

**HIGHER QUALITY  
BETTER SERVICE**

# CERTTREE

---

QUESTION & ANSWER



Provide One Year  
Free Update!

<https://www.certtree.com>

**Exam : 350-701**

**Title :** Implementing and Operating  
Cisco Security Core  
Technologies (SCOR)

**Version : DEMO**

1.What is a characteristic of traffic storm control behavior?

- A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
- B. Traffic storm control cannot determine if the packet is unicast or broadcast.
- C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
- D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

**Answer: A**

2.An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address.

Which list contains the allowed recipient addresses?

- A. SAT
- B. BAT
- C. HAT
- D. RAT

**Answer: D**

3.Refer to the exhibit.

```
*Jun 30 14:52:33.795: ISAKMP:(1002): retransmission skipped for phase 1 (time
since last transmission 504)
R1#
*Jun 30 16:52:40.183: ISAKMP:(1001):purging SA., sa=68CEE050, delme=68CEE056
R1#
*Jun 30 16:52:43.291: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 14:52:43.291: ISAKMP (1002): incrementing error counter on sa, attempt 5
of 5: retransmit phase 1
*Jun 30 14:52:43.295: ISAKMP:(1002): retransmitting phase 1 MH_KEY_EXCH
*Jun 30 14:52:43.295: ISAKMP:(1002): sending packet to 10.10.12.2 my_port 500
peer_port 500 (I) MM_KEY_EXCH
*Jun 30 14:52:43.295: ISAKMP:(1002):Sending an IKE IPv4 Packet.
R1#
*Jun 30 14:52:53.299: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 14:52:53.299: ISAKMP:(1002): peer does not do paranoid keepalives.

*Jun 30 14:52:53.299: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 14:52:53.303: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 14:52:53.307: ISAKMP: Unlocking peer struct 0x48207318 for
isadb_mark_sa_deleted(), count 0
*Jun 30 14:52:53.307: ISAKMP: Deleting peer node by peer_reap for 10.10.12.2:
68207318
*Jun 30 14:52:53.311: ISAKMP:(1002):deleting node 79075537 error FALSE reason "IKE
deleted"
R1#
*Jun 30 14:52:53.311: ISAKMP:(1002):deleting node -484575753 error FALSE reason
"IKE deleted"
*Jun 30 14:52:53.315: ISAKMP:(1002):Input = IKE_MSG_INTERNAL, IKE_PHASE1_DEL
*Jun 30 14:52:53.319: ISAKMP:(1002):Old State = IKE_I_MM5 New State = IKE_DEST_SA
```

A network administrator configured a site-to-site VPN tunnel between two Cisco IOS routers, and hosts are unable to communicate between two sites of VPN. The network administrator runs the debug crypto isakmp sa command to track VPN status.

What is the problem according to this command output?

- A. hashing algorithm mismatch
- B. encryption algorithm mismatch
- C. authentication key mismatch
- D. interesting traffic was not applied

**Answer: C**

4.Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two)

- A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS
- B. Cisco FTDv with one management interface and two traffic interfaces configured
- C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises
- D. Cisco FTDv with two management interfaces and one traffic interface configured
- E. Cisco FTDv configured in routed mode and IPv6 configured

**Answer: A,C**

5.What are two list types within AMP for Endpoints Outbreak Control? (Choose two)

- A. blocked ports
- B. simple custom detections
- C. command and control
- D. allowed applications
- E. URL

**Answer: B,D**

**Explanation:**

Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists. A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine. Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company

Reference: <https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf>