

Cisco.Premium.400-251.by.VCEplus.423q

Number: 400-051 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 3.0



Exam Code: 400-251

Exam Name: CCIE Security Written Exam

Certification Provider: Cisco

Corresponding Certification: CCIE Security

Website: www.vceplus.com

Free Exam: <https://vceplus.com/ccie-exam-400-251/>

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in 400-251 exam products and you get latest questions. We strive to deliver the best 400-251 exam product for top grades in your first attempt.

Exam A**QUESTION 1**

According to OWASP guidelines, what is the recommended method to prevent cross-site request forgery?

- A. Allow only POST requests.
- B. Mark all cookies as HTTP only.
- C. Use per-session challenge tokens in links within your web application.
- D. Always use the "secure" attribute for cookies.
- E. Require strong passwords.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

What is the maximum pattern length supported by FPM searches within a packet?

- A. 256 bytes
- B. 128 bytes
- C. 512 bytes
- D. 1500 bytes

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

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. 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.
- C. A view is created on the Cisco IOS device to leverage role-based access controls.

- D. Network administrators have read and write access to all system logs by default.
- E. The user profile on an AAA server is configured with the roles that grant user privileges.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

Which three global correlation feature can be enabled from cisco IPD device manager (Cisco IDM)? (Choose three)

- A. Network Reputation
- B. Global Data Interaction
- C. Signature Correlation
- D. Reputation Filtering
- E. Global Correlation Inspection
- F. Data Contribution
- G. Reputation Assignment



Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

http://www.cisco.com/c/en/us/td/docs/security/ips/70/configuration/guide/idm/idmguide7/idm_collaboration.html

QUESTION 5

According to RFC 4890, which three message must be dropped at the transit firewall/router?(Choose three.)

- A. Router Renumbering (Type 138)
- B. Node Information Query (Type 139)
- C. Router Solicitation (Type 133)
- D. Node information Response (Type 140)
- E. Router Advertisement (Type 134)
- F. Neighbor Solicitation (Type 135)

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

What is the effect of the following command on Cisco IOS router?

```
ip dns spoofing 1.1.1.1
```

- A. The router will respond to the DNS query with its highest loopback address configured
- B. The router will respond to the DNS query with 1.1.1.1 if the query id for its own hostname
- C. The router will respond to the DNS query with the IP address of its incoming interface for any hostname query
- D. The router will respond to the DNS query with the IP address of its incoming interface for its own hostname

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 7

Which two options are differences between automation and orchestration? (Choose two)

- A. Automation is to be used to replace human intervention
- B. Automation is focused on automating a single or multiple tasks
- C. Orchestration is focused on an end-to-end process or workflow
- D. Orchestration is focused on multiple technologies to be integrated together
- E. Automation is an IT workflow composed of tasks, and Orchestration is a technical task

Correct Answer: BC

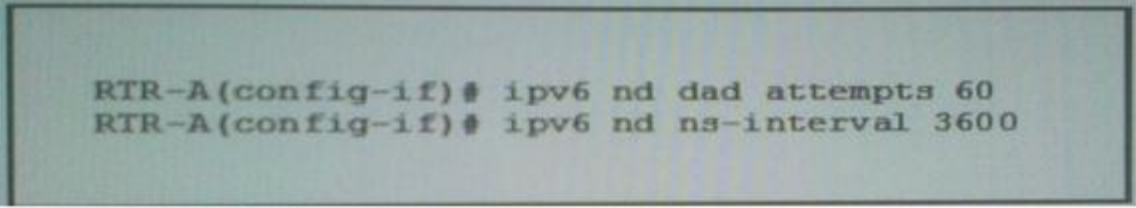
Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

Refer to the exhibit. What is the effect of the given configuration?



```
RTR-A(config-if)# ipv6 nd dad attempts 60  
RTR-A(config-if)# ipv6 nd ns-interval 3600
```

- A. It sets the duplicate address detection interval to 60 second and sets the IPv6 neighbor reachable time to 3600 milliseconds.
- B. It sets the number of neighbor solicitation messages to 60 and sets the retransmission interval to 3600 milliseconds.
- C. It sets the number of duplicate address detection attempts to 60 and sets the duplicate address detection interval to 3600 millisecond.
- D. It sets the number of neighbor solicitation message to 60 and set the duplicate address detection interval to 3600 second.
- E. It sets the duplicate address detection interval to 60 second and set the IPv6 neighbor solicitation interval to 3600 millisecond.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/command/ipv6-cr-book/ipv6i3.html#wp3064574124>
<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/command/ipv6-cr-book/ipv6i3.html#wp3676879817>

QUESTION 9

What are two characteristics of RPL, used in IoT environments? (Choose two)

- A. It is an Exterior Gateway Protocol
- B. It is a Interior Gateway Protocol
- C. It is a hybrid protocol
- D. It is link-state protocol
- E. It is a distance-vector protocol

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

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

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

Which VPN technology is based on GDOI (RFC 3547)?



- A. MPLS Layer 3 VPN
- B. MPLS Layer 2 VPN
- C. GET VPN
- D. IPsec VPN

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Which statement about the 3DES algorithm is true?

- A. The 3DES algorithm uses the same key for encryption and decryption,
- B. The 3DES algorithm uses a public-private key pair with a public key for encryption and a private key for decryption.
- C. The 3DES algorithm is a block cipher.
- D. The 3DES algorithm uses a key length of 112 bits.

E. The 3DES algorithm is faster than DES due to the shorter key length.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

Which significant change to PCI DSS standards was made in PCI DSS version 3.1?

- A. No version of TLS is now considered to provide strong cryptography.
- B. Storage of sensitive authentication data after authorization is now permitted when proper encryption is applied.
- C. Passwords are now required to be changed at least once every 30 days.
- D. SSL is now considered a weak cryptographic technology.
- E. If systems that are vulnerable to POODLE are deployed in an organization, a patching and audit review process must be implemented.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 14

Refer to the Exhibit, what is a possible reason for the given error?

```
sensor# show statistics virtual-sensor
Error : getVirtualSensorStatistics : Analysis Engine is busy.
```

- A. One or more require application failed to respond.
- B. The IPS engine is busy building cache files.
- C. The IPS engine is waiting for a CLI session to terminate.
- D. The virtual sensor is still initializing.

Correct Answer: D

Section: (none)

Explanation**Explanation/Reference:****QUESTION 15**

Which three statements about the keying methods used by MAC Sec are true (Choose Three)

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

Correct Answer: AEF

Section: (none)

Explanation**Explanation/Reference:**

Explanation: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/150_1_se/configuration/guide/3750xcg/swmacsec.pdf

SAP is disabled by default in Cisco TrustSec manual mode

QUESTION 16

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

- A. It uses attribute maps to map the AD memberOf attribute to the cisco ASA Group-Policy attribute
- B. It uses AD attribute maps to assign users to group policies configured under the WebVPN context
- C. The Cisco ASA can use more than one AD memberOf attribute to match a user to multiple group policies
- D. It can assign a group policy to a user based on access credentials
- E. It can combine AD attributes and LDP attributes to configure group policies on the Cisco ASA
- F. It is a closed standard that manages directory-information services over distributed networks

Correct Answer: BD

Section: (none)

Explanation**Explanation/Reference:**

QUESTION 17

With this configuration you notice that the IKE and IPsec SAs come up between the spoke and the hub, but NHRP registration fails. Registration will continue to fail until you do which of these?

```
Hub:
interface Tunnel0
ip address 172.16.1.1 255.255.255.0
no ip redirects
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 10
ip nhrp holdtime 600
ip nhrp redirect
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 10000
tunnel protection ipsec profile dmvpnprofile

Spoke 1:
interface Tunnel0
ip address 172.16.1.2 255.255.255.0
no ip redirects
ip nhrp authentication cisco
ip nhrp map multicast 1.1.1.2
ip nhrp map 172.16.1.1 1.1.1.2
ip nhrp network-id 20
ip nhrp holdtime 300
ip nhrp nhs 172.16.1.1
ip nhrp shortcut
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 1000
tunnel protection ipsec profile dmvpnprofile
```



- A. Modify the NHRP network IDs to match on the hub and spoke.
- B. configure the ip nhrp caches non-authoritative command on the hub's tunnel interface.
- C. modify the tunnel keys to match on the hub and spoke.
- D. modify the NHRP hold time to match on the hub and spoke.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nhrp/configuration/xr-16/nhrp-xr-16book/config-nhrp.html

QUESTION 18

Which three statements are true regarding Security Group Tags? (Choose three.)

