# Cisco

## Exam 350-018

### CCIE Security Exam (4.0)

**Version: 36.0**

**[ Total Questions: 763 ]**

**Question No : 1**

Refer to the exhibit.

It shows the format of an IPv6 Router Advertisement packet. If the Router Lifetime value is set to 0, what does that mean?

**A.** The router that is sending the RA is not the default router.
**B.** The router that is sending the RA is the default router.
**C.** The router that is sending the RA will never power down.
**D.** The router that is sending the RA is the NTP master.
**E.** The router that is sending the RA is a certificate authority.
**F.** The router that is sending the RA has its time synchronized to an NTP source.

**Answer: A**

**Question No : 2**

What SNMFV3 command disables descriptive error messages?

**A.** snmp-server usm Cisco
**B.** snmp-server ifindex persist
**C.** snmp-server trap link switchover
**D.** snmp-server inform

**Answer: A**

**Question No : 3**

EAP-MD5 provides one-way client authentication. The server sends the client a random challenge. The client proves its identity by hashing the challenge and its password with MD5. What is the problem with EAP-MD5?

**A.** EAP-MD5 is vulnerable to dictionary attack over an open medium and to spoofing because there is no server authentication.
**B.** EAP-MD5 communication must happen over an encrypted medium, which makes it operationally expensive.
**C.** EAP-MD5 is CPU-intensive on the devices.

**D.** EAP-MD5 not used by RADIUS protocol.

**Answer: A**

## Question No : 4

Which statement describes an IPv6 benefit?

**A.** Broadcast is not available.
**B.** Routing tables are more complicated.
**C.** The address pool is limited.
**D.** Data encryption is not built into the packet frame.
**E.** Increased NAT is required.

**Answer: A**

## Question No : 5

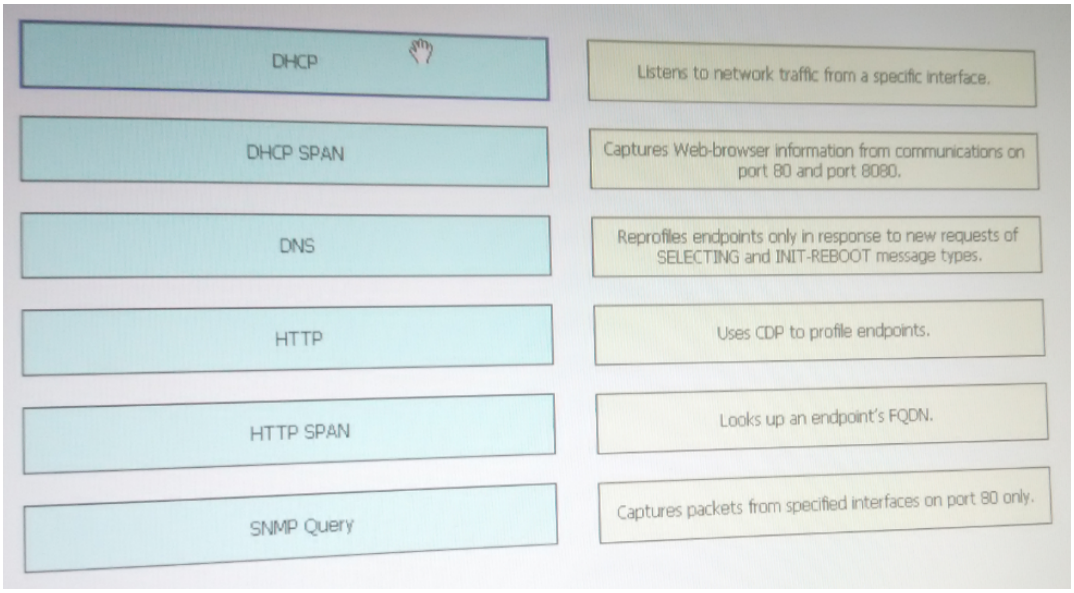
Which traffic class is defined for non-business-relevant applications and receives any bandwidth that remains after QoS policies have been applied?

