to the originator.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 73
Which statement about MDM with the Cisco ISE is true?
A. The MDM's server certificate must be imported into the Cisco ISE Certificate Store before the MDM and ISE can establish a connection.
B. MDM servers can generate custom ACLs for the Cisco ISE to apply to network devices.
C. The Cisco ISE supports limited built-in MDM functionality.
D. The Cisco ISE supports a built-in list of MDM dictionary attributes if can use in authorization policies.
E. When a mobile endpoint becomes complaint, the Cisco ISE records the updated device status in its internal database.
F. If a mobile endpoint fails posture compliance, both the user and the administrator are notified immediately.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 74
Which three ESMTP extensions are supported by the Cisco ASA? (Choose three.)
A. 8BITMIME
B. STARTTLS
C. NOOP
D. PIPELINING
E. SAML
F. ATRN
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Reference: http://www.cisco.com/c/en/us/about/security-center/intelligence/asa-esmtp-starttls.html

NEW QUESTION: 75
View the Exhibit.

```
class-map type inspect ftp match-any ccie-ftp
policy-map type inspect ftp ccie-ftp
   parameters
       no mask-syst-reply
service-police ccie-ftp interface inside
```


Refer to the exhibit. What are two effects of the given configuration? (Choose two.)
A. The connection will remain open if the PASV reply command include 5 commas.
B. TCP connections will be completed only to TCP ports from 1 to 1024
C. FTP clients will be able to determine the server's system type

D. The client must always send the PASV reply
E. The connection will remain open if the size of the STOR command is greater than a fixed constant
Answer: A,C (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 76
In FMC the correlation rule could be based on which two elements? (Choose two.)
A. Traffic profile variation
B. NDAC (Network Device Admission Control)
C. Intrusion event
D. SGT (Security Group Tag) mapping
E. Database type
F. Authentication condition
G. CoA (Change of Authorization)
H. Authorization rule
Answer: (SHOW ANSWER)

NEW QUESTION: 77
Which three options are fields in a CoA Request code packet? (Choose three.)
A. length
B. calling-station-ID
C. authenticator
D. acct-session-ID
E. state
F. identifier
Answer: A,C,F (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-
15-sy-book/sec-rad-coa.html

NEW QUESTION: 78
Which two options are important considerations when you use NetFlow to obtain the full picture of network traffic? (Choose two.)
A. It monitors only routed traffic.
B. It is unable to monitor over time.
C. It monitors only ingress traffic on the interface on which it is deployed.
D. It monitors all traffic on the interface on which it is deployed.
E. It monitors only TCP connections.
Answer: A,C (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 79
Within Platform as a Service, which two components are managed by the customer? (Choose two.)
A. middleware
B. applications
C. data
D. operating system
E. networking
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 80
The purpose of an authentication proxy is to force the user to authenticate to a network device before users are allowed access through the device. This is primarily used for HTTP based services, but can also be used for other services. In the case of an ASA, what does ISE have to send to enforce this access policy?

A. Redirect URL to ISE
B. Not possible on the ASA
C. VLAN
D. Group Policy enabled for proxy-auth
E. LDAP attribute with ACL
F. Downloadable ACL
Answer: (SHOW ANSWER)

NEW QUESTION: 81
When TCP Intercept is enabled in its default mode, how does it react to a SYN request?
A. It drops the connection.
B. It intercepts the SYN before it reaches the server and responds with a SYN-ACK.

