IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **642-532**

Title : Securing Networks Using Intrusion Prevention Systems Exam (IPS)

Version : DEMO

1.Which three steps must you perform to prepare sensor interfaces for inline operations? (Choose three.)

A.Disable all interfaces except the inline pair.

B.Add the inline pair to the default virtual sensor.

C.Enable two interfaces for the pair.

D.Disable any interfaces that are operating in promiscuous mode.

E.Create the interface pair.

F.Configure an alternate TCP-reset interface

Correct:B C E

2.Your Cisco router is hosting an NM-CIDS. The router configuration contains an inbound ACL. Which action does the router take when it receives a packet that should be dropped, according to the inbound ACL?

A.The router forwards the packet to the NM-CIDS for inspection, then drops the packet.

B.The router drops the packet and does not forward it to the NM-CIDS for inspection.

C.The router filters the packet through the inbound ACL, tags it for drop action, and forwards the packet to the NM-CIDS. Then the router drops it if it triggers any signature, even a signature with no action configured.

D.The router filters the packet through the inbound ACL, forwards the packet to the NM-CIDS for inspection only if it is an ICMP packet, and then drops the packet.

Correct:B

3.Which action is available only to signatures supported by the Normalizer engine

A.Produce Verbose Alert

B.Modify Packet Inline

C.Deny Packet Inline

D.Log Pair Packets

E.Request SNMP Trap

F.Reset TCP Connection

Correct:B

4.You would like to have your inline sensor deny attackers inline when events occur that have Risk Ratings over 85. Which two actions will accomplish this? (Choose two.)

A.Create Target Value Ratings of 85 to 100.

B.Create an Event Variable for the protected network.

C.Enable Event Action Overrides.

D.Create an Event Action Filter, and assign the Risk Rating range of 85 to 100 to the filter.

E.Enable Event Action Filters.

F.Assign the Risk Rating range of 85 to 100 to the Deny Attacker Inline event action.

Correct:C F

5.Which two are appropriate installation points for a Cisco IPS sensor? (Choose two.)

A.on publicly accessible servers

B.on critical network servers

C.at network entry points

D.on user desktops

E.on corporate mail servers

F.on critical network segments

Correct:C F

6.In which three ways does a Cisco network sensor protect network devices from attacks? (Choose three.)

A.It uses a blend of intrusion detection technologies to detect malicious network activity.

B.It can generate an alert when it detects traffic that matches a set of rules that pertain to typical intrusion activity.

C.It permits or denies traffic into the protected network that is based on access lists that you create on the sensor.

D.It can take a variety of actions when it detects traffic that matches a set of rules that pertain to typical intrusion activity.

E.It uses behavior-based technology that focuses on the behavior of applications to protect network devices from known attacks and from new attacks for which there is no known signature.

Correct:A B D

7.Which command displays the statistics for Fast Ethernet interface 0/1?

A.show interfaces FastEthernet0/1

B.show interface int1

C.show statistics FastEthernet0/1

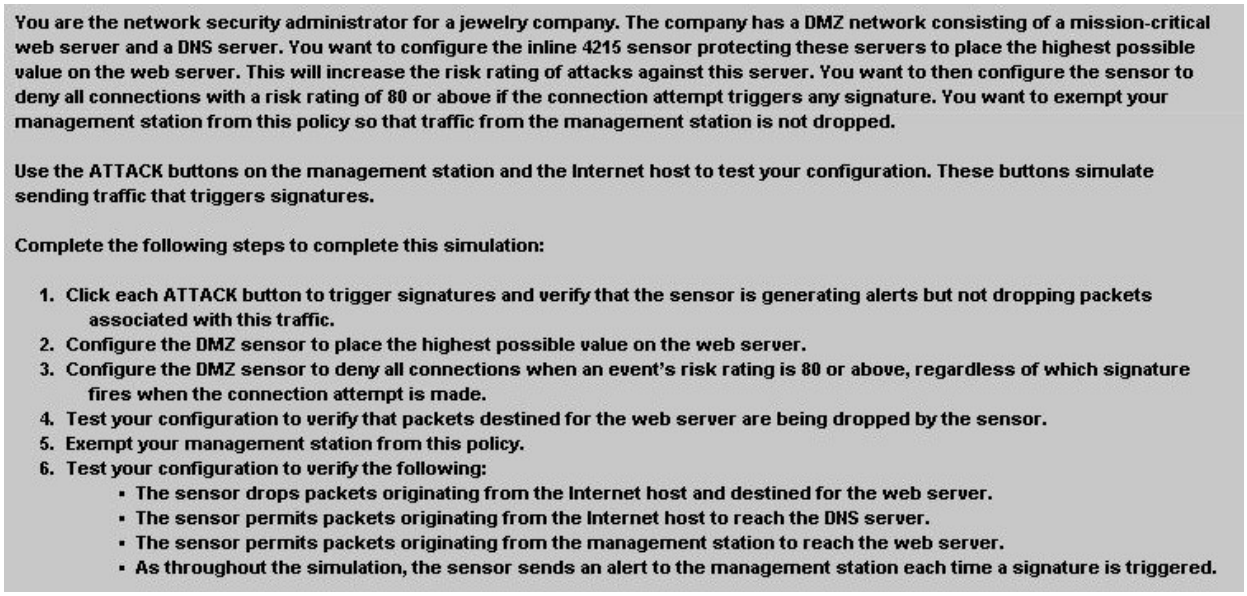
D.show statistics virtual-sensor

E.packet capture FastEthernet0/1

F.show statistics event-store

Correct:A

8.Drag Drop question



Correct:

9.What is a configurable weight that is associated with the perceived importance of a network asset?

A.Risk Rating

B.parameter value

C.Target Value Rating

D.severity level

E.storage key
F.rate parameter
Correct:C

10.You are using multiple monitoring interfaces on a sensor appliance running software version 5.0. Which statement is true?

A.You can have the simultaneous protection of multiple network subnets, which is like having multiple sensors in a single appliance.
B.You can use different sensing configurations for each monitoring interface.
C.You can enable an interface only if the interface belongs to an interface group.
D.Multiple monitoring interfaces can be assigned to Group 0 at any given time.
E.All interfaces must operate in a single mode; you cannot mix inline- and promiscuous-mode operations.
Correct:A