

Cisco.400-251.v2018-07-30.q107

Exam Code:	400-251
Exam Name:	CCIE Security Written Exam (v5.0)
Certification Provider:	Cisco
Free Question Number:	107
Version:	v2018-07-30
# of views:	1012
# of Questions views:	42256
https://www.freecram.net/torrent/Cisco.400-251.v2018-07-30.q107.html	

NEW QUESTION: 1

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: 2

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

- A. It allows a virtual machine to retain its MAC and IP addresses when it is moved to a different hypervisor on a different L3 network.
- B. The virtual machines reside on a single virtual network regardless of their physical location.
- C. NVGRE endpoints can reside within a virtual machine.
- D. The network switch handles the addition and removal of NVGRE encapsulation.
- E. It supports up to 32 million virtual segments per instance.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 3

Which two options are benefits of network summarization? (Choose two.)

- A. It can summarize discontinuous 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: C,D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 4

Various methods are available for load-balancing across WSA deployment. Which method requires the least effort for all types of endpoints (campus and data center) across the enterprise?

- A. Use WPAD that uses the IP addresses of the WSAs.
- B. Use transparent Layer 4 redirection with multiple WSAa behind a load-balancer.
- C. Host a PAC file on the WSA or an intranet web server and point all endpoints to it for auto-configuration.
- D. Configure an SRV DNS record to point to the WSA for all web services.
- E. Configure the WSA as an SXP speaker to push static SGT-To-IP bindings to a load-balancer for traffic prioritization.
- F. Push out proxy settings to endpoints through Windows GPO settings.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 5

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: 6

Which two statements about Cisco ASA authentication using LDAP are true? (Choose two.)

- A. The Cisco ASA can use more than one AD memberOf attribute to match a user to multiple group policies.
- B. It can assign a group policy to a user based on access credentials.
- C. It can combine AD attributes and LDAP attributes to configure group policies on the Cisco ASA.

- D. It uses attribute maps to map the AD memberOf attribute to the Cisco ASAGroup-Policy attribute.
- E. It is a closed standard that manages directory-information services over distributed networks.
- F. It uses AD attribute maps to assign user of group policies configured under the WebVPN context.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 7

In your network, you require all guests to authenticate to the network before getting access, however, you don't want to be stuck creating or approving accounts. It is preferred that this is all taken care of by the user, as long as their device is registered. Which two mechanisms can be used to provide this functionality? (Choose two.)

- A. Guest's own organization's authentication service, with device registration.
- B. 802.1x based guest user registration, with device registration.
- C. Active Directory, with device registration.
- D. PAP based authentication, with device registration.
- E. Social media login, with device registration.
- F. Self-registration of user, with device registration.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 8

Which of the following could be an evasion technique used by the attacker?

- A. ACL implementation to drop unwanted traffic.
- B. NAT translations on routers and switches.
- C. Traffic encryption to bypass IPS detection.
- D. TELNET to launch device administrative session.
- E. URL filtering to block malicious sites.
- F. Port access using Dot1x.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 9

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: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 10

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: 11

Which effect of the crypto key encrypt write rsa command on a router is true?

- A. The device saves the unlocked encrypted key to the NVRAM.
- B. The device encrypts and locks the key before authenticating it with an external CA server.
- C. The device locks the encrypted key, but the key is lost when the router is reloaded.
- D. The devices unlocks the encrypted key, but the key is lost when the router is reloaded.
- E. The device locks the encrypted key and saves it to the NVRAM.

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:

NEW QUESTION: 12

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: 13

View the Exhibit.

```
aaa new-model
aaa authentication username-prompt "Local Username:"
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
no aaa authorization config-commands
aaa authorization exec default group tacacs+ local if-
authenticated
aaa authorization commands 15 default group tacacs+ if-
authenticated
aaa authorization reverse-access default group tacacs+
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
```

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: 14

Refer to the exhibit.

```

R9:
crypto ikev2 keyring ccier10
peer r10
  address 20.1.4.11
  pre-shared-key local ccier10
  pre-shared-key remote ccier10
!
crypto ikev2 profile ccier10
match identity remote address 20.1.4.10 255.255.255.255
authentication local pre-share
authentication remote pre-share
keyring local ccier10
!
crypto ipsec profile ccier10
set ikev2-profile ccier10
!
interface Loopback1
ip address 192.168.9.9 255.255.255.0
!
interface Tunnel134
ip address 172.16.2.9 255.255.255.0
!
interface GigabitEthernet1
tunnel destination 20.1.4.10
tunnel protection ipsec profile ccier10
!
interface GigabitEthernet1
ip address 20.1.3.9 255.255.255.0
negotiation auto
!
router eigrp 34
network 172.16.2.0.0.0.0.255
network 192.168.9.0
!
router bgp 3
  bgp log neighbor changes
  network 20.1.3.0 mask 255.255.255.0
  neighbor 20.1.3.12 remote as 345
  neighbor 20.1.3.12 password cisco

```

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 IPSec profile configuration.
- B. Incorrect tunnel source for the tunnel interface.
- C. Incorrect local network address in BGP routing process.
- D. Incorrect IKEv2 profile configuration.
- E. Incorrect tunnel network address in EIGRP routing process.
- F. Incorrect keyring configuration.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 15

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: 16

Which of these command sequences will send an email to holly@invalid.com using SMTP?

