



**Vendor:** Cisco

**Exam Code:** 400-251

**Exam Name:** CCIE Security Written Exam v5.1

**Version:** DEMO

### QUESTION 1

Drag and drop the step in the Cisco ASA packet processing flow on the left into the correct order of operations on the right.

The egress interface counter is incremented.	Step 1
The input counter is incremented.	Step 2
The packet arrives at the ingress interface.	Step 3
The packet is forwarded to the egress interface.	Step 4
The packet is checked against the global (or interface) ACL.	Step 5
The packet is checked against existing translation rules.	Step 6

**Answer:**

The egress interface counter is incremented.	The packet arrives at the ingress interface.
The input counter is incremented.	The input counter is incremented.
The packet arrives at the ingress interface.	The packet is checked against the global (or interface) ACL.
The packet is forwarded to the egress interface.	The packet is checked against existing translation rules.
The packet is checked against the global (or interface) ACL.	The packet is forwarded to the egress interface.
The packet is checked against existing translation rules.	The egress interface counter is incremented.

### QUESTION 2

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 3

You have configured a DMVPN hub and spoke as follows (assume the IPsec profile "dmvpnprofile" is configured correctly):

```
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
```

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?

- A. Configure the ipnhrp cache non-authoritative command on the hub's tunnel interface
- B. Modify the NHRP hold times to match on the hub and spoke
- C. Modify the NHRP network IDs to match on the hub and spoke
- D. Modify the tunnel keys to match on the hub and spoke

**Answer: D**

#### QUESTION 5

Which two options are unicast address types for IPv6 addressing? (Choose two)

- A. Established
- B. Static
- C. Global
- D. Dynamic
- E. Link-local

**Answer: CE**

#### QUESTION 6

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

```
R1
interface Loopback0
 ip address 1.1.1.1 255.255.255.0
interface FastEthernet0/0
 ip address 10.10.10.1 255.255.255.0
router bgp 100
 no synchronization
 bgp router-id 1.1.1.1
 neighbor 2.2.2.2 remote-as 200
 neighbor 2.2.2.2 ebgp-multihop 2
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 2.2.2.2 maximum-prefix 200
 no auto-summary

R2
interface Loopback0
 ip address 2.2.2.2 255.255.255.0
interface FastEthernet0/0
 ip address 10.10.10.2 255.255.255.0
router bgp 100
 no synchronization
 bgp router-id 2.2.2.2
 neighbor 1.1.1.1 remote-as 200
 neighbor 1.1.1.1 ebgp-multihop 2
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 1.1.1.1 maximum-prefix 200 50 warning-only
 no auto-summary
```

- A. The BGP neighbor session tears down after R1 receives 100 prefixes from the neighbor 1.1.1.1
- B. The BGP neighbor session between R1 and R2 re-establishes after 50 minutes
- C. A warning message is displayed on R2 after it receives 50 prefixes
- D. A warning message is displayed on R2 after it receives 100 prefixes from neighbor 1.1.1.1
- E. The BGP neighbor session tears down after R1 receives 200 prefixes from neighbor 2.2.2.2
- F. The BGP neighbor session between R1 and R2 re-establishes after 100 minutes

**Answer: DE**

#### QUESTION 7

From the list below, which one is the major benefit of AMP Threat GRID?

- A. AMP Threat Grid collects file information from customer servers and run tests on them to see if they are infected with viruses
- B. AMP Threat Grid learns ONLY from data you pass on your network and not from anything else to monitor for suspicious behavior. This makes the system much faster and efficient

- C. AMP Threat Grid combines Static, and Dynamic Malware analysis with threat intelligence into one combined solution
- D. AMP Threat Grid analyzes suspicious behavior in your network against exactly 400 behavioral indicators

**Answer:** C

#### **QUESTION 8**

Which two characteristics of DTLS are true? (Choose two)

- A. It includes a congestion control mechanism
- B. It supports long data transfers and connections data transfers
- C. It completes key negotiation and bulk data transfer over a single channel
- D. It is used mostly by applications that use application layer object-security protocols
- E. It includes a retransmission method because it uses an unreliable datagram transport
- F. It cannot be used if NAT exists along the path

**Answer:** AE

#### **QUESTION 9**

Which two of the following ICMP types and code should be allowed in a firewall to enable traceroute? (Choose two)

- A. Destination Unreachable-protocol Unreachable
- B. Destination Unreachable-port Unreachable
- C. Time Exceeded-Time to Live exceeded in Transit
- D. Redirect-Redirect Datagram for the Host
- E. Time Exceeded-Fragment Reassembly Time Exceeded
- F. Redirect-Redirect Datagram for the Type of service and Host

**Answer:** BC

#### **QUESTION 10**

Which three Cisco attributes for LDAP authorization are supported on the ASA? (Choose three)

- A. L2TP-Encryption
- B. Web-VPN-ACL-Filters
- C. IPsec-Client-Firewall-Filter-Name
- D. Authenticated-User-Idle-Timeout
- E. IPsec-Default-Domain
- F. Authorization-Type

**Answer:** BDE

#### **QUESTION 11**

Which two statements about global ACLs are true? (Choose two)

- A. They support an implicit deny

- B. They are applied globally instead of being replicated on each interface
- C. They override individual interface access rules
- D. They require an explicit deny
- E. They can filter different packet types than extended ACLs
- F. They require class-map configuration

**Answer:** AB

#### **QUESTION 12**

When TCP intercept is enabled in its default mode, how does it react to a SYN request?

- A. It intercepts the SYN before it reaches the server and responds with a SYN-ACK
- B. It drops the connection
- C. It monitors the attempted connection and drops it if it fails to establish within 30 seconds
- D. It allows the connection without inspection
- E. It monitors the sequence of SYN, SYN-ACK, and ACK messages until the connection is fully established

**Answer:** E

#### **QUESTION 13**

Which two statements about IPsec in a NAT-enabled environment are true? (Choose two)

- A. The hashes of each peer's IP address and port number are compared to determine whether NAT-T is required
- B. NAT-T is not supported when IPsec Phase 1 is set to Aggressive Mode
- C. The first two messages of IPsec Phase 2 are used to determine whether the remote host supports NAT-T
- D. IPsec packets are encapsulated in UDP 500 or UDP 10000 packets
- E. To prevent translations from expiring, NAT keepalive messages that include a payload are sent between the peers

**Answer:** AD

## Thank You for Trying Our Product

### PassLeader Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.passleader.com/all-products.html>



**10% Discount Coupon Code: STNAR2014**