C. It allows the connection without inspection.
D. It monitors the attempted connection and drops it if it fails to establish within 30 seconds.
E. It monitors the sequence of SYN, SYN-ACK, and ACK messages until the connection is fully established.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 82
Which command on Cisco ASA you can enter to send debug messages to a syslog server?
A. logging host
B. logging debug-trace
C. logging traps
D. logging syslog
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 83
Which command sequence do you enter to add the host 10.2.1.0 to the CISCO object group?
A. object-group network CISCOgroup-object 10.2.1.0
B. object network CISCOnetwork-object object 10.2.1.0
C. object network CISCOgroup-object 10.2.1.0
D. object-group network CISCOnetwork-objecthost10.2.1.0
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:

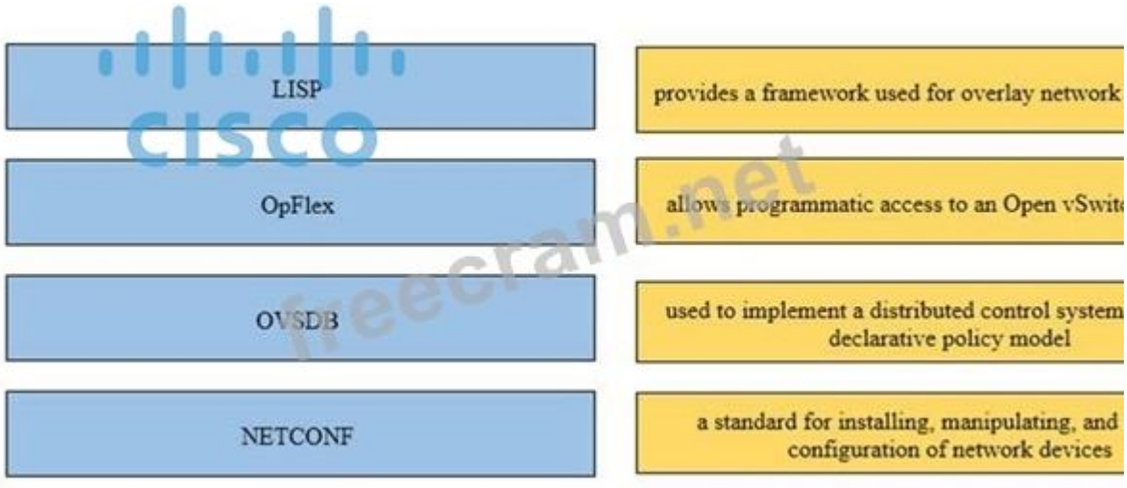
NEW QUESTION: 84
View the Exhibit.

Refer to the exhibit. Which data format is used in this script?
A. API
B. JSON
C. JavaScript

D. YANG
E. XML
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 85
Which statement describes a pure SDN framework environment?
A. The data plane is pulled from the networking element and put a SDN controller.
B. The control plane and data plane is pulled from the networking element and put in a SDN controller and SDN agent.
C. The control plane is pulled from the networking element and put a SDN controller.
D. The data plane is controlled by a centralized SDN element.
E. the control plane functions is split between a SDN controller and the networking element.
Answer: (SHOW ANSWER)

NEW QUESTION: 86
DRAG DROP
Drag and drop the protocols on the left onto their descriptions on the right.
Select and Place:



Answer:

NEW QUESTION: 87
Which three VSA attributes are present in a RADIUS WLAN Access-Accept packet? (Choose three.)
A. EAP-Message
B. Tunnel-Type
C. LEAP Session-Key
D. Tunnel-Private-Group-ID
E. Authorization-Algorithm-Type
F. SSID
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 88
View the Exhibit.

```
Name = xxxx dACL
Description = dACL for xxx dACL users
DACL Content = permit udp any host
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
permit ip any any
```

Refer to the exhibit. For which type of user is this downloadable ACL appropriate?
A. onsite contractors
B. management
C. network administrators
D. employees

E. guest users
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 89
What are the advantages of using LDAP over AD?
A. The closest LDAP servers are used for authentication.
B. LDAP can be configured to use a primary and secondary server, whereas AD cannot.
C. LDAP does not require ISE to join the AD domain.
D. LDAP allows for granular policy control, whereas AD does not.
E. LDAP provides for faster authentication.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 90
Which two statements about Botnet Traffic Filter snooping are true? (Choose two.)
A. It can log and block suspicious connections from previously unknown bad domains and IP addresses.
B. It checks inbound and outbound traffic.
C. It can inspect both IPv4 and IPv6 traffic.
D. It requires the Cisco ASA DNS server to perform DNS lookups.
E. It checks inbound traffic only.
F. It requires DNS packet inspection to be enabled to filter domain names in the dynamic database.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 91
Which statement is true regarding Dynamic ARP inspection (DAI)?
A. It drops invalid ARP responses and requests on the switch trusted ports.
B. It forwards invalid ARP responses and requests on switch untrusted ports.
C. It requires to enable DHCP snooping to build untrusted database for dropping invalid APR requests and responses.
D. It validates ARP requests and responses on untrusted ports using IP-To-MAC address binding.
E. It is only supported in DHCP environments to detect invalid ARP requests and responses.
F. It validates ARP requests and responses on trusted ports using IP-To-MAC address binding.
Answer: (SHOW ANSWER)

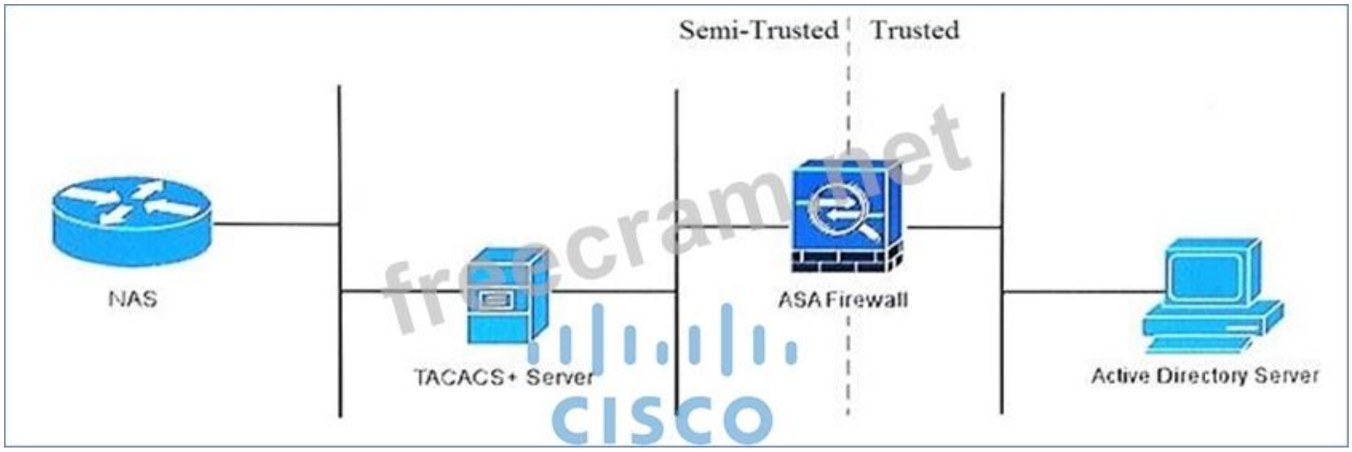
NEW QUESTION: 92
What are the two most common methods that security auditors use to assess an organization's security processes? (Choose two.)
A. social engineering attempts
B. penetration testing
C. physical observation
D. document review
E. interviews
F. policy assessment
Answer: D,E (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 93
View the Exhibit.

```
enable password cisco213
aaa-server TACACS+ protocol tacacs+
   reactivation-mode depletion deadtime 1440
aaa authentication serial console TACACS+ LOCAL
```

Refer to the exhibit. Which effect of this configuration is true?
A. Any VPN user with a session timeout of 24 hours can access the device.
B. Users attempting to access the console port are authenticated against the TACACS+ server.
C. If TACACS+authentication fails, the ASA uses cisco123 as its default password.
D. The device tries to reach the server every 24 hours and falls back to the LOCAL database if it fails.
E. The servers in the TACACS+ group are reactivated every 1440 seconds.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 94
View the Exhibit.



Refer to the exhibit. A user authenticates to the NAS, which communicates to the TACACS+ server for authentication. The TACACS+ server then accesses the Active Directory Server through the ASA firewall to validate the user credentials.