- A. MAIL FROM: <david@invalid.com>RCPT TO: <holly@invalid.com>MESSAGE
- B. MAIL FROM: <david@invalid.com>RCPT TO: <holly@invalid.com>DATA
- C. HELO invalid.comMAIL FROM: <david@invalid.com>RCPT TO: <holly@invalid.com>BODY
- D. HELO invalid.comMAIL TO: <holly@invalid.com>MESSAGEEND

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

Valid 400-251 Dumps shared by ExamDiscuss.com for Helping Passing 400-251 Exam!
ExamDiscuss.com now offer the **newest 400-251 exam dumps**, the ExamDiscuss.com 400-251 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 400-251 dumps with Test Engine here:
<https://www.examdiscuss.com/Cisco/exam/400-251/premium/> (125 Q&As Dumps, **35%OFF Special**
Discount Code: freecram)

NEW QUESTION: 17

Which two statements about a wireless access point configured with the guest-mode command are true?
(Choose two.)

- A. If one device on a network is configured is guest mode, clients can use the guest mode SSID to connect to any device on the same network.
- B. It supports associations by clients that perform passive scans.
- C. It allows associated clients to transmit packets using its SSID.
- D. It can support more than one guest-mode SSID.
- E. It allows clients configured without SSID to associate.

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. Enable Change of Authorization (CoA) on ISE.
- C. Enable Period Compliance Checking (PCC) on ISE.
- D. Enable Change of Authorization (CoA) on MDM.
- E. The MDM agent periodically sends a packet with compliance info that the Wireless Controller can be used to limit network access.
- F. The MDM agent will automatically disconnect the device from the network when it is non-compliant.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 19

Which three authorization technologies does Cisco TrustSec support? (Choose three.)

- A. SGT
- B. SGACL
- C. MAB
- D. 802.1x
- E. DACL
- F. VLAN

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 20

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 as 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: ([SHOW ANSWER](#))

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: 21

Which two statements about SPAN sessions are true? (Choose two.)

- A. A single switch stack can support up to 32 source and RSPAN destination sessions.
- B. They can monitor sent and received packets in the same session.
- C. Multiple SPAN sessions can use the same destination port.
- D. Source ports and source VLANs can be mixed in the same session.
- E. They can be configured on ports in the disabled state before enabling the port.
- F. Local SPAN and RSPAN can be mixed in the same session.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 22

Which two statements about MPP (Management Plane Protection) are true? (Choose two.)

- A. It is supported on both distributed and hardware-switched platforms.
- B. Only virtual interfaces associated with physical interfaces are supported.
- C. It is supported on both active and standby management interfaces.
- D. Only in-band management interfaces are supported.
- E. Only virtual interfaces associated with sub-interfaces are supported.
- F. Only out-of-band management interfaces are supported.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 23

How would you best describe Jenkins?

- A. Operates in a client/server model
- B. Web-based repository hosting service
- C. Continuous integration and delivery application
- D. A REST client
- E. An orchestration tool

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 24

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: 25

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: 26

Which of the following is true regarding failover link when ASAs are configured in the failover mode?

- A. Only the configuration replication sent across the link can be secured using a failover key.
- B. It is not recommended to use secure communication over failover link when ASA terminating the VPN tunnel.
- C. The information sent over the failover link can only be in clear text.
- D. Failover key is not required for the secure communication over the failover link.
- E. The information sent over the failover link can be sent in clear text or it could be secured communication using a failover key.
- F. The information sent over the failover link can only be sent as a secured communication.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 27

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: 28

```
ASA(config)# dynamic-filter updater-client enable
ASA(config)# changeto context context1
ASA/context1(config)# dynamic-filter use-database
ASA/context1(config)# changeto context context2
ASA/context2(config)# dynamic-filter use-database
```

Refer to the exhibit. What are two effects of the given configuration? (Choose two.)

- A. It enables botnet filtering in multiple context mode.
- B. It enables botnet filtering in single context mode.
- C. It enables the ASA to download the static botnet filter database.
- D. It enables multiple context mode.
- E. It enables single context mode.
- F. It enables the ASA to download the dynamic botnet filter database.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 29

What is the purpose of the BGP TTL security check?

- A. to protect against routing table corruption
- B. to authenticate a peer
- C. to protect against CPU utilization-based attacks
- D. to check for a TTL value in packet header of less than or equal to for successful peering
- E. to use for iBGP session

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 30

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: 31

Which connection mechanism does the eSTREAMER service use to communicate?

- A. SSH
- B. IPsec tunnels with 3DES encryption only
- C. TCP over SSL only
- D. EAP-TLS tunnels
- E. TCP with optional SSL encryption
- F. IPsec tunnels with 3DES or AES encryption

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

Valid 400-251 Dumps shared by ExamDiscuss.com for Helping Passing 400-251 Exam!
ExamDiscuss.com now offer the **newest 400-251 exam dumps**, the ExamDiscuss.com 400-251 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 400-251 dumps with Test Engine here:
<https://www.examdumps.com/Cisco/exam/400-251/premium/> (125 Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 32

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: 33

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: 34

Which statement is true regarding securing connection using MACSec?

- A. ISAKMP protocol is used to manage MACSec encryption keys.
- B. Switch configured for MACSec can only accept MACSec frames from the MACSec client.
- C. It provides network layer encryption on a wireless network.
- D. It is implemented after a successful MAB authentication of a supplicant.
- E. Switch uses session keys to calculate decrypted packet ICV value for the frame integrity check.
- F. It secures connection between two supplicant clients.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 35

Which statement is true regarding Private VLAN?

- A. In a private VLAN domain a secondary VLAN can have only one promiscuous port.
- B. Each secondary VLAN in a private VLAN domain needs to have a separate associated primary VLAN.
- C. Each port in a private VLAN domain is a member of all the secondary VLANs in that domain.
- D. A subdomain in a primary VLAN domain consists of a primary and secondary VLAN pair.
- E. A private VLAN domain can have multiple primary VLAN.
- F. In a private VLAN domain a secondary VLAN port needs to be an isolated port for it to be able to communicate with a layer 3-device.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 36

Refer to the exhibit.

```

ASA1:
ROUTER OSPF 12
NETWORK 10.1.11.0 255.255.255 0 area 1
area 1 authentication message-digest

interface GigabitEthernet0/1
nameif inside
security level 100
ip address 10.1.11.1 255.255.255 0 standby 10.1.11.2
ospf message-digest-key 12 md5 cisco

R2
router ospf 12
area 0 authentication message-digest
area 1 authentication message-digest
network 10.1.11.0.0.0.0 255 area 1
network 10.1.12.0.0.0.0 255 area 0
network 172.16.100.0.0.0.0 255 area 0
!
interface GigabitEthernet2
ip address 10.21.11.22 255.255.255.0
ip ospf message-digest-key 21 md2 cisco

```

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 ASA1 standby interface need to be disabled on Gi0/1 interface.
- C. The R2 has mismatched message-digest key id.
- D. On R2 Incorrect subnet defined for the Gi2 interface.
- E. On ASA1 Gi0/1 interface should have security level at "0".
- F. On R2 10.1.11.0/24 subnet should be in area "0" in OSPF routing process.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 37

Which of the following is part of DevOps Virtuous Cycle?

- A. Slower Releases
- B. Increased Latency
- C. Lower Quality
- D. Improved Scalability

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

NEW QUESTION: 38

If an ASA device is configured as a remote access IPsec server with RADIUS authentication and password management enabled which type of authentication will it use?

- A. MS-CHAPv1
- B. NTLM
- C. PAP
- D. RSA
- E. MS-CHAPv2

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 39

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 multicasting
- 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#pgfld-1099362

NEW QUESTION: 40

View the Exhibit.

%ASA-6-110001: No route to <dest_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: 41

Which statement describes a pure SDN framework environment?

- A. The data plane is controlled by a centralized SDN element.

- B. The data plane is pulled from the networking element and put a SDN controller.
- C. The control plane and data plane is pulled from the networking element and put in a SDN controller and SDN agent.
- D. The control plane is pulled from the networking element and put a SDN controller.
- E. the control plane functions is split between a SDN controller and the networking element.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 42

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: 43

The SAML Single Sign-On on ISE is supported by which four portals? (Choose Three.)

- A. Contractor Portal
- B. Certificate Provisioning Portal
- C. BYOD Portal
- D. Sponsor Portal
- E. My Devices Portal
- F. Guest Portal (sponsored and self-registered)
- G. Wireless Client Portal
- H. Employee Portal

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 44

Which statement is an advantage of network segmentation?

- A. It improves network performance by having broadcast traffic not limited to local subnets.
- B. It takes less time to design a complex network with segmentation as one of the critical requirements.
- C. It enables efficient network monitoring due to a flat network.

- D. It allows flat network design for better security implementation.
- E. It allows efficient containment of a security incident as the effect will be limited to a local subnet.
- F. It allows users to access the resource even though they won't need to for better visibility.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 45

Which statement about deploying policies with the Firepower Management Center is true?

- A. The global domain can deploy changes to individual subdomains.
- B. The leaf domain can deploy changes to all subdomains simultaneously.
- C. Deploy tasks can be scheduled to deploy policies automatically.
- D. All policies are deployed on-demand when the administrator triggers them.
- E. Policies are deployed automatically when the administrator saves them.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 46

Which statement is true about Remote Triggered Black Hole Filtering feature (RTBH)?

- A. It drops malicious traffic at the customer edge router by forwarding it to a Null0 interface.
- B. In RTBH filtering the trigger device redistributes static route to the iBGP peers.
- C. It works in conjunction with QoS to drop the traffic that has a less priority.
- D. It helps mitigate DDoS attack based only on source address.
- E. The Null0 interface used for filtering able to receive the traffic but never forwards it.
- F. In RTBH filtering the trigger device is always an ISP edge router.

Answer: F ([LEAVE A REPLY](#))

Valid 400-251 Dumps shared by ExamDiscuss.com for Helping Passing 400-251 Exam!

ExamDiscuss.com now offer the **newest 400-251 exam dumps**, the ExamDiscuss.com 400-251 exam **questions have been updated** and **answers have been corrected** get the **newest**

ExamDiscuss.com 400-251 dumps with Test Engine here:

<https://www.examdiscuss.com/Cisco/exam/400-251/premium/> (125 Q&As Dumps, **35%OFF Special**

Discount Code: freecram)

NEW QUESTION: 47

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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 48

What are the major components of a Firepower health monitor alert?

- A. A health monitor, one or more alert responses, and a remediation policy.
- B. One or more health modules, one or more alert responses, and one or more alert actions.
- C. The severity level, one or more alert responses, and a remediation policy.
- D. One or more health modules, the severity level, and an alert response.
- E. One health module and one or more alert responses.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 49

```

Router#show policy-map interface f0/0
FastEthernet0/0
Service-policy output: sql
  Class-map: sqlnettraffic (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: protocol sqlnet
    QoS Set:
      precedence 5
      Packets marked 0
  Class-map: class-default (match-any)
    2 packets, 409 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any

```

Refer to the exhibit. What feature must be implemented on the network to produce the given output?

- A. NBAR
- B. CAR
- C. WFQ
- D. PQ
- E. CQ

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 50

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

- A. CRL retrieval is supported through Certificate Distribution Point queries.
- B. The certificate request format uses PKCS#10.

- C. It supports synchronous granting.
- D. It supports multiple cryptographic algorithms, including RSA.
- E. It supports online certification revocation.
- F. Cryptographically signed and encrypted messages are conveyed using PKCS#7.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 51

Exhibit

```

R15
crypto pki trustpoint ccier15
enrollment url http://172.16.100.17.8080
serial-number
ip-address 172.16.100.15
subject-name CN-r15 O-cisco.com
revocation-check none
source interface Loopback0
rskeypair ccier15
!
crypto isakmp policy 1516
encr aes
hash md5
group 2
!
crypto ipsec transform-set ts1516 esp-aes esp-she-hmac
mode tunnel
!
crypto map r1516 1516 ipsec-isakmp
set peer 20.1.7.16
set transform-set ts1516
match address 120
!
interface Loopback0
ip address 192.168.15.15.255.255.255.0
!
interface GigabitEthernet1
ip address 20.1.6.15.255.255.255.0
negotiation auto
crypto map r1516
!
router bgp 6
bgp log-neighbor-changes
network 172.16.100.15 msec 255.255.155.255
neighbor 10 16 18 remote-es 678
neighbor 20 16 18 password cisco
!
ip route 192.168.16.0.255.255.255.0.20.17.16
access-list 120 permit ip 192 168 15.0.0.0.255.192.168.16.0.0.0.255
!
ntp authentication-key 12 mds ccie
ntp authenticate
ntp trusted-key 12
ntp server 150 17 231 key 12
! ip domain name cisco.com

```



Refer to the exhibit. R15 is trying to initiate Site-To-Site IPsec certificate based VPN tunnel with the peer at 20.1.7.16. The CA is running at port 80 on address 172.16.100.18. R15 has a BGP peer 20.1.6.18 doing an authenticated session to establish reachability with the VPN remote site. The VPN tunnel will secure traffic between 192.168.15.0/24 and 192.168.16.0/24 networks. It has been reported that VPN tunnel is not coming up with the remote site, what could be the issue?

- A. The crypto map is not applied on the correct interface.
- B. Incorrect BGP peer configuration.
- C. Incorrect crypto map configuration.
- D. Incorrect ACL defined for the traffic encryption.
- E. Incorrect ISAKMP policy configuration.
- F. Incorrect trustpoint configuration.
- G. Incorrect static route.
- H. Incorrect transform set configuration.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 52

Which three ESMTTP 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: 53

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: 54

Which two commands would enable secure logging on a Cisco ASA to a syslog server at 10.0.0.1? (Choose two.)

- A. logging host inside 10.0.0.1 TCP/1470 secure
- B. logging host inside 10.0.0.1UDP/447 secure
- C. logging host inside 10.0.0.1 UDP /500 secure

- D. logging host inside 10.0.0.1 UDP /514 secure
- E. logging host inside 10.0.0.1 TCP/1500 secure

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 55

What is the best description of a docker file?

- A. Software used to manage containers
- B. Text document used to build an image
- C. Message Daemon files
- D. Repository for a docker images

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 56

```
R1(config)#parameter-map type inspect param-map
R1(config-profile)#sessions maximum 10000
R1(config-profile)#ipv6 routing-header-enforcement loose
R1(config-profile)#
R1(config-profile)#class-map type inspect match-any class
R1(config-cmap)#match protocol tcp
R1(config-cmap)#match protocol udp
R1(config-cmap)#match protocol icmp
R1(config-cmap)#match protocol ftp
R1(config-cmap)#
R1(config-cmap)#policy-map type inspect policy
R1(config-pmap)#class type inspect class
R1(config-pmap-c)#inspect param-map
R1(config-pmap-c)#
R1(config-pmap-c)#zone security z1
R1(config-sec-zone)#zone security z2
R1(config-sec-zone)#
R1(config-sec-zone)#zone-pair security zp source z1 destination z2
R1(config-sec-zone-pair)#service-policy type inspect policy
```

Refer to the exhibit. Which two statements about the given IPv6 ZBF configuration are true? (Choose two.)

- A. It inspects TCP, UDP, ICMP, and FTP traffic from z1 to z2.
- B. It passes TCP, UDP, ICMP, and FTP traffic from z1 to z2.
- C. It inspects TCP, UDP, ICMP, and FTP traffic from z2 to z1.
- D. It passes TCP, UDP, ICMP, and FTP traffic in both directions between z1 and z2.
- E. It provides backward compatibility with legacy IPv4 inspection.
- F. It provides backward compatibility with legacy IPv6 inspection.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 57

Your organization is deploying an ESA for email security for inbound and outbound email. To receive inbound emails from external organizations, you must set up your DNS servers with the appropriate records so that the sending email server can determine which email gateway to send to. Assume that you have two ESAs deployed and the hostnames and IP addresses are as follows:

esa1.myesa.com: 5.5.5.25 (Preferred)

esa2.myesa.com: 5.5.5.26

Which two commands must you include in your DNS server to receive email from all external senders? (Choose two.)

A:

Forward Lookup Zone:

@ 3600 IN A 10 esa1.myesa.com.

@ 3600 IN A 20 esa2.myesa.com.

B:

Reverse Lookup Zone for 5.5.5.:

25 3600 IN PTR esa1.myesa.com.

26 3600 IN PTR esa2.myesa.com.

C:

Forward Lookup Zone:

esa1 IN 3600 A 5.5.5.25

esa2 IN 3600 A 5.5.5.26

D:

Forward Lookup Zone:

esa1 IN 3600 A 5.5.5.26

esa2 IN 3600 A 5.5.5.25

E:

Forward Lookup Zone:

mail1.myesa.com 120 CNAME esa1.myesa.com

mail2.myesa.com 120 CNAME esa2.myesa.com

F:

Forward Lookup Zone:

@ 3600 IN MX 10 mail1.myesa.com.

@ 3600 IN MX 20 mail1.myesa.com.

A. Option E

B. Option B

C. Option D

D. Option C

E. Option F

F. Option A

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 58

Which statement is true about Social Engineering attack?