- A. When using the Cisco ISE solution, the Security Group Tag gets defined as a separate authorization result.
- B. When using the Cisco ISE solution, the Security Group Tag gets defined as part of a standard authorization profile.
- C. Security Group Tags are a supported network authorization result using Cisco ACS 5.x.
- D. Security Group Tags are a supported network authorization result for 802.1X, MAC Authentication Bypass, and WebAuth methods of authentication.
- E. A Security Group Tag is a variable length string that is returned as an authorization result.

Correct Answer: ACD

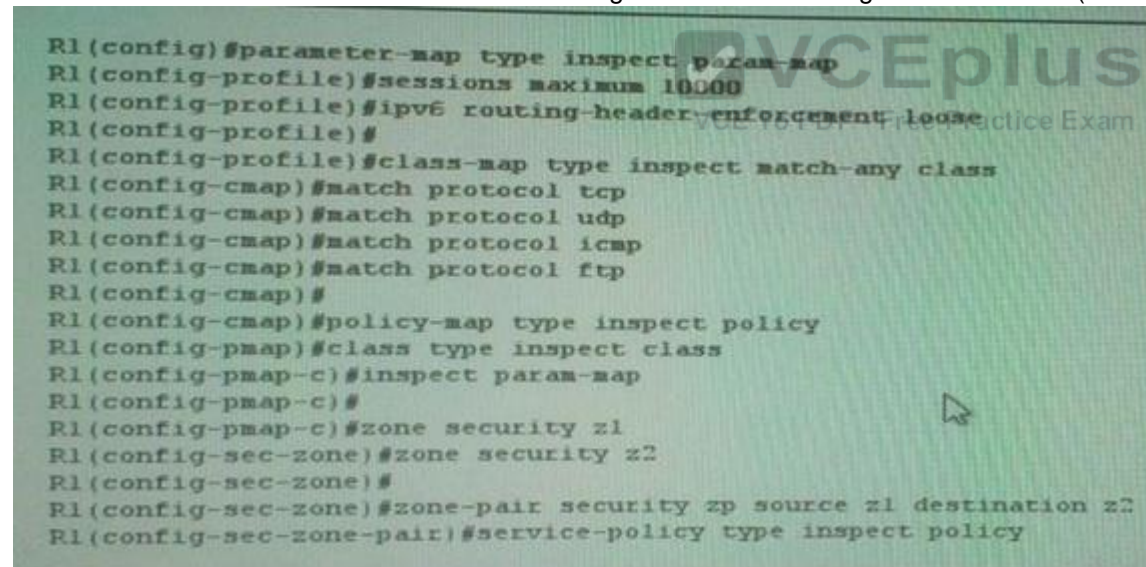
Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

Refer to the exhibit which two statement about the given IPV6 ZBF configuration are true? (Choose two)



```
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
```

- A. It provides backward compatibility with legacy IPv6 inspection
- B. It inspect TCP, UDP,ICMP and FTP traffic from Z1 to Z2.
- C. It inspect TCP, UDP,ICMP and FTP traffic from Z2 to Z1.

- D. It inspect TCP,UDP,ICMP and FTP traffic in both direction between z1 and z2.
- E. It passes TCP, UDP,ICMP and FTP traffic from z1 to z2.
- F. It provide backward compatibility with legacy IPv4 insection.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

In which class of applications security threads does HTTP header manipulation reside?

- A. Session management
- B. Parameter manipulation
- C. Software tampering
- D. Exception managements

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

Explanation: <http://www.cgisecurity.com/owasp/html/ch11s04.html>

Session management doesn't have anything to do with HTTP header

QUESTION 21

What is the most commonly used technology to establish an encrypted HTTP connection?

- A. the HTTP/1.1 Upgrade header
- B. the HTTP/1.0 Upgrade header
- C. Secure Hypertext Transfer Protocol
- D. HTTPS

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

What functionality is provided by DNSSEC?

- A. origin authentication of DNS data
- B. data confidentiality of DNS queries and answers
- C. access restriction of DNS zone transfers
- D. storage of the certificate records in a DNS zone file

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

What are the two mechanism that are used to authenticate OSPFv3 packets?(Choose two)

- A. MD5
- B. ESP
- C. PLAIN TEXT
- D. AH
- E. SHA



Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

You have been asked to configure a Cisco ASA appliance in multiple mode with these settings:

- (A) You need two customer contexts, named contextA and contextB
- (B) Allocate interfaces G0/0 and G0/1 to contextA
- (C) Allocate interfaces G0/0 and G0/2 to contextB
- (D) The physical interface name for G0/1 within contextA should be "inside".

(E) All other context interfaces must be viewable via their physical interface names.

If the admin context is already defined and all interfaces are enabled, which command set will complete this configuration?

- A. context contextA config-url disk0:/contextA.cfg allocate-interface GigabitEthernet0/0 visible allocate-interface GigabitEthernet0/1 inside context contextB config-url disk0:/contextB.cfg allocate-interface GigabitEthernet0/0 visible allocate-interface GigabitEthernet0/2 visible
- B. context contexta config-url disk0:/contextA.cfg allocate-interface GigabitEthernet0/0 visible allocate-interface GigabitEthernet0/1 inside context contextb config-url disk0:/contextB.cfg allocate-interface GigabitEthernet0/0 visible allocate-interface GigabitEthernet0/2 visible
- C. context contextA config-url disk0:/contextA.cfg allocate-interface GigabitEthernet0/0 invisible allocate-interface GigabitEthernet0/1 inside context contextB config-url disk0:/contextB.cfg allocate-interface GigabitEthernet0/0 invisible allocate-interface GigabitEthernet0/2 invisible
- D. context contextA config-url disk0:/contextA.cfg allocate-interface GigabitEthernet0/0 allocate-interface GigabitEthernet0/1 inside context contextB config-url disk0:/contextB.cfg allocate-interface GigabitEthernet0/0 allocate-interface GigabitEthernet0/2
- E. context contextA config-url disk0:/contextA.cfg allocate-interface GigabitEthernet0/0 visible allocate-interface GigabitEthernet0/1 inside context contextB config-url disk0:/contextB.cfg allocate-interface GigabitEthernet0/1 visible allocate-interface GigabitEthernet0/2 visible

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 25

Which statement about the cisco anyconnect web security module is true ?