Which protocol-port must be allowed access through the ASA firewall?

A. DNS over TCP 53

B. global catalog over UDP 3268

C. LDAP over UDP 389

D. DNS over UDP 53

E. TACACS+ over TCP 49

F. SMB over TCP 455

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 95

In which two situations is web authentication appropriate? (Choose two.)

A. when a fallback authentication method is necessary

B. when 802.1x authentication is required

C. when WEP encryption must be deployed on a large scale

D. when devices outside the control of the organization's IT department are permitted to connect to the network

E. when secure connections to the network are unnecessary

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 96

Refer to the exhibit. Users are unable to access web servers 192.168.101.3/24 and 192.168.102.3/24 using Firefox web browser when initiated from 172.16.1.0/24 network. What could be the possible cause?

Identification Profiles

Client/User Identification Profiles	
Add Identification Profile...	
Order	Transaction Criteria
1	**Allow Profile** Subnets: 172.16.1.0/24 Protocols: HTTP/HTTPS User Agent: All except Firefox: Firefox Any Versions

Access Policies

Policies			
Add Policy...			
Order	Group	Protocols and User Agents	URL Filtering
1	**Allow Policy** Identification Profile: Allow Profile Add identified users	(global policy)	Allow:1

Access Policies: URL Filtering: Allow Policy

Custom URL Category Filtering				
These URL Categories are defined as group membership criteria. All other categories are not applic...				
	Use Global Settings	Block	Redirect	Allow
Category	Select all	Select all	Select all	Select all
Allowed Sites				✓

Custom URL Categories: Edit Category

Edit Custom URL Category	
Category Name:	Allowed Sites
List Order:	1
Sites:	192.168.101.3 192.168.102.3

A. Access policy "Allow policy" is pointing to incorrect identification profile.

B. Identification profile "Allow Profile" has incorrect protocol.

C. Identification profile "Allowed Profile" has misconfigured user agent.

D. Custom URL category "Allowed Sites" has incorrect servers address listed.

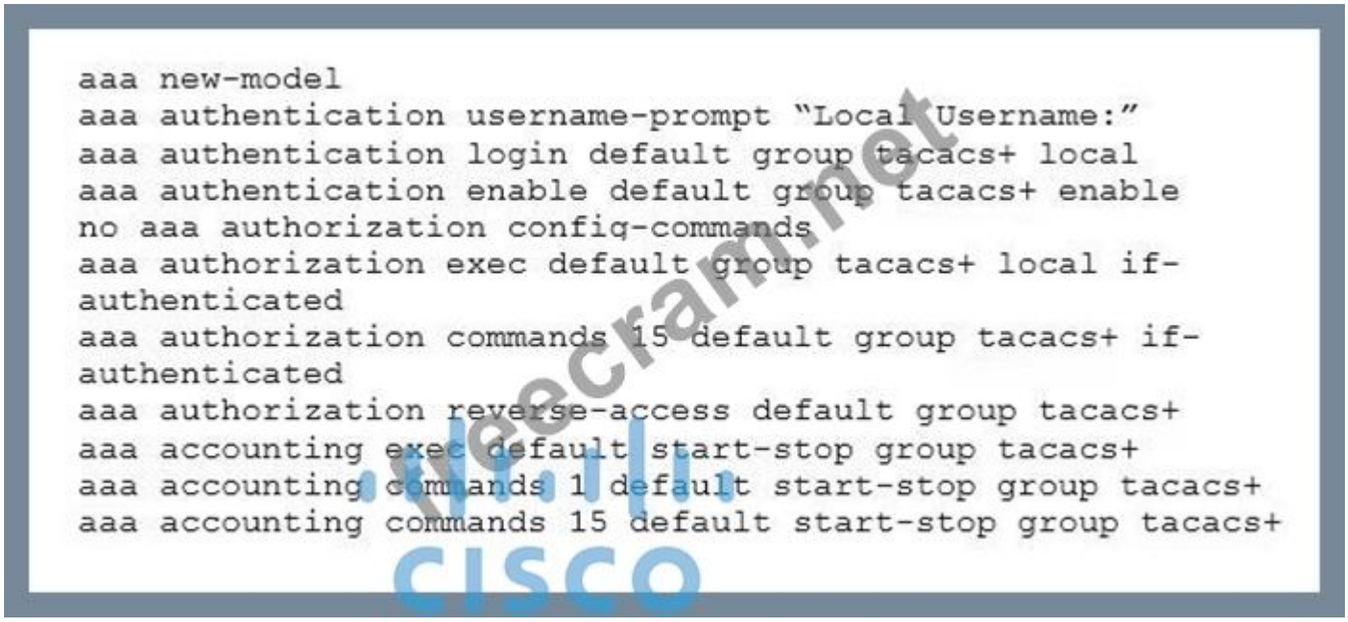
E. Identification profile "Allow Profile" has incorrect source subnet.