- A. It is a method of extracting a non-confidential information.
- B. It can be only done by a person who is not part of the organization.
- C. It is always done by having malicious ads on untrusted websites for the users to browse.
- D. It is always performed through an email from a person that you know.
- E. The "Phishing" technique is one of the ways to launch the attack.
- F. It uses the reconnaissance method for exploitation.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 59

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: 60

Refer to the exhibit.

```
aaa new-model
aaa authentication login default group radius
aaa authentication login NO_AUTH none
aaa authentication login vty local
aaa authentication dot1x default group radius
aaa accounting network default start-stop group radius
!
username cisco privilege 15 password o cisco
!
interface GigabitEthernet0/2
switchport mode access
ip access-group Pre-Auth in
authentication host-mode multi-auth
authentication open
authentication port-control auto
dot1x pae authenticator
!
vlan50
interface Vlan50
ip address 50.1.1.1 255.255.255.0
!
ip dhcp excluded-address 50.1.1.1
ip dhcp pool pc-pool
network 50.1.10 255.255.255.0
default-router 50.1.1.1
!
ip access-list extended Pre-Auth
permit udp any eq bootpc any eq bootps
deny ip any any
!
radius server ccie
address ipv4 161.1.7.12 auth-port 1645 acct-port 1646
key cisco
!
line con 0
login authentication NO-AUTH
line vty 04
login authentication vty
```

One of the Windows machines in your network is having connectivity issues using 802.1X. Windows machines are setup to acquire an IP address from the DHCP server configured on the switch, which is supposed to hand over IP addresses from the 50.1.1.0/24 network, and forward AAA requests to the RADIUS server at 161.1.7.14 using shared key "cisco". Knowing that interface Gi0/2 on the switch may receive authentication requests from other devices and looking at the provided switch configuration, what could be the possible cause of failure?

A. aaa network authorization is not configured.

- B. There is a RADIUS key mismatch.
- C. an incorrect default route is pushed on the supplicant from SW1
- D. 801.1X authentication is not configured.
- E. an incorrect ip address is configured for SVI 50
- F. authentication for multiple hosts is not configured on interface Gi0/2
- G. 802.1X is disabled is on the switch

Answer: (SHOW ANSWER)

NEW QUESTION: 61

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

- A. Traffic to remediation servers, if needed.
- B. DNS Traffic.
- C. Traffic from AnyConnect client, with posture module, to ASA.
- D. DHCP Traffic.
- E. Traffic to FireAMP cloud for AMP for endpoint scan results.
- F. Traffic to public search engines.
- G. Traffic to ISE PSNs to which Client Provisioning Portal FQDN points.
- H. SSH traffic for network device administration.

Answer: (SHOW ANSWER)

Valid 400-251 Dumps shared by ExamDiscuss.com for Helping Passing 400-251 Exam!
ExamDiscuss.com now offer the **newest 400-251 exam dumps**, the ExamDiscuss.com 400-251 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 400-251 dumps with Test Engine here:
<https://www.examdiscuss.com/Cisco/exam/400-251/premium/> (125 Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 62

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: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

NEW QUESTION: 63

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

Answer: (SHOW ANSWER)

NEW QUESTION: 64

Which statement currently describes Botnet attack?

- A. It is a form of a fragmentation attack to evade an intrusion prevention security device.
- B. It is a form of a man-in-the-middle attack where the compromised machine is controlled remotely.
- C. It is a form a wireless attack where attacker installs an access point to create backdoor to a network.
- D. It is a launched by a single machine controlled by Command and Control system.
- E. It is launched by a collection of machines to execute DDoS against the attacker.

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 65

Which statement is true regarding the wireless security technologies?

- A. WPA2 is more secure than WPA because it uses TKIP for encryption.
- B. WPA2-PSK mode allows passphrase to store locally on the device.
- C. WEP is more secure than WPA2 because it uses AES for encryption.
- D. WPA provides message integrity using AES.
- E. WPA2-ENT mode does not require RADIUS for authentication.
- F. WPA2-PSK mode provides better security by having same passphrase across the network.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 66

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: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 67

Which of the following is the correct statement regarding enabling SMTP encryption on ESA?

- A. Enabling TLS is an optional step.
- B. It only allows to import certificate from CA.
- C. It only allows to use the self signed certificates.
- D. TLS can be enabled only for receiving.
- E. Enabling TLS for delivery goes under the "Destination Controls" menu of mail policies.
- F. TLS can be enabled only for delivery.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 68

View the Exhibit.

```
<featureCheck>
  <deviceResponse>
    <feature>
      name="json"
      support="yes"
    </feature>
  </deviceResponse>
</featureCheck>
```



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: 69

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: 70

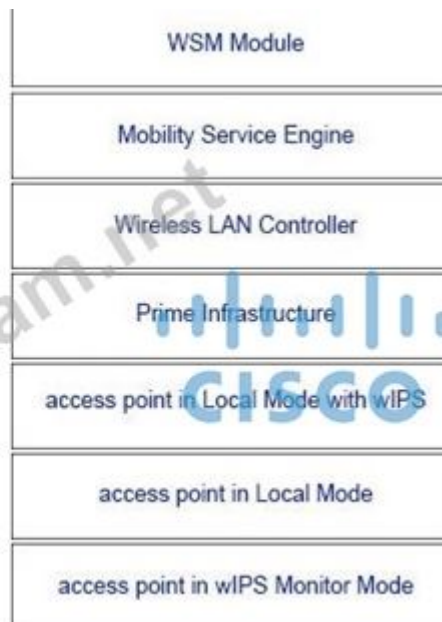
DRAG DROP

Drag each component of an Adaptive Wireless IPS deployment on the left to the matching description on the right.

Select and Place:

access point in Local Mode	A separate component that provides attack detection without supporting clients
access point in Local Mode with wIPS	Aggregates and stores alarms from controllers and access points.
access point in wIPS Monitor Mode	Forwards configurations and information about attacks to and from access points.
Mobility Service Engine	Provides administrative functionality for configuring wIPS, pushing configurations, and viewing alarms.
Prime Infrastructure	Supports enhanced detection of attacks by scanning radio channels for extended periods.
Wireless LAN Controller	Supports limited scanning for attackers while providing wireless service.
WSM Module	Supports packet-capture functions for forensic examination.

Answer:



NEW QUESTION: 71

Which three statements about the keying methods used by MACSec are true? (Choose three.)

- A. SAP is enabled by default for Cisco TrustSec in manual configuration mode.
- B. Key management for host-to-switch and switch-to-switch MACSec sessions is provided by MKA.
- C. A valid mode for SAP is NULL.
- D. SAP is not supported on switch SVIs.
- E. SAP is supported on SPAN destination ports.
- F. MKA is implemented as an EAPoL packet exchange.

Answer: C,D,F (LEAVE A REPLY)

Explanation/Reference:

Explanation:

NEW QUESTION: 72

In your ISE design, there are two TACACS profiles that are created for device administration: IOS_HelpDesk_Profile, and IOS_Admin_Profile. The HelpDesk profile should login the user with privilege 1, with ability to change privilege level to 15. The Admin profile should login the user with privilege 15 by default. Which two commands must the HelpDesk user enter on the IOS device to access privilege level 15? (Choose two.)

- A. enable privilege 15
- B. enable
- C. privilege level 15
- D. enable IOS_Admin_Profile
- E. enable password
- F. enable 15
- G. enable secret

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 73

Which statement is true regarding TLS security protocol?

- A. There is no difference between TLS and SSL versions 2 and 3.
- B. You need to replace SSL certificate with TLS certificate for successful TLS operation.
- C. TLS version 1.0 is more secure than SSL version 3.0
- D. It is always recommended to disable TLS version 1.0 in the browser so that it only supports SSL for better security.
- E. It only supports data authentication for the client-server session using a browser.
- F. TLS and SSL versions can interoperate in the client-server handshake.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 74

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. 5
- C. 2
- D. 4
- E. 1
- F. 0

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 75

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: 76

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: (SHOW ANSWER)

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

Valid 400-251 Dumps shared by ExamDiscuss.com for Helping Passing 400-251 Exam!
ExamDiscuss.com now offer the **newest 400-251 exam dumps**, the ExamDiscuss.com 400-251 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 400-251 dumps with Test Engine here:
<https://www.examdiscuss.com/Cisco/exam/400-251/premium/> (125 Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 77

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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 78

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: 79

Which statement correctly describes 3DES encryption algorithm?

- A. It is a block cipher algorithm but weaker than DES due to smaller key size.
- B. It is an asymmetric algorithm with a key size of 168 bits.
- C. It is a block cipher algorithm with a key size of 56 bits.
- D. It uses a set of three keys for encryption and a different set of three keys for decryption.
- E. It does decryption in reverse order with the same set of keys used during encryption.
- F. It is a stream cipher algorithm with a key size of 168 bits.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 80

View the Exhibit.

```
enable password cisco213
aaa-server TACACS+ protocol tacacs+
  reactivation-mode depletion deadline 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: 81

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 EAP-FAST
- B. Use PAP-CHAP-MSCHAP
- C. Use PEAP-EAP-TLS
- D. Use EAP-MSCHAPv2
- E. Use EAP-TLS or EAP-TTLS
- F. Use PEAP-EAP-MSCHAPv2

Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 82

```
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: 83

In a Cisco ASA multiple-context mode of operation configuration, what three session types are resource-limited by default when their context is a member of the default class? (Choose three.)

- A. ASDM sessions
- B. Telnet sessions
- C. IPSec sessions
- D. TCP sessions
- E. SSH sessions
- F. SSL VPN sessions

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 84

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-policy 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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 85

Which statement is true regarding x.509 certificate?

- A. The serial number in the certificate is common across the certificates issued by the same CA.
- B. The issuer distinguished name in the certificate is of the entity to which the certificate is issued.
- C. The version number in the certificate is the OS version of CA.
- D. The algorithm in the certificate used by the subject to encrypt the traffic.
- E. The algorithm in the certificate used by the issuer to sign the certificate.
- F. The Subject distinguished name in the certificate is of the entity who issued the certificate.

Answer: (SHOW ANSWER)

NEW QUESTION: 86

Which statement about the Cisco AMP Virtual Private Cloud Appliance is true for deployments in air-gap mode?

- A. The appliance can perform disposition lookup against either the Protect DB or the AMP public cloud.
- B. The appliance evaluates files against the threat intelligence and disposition information residing on the Update Host.
- C. The Upgrade Host automatically downloads updates and deploys them to the Protect DB on a daily basis.
- D. The appliance can perform disposition lookups against the Protect DB without an Internet connection.
- E. The amp-sync tool syncs the threat-intelligence repository on the appliance directly with the AMP public cloud.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 87

In a large organization, with thousands of employees scattered across the globe, it is difficult to provision and onboard new employee devices with the correct profiles and certificates. With ISE, it is possible to do client provisioning provided which four conditions are met. (Choose four.)

- A. Microsoft Windows Server is configured with Certificate Services
- B. Device MAC Addresses are added to the Endpoint Identity Group
- C. Endpoint Operating System should be supported
- D. The pxGrid controller should be enabled on ISE.
- E. SCEP Proxy enabled on ISE
- F. Network access devices and ISE should have the PAC provisioning for CTS environment authentication.
- G. ISE should be configured as SXP listener to push SGT-To-Ip mapping to network access devices.
- H. Profiting is enabled on ISE
- I. Client Provisioning is enabled on ISE

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 88

Which statement regarding the routing functions of the Cisco ASA is true running software version 9.2?