- A. It is VPN client software that works over the SSI protocol.
- B. It is an endpoint component that is used with smart tunnel in a clientless SSL VPN.
- C. It operates as an NAC agent when it is configured with the Anyconnect VPN client.
- D. It is deployed on endpoints to route HTTP traffic to SCANsafe

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

Which two statements about the SeND protocol are true? (Choose two)

- A. It uses IPsec as a baseline mechanism

- B. It supports an autoconfiguration mechanism
- C. It must be enabled before you can configure IPv6 addresses
- D. It supports numerous custom neighbor discovery messages
- E. It counters neighbor discovery threats
- F. It logs IPv6-related threats to an external log server

Correct Answer: BE

Section: (none)

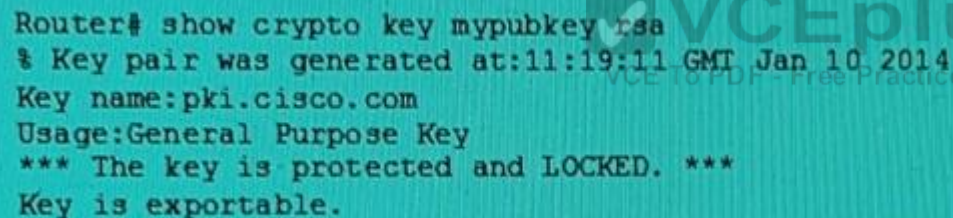
Explanation

Explanation/Reference:

QUESTION 27

Refer to the exhibit. You executed the show crypto key mypubkey rsa command to verify that the RSA key is protected and it generated the given output.

What command must you have entered to protect the key?



```
Router# show crypto key mypubkey rsa
% Key pair was generated at:11:19:11 GMT Jan 10 2014
Key name:pki.cisco.com
Usage:General Purpose Key
*** The key is protected and LOCKED. ***
Key is exportable.
```

- A. crypto key decrypt rsa name pki.cisco.com passphrase CiscoPKI
- B. crypto key zeroize rsa CiscoPKI
- C. crypto key export ras pki.cisco.com pem url flash: 3des CiscoPKI
- D. crypto key lock rsa name pki.cisco.com passphrase CiscoPKI
- E. crypto key import rsa pki.cisco.com pem url nvram: CiscoPKI

Correct Answer: D

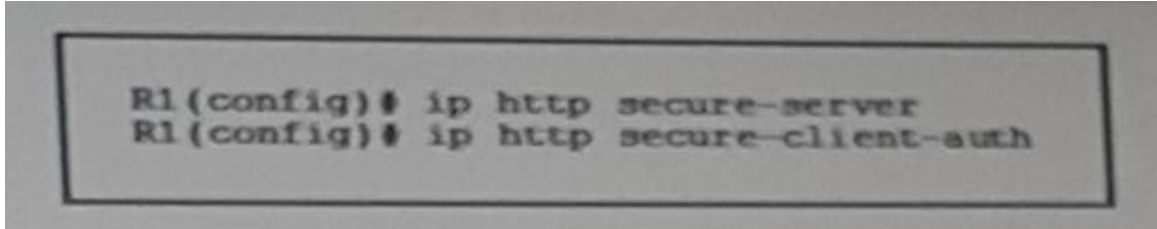
Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

Refer to the exhibit. What is the effect of the given command sequence?



```
R1(config)# ip http secure-server
R1(config)# ip http secure-client-auth
```

- A. The HTTP server and client will negotiate the cipher suite encryption parameters.
- B. The server will accept secure HTTP connections from clients with signed security certificates.
- C. The client profile will match the authorization profile defined in the AAA server.
- D. The clients are added to the cipher suite's profile.
- E. The server will accept secure HTTP connections from clients defined in the AAA server.

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

QUESTION 29

In ISO 27002, access control code of practice for information Security Management servers which of the following objective?

- A. Implement protocol control of user, network and application access
- B. Optimize the audit process
- C. Prevent the physical damage of the resources
- D. Educating employees on security requirements and issues

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

Which two options are differences between a automation and orchestration? (Choose two)

- A. Automation is an IT workflow composed of tasks, and orchestration is a technical task.
- B. Orchestration is focused on multiple technologies to be integrated together.
- C. Orchestration is focused on an end-to-end process or workflow
- D. Automation is to be used to replace human intervention.
- E. Automation is focused on automating a single or multiple tasks.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

What is the first step in performing a risk assessment?

- A. Identifying critical services and network vulnerabilities and determining the potential impact of their compromise or failure.
- B. Investigating reports of data theft or security breaches and assigning responsibility.
- C. Terminating any employee believed to be responsible for compromising security.
- D. Evaluating the effectiveness and appropriateness of the organization's current risk-management activities.
- E. Establishing a security team to perform forensic examinations of previous known attacks.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

Which description of a virtual private cloud is true?

- A. An on-demand configurable pool of shared software applications allocated within a public cloud environment, which provides tenant isolation
- B. An on-demand configurable pool of shared data resources allocated within a private cloud environment, which provides assigned DMZ zones
- C. An on-demand configurable pool of shared networking resources allocated within a private cloud environment, which provides tenant isolation
- D. An on-demand configurable pool of shared computing resources allocated within a public cloud environment, which provides tenant isolation

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

On which two protocols is VNC based? (Choose two)

- A. Rdesktop
- B. UDP
- C. RFB
- D. Terminal Services Client
- E. CoRD
- F. TCP

Correct Answer: CF

Section: (none)

Explanation

Explanation/Reference:



QUESTION 34

How can the tail drop algorithm support traffic when the queue is filled?

- A. It drop older packet with a size of 64 byts or more until queue has more traffic
- B. It drop older packet with a size of less than 64 byts until queue has more traffic
- C. It drops all new packets until the queue has room for more traffic
- D. It drops older TCP packets that are set to be redelivered due to error on the link until the queue has room for more traffic.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

Which two statements about the 3DES encryption protocol are true? (Choose two)

- A. It can operate in the Electronic Code Book and Asymmetric Block Chaining modes.
- B. Its effective key length is 168 bits.
- C. It encrypts and decrypts data in three 64-bit blocks with an overall key length of 192 bits.
- D. The algorithm is most efficient when it is implemented in software instead of hardware.
- E. It encrypts and decrypts data in three 56-bit blocks with an overall key length of 168 bits.
- F. Its effective key length is 112 bits.

Correct Answer: EF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

You want to enable users in your company's branch offices to deploy their own access points using WAN link from the central office, but you are unable to deploy a controller in the branch offices. What lightweight access point wireless mode should you choose?

- A. TLS mode
- B. H-REAP mode
- C. Monitor mode
- D. REAP mode
- E. Local mode

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

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

```
aaa-server SERVERGROUP (inside) host 10.10.10.1
  timeout 20
  ldap-base-dn dc=security, dc=cisco, dc=com
  ldap-login-password cisco
  ldap-login-dn cn=admin, cn=users, dc=security, dc=cisco, dc=com
  server-type auto-detect
```

- A. The Cisco ASA first check the user credentials against the AD tree of the security.cisco.com.
- B. The Cisco ASA use the cisco directory as the starting point for the user search.
- C. The AAA server SERVERGROUP is configured on host 10.10.10.1 with the timeout of 20 seconds.
- D. The Cisco ASA uses the security account to log in to the AD directory and search for the user cisco.
- E. The Cisco ASA authentication directly with the AD server configured on host 10.10.10.1 with the timeout of 20 second.
- F. The admin user is authenticated against the members of the security.cisco.com group.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:



QUESTION 38

Which object table contains information about the clients know to the server in Cisco NHRP MIB implementation?

- A. NHRP Cache Table
- B. NHRP Client Statistics Table
- C. NHRP Purge Request Table
- D. NHRP Server NHC Table

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

What is the default communication port used by RSA SDI and ASA ?

- A. UDP 500
- B. UDP 848
- C. UDP 4500
- D. UDP 5500

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

when a client tries to connect to a WLAN using the MAC filter (RADIUS server), if the client fails the authentication, what is the web policy used to fallback authentication to web authentication ?

- A. Authentication
- B. Passthrough
- C. Conditional Web Redirect
- D. Splash Page Web Redirect
- E. On MAC Filter Failure



Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

Refer the exhibit. Which of the following is the correct output of the above executed command?

```
R(config)#ip port-map http port 8080
```

A.

```
R#sh ip port-map | i http
Default mapping: http tcp port 80
Default mapping: http tcp port 8008
Default mapping: https tcp port 443
```

B.

```
R#sh ip port-map | i http
Default mapping: http tcp port 80
Default mapping: http tcp port 8081
Default mapping: https tcp port 443
```

C.

```
R#sh ip port-map | i http
Default mapping: http tcp port 80
Default mapping: http tcp port 8080
Default mapping: https tcp port 443
```

D.

```
R#sh ip port-map | .i http
Default mapping:  http    tcp port 80
Default mapping:  http    tcp port 8180
Default mapping:  https   tcp port 443
```

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

Which two statement about IPv6 path MTU discovery are true? (Choose two)

- A. The discover packets are dropped if there is congestion on the link.
- B. the initial path MTU is the same as the MTU of the original node's link layer interface
- C. It can allow fragmentation when the minimum MTU is blow a configured value
- D. During the discover process the DF bit is set to 1
- E. If the source host receiver an ICMPv6 packet too BIG message from a router it reduces its path MTU
- F. IF the destination host receives and ICMPv6 packet too Big message from a router it reduces its path MTU

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

Which two effects of configuring the tunnel path-mtu-discovery command on a GRE tunnel interface are true? (Choose two)

- A. The maximum path MTU across the GRE tunnel is set to 65534 bytes.
- B. If a lower MTU link between the IPsec peers is detected , the GRE tunnel MTU are changed.
- C. The router adjusts the MTU value it sends to the GRE tunnel interface in the TCP SYN packet.
- D. It disables PMTUD discovery for tunnel interfaces.

- E. The DF bit are copied to the GRE IP header.
- F. The minimum path MTU across the GRE tunnel is set to 1476 bytes.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

Which option describes the purpose of the RADIUS VAP-ID attribute?

- A. It specifies the ACL ID to be matched against the client
- B. It specifies the WLAN ID of the wireless LAN to which the client belongs
- C. It sets the minimum bandwidth for the connection
- D. It sets the maximum bandwidth for the connection
- E. It specifies the priority of the client
- F. It identifies the VLAN interface to which the client will be associated

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

You are developing an application to manage the traffic flow of a switch using an OpenDaylight controller. Knowing you use a Northbound REST API ,which statement is true?

- A. Different applications, even in different languages, cannot use the same functions in a REST API at same time.
- B. The server retains client state records
- C. We must teach our applications about the Southbound protocol(s) used
- D. The applications are considered to be the clients, and the controller is considered to be the server

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

Which option describes the purpose of Fog architecture in IoT?

- A. To provide compute services at the network edge
- B. To provide intersensor traffic routing
- C. To provide centralized compute resources
- D. To provide highly available environmentally hardened network access

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

What are feature that can stop man-in-the-middle attacks? (Choose two)

- A. ARP sniffing on specific ports
- B. ARP spoofing
- C. Dynamic ARP inspection
- D. DHCP snooping
- E. destination MAC ACLs

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

Which two statements about CoPP are true? (Choose two)

- A. When a deny rule in an access list is used for MQC is matched, classification continues on the next class
- B. It allows all traffic to be rate limited and discarded
- C. Access lists that are used with MQC policies for CoPP should omit the log and log-input keywords

- D. The mls qos command disables hardware acceleration so that CoPP handles all QoS
- E. Access lists that use the log keyword can provide information about the device's CPU usage
- F. The policy-map command defines the traffic class

Correct Answer: AC

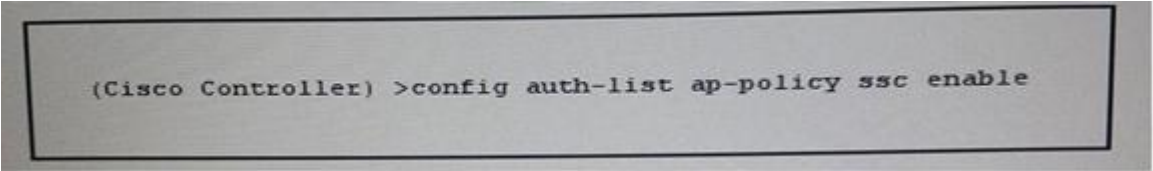
Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

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



```
(Cisco Controller) >config auth-list ap-policy ssc enable
```

- A. The WLC accepts self-signed certificates from the RADIUS server to authorize APs.
- B. The WLC adds the MAC addresses listed in the ssc ap-policy to its internal authorization list.
- C. The WLC adds the ssc access point to the auth-list internal authorization list.
- D. The WLC accepts the manufacture-installed certificate from the local access point.
- E. The WLC accepts self-signed certificates from devices added to its internal authorization list.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

Which two network protocols can operate on the Application Layer?(Choose two)

- A. DNS
- B. UDP
- C. TCP
- D. NetBIOS

- E. DCCP
- F. SMB

Correct Answer: AF

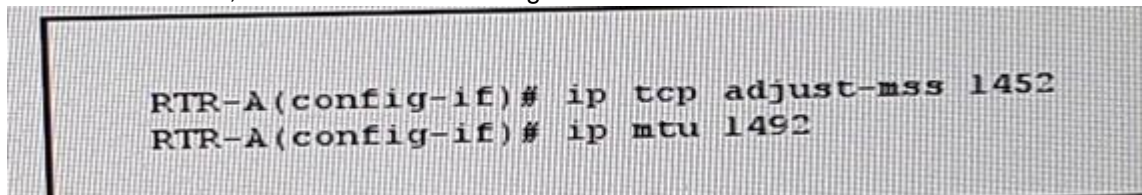
Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

Refer to the exhibit, which effect of this configuration is true?



```
RTR-A(config-if)# ip tcp adjust-mss 1452
RTR-A(config-if)# ip mtu 1492
```

- A. The PMTUD value sets itself to 1452 bytes when the interface MTU is set to 1492 bytes
- B. SYN packets carries 1452 bytes in the payload when the Ethernet MTU of the interface is set to 1492 bytes
- C. The maximum size of TCP SYN+ACK packets passing the transient host is set to 1452 bytes and the IP MTU of the interface is set to 1492 bytes
- D. The MSS to TCP SYN packets is set to 1452 bytes and the IP MTU of the interface is set to 1492 bytes
- E. The minimum size of TCP SYN+ACK packets passing the router is set to 1452 bytes and the IP MTU of the interface is set to 1492 bytes

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

Which of the following statement is true about the ARP spoofing attack?

- A. Attacker sends the ARP request with the MAC address and IP address of the legitimate resource in the network.
- B. Attacker of ends the ARP request with MAC address and IP address of its own.
- C. ARP spoofing does not facilitate man in-the-middle attack for the attacker.
- D. Attacker sends the ARP request with its own MAC address and IP address of legitimate resource in the network.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

Which command can you enter to cause the locally-originated Multicast Source Discovery Protocol Source-Active to be prevented from going to specific peers?

- A. ip msdp mesh-group mesh-name {<peer-address>|<peer-name>}
- B. ip msdp redistribute [list <acl>][asn as-access-list][route-map <map>]
- C. ip msdp sa-filter out <peer> [list<acl>] [route-map<map>]
- D. ip msdp default-peer {<peer-address> | <peer-name>}[prefix-list<list>]
- E. ip msdp sa-filter in <peer> [list<acl>][route-map <map>]

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 54

CCMP (CCM mode Protocol) is based on which algorithm?

- A. 3DES
- B. Blowfish
- C. RC5
- D. AES
- E. IDEA

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

Which command can you enter on the Cisco ASA to disable SSH?

- A. Crypto key generate ecdsa label
- B. Crypto key generate rsa usage-keys noconfirm
- C. Crypto keys generate rsa general-keys modulus 768
- D. Crypto keys generate ecdsa noconfirm
- E. Crypto keys zeroize rsa noconfirm

Correct Answer: E

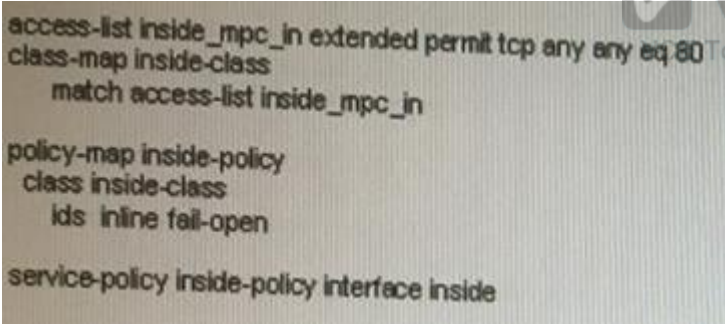
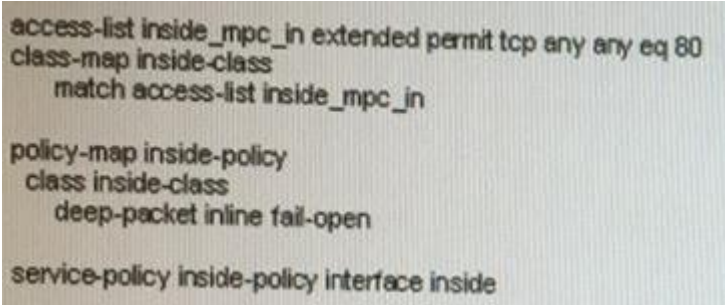
Section: (none)


Explanation

Explanation/Reference:

QUESTION 56

Which one of the following Cisco ASA adapts security appliance rule samples will send HTTP data to the AIP-SSM module to evaluate and stop HTTP attacks?

- A. 
- B. 

C.  access-list inside_mpc_in extended permit udp any any eq 80
class-map inside-class
match access-list inside_mpc_in

policy-map inside-policy
class inside-class
ips inline fail-open

D. access-list inside_mpc_in extended permit tcp any any eq 80
class-map inside-class
match access-list inside_mpc_in

policy-map inside-policy
class inside-class
ips inline fail-open

service-policy inside-policy interface inside

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

QUESTION 57

Why is the IPv6 type 0 routing header vulnerable to attack?

- A. It allows the receiver of a packet to control its flow.
- B. It allows the sender to generate multiple NDP requests for each packet.
- C. It allows the sender of a packet to control its flow.
- D. It allows the sender to generate multiple ARP requests for each packet.
- E. It allows the receiver of a packet to modify the source IP address.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 58

What context-based access control (CBAC) command sets the maximum time that a router running Cisco IOS will wait for a new TCP session to reach the established state?

- A. IP inspect max-incomplete
- B. IP inspect tcp finwait-time
- C. Ip inspect udp idle-time
- D. Ip inspect tcpsynwait-time
- E. Ip inspect tcp idle-time

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59

Which three statements about Cisco Flexible NetFlow are true? (Choose three.)

- A. The packet information used to create flows is not configurable by the user.
- B. It supports IPv4 and IPv6 packet fields.
- C. It tracks all fields of an IPv4 header as well as sections of the data payload.
- D. It uses two types of flow cache, normal and permanent.
- E. It can be a useful tool in monitoring the network for attacks.

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

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. interviews
- C. policy assessment

- D. penetration testing
- E. document review
- F. physical observations

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 61

On Which encryption algorithm is CCMP based?

- A. IDEA
- B. BLOWFISH
- C. RCS
- D. 3DES
- E. AES

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 62

By defaults which amount of time does the ASA add to the TTL value of a DNS entry to determine the amount of time a DNS entry is valid?

- A. 60 seconds
- B. 30 seconds
- C. 0 second
- D. 180 seconds
- E. 120 seconds
- F. 100 seconds

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****QUESTION 63**

What is the name of the unique tool/feature in cisco security manager that is used to merge an access list based on the source/destination IP address service or combination of these to provide a manageable view of access policies?

- A. merge rule tool
- B. policy simplification tool
- C. rule grouping tool
- D. object group tool
- E. combine rule tool

Correct Answer: E

Section: (none)

Explanation**Explanation/Reference:****QUESTION 64**

Refer to the exhibit. Which statement about the effect of this configuration is true?

```
SW1 (config)# mka policy security-policy  
SW1 (config-mka-policy)# replay-protection window-size 0  
SW1 (config-mka-policy)# end
```

- A. reply protection is disable
- B. It prevent man-in-the-middle attacks
- C. The replay window size is set to infinity
- D. Out-of-order frames are dropped

Correct Answer: D

Section: (none)

Explanation**Explanation/Reference:**

QUESTION 65

when a host initiates a TCP session, what is the numerical range into which the initial sequence number must fall?

- A. 0 to 65535
- B. 1 to 1024
- C. 0 to 4,294,967,295
- D. 1 to 65535
- E. 1 to 4,294,967,295
- F. 0 to 1024

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 66

What port has IANA assigned to the GDOI protocol?

- A. UDP 4500
- B. UDP 500
- C. UDP 1812
- D. UDP 848

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 67

Which statement is true about SYN cookies?

- A. The state is kept on the server machine TCP stack
- B. A system has to check every incoming ACK against state tables
- C. NO state is kept on the server machine state but is embedded in the initial sequence number

D. SYN cookies do not help to protect against SYN flood attacks

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 68

Refer to the exhibit. R1 and R2 are connected across and ASA with MD5 authentication. Which statement about eBGP peering between the routers could be true?



- A. eBGP peering will fail because ASA is transit lacks BGP support.
- B. eBGP peering will be successful.
- C. eBGP peering will fail because the two routers must be directly connected to allow peering.
- D. eBGP peering will fail because of the TCP random sequence number feature.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

What is the maximum pattern length supported by FPM searches within a packet ?

- A. 256 bytes
- B. 1500 bytes
- C. 512 bytes
- D. 128 bytes

Correct Answer: A

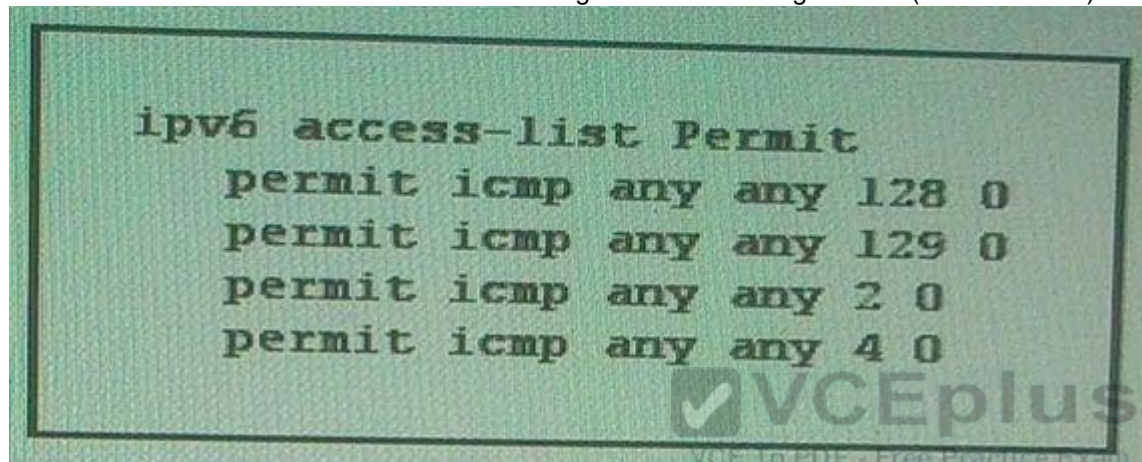
Section: (none)

Explanation

Explanation/Reference:

QUESTION 70

Refer to the exhibit. What are three effect of the given firewall configuration? (Choose three.)



- A. The firewall allows Echo Request packets from any source to pass server.
- B. The firewall allows time Exceeded error messages from any source to pass to the server.
- C. PCs outside the firewall are unable to communicate with the server over HTTP
- D. The firewall allows Echo Reply packets from any source to pass to the server.
- E. The firewall allows Destination Unreachable error messages from any source to pass to the server.
- F. The firewall allows Packet too big error messages from any source to pass to the server.

Correct Answer: ADF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 71

Refer to the exhibit Flexible NetFlow is failing to export flow records from RouterA to your flow collector. What action can you take to allow the IPv6 flow records to be sent to the collect?

```
ROUTER#
flow exporter IPV4-EXPORTER
  destination 172.16.1.2
  transport udp 2055
exit

flow record IPV6-RECORD
match ipv6 traffic-class
match ipv6 protocol
match ipv6 source address
match ipv6 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long

flow record IPV4-RECORD
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long

flow monitor FLOW-MONITOR-IPV6
record IPV6-RECORD
exporter IPV4-EXPORTER
exit

flow monitor FLOW-MONITOR-IPv4
record IPV4-RECORD
exporter IPV4-EXPORTER
exit

ip cef

interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ip flow monitor FLOW-MONITOR-IPv4 output
 ipv6 flow monitor FLOW-MONITOR-IPV6 output
```

- A. Set the NetFlow export protocol to v5
- B. Configure the output-features command for the IPV4-EXPORTER
- C. Add the ipv6 cef command to the configuration
- D. Remove the ip cef command from the configuration
- E. Create a new flow exporter with an IPv6 destination and apply it to the flow monitor

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

We need to have ipv6 cef enabled either globally or on interfaces for IPv6 Netflow

<https://supportforums.cisco.com/document/105221/ipv6-flexible-netflow-configuration-example>

QUESTION 72

When you configure an ASA with RADIUS authentication and authorization, which attribute is used to differentiate user roles?

- A. login-ip-host
- B. cisco-priv-level
- C. service-type
- D. termination-action
- E. tunnel-type

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

Which two statement about the IPv6 Hop-by-Hop option extension header (EH) are true?
(Choose two)

- A. The Hop-by-Hop EH is processed in hardware at the source and the destination devices only.
- B. If present, network devices must process the Hop-by-Hop EH first
- C. The Hop-by-Hop extension header is processed by the CPU by network devices
- D. The Hop-by-Hop EH is processed in hardware by all intermediate network devices
- E. The Hop-by-Hop EH is encrypted by the Encapsulating Security Header.
- F. If present the Hop-by-Hop EH must follow the Mobility EH.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 74

Which configuration option will correctly process network authentication and authorization using both 802.1X and MAB on a single port?

- A. `interface FastEthernet1/0/9`
 `switchport access vlan 200`
 `switchport mode access`
 `switchport voice vlan 40`
 `ip access-group ACL-DEFAULT in`
 `authentication event fail action next-method`
 `authentication event server dead action authorize vlan 200`
 `authentication event server alive action reinitialize`
 `authentication host-mode multi-domain`
 `authentication open`
 `authentication order mab dot1x`
 `authentication priority dot1x mab`
 `authentication port-control auto`
 `authentication violation restrict`
 `mab`
 `dot1x pae authenticator`
 `dot1x timeout tx-period 10`
 `spanning-tree portfast`
 `ip dhcp snooping information option allow-untrusted`
 `end`
- B. `interface FastEthernet1/0/9`
 `switchport access vlan 200`
 `switchport mode access`
 `switchport voice vlan 40`
 `ip access-group ACL-DEFAULT in`
 `authentication event fail action next-method`
 `authentication event server dead action authorize vlan 200`
 `authentication event server alive action reinitialize`
 `authentication host-mode multi-domain`
 `authentication open`
 `authentication order mab dot1x`
 `authentication priority dot1x mab`
 `authentication violation restrict`
 `mab`
 `dot1x pae authenticator`
 `dot1x timeout tx-period 10`
 `spanning-tree portfast`
 `ip dhcp snooping information option allow-untrusted`
 `end`

C. `interface FastEthernet1/0/9`
`switchport access vlan 200`
`switchport mode access`
`switchport voice vlan 40`
`ip access-group ACL-DEFAULT in`
`authentication event fail action next-method`
`authentication event server dead action authorize vlan 200`
`authentication event server alive action reinitialize`
`authentication host-mode multi-domain`
`authentication open`
`authentication order mab dot1x`
`authentication priority dot1x mab`
`authentication violation restrict`
`mab`
`dot1x pae authenticator`
`dot1x timeout tx-period 10`
`spanning-tree portfast`
`ip dhcp snooping information option allow-untrusted`
`end`

D. `interface FastEthernet1/0/9`
`switchport access vlan 200`
`switchport mode access`
`switchport voice vlan 40`
`ip access-group ACL-DEFAULT in`
`authentication event fail action next-method`
`authentication event server dead action authorize vlan 200`
`authentication event server alive action reinitialize`
`authentication host-mode multi-domain`
`authentication open`
`authentication order mab dot1x`
`authentication priority dot1x mab`
`authentication port-control force-unauthorized`
`authentication violation restrict`
`mab`
`dot1x pae authenticator`
`dot1x timeout tx-period 10`
`spanning-tree portfast`
`ip dhcp snooping information option allow-untrusted`
`end`

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 75

Which two current RFCs discuss special use IP addresses that may be used as a checklist of invalid routing prefixes for IPv4 and IPv6 addresses? (Choose two.)

- A. RFC 5156
- B. RFC 5735
- C. RFC 3330
- D. RFC 1918
- E. RFC 2827

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:



QUESTION 76

What are two protocols that HTTP can use to secure sessions? (Choose two)

- A. HTTPS
- B. AES
- C. TLS
- D. AH
- E. SSL

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://www.instantssl.com/ssl-certificate-products/https.html>

QUESTION 77

Which three statements about the IANA are true? (Choose three.)

- A. IANA is a department that is operated by the IETF
- B. IANA oversees global IP address allocation.
- C. IANA managed the root zone in the DNS.
- D. IANA is administered by the ICANN.
- E. IANA defines URI schemes for use on the Internet.

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 78

A cloud service provider is designing a large multitenant data center to support thousands of tenants. The provider is concerned about the scalability of the Layer 2 network and providing Layer 2 segmentation to potentially thousands of tenants. Which Layer 2 technology is best suited in this scenario?

- A. LDP
- B. VXLAN
- C. VRF
- D. Extended VLAN ranges

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

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



```
RTR-A(config-if)# ip pim passive
```

- A. The router sends PIM messages only to other routers on the same LAN.
- B. The router sends PIM messages, but it rejects any PIM message it receives.
- C. The router acts as a stub multicast router for the EIGRP routing protocol.
- D. The router accepts all PIM control messages.
- E. The router acts as the DR and DF for all bidir-PIM group ranges.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:



QUESTION 80

What is the purpose of enabling the IP option selective Drop feature on your network routers?

- A. To protect the internal network from IP spoofing attacks.
- B. To drop IP fragmented packets.
- C. To drop packet with a TTL value of Zero.
- D. To protect the network from DoS attacks.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 81

Which two answers describe provisions of the SOX Act and its international counterpart Acts?
(Choose two.)

- A. confidentiality and integrity of customer records and credit card information
- B. accountability in the event of corporate fraud
- C. financial information handled by entities such as banks, and mortgage and insurance brokers
- D. assurance of the accuracy of financial records
- E. US Federal government information
- F. security standards that protect healthcare patient data

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 82

What are two method of preventing DoS attacks on your network? (Choose two)

- A. Increase the ICMP Unreachable message rate limit interval.
- B. Implement shaping on the perimeter router.
- C. Disable the ICMP Unreachable response on the loopback and Null0 interfaces
- D. Decreases the ICMP Unreachable message interval
- E. Implement CWBQ on the perimeter router

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 83

What protocol does SMTPS use to secure SMTP connections?

- A. AES
- B. TLS
- C. Telnet
- D. SSH

Correct Answer: B

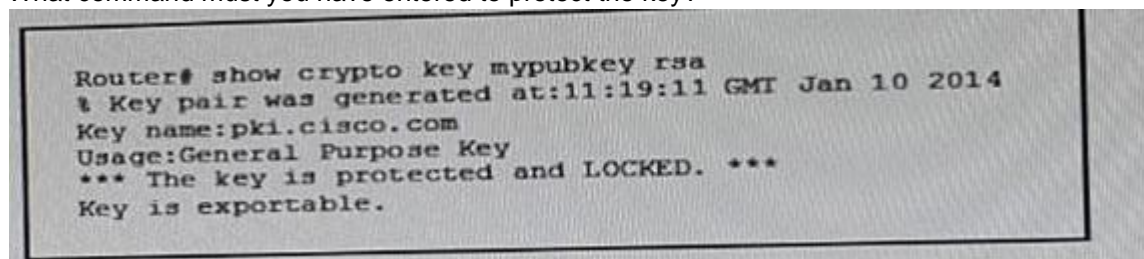
Section: (none)

Explanation

Explanation/Reference:

QUESTION 84

Refer to the exhibit, you executed the show crypto key mypubkeyrsa command to verify that the RSA key is protected and it generated the given output. What command must you have entered to protect the key?



- A. crypto key export rsa pki.cisco.com pern url flash: 3des CiscoPKI
- B. crypto key decrypt rsa name pki.cisco.com passphrase CiscoPKI
- C. crypto key import rsa pki.cisco.com pern url nvram: CiscoPKI
- D. crypto key zeroize rsa CiscoPKI
- E. crypto key lock rsa name pki.cisco.com passphrase CiscoPKI

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 85

All of these Cisco security products provide event correlation capabilities excepts which one?

- A. Cisco Security MARS
- B. Cisco Guard/Detector
- C. Cisco ASA adaptive security appliance
- D. Cisco IPS
- E. Cisco Security Agent.

Correct Answer: C

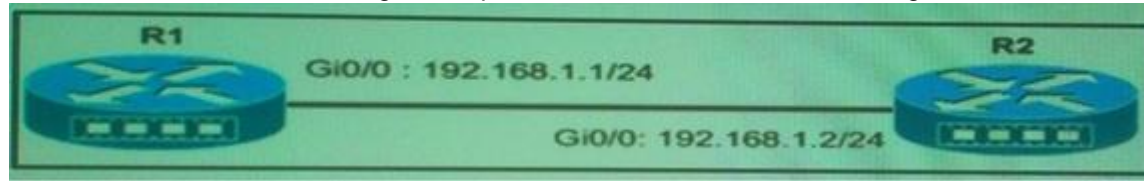
Section: (none)

Explanation

Explanation/Reference:

QUESTION 86

Refer to the exhibit, which configuration prevents R2 from become a PIM neighbor with R1?



- A. Access-list 10 deny 192.168.1.2.0.0.0.0
!
Interface gi0/0
Ippim neighbor-filter 1
- B. Access-list 10 deny 192.168.1.2.0.0.0.0
!
Interface gi0/0
Ipigmp access-group 10
- C. Access-list 10 deny 192.168.1.2.0.0.0.0
!
Interface gi0/0
Ippimneighbour-filter 10
- D. Access-list 10 permit 192.168.1.2.0.0.0.0
!
Interface gi0/0
Ippim neighbor-filter 10

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 87

Which two certificate enrollment methods can be completed without an RA and require no direct connection to a CA by the end entity? (Choose two.)

- A. SCEP
- B. TFTP
- C. manual cut and paste
- D. enrollment profile with direct HTTP
- E. PKCS#12 import/export

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 88

Which two statements about the MD5 Hash are true? (Choose two.)

- A. Length of the hash value varies with the length of the message that is being hashed.
- B. Every unique message has a unique hash value.
- C. Its mathematically possible to find a pair of message that yield the same hash value.
- D. MD5 always yields a different value for the same message if repeatedly hashed.
- E. The hash value cannot be used to discover the message.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 89

Which three statement about VRF-Aware Cisco Firewall are true? (Choose three)

- A. It can run as more than one instance.
- B. It supports both global and per-VRF commands and DoS parameters.
- C. It can support VPN networks with overlapping address ranges without NAT.
- D. It enables service providers to implement firewalls on PE devices.
- E. It can generate syslog messages that are visible only to individual VPNs.
- F. It enables service providers to deploy firewalls on customer devices.

Correct Answer: ADE

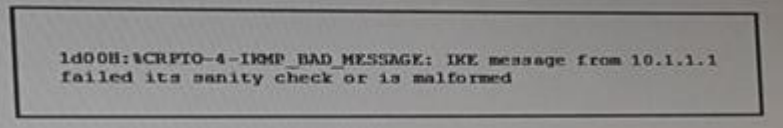
Section: (none)

Explanation

Explanation/Reference:

QUESTION 90

Refer to the exhibit. What is the meaning of the given error message?



```
1d00H:1CRPTO-4-IMP_BAD_MESSAGE: IKE message from 10.1.1.1
failed its sanity check or is malformed
```

- A. The PFS groups are mismatched.
- B. The pre-shared keys are mismatched.
- C. The mirrored crypto ACLs are mismatched.
- D. IKE is disabled on the remote peer.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 91

Which two value must you configure on the cisco ASA firewall to support FQDN ACL ? (Choose two)

- A. A DNS server
- B. A Service policy
- C. An FQDN object
- D. A Class map
- E. A services object
- F. A policy map