**A.** scavenger class
**B.** best effort
**C.** discard eligible
**D.** priority queued

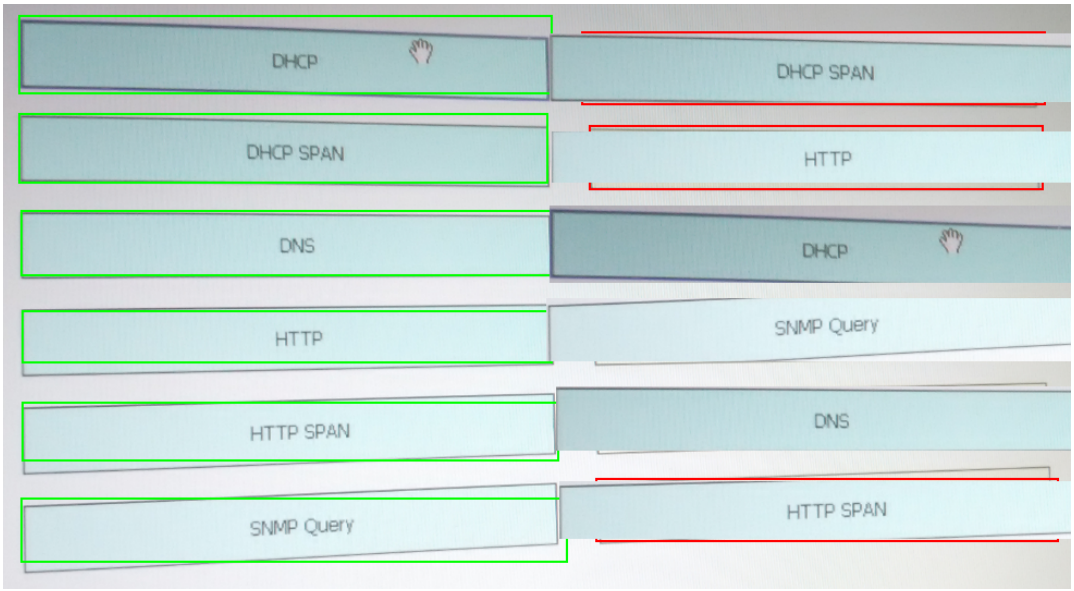
**Answer: A**

## Question No : 6 DRAG DROP

Drag each ISE probe on the left to the matching statement on the right.




**Answer:**




**Explanation:**

1x32x13x54x25x66x4
http://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_010101.html

**Question No : 7**

Which transport mechanism is used between a RADIUS authenticator and a RADIUS authentication server?

**A.** UDP, with only the password in the Access-Request packet encrypted
**B.** UDP, with the whole packet body encrypted
**C.** TCP, with only the password in the Access-Request packet encrypted
**D.** EAPOL, with TLS encrypting the entire packet
**E.** UDP RADIUS encapsulated in the EAP mode enforced by the authentication server.

**Answer: A**

## Question No : 8

What are three scanning engine that the Cisco IronPort dynamic vectoring and streaming engine can use to protect against malware? (Choose three)

**A.** McAfee
**B.** F-Secure
**C.** TrendMicro
**D.** Symantec
**E.** Webroot
**F.** Sophos

**Answer: A,E,F**

## Question No : 9

You are preparing Control Plane Protection configurations for implementation on the router, which has the EBGP peering address 1.1.1.2. Which ACL statement can you use to classify the related traffic into the EBGP traffic compartment?

**A.** permit tcp host 1.1.1.1 gt 1024 host 1.1.1.2 eq bgp
permit tcp host 1.1.1.1 eq bgp host 1.1.1.2 gt 1024
**B.** permit tcp host 1.1.1.2 gt 1024 host 1.1.1.2 eq bgp
permit tcp host 1.1.1.2 eq bgp host 1.1.1.2 gt 1024
**C.** permit tcp host 10.1.1.1 gt 1024 host 10.1.1.2 eq bgp
permit tcp host 10.1.1.1 eq bgp host 10.1.1.2 gt 1024
**D.** permit tcp host 1.1.1.1 gt 1024 host 1.1.1.1 eq bgp
permit tcp host 1.1.1.1 eq bgp host 1.1.1.1 gt 1024

**Answer: A**

**Question No : 10**

Which three statements are true regarding RFC 5176 (Change of Authorization)? (Choose three.)

**A.** It defines a mechanism to allow a RADIUS server to initiate a communication inbound to a NAD.
**B.** It defines a wide variety of authorization actions, including "reauthenticate."
**C.** It defines the format for a Change of Authorization packet.
**D.** It defines a DM.
**E.** It specifies that TCP port 3799 be used for transport of Change of Authorization packets.

