

➤ **Vendor: Cisco**

➤ **Exam Code: 400-251**

➤ **Exam Name: CCIE Security**

➤ **Question 1 – Question 50**

[Visit PassLeader and Download Full Version 400-251 Exam Dumps](#)

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.

Answer: C

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

Answer: A

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.

Answer: DE

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

Answer: CDE

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)

Answer: ABD

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

Answer: D

QUESTION 7

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

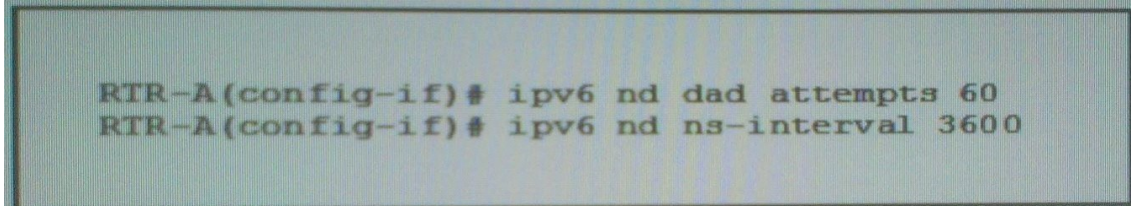
- A. Automation is to be used to replace human intervention
- B. Automation is focused on automating a single or multiple tasks
- C. Orchestration is focused on an end-to-end process or workflow
- D. Orchestration is focused on multiple technologies to be integrated together

E. Automation is an IT workflow composed of tasks, and Orchestration is a technical task

Answer: BC

QUESTION 8

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



- 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.

Answer: E

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

Answer: BE

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

Answer: ABD

QUESTION 11

Drag and Drop Question

Drag each OSPF security feature on the left to its description on the right.

Prefix Length	Protects OSPF neighbor sessions against CPU utilization attacks.
TTL Security Check	Uses MD5 authentication to protect OSPF sessions.
Type 0	Uses clear-text authentication to protect OSPF sessions.
Type 1	Protects the routers in an OSPF neighbor session by limiting route injection.
Type 2	Establishes OSPF sessions without authentication.

Answer:

Prefix Length	TTL Security Check
TTL Security Check	Type 2
Type 0	Type 1
Type 1	Prefix Length
Type 2	Type 0

QUESTION 12

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

Answer: C

QUESTION 13

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.

Answer: C

QUESTION 14

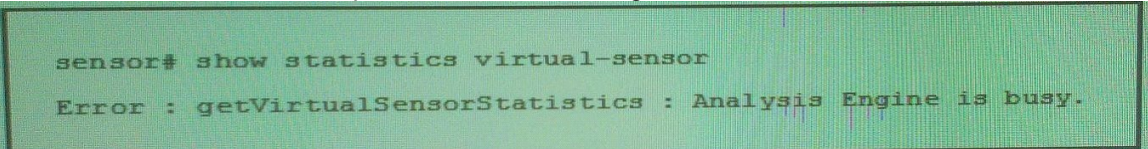
Which significant change to PCI DSS standards was made in PCI DSS version 3.1?

- 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.

Answer: D

QUESTION 15

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.

Answer: D

QUESTION 16

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.

Answer: ABF

QUESTION 17

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

Answer: AB

QUESTION 18

Drag and Drop Question

Drag each IPS signature engine on the left to its description on the right.

AIC	Inspects traffic on a specific protocol.
Atomic	Analyzes Bo2k, Tfn2k, and UDP traffic.
Flood	Combines Layer 3 and Layer 4 attributes in one signature.
Normalizer	Analyzes FTP and HTTP traffic.
Service	Configures IP and TCP functions to enforce RFC compliance.
Trojan	Detects ICMP DoS attacks against networks and hosts.

Answer:

AIC	Inspects traffic on a specific protocol.
Atomic	Analyzes Bo2k, Tfn2k, and UDP traffic.
Flood	Combines Layer 3 and Layer 4 attributes in one signature.
Normalizer	Analyzes FTP and HTTP traffic.
Service	Configures IP and TCP functions to enforce RFC compliance.
Trojan	Detects ICMP DoS attacks against networks and hosts.

Note: The image shows red X marks over the entire table, indicating that the correct answer is not visible or that the question is invalid.

QUESTION 19

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.

Answer: C

QUESTION 20

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.

Answer: ACD

QUESTION 21

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 inspection.