F. Access policy "Allow Policy" has incorrect action set for the custom URL category.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 97

View the Exhibit.



Refer to the exhibit. Which two effects of this configuration are true? (Choose two.)

A. Configuration commands in the router are authorized without checking the TACACS+ server.

B. When a user logs in to privilege EXEC mode, the router will track all user activity.

C. Requests to establish a reverse AUX connection to the router will be authorized against the TACACS+ server.

D. When a user attempts to authenticate on the device, the TACACS+ server will be prompt the user to enter the username stored in the router's database.

E. If a user attempts to log in as a level 15 user, the local database will be used for authentication and TACACS+ server will be used for authorization.

F. It configures the router's local database as the backup authentication method for all TTY, console, and aux logins.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 98

As an enterprise, you have decided to use Cisco Umbrella (OpenDNS) services for all public DNS requests. In which two ways can you ensure that all DNS clients (endpoints) use this service for external requests only? (Choose two.)

A. Install the Umbrella client on all the supported operating systems and configure it appropriately.

B. Use DHCP to push the OpenDNS servers to the endpoints.

C. Use DHCP to push a proxy DNS server to the endpoints that would chain the external requests to OpenDNS servers for resolution.

D. Install the Umbrella proxy server on all the supported operating systems and configure it appropriately.

E. Install the Umbrella server in your data center that will provide these services locally.

F. Configure the Open DNS servers as forwarders on your internal DNS servers.

G. Configure your internal DNS servers as forwarders on the OpenDNS servers.

Answer: (SHOW ANSWER)

NEW QUESTION: 99
Which three statements about SXP are true? (Choose three.)
A. To enable an access device to use IP device tracking to learn source device IP addresses, DHCP snooping must be configured.
B. Each VRF supports only one CTS-SXP connection.
C. It resides in the control plane, where connections can be initiated from a listener.
D. Separate VRFs require different CTS-SXP peers, but they can use the same source IP addresses.
E. The SGA ZBPF uses the SGT to apply forwarding decisions.
F. Packets can be tagged with SGTs only with hardware support.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 100
Which file extensions are supported on the Firesight Management Center 6.1 file policies that can be analyzed dynamically using the Threat Grid Sandbox integration?

A. MSEXE, MSOLE2, NEW-OFFICE, PDF
B. DOCX, WAV, XLS, TXT
C. DOC, MSOLE2, XML, PDF
D. TXT, MSOLE2, WAV, PDF
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 101
Which three statements about VRF-Aware Cisco Firewall are true? (Choose three.)
A. It supports both global and per-VRF commands and DoS parameters.
B. It can generate syslog messages that are visible only to individual VPNs.
C. It enables service providers to deploy firewalls on customer devices.
D. It can run as more than one instance.
E. It enables service providers to implement firewalls on PE devices.
F. It can support VPN networks with overlapping address ranges without NAT.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 102
Which statement is true about Dual-Hub DMVPN implementation where each spoke has two connections, one to each hub via different ISPs.