- A. The ASA supports policy-based routing with route maps.
- B. In a failover pair of ASAs, the standby firewall establishes a peer relationship with OSPF neighbors.
- C. The translation table cannot override the routing table for new connections.
- D. Routes to the Null0 interface cannot be configured to black-hole traffic.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 89

A device on your internal network is hard-coded with two DNS servers on the Internet (1.1.1.53, 2.2.2.53). However, you want to send all requests to your OpenDNS server (208.67.222.222). Which set of commands do you run on the ASA to achieve this goal?

A:

```
static (inside, outside) source any destination 208.67.222.222 eq domain
```

B:

```
static (inside, outside) source any 1.1.1.53 destination 208.67.222.222 eq domain  
static (inside, outside) source any 2.2.2.53 destination 208.67.222.222 eq domain
```

C:

```

object network OpenDNS
host 208.67.222.222
!
object network Rogue1-DNS
host 1.1.1.53
object network Rogue2-DNS
host 2.2.2.53
!
object-group network Rogue-DNS
network-object object Rogue1-DNS
network-object Rogue2-DNS
!
object service udp-DNS
service udp destination eq domain
!
object service tcp-DNS
service tcp destination eq domain
!
nat (inside, outside) source static any interface destination static OpenDNS
Rogue-DNS service udp-DNS udp-DNS
nat (inside, outside) source static any interface destination static OpenDNS
Rogue-DNS service tcp-DNS tcp-DNS

```

D:

```

nat (outside, inside) source 1.1.1.53 destination 208.67.222.222 eq.domain
nat (outside, inside) source 2.2.2.53 destination 208.67.222.222 eq.domain

```

E:

```

static (outside, inside) source any 208.67.222.222 destination 1.1.1.53 eq domain
static (outside, inside) source any 208.67.222.222 destination 2.2.2.53 eq domain

```

F:

```

nat (inside, outside) source any 1.1.1.53 destination 208.67.222.222 eq domain
nat (inside, outside) source any 2.2.2.53 destination 208.67.222.222 eq domain

```

G:

```

object network OpenDNS
host 208.67.222.222
!
object network Rogue1-DNS
host 1.1.1.53
object network Rogue2-DNS
host 2.2.2.53
!
object-group network Rogue-DNS
network-object object Rogue1-DNS
network-object object Rogue2-DNS
!
object service udp-DNS
service udp destination eq domain
!
object service tcp-DNS
service tcp destination eq domain
!
nat (inside, outside) source static any interface destination static Rogue-
DNS OpenDNS service udp-DNS udp-DNS
nat (inside, outside) source static any interface destination static Rogue-
DNS OpenDNS service tcp-DNS tcp-DNS

```

H:

```

static (inside, outside) source any 208.67.222.222 destination 1.1.1.53 eq domain
static (inside, outside) source any 208.67.222.222 destination 2.2.2.53 eq domain

```

- A. Option F
- B. Option C
- C. Option D
- D. Option A
- E. Option B
- F. Option E
- G. Option H
- H. Option G

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 90

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: 91

Which statement about managing Cisco ISE Guest Services is true?

- A. Only a Super Admin or System Admin can delete the default Sponsor portal.
- B. ISE administrators can view and set a guest's password to a custom value in the Sponsor portal.
- C. ISE administrators can access the Sponsor portal only if they have valid Sponsor accounts.
- D. By default, and ISE administrator can manage only the guest accounts he or she created in the Sponsor portal.
- E. Only ISE administrators from an external identity store can be members of a Sponsor group.
- F. ISE administrators can access the Sponsor portal only from the Guest Access menu.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

Valid 400-251 Dumps shared by ExamDiscuss.com for Helping Passing 400-251 Exam!
ExamDiscuss.com now offer the **newest 400-251 exam dumps**, the ExamDiscuss.com 400-251 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 400-251 dumps with Test Engine here:
<https://www.examdiscuss.com/Cisco/exam/400-251/premium/> (125 Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 92

What are the advantages of using LDAP over AD?

- A. LDAP can be configured to use a primary and secondary server, whereas AD cannot.
- B. The closest LDAP servers are used for authentication.
- C. LDAP does not require ISE to join the AD domain.
- D. LDAP provides for faster authentication.
- E. LDAP allows for granular policy control, whereas AD does not.

Answer: (SHOW ANSWER)

NEW QUESTION: 93

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: 94

DRAG DROP

Drag the components of WIPS architecture on the left to their respective functionalities on the right.

Select and Place:

Access Points	Scans channels data-sen
Wireless Security Module	Performs the correla
WLC	Provides view
MSE	Applies rouge policy
Cisco Prime Infrastructure	Detects over-th anomalies

Answer:

	MS
	Cisco Prime
	Wireless Se
	Acces
	WLC

NEW QUESTION: 95

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

- A. EVPN routes can advertise VLAN membership and verify the reachability of Ethernet segments.
- B. EVPN route exchange enables PEs to discover one another and elect a DF.
- C. It is a next-generation Ethernet L3VPN solution that simplifies control-plane operations and enhances scalability.
- D. EVPN routes can advertise backbone MAC reachability.
- E. EVIs allow you to map traffic on one or more VLANs or ports to a Bridge Domain.
- F. It is a next-generation Ethernet L2VPN solution that supports load balancing at the individual flow level and provides advanced access redundancy.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 96

Which two statements about 6to4 tunneling are true? (Choose two.)

- A. It provides a /48 address block.
- B. The prefix address of the tunnel is determined by the IPv6 configuration of the interface.
- C. It supports static and BGPv4 routing.
- D. It supports managed NAT along the path of the tunnel.
- E. It provides a /128 address block.
- F. It supports multihoming.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 97

Which statement about SenderBase reputation scoring on an ESA device is true?

