



**Vendor:** Cisco

**Exam Code:** 400-251

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

**Version:** DEMO

### QUESTION 1

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

- A. CA servers must support GetCACaps response messages in order to implement extended functionality
- B. The GetCRL exchange is signed and encrypted only in the response direction.
- C. It is vulnerable to downgrade attacks on its cryptographic capabilities
- D. The GetCert exchange is signed and encrypted only in the response direction.
- E. The GetCACaps response message supports DES encryption and the SHA-128 hashing algorithm.

**Answer:** AC

### QUESTION 2

Which two events can cause a failover event on an active/standby setup? (Choose two.)

- A. The active unit experiences interface failure above the threshold.
- B. The unit that was previously active recovers.
- C. The stateful failover link fails.
- D. The failover link fails.
- E. The active unit fails

**Answer:** AE

### QUESTION 3

Which two statements about the MACsec security protocol are true? (choose two.)

- A. Stations broadcast an MKA heartbeat that contains the key server priority
- B. The SAK is secured by 128 bit AES-GCM by default
- C. When switch-to-switch link security is configured in manual mode, the SAP operation mode must be set to GCM
- D. MACsec is not supported in MDA mode.
- E. MKA heartbeats are sent at a default interval of 3 seconds.

**Answer:** AB

### QUESTION 4

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

- A. It can summarize discontinuous IP addresses.
- B. It can easily be added to existing networks
- C. it can increase the convergence of the network
- D. It reduces the number of routes
- E. It prevents unnecessary routing updates at the summarization boundary if one of the routes in the summary is unstable.

**Answer:** DE

### QUESTION 5

Refer to the exhibit. Which meaning of this error message on a Cisco ASA is true?

```
%ASA-6-110001: No route to <dest_address> from <source_address>
```

- A. The route map redistribution is configured incorrectly.
- B. The default route is undefined.
- C. A packet was denied and dropped by an ACL.
- D. The host is connected directly to the firewall

**Answer: B**

#### QUESTION 6

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

- A. The administrator can configure the allow-default command to force the routing table to use only the default route
- B. It is not supported on the Cisco ASA security appliance.
- C. The administrator can configure the ip verify unicast source reachable-via any command to enable the RPF check to work routing groups.
- D. The administrator can use the show cef interface command to determine whether uRPF is enabled
- E. In strict mode, only one routing path can be available to reach network devices on a subnet

**Answer: DE**

#### QUESTION 7

Which type of header attack is detected by Cisco ASA basic threat detection?

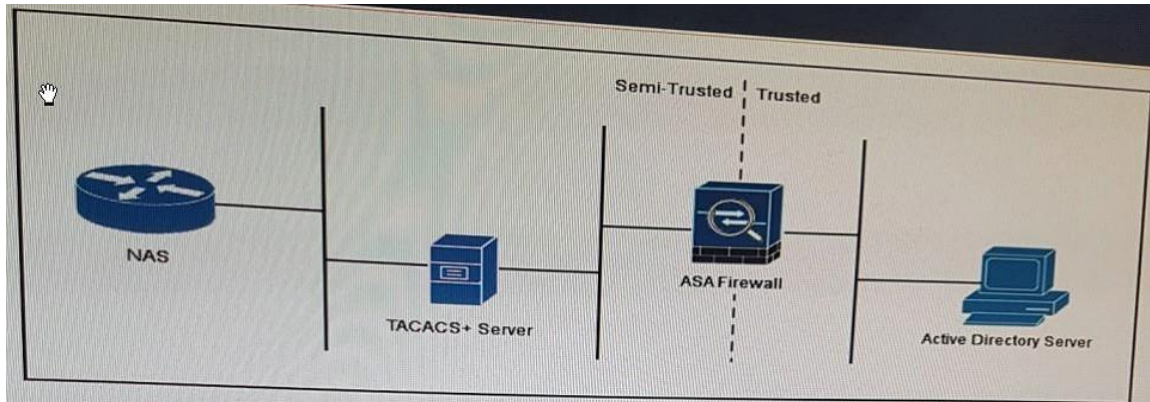
- A. connection limit exceeded
- B. denial by access list
- C. failed application inspection
- D. bad packet format

**Answer: D**

#### QUESTION 8

Refer to the exhibit. A user authenticates to the NAS, which communicates to the VACACS+ server authentication. The TACACS+ SERVER Then accesses the Active Directory Server through the ASA firewall to validate the user credentials.

Which protocol-port pair must be allowed access through the ASA firewall?



- A. SMB over TCP 455
- B. DNS over UDP 53
- C. LDAP over UDP 389
- D. global catalog over UDP 3268
- E. TACACS+ over TCP 49
- F. DNS over TCP 53

**Answer: C**

#### 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

### Lead2pass 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.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives®

**10% Discount Coupon Code: ASTR14**