Answer: AB

QUESTION 22

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

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

Answer: A

QUESTION 23

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

Answer: D

QUESTION 24

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

Answer: A

QUESTION 25

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

Answer: BD

QUESTION 26

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

Answer: A

QUESTION 27

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.

Answer: D

QUESTION 28

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

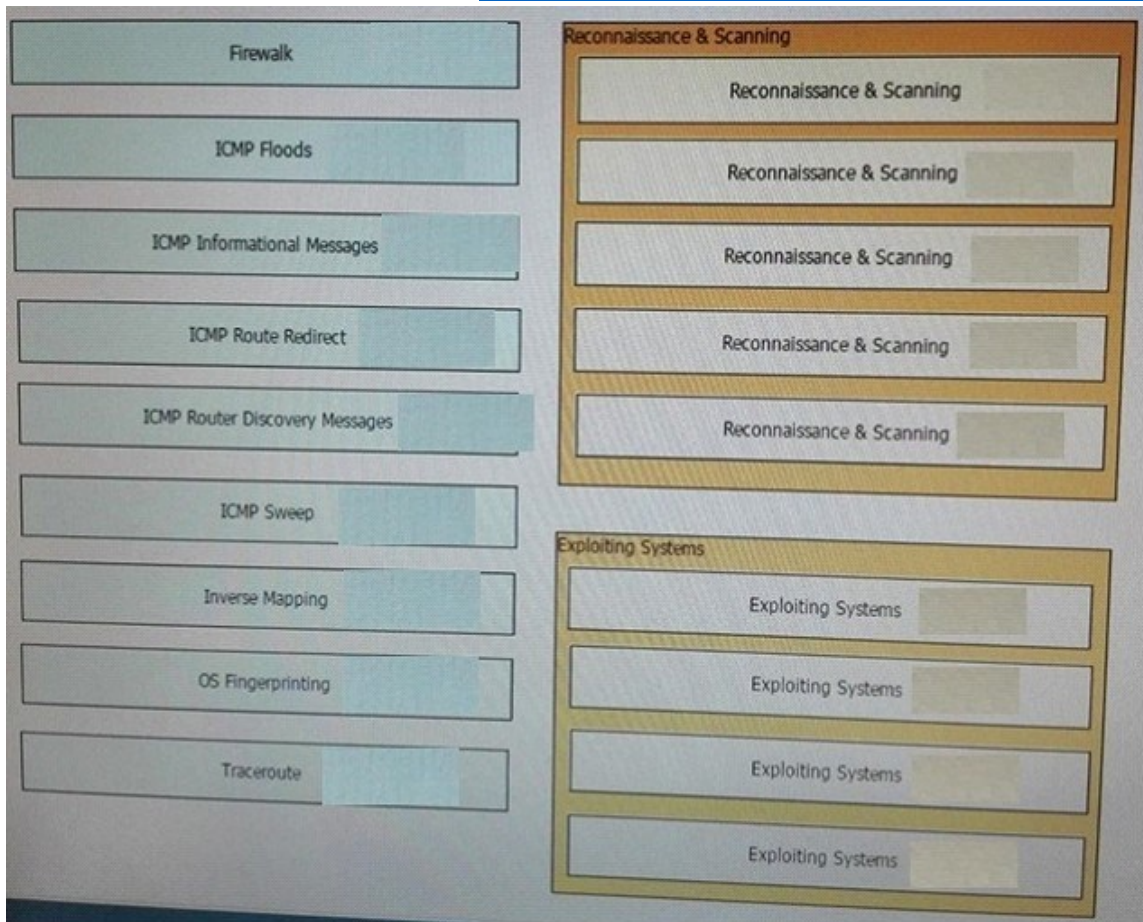
- A. It uses IPsec as a baseline mechanism
- B. It supports an autoconfiguration mechanism
- C. It must be enabled before you can configure IPv6 addresses
- D. It supports numerous custom neighbor discovery messages
- E. It counters neighbor discovery threats
- F. It logs IPv6-related threats to an external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

Answer: BE

QUESTION 29

Drag and Drop Question

Drag each attack type on the left to the matching attack category on the right.



Answer:



QUESTION 30

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`

Answer: D

QUESTION 31

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

```
Router_AP (Config)#interface wlan-ap0
ip address 20.20.20.1 255.255.255.0
no shutdown
Router_AP#service-module wlan-ap0 session
Trying 20.20.20.1, 2002 ... Open
```

- 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.

Answer: B

QUESTION 32

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

Answer: A

QUESTION 33

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.

Answer: BC

QUESTION 34

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.

Answer: A

QUESTION 35

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

Answer: D

QUESTION 36

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

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

Answer: CF

QUESTION 37

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

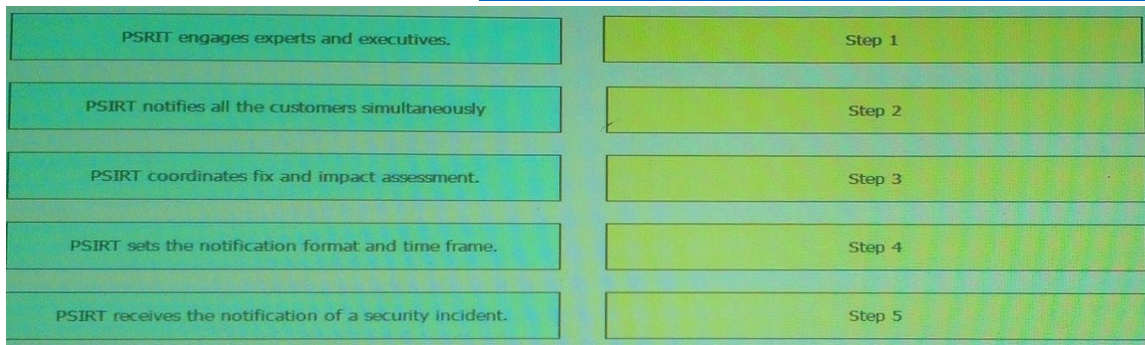
- A. It drop older packet with a size of 64 byts or more until queue has more traffic.
- B. It drop older packet with a size of less than 64 byts until queue has more traffic.
- C. It drops all new packets until the queue has room for more traffic.
- D. It drops older TCP packets that are set to be redelivered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

Answer: C

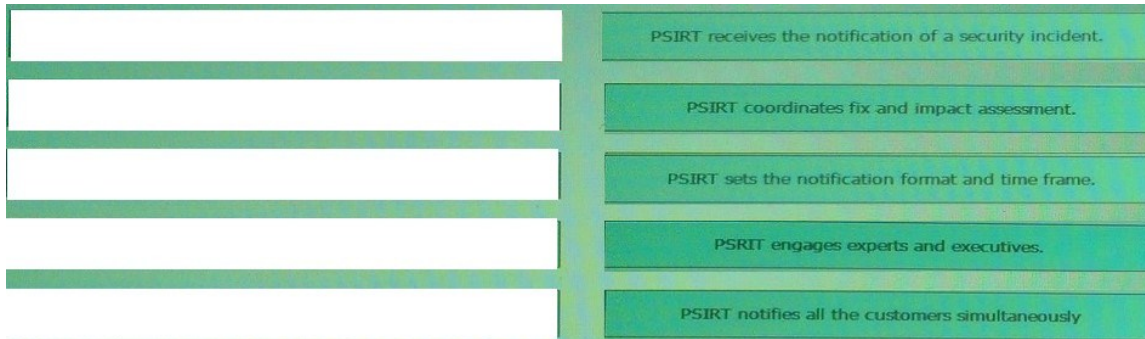
QUESTION 38

Drag and Drop Question

Drag each step in the cisco PRIST response to incidents and vulnerability involving cisco product on the left into the correct order on the right.



Answer:



QUESTION 39

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.

Answer: EF

QUESTION 40

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 a 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

Answer: B

QUESTION 41

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.

Answer: CF

QUESTION 42

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

Answer: D

QUESTION 43

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

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

Answer: D

QUESTION 44

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

Answer: E

QUESTION 45

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

Answer: C

QUESTION 46

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 below a configured value.
- D. During the discover process the DF bit is set to 1.
- E. If the source host receives an ICMPv6 packet too BIG message from a router it reduces its path MTU.
- F. If the destination host receives an ICMPv6 packet too Big message from a router it reduces its path MTU.

Answer: BE

QUESTION 47

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

Answer: BE

QUESTION 48

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

Answer: B

QUESTION 49

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 the 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

Answer: D

QUESTION 50

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

Answer: A

[Visit PassLeader and Download Full Version 400-251 Exam Dumps](#)