A. It uses two tunnel interfaces on each hub to terminate connection from each spoke,
B. It does not allow NHRP authentication.
C. It uses multipoint GRE tunnel.
D. It uses a single tunnel interface on a spoke to connect two different hubs.
E. It uses point-to-point GRE tunnel.
F. It does not allow tunnel protection using IPSec.
Answer: (SHOW ANSWER)

NEW QUESTION: 103
Which two statements about the SeND protocol are true? (Choose two.)
A. It counters neighbor discovery threats.
B. It logs IPv6-related treats to an external log server.
C. It supports numerous custom neighbor discovery messages.
D. It supports an auto-configuration mechanism.
E. It uses IPsec as a baseline mechanism.
F. It must be enabled before you can configure IPv6 addresses.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 104
A client computer at 10.10.7.4 is trying to access a Linux server (11.0.1.9) that is running a Tomcat Server application.
What TCP dump filter would be best to verify that traffic is reaching the Linux Server eth0 interface?
A. tcpdump -i eth0 host 10.10.7.4 and host 11.0.1.9 and port 8080
B. tcpdump -i eth0 host 10.10.7.4 and host 11.0.1.9
C. tcpdump -ieth0 dst 11.0.1.9 anddstport 8080
D. tcpdump -i eth0src10.10.7.4 anddst11.0.1.9 anddstport 8080
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 105
Which three EAP protocols are supported in WPA and WPA2? (Choose three.)
A. EAP_FAST
B. EAP_AKA
C. EAP_EKE
D. EAP_EEE
E. EAP_SIM
F. EAP_PSK
Answer: A,E,F (LEAVE A REPLY)

Explanation/Reference:
Explanation:

NEW QUESTION: 106
Which of the following is true regarding failover link when ASAs are configured in the failover mode?
A. The information sent over the failover link can only be sent as a secured communication.
B. It is not recommended to use secure communication over failover link when ASA terminating the VPN tunnel.
C. Only the configuration replication sent across the link can be secured using a failover key.
D. The information sent over the failover link can be sent in clear text or it could be secured communication using a failover key.
E. The information sent over the failover link can only be in clear text.
F. Failover key is not required for the secure communication over the failover link.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 107
Which two protocols are used by the management plane in a Cisco IOS device? (Choose two.)
A. NETFLOW
B. DHCP
C. 3DES
D. FTP
E. IKEv2
F. TLS
G. CHAP
H. NTP
I. PAP
Answer: (SHOW ANSWER)

NEW QUESTION: 108
Which three types of addresses can the Botnet Traffic Filter feature of the Cisco ASA monitor? (Choose three.)
A. known allowed addresses

B. dynamic addresses
C. internal addresses
D. ambiguous addresses
E. known malware addresses
F. listed addresses
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Addresses monitored by the Botnet Traffic Filter include:
- Known malware addresses-These addresses are on the blacklist identified by the dynamic database and the static blacklist.
- Known allowed addresses-These addresses are on the whitelist. The whitelist is useful when an address is blacklisted by the dynamic database and also identified by the static whitelist.
- Ambiguous addresses-These addresses are associated with multiple domain names, but not all of these domain names are on the blacklist. These addresses are on the greylist.
- Unlisted addresses-These addresses are unknown, and not included on any list.

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/special/botnet/guide/asa-botnet.html

NEW QUESTION: 109
Which statement about VRF-aware GDOI group members is true?
A. IPsec is used only to secure data traffic.
B. Registration traffic and rekey traffic must operate on different VRFs.
C. Multiple VRFs are used to separate control traffic and data traffic.
D. The GM cannot route control traffic through the same VRF as data traffic.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 110
Which two statements about MAB are true? (Choose two.)
A. MAC addresses stored in the MAB database can be spoofed.
B. It operates at Layer 2 and Layer 3 of the OSI protocol stack.
C. It can be used to authenticate network devices and users.
D. It serves at the primary authentication mechanism when deployed in conjunction with 802.1x.
E. It requires the administrator to create and maintain an accurate database of MAC addresses.
F. It is a strong authentication method.
Answer: A,B (LEAVE A REPLY)
Explanation/Reference:
Explanation:

Reference:http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html

NEW QUESTION: 111
Which feature does Cisco VSG use to redirect traffic in a Cisco Nexus 1000V Series Switch?
A. VPC
B. VDC
C. VEM
D. vPath
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 112
Which two statements about Cisco AnyConnect VPN Client are true (Choose two.)
A. It enables users to manage their own profiles.
B. By default, DTLS connections can fall back to TLS.
C. It can be configured to download automatically without prompting the user.
D. To improve security, keepalives are disabled by default.
E. it can use an SSL tunnel and a DTLS tunnel simultaneously.
Answer: B,E (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 113
Which three ISAKMP SA Message States can be output from the device that initiated an IPSec tunnel? (Choose three.)
A. MM_WAIT_MSG3
B. MM_WAIT_MSG2
C. MM_WAIT_MSG1
D. MM_WAIT_MSG4
E. MM_WAIT_MSG6
F. MM_WAIT_MSG5
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 114
Which statement about SenderBase reputation scoring on an ESA device is true?
A. You can configure a custom score threshold for whitelisting messages.
B. A high score indicates that a message is very likely to be spam.

C. Application traffic from known bad sites can be throttled or blocked.
D. By default, all messages with a score below zero are dropped or throttled.
E. Sender reputation scores can be assigned to domains, IP addresses, and MAC addresses.
F. Mail with scores in the medium range can be automatically routed for antimalware scanning.
Answer: (SHOW ANSWER)

NEW QUESTION: 115

```
Router(config)#cts sxp reconciliation period 180
```

Refer to the exhibit. Which two statements about a device with this configuration are true? (Choose two.)
A. When a peer re-establishes a previous connection to the device. CTS retains all existing SGT mapping entries for 3 minutes.
B. If a peer reconnects to the device within 120 seconds of terminating a CTS-SXP connection, the reconciliation timer starts.
C. If a peer re-establishes a connection to the device before the hold-down timer expires, the device retains the SGT mapping entries it learned during the previous connection for an additional 3 minutes.
D. It sets the internal hold-down timer of the device to 3 minutes.
E. When a peer establishes a new connection to the device, CTS retains all existing SGTmapping entries for 3 minutes.
F. If a peer reconnects to the device within 180 seconds of terminating a CTS-SXP connection, the reconciliation timer starts.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 116
Which two statements about the MACsec security protocol are true? (Choose two.)
A. MACsec is not supported in MDA mode.
B. Stations broadcast an MKA heartbeat that contains the key server priority.
C. When switch-to-switch link security is configured in manual mode, the SAP operation mode must be set to GCM.
D. MKA heartbeats are sent at a default interval of 3 seconds.
E. The SAK is secured by 128-bit AES-GCM by default.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 117
What are two of the valid IPv6 extension headers? (Choose two.)
A. Protocol

B. Options
C. Authentication Header
D. Next Header
E. Mobility
F. Hop Limit
Answer: C,E (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 118
From the list below, which one is the major benefit of AMP Threat GRID?
A. AMP Threat Grid analyzes suspicious behavior in your network against exactly 400 behavioral indicators.
B. AMP Threat Grid combines Static, and Dynamic Malware analysis with threat intelligence into one combined solution.
C. AMP Threat Grid learns ONLY from data you pass on your network and not from anything else to monitor for suspicious behavior. This makes the system much faster and efficient.
D. AMP Threat Grid collects file information from customer servers and run tests on them to see if they are infected with viruses.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 119
What does NX-API use as its transport?
A. FTP
B. HTTP/HTTPS
C. SCP
D. SFTP
E. SSH
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Which three of these are properties of RC4? (Choose three.)
A. It is used in AES.
B. It is an asymmetric cipher.
C. It is a stream cipher.
D. It is a symmetric cipher.
E. It is used in SSL.
F. It is a block cipher.
Answer: (SHOW ANSWER)

Explanation/Reference:
Explanation: