



**Vendor:** Cisco

**Exam Code:** 350-018

**Exam Name:** CCIE Security Written Exam v4.1

**Version:** DEMO

### QUESTION 1

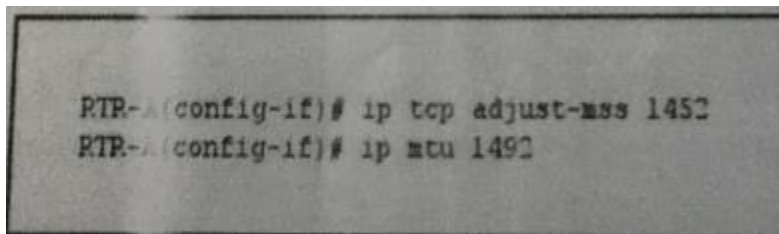
The computer at 10.10.10.4 on your network has been infected by a botnet that directs traffic to a malware site at 168.65.201.120. Assuming that filtering will be performed on a Cisco ASA. What command can you use to block all current and future connections from the infected host?

- A. ip access-list extended BLOCK\_BOT\_OUT deny ip any host 10.10.10.4
- B. shun 168.65.201.120 10.10.10.4 6000 80
- C. ip access-list extended BLOCK\_BOT\_OUT deny ip host 10.10.10.4 host 168.65.201.120
- D. shun 10.10.10.4 168.65.201.120 6000 80

**Answer: B**

### QUESTION 2

Refer to the exhibit. Which effect of this configuration is true?

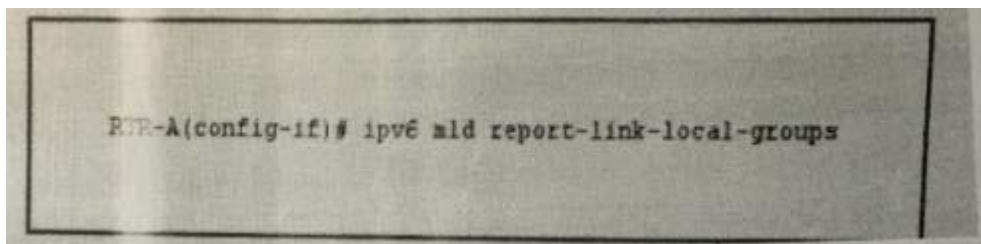


- A. The MSS of TCP SYN packets is set to 1452 bytes and the IP MTU of the interface is set to 1942 bytes
- B. The maximum size of TCP SYN+ACK packets passing the transient host is set to 1452 bytes and the IP MTU of the interface is set to 1492 bytes
- C. The PMTUD values sets itself to 1452 bytes when the interface MTU is set to 1492 bytes
- D. SYN packets carries 1452 bytes in the payload when the Ethernet MTU of the interface is to 1492 bytes
- E. The maximum size of TCP SYN+ACK packets passing the router is set to 452 bytes and the IP MTU of the interface is set to 1492 bytes

**Answer: A**

### QUESTION 3

Refer to the exhibit. Which effect of this configuration is true?



- A. It configures the node to generate a link-local group report when it joins the solicited-node multicast group
- B. It enables local group membership for MLDv1 and MLDv2
- C. It enables hosts to send MLD report messages for groups in 224.0.0.0/24

- D. It enables MLD query messages for all link-local groups
- E. It enables the host to send MLD report messages for nonlink local groups

**Answer: C**

#### QUESTION 4

You have configured an ASA firewall in multiple context mode. If the context are sharing an Interface.

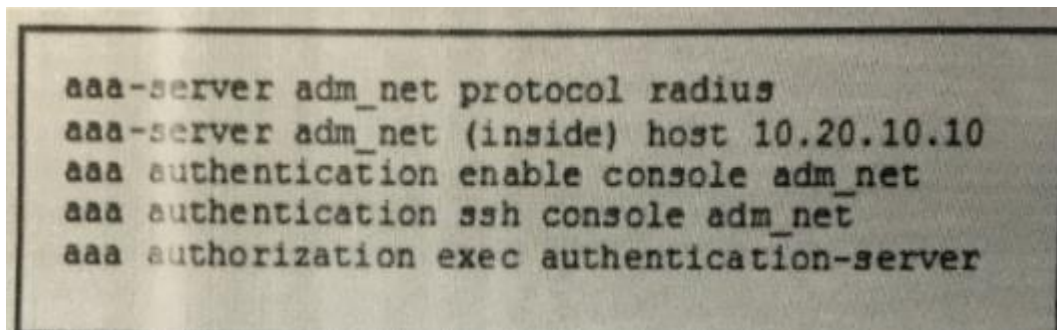
What are two of the actions you could take to classify packets to the appropriate Context?  
(Choose two)

- A. Enable DHCP
- B. Disable MAC auto-generation and adding unique IP addresses to each interface
- C. Enable MAC auto-generation globally
- D. Assign a unique MAC address to each interface
- E. Apply QoS to each interface

**Answer: CD**

#### QUESTION 5

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



```
aaa-server adm_net protocol radius
aaa-server adm_net (inside) host 10.20.10.10
aaa authentication enable console adm_net
aaa authentication ssh console adm_net
aaa authorization exec authentication-server
```

- A. It requires the enable password to be authorized by the LOCAL database
- B. It allows users to log in with any user name in the LOCAL database
- C. It enables management authorization for a user-authenticated RADIUS server
- D. Users will be authenticated against the RADIUS servers defined in the adm\_net list
- E. It allows SSH connections to console login into the ASA

**Answer: D**

#### QUESTION 6

What feature enables extended secure access form non-secure physical locations?

- A. NEAT
- B. 802.1X port-based authentication
- C. port security
- D. storm-control
- E. CBAC

**Answer: A**

**QUESTION 7**

What are the two technologies that support AFT?(Choose two)

- A. NAT-6to 4
- B. NAT-PT
- C. DNAT
- D. NAT64
- E. NAT-PMP
- F. SNAT

**Answer: BD**

**QUESTION 8**

On an ASA firewall in multiple context mode running version 8.X, what is the default number of VPN site-to-site tunnels per context?

- A. 2 sessions
- B. 4 sessions
- C. 1 session
- D. 0 sessions

**Answer: A**

**QUESTION 9**

Which three statements about Unicast RPF in strict mode and loose mode are true? (Choose three)

- A. Inadvertent packet loss can occur when loose mode is used with asymmetrical routing
- B. Interface in strict mode drop traffic with return routes that point to the Null 0 interface
- C. Strict mode requires a default route to be associated with the uplink network interface
- D. Loose mode requires the source address to be present in the routing table
- E. Both loose and strict modes are configured globally on the router
- F. Strict mode is recommended on interfaces that will receive packets only from the same subnet to which the interface is assigned

**Answer: BDF**

**QUESTION 10**

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

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

F. TrendMicro

Answer: ABE

**QUESTION 11**

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 screenshot shows a drag-and-drop interface with two columns. The left column contains six light blue boxes with the following text from top to bottom: "The egress interface counter is incremented.", "The input counter is incremented.", "The packet arrives at the ingress interface.", "The packet is forwarded to the egress interface.", "The packet is checked against the global (or interface) ACL.", and "The packet is checked against existing translation rules.". The right column contains six light yellow boxes labeled "Step 1" through "Step 6" from top to bottom.

Answer:

The screenshot shows the same drag-and-drop interface as above, but with the boxes rearranged to show the correct sequence. The left column (source boxes) remains the same as in the question. The right column (target boxes) now contains the following text from top to bottom: "The packet arrives at the ingress interface.", "The input counter is incremented.", "The packet is checked against the global (or interface) ACL.", "The packet is checked against existing translation rules.", "The packet is forwarded to the egress interface.", and "The egress interface counter is incremented.".

## 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**