- A. A high score indicates that a message is very likely to be spam.
- B. By default, all messages with a score below zero are dropped or throttled.
- C. You can configure a custom score threshold for whitelisting messages.
- D. Application traffic from known bad sites can be throttled or blocked.
- E. Mail with scores in the medium range can be automatically routed for antimalware scanning.
- F. Sender reputation scores can be assigned to domains, IP addresses, and MAC addresses.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 98

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: 99

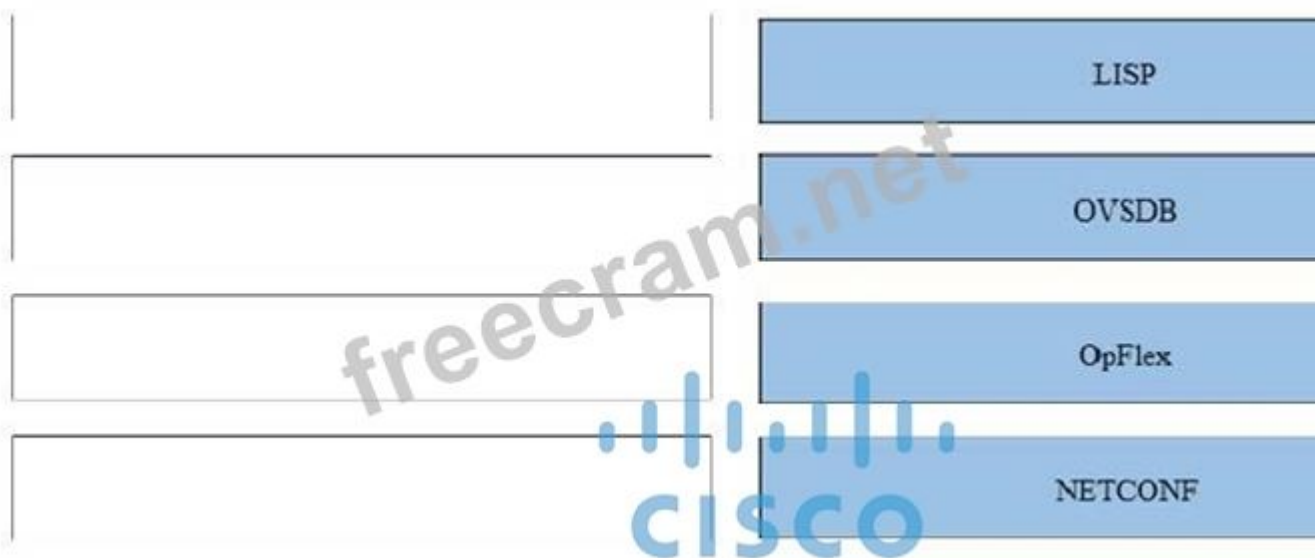
DRAG DROP

Drag and drop the protocols on the left onto their descriptions on the right.

Select and Place:

LISP	provides a framework used for overlay network
OpFlex	allows programmatic access to an Open vSwitch
OVSDB	used to implement a distributed control system declarative policy model
NETCONF	a standard for installing, manipulating, and configuration of network devices

Answer:



NEW QUESTION: 100

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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 101

Which are two important guidelines to follow when implementing VTP? (Choose two.)

- A. Enabling VTP pruning on a server will enable the feature for the entire management domain.
- B. When using secure mode VTP, only configure management domain passwords on VTP servers.
- C. All switches in the VTP domain must run the same version of VTP.
- D. Use of the VTP multi-domain feature should be restricted to migration and temporary implementation.
- E. CDP must be enabled on all switches in the VTP management domain.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 102

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: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 103

Which statement is correct regarding Cisco VSG functionality?

- A. It does not provide trusted access to VMs in an enterprise data center.
- B. It allows third-party orchestration tool to interact with XML APIs for its provisioning.
- C. It allows administrative segregation due to which Security administrator can author and manage port profiles.
- D. It does not allow to extend Zone-Based firewall capabilities to VMs on VXLAN.
- E. It applies security profile only after VM instantiation.
- F. It allows Active-Active failover operation mode when deployed as HA pair.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 104

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

- A. Clients can be authenticated with an LDAP bind or by fetching a passphrase as an attribute.
- B. It enables users at remote sites to retrieve their email messages via a secure client.
- C. It enables users at remote sites to release email messages from spam quarantine.
- D. When SMTP authentication with forwarding is performed by a second SMTP server, the second server also performs the transfer of queued messages.
- E. 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.
- F. The LDAP servers used by an ESA must share a single SMTP authentication profile.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 105

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

- A. RPC
- B. Proprietary protocol over TCP/8302
- C. EAP
- D. SXP
- E. RADIUS
- F. pxGrid

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 106

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:

Valid 400-251 Dumps shared by ExamDiscuss.com for Helping Passing 400-251 Exam!
ExamDiscuss.com now offer the **newest 400-251 exam dumps**, the ExamDiscuss.com 400-251 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 400-251 dumps with Test Engine here:
<https://www.examdiscuss.com/Cisco/exam/400-251/premium/> (125 Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 107

When applying MD5 route authentication on routers running RIP or EIGRP, which two important key chain considerations should be accounted for? (Choose two.)

- A. Key 0 of all key chains must match for all routers in the autonomous system.
- B. No more than three keys should be configured in any single chain.
- C. Routers should be configured for NTP to synchronize their clocks.
- D. The lifetimes of the keys in the chain should overlap.
- E. Link compression techniques should be disabled on links transporting any MD5 hash.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

Valid 400-251 Dumps shared by ExamDiscuss.com for Helping Passing 400-251 Exam!
ExamDiscuss.com now offer the **newest 400-251 exam dumps**, the ExamDiscuss.com 400-251 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 400-251 dumps with Test Engine here:

<https://www.examdiscuss.com/Cisco/exam/400-251/premium/> (125 Q&As Dumps, **35%OFF** Special

Discount Code: **freecram**)