Correct Answer: AC

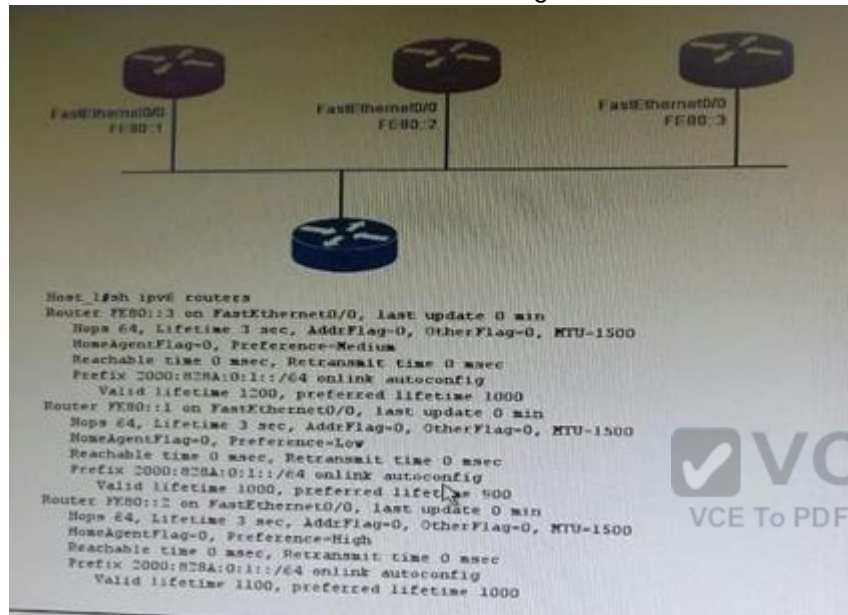
Section: (none)

Explanation

Explanation/Reference:

QUESTION 92

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



- A. Host_1 learns about R2 and only and prefers R2 as its default router
- B. Host_1 selects R2 as its default router and load balances between R2 and R3
- C. Host_1 learns about R2 and R3 only and prefers R3 as its default router
- D. Host_1 learns about R1, R2 and R3 and load balances between them
- E. Host_1 learns about R1, R2 and R3 and prefers R2 as its default router

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 93

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 94

Which two statement about router Advertisement message are true? (Choose two)

- A. Local link prefixes are shared automatically.
- B. Each prefix included in the advertisement carries lifetime information for that prefix.
- C. Message are sent to the multicast address FF02::1
- D. It support a configurable number of retransmission attempts for neighbor solicitation message.
- E. Flag setting are shared in the message and retransmitted on the link.
- F. Router solicitation message are sent in response to router advertisement message

Correct Answer: AF

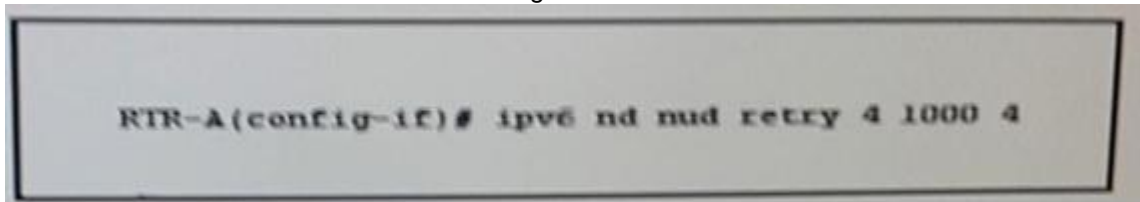
Section: (none)

Explanation

Explanation/Reference:

QUESTION 95

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



- A. NUD retransmits 1000 Neighbor solicitation messages every 4 hours and 4 minutes.
- B. NUD retransmits Neighbor Solicitation messages after 4, 16, 64 and 256 seconds.
- C. NUD retransmits Neighbor Solicitation messages every 4 seconds.
- D. NUD retransmits unsolicited Neighbor advertisements messages every 4 hours.
- E. NUD retransmits four Neighbor Solicitation messages every 1000 seconds.
- F. NUD retransmits Neighbor Solicitation messages after 1, 4, 16, and 64 seconds.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 96

What are two features of cisco IOS that can help mitigate Blaster worm attack on RPC ports? (Choose two)

- A. FPM
- B. DCAR
- C. NBAR
- D. IP source Guard
- E. URPF
- F. Dynamic ARP inspection



Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 97

Which two statement about the multicast addresses query message are true?(Choose two)

- A. They are solicited when a node initialized the multicast process.
- B. They are used to discover the multicast group to which listeners on a link are subscribed
- C. They are used to discover whether a specified multicast address has listeners
- D. They are send unsolicited when a node initializes the multicast process
- E. They are usually sent only by a single router on a link

F. They are sent when a node discover a multicast group

Correct Answer: BC

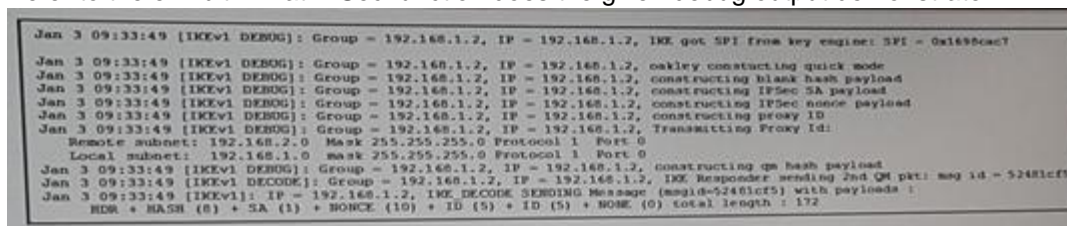
Section: (none)

Explanation

Explanation/Reference:

QUESTION 98

Refer to the exhibit. What IPSec function does the given debug output demonstrate?



```
Jan 3 09:33:49 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, IKE got SPI from key engine: SPI = 0x169b0ac7
Jan 3 09:33:49 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, oakley constructing quick mode
Jan 3 09:33:49 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing blank hash payload
Jan 3 09:33:49 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing IPSec SA payload
Jan 3 09:33:49 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing IPSec nonce payload
Jan 3 09:33:49 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing proxy ID
Jan 3 09:33:49 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Transmitting Proxy ID:
Remote subnet: 192.168.2.0 Mask 255.255.255.0 Protocol 1 Port 0
Local subnet: 192.168.1.0 mask 255.255.255.0 Protocol 1 Port 0
Jan 3 09:33:49 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing qm hash payload
Jan 3 09:33:49 [IKEv1 DECODE]: Group = 192.168.1.2, IP = 192.168.1.2, IKE Responder: sending 2nd QM pkt: msg id = 52481cfs
Jan 3 09:33:49 [IKEv1]: IP = 192.168.1.2, IKE DECODE: SENDING Message (msgid=52481cfs) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172
```

- A. DH exchange initiation
- B. setting SPIs to pass traffic
- C. PFS parameter negotiation
- D. crypto ACL confirmation

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

This Cisco IPSec troubleshooting guide explains details about every packet exchange during IPSec phase 1 and 2. Take a look at the section about QM2. It is exact match of the above exhibit.

<http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generationfirewalls/113574-tg-asa-ipsec-ike-debug-main-00.html>

QUESTION 99

IANA is responsible for which three IP resources? (Choose three.)

- A. IP address allocation
- B. Detection of spoofed address
- C. Criminal prosecution of hackers

- D. Autonomous system number allocation
- E. Root zone management in DNS
- F. BGP protocol vulnerabilities

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 100

When you are configuring QoS on the Cisco ASA appliance.
Which four are valid traffic selection criteria? (Choose four)

- A. default-inspection-traffic
- B. qos-group
- C. DSCP
- D. VPN group
- E. tunnel group
- F. IP precedence



Correct Answer: ACEF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 101

Which two statements about the anti-replay feature are true? (Choose two)

- A. By default, the sender uses a single 1024-packet sliding window
- B. By default, the receiver uses a single 64-packet sliding window
- C. The sender assigns two unique sequence numbers to each clear-text packet
- D. The sender assigns two unique sequence numbers to each encrypted packet
- E. the receiver performs a hash of each packet in the window to detect replays
- F. The replay error counter is incremented only when a packet is dropped