**Answer: A,C,D**

**Question No : 11**

What is the default duration of IPS anomaly detection's learning accept mode?

**A.** 12 hours
**B.** 48 hours
**C.** 24 hours
**D.** 8 hours

**Answer: C**

**Explanation:**

Although anomaly detection is in detect mode by default, it conducts an initial learning accept mode for the default period of 24 hours.
Reference:
http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-1/user/guide/CSMUserGuide_wrapper/ipsanom.html

**Question No : 12**

Aggregate global IPv6 addresses begin with which bit pattern in the first 16-bit group?

**A.** 000/3
**B.** 001/3
**C.** 010/2
**D.** 011/2

**Answer: B**

**Question No : 13**

Which two statements about ASA transparent mode are true? (Choose two.)

**A.** Transparent mose acts as a Layer-3 firewall.
**B.** The inside and outside interface must be in a different subnet.
**C.** IP traffic will not pass unless it is permitted by an access-list.
**D.** ARP traffic is dropped unless it is permitted.
**E.** A configured route applies only to the traffic that is originated by the ASA.
**F.** In multiple context mode, all contexts need to be in transparent mode.

**Answer: C,E**

**Question No : 14**

Which three options are the types of zones that are defined for anomaly detection on the Cisco IPS Sensor? (Choose three.)

**A.** inside
**B.** outside
**C.** internal
**D.** external
**E.** illegal
**F.** baseline

**Answer: C,D,E**

**Question No : 15**

Which method of output queuing is supported on the Cisco ASA appliance?

**A.** CBWFQ
**B.** priority queuing
**C.** MDRR
**D.** WFQ
**E.** custom queuing

**Answer: B**

**Question No : 16**

Refer to the exhibit.

```
crypto ipsec transform-set Hub-Spoke esp-aes esp-sha-hmac
!
crypto ipsec profile Hub-Spoke
 set transform-set Hub-Spoke
!
interface Tunnel0
 ip address 192.168.10.1 255.255.255.0
 no ip redirects
 no ip next-hop-self eigrp 101
 ip nhrp map multicast dynamic
 ip nhrp network-id 10
 no ip split-horizon eigrp 101
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 1000
 tunnel protection ipsec profile Hub-Spoke
```

Which three descriptions of the configuration are true? (Choose three.)

**A.** The configuration is on the NHS.
**B.** The tunnel IP address represents the NBMA address.
**C.** This tunnel is a point-to-point GRE tunnel.
**D.** The tunnel is not providing peer authentication.
**E.** The configuration is on the NHC.
**F.** The tunnel encapsulates multicast traffic.
**G.** The tunnel provides data confidentiality.

**Answer: A,F,G**

**Question No : 17**

IKEv2 provides greater network attack resiliency against a DoS attack than IKEv1 by utilizing which two functionalities? (Choose two)

**A.** An IKEv2 responder does not initiate a DH exchange until the initiator responds with a cookie.
**B.** IKEv2 interoperates with IKEv1 to increase security in IKEv1.
**C.** IKEv2 only allows certificates for peer authentication.
**D.** With cookie challenge, IKEv2 does not track the state of the initiator until the initiator responds with a cookie.
**E.** IKEv2 only allows symmetric keys for peer authentication.
**F.** IKEv2 performs TCP intercept on all secure connections.

**Answer: A,D**

**Explanation:** http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113597-ptn-113597.html

**Question No : 18**

Which algorithm is used to generate the IKEv2 session key?

**A.** Diffie-Hellman
**B.** Rivest, Shamir, and Adleman
**C.** Secure Hash Algorithm
**D.** Rivest Cipher 4

**Answer: A**

**Question No : 19**

With the Cisco FlexVPN solution, which four VPN deployments are supported? (Choose four.)

**A.** site-to-site IPsec tunnels?

**B.** dynamic spoke-to-spoke IPSec tunnels? (partial mesh)
**C.** remote access from software or hardware IPsec clients?
**D.** distributed full mesh IPsec tunnels?
**E.** IPsec group encryption using GDOI?
**F.** hub-and-spoke IPsec tunnels?

**Answer: A,B,C,F**

**Question No : 20**

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

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

**Answer: A**

**Question No : 21**

Refer to the exhibit.