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 : **642-533**

Title : Implementing Cisco Intrusion Prevention System (IPS)

Version : Demo

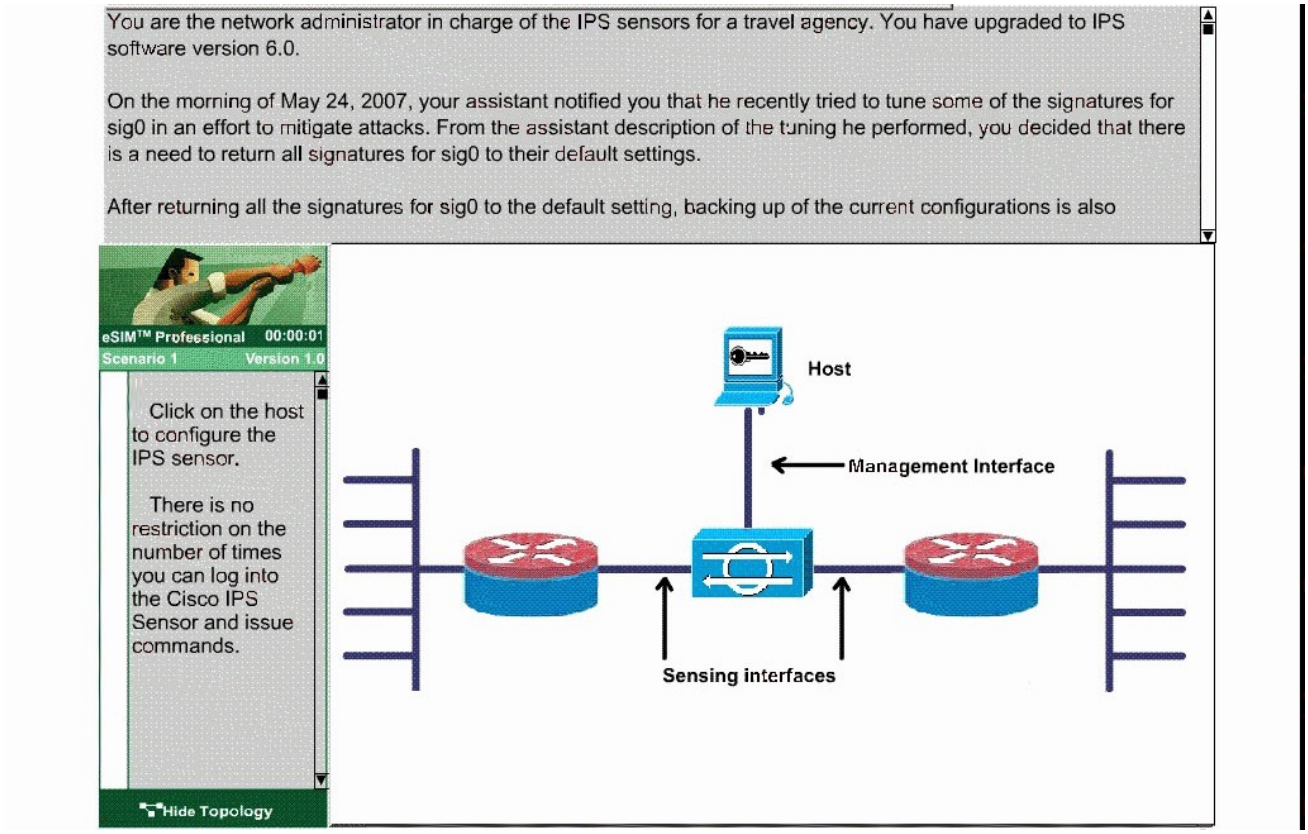
1. You think users on your corporate network are disguising the use of file-sharing applications by tunneling the traffic through port 80. How can you configure your Cisco IPS Sensor to identify and stop this activity?
A. Enable all signatures in the Service HTTP engine.
B. Assign the Deny Packet Inline action to all signatures in the Service HTTP engine.
C. Enable all signatures in the Service HTTP engine. Then create an event action override that adds the Deny Packet Inline action to events triggered by these signatures if the traffic originates from your corporate network.
D. Enable the alarm for the non-HTTP traffic signature. Then create an Event Action Override that adds the Deny Packet Inline action to events triggered by the signature if the traffic originates from your corporate network.
E. Enable both the HTTP application policy and the alarm on non-HTTP traffic signature. Answer: E

2. A user with which user account role on a Cisco IPS Sensor can log into the native operating system shell for advanced troubleshooting purposes when directed to do so by Cisco TAC?
A. administrator
B. operator
C. viewer
D. service
E. root
F. super
Answer: D

3. Which character must precede a variable to indicate that you are using a variable rather than a string?
A. percent sign
B. dollar sign
C. ampersand
D. pound sign
E. asterisk
Answer: B

4. Which statement accurately describes Cisco IPS Sensor automatic signature and service pack updates?
A. The Cisco IPS Sensor can automatically download service pack and signature updates from Cisco.com.
B. The Cisco IPS Sensor can download signature and service pack updates only from an FTP or HTTP server.
C. You must download service pack and signature updates from Cisco.com to a locally accessible server before they can be automatically applied to your Cisco IPS Sensor.
D. When you configure automatic updates, the Cisco IPS Sensor checks Cisco.com for updates hourly.
E. If multiple signature or service pack updates are available when the sensor checks for an update, the Cisco IPS Sensor installs the first update it detects.
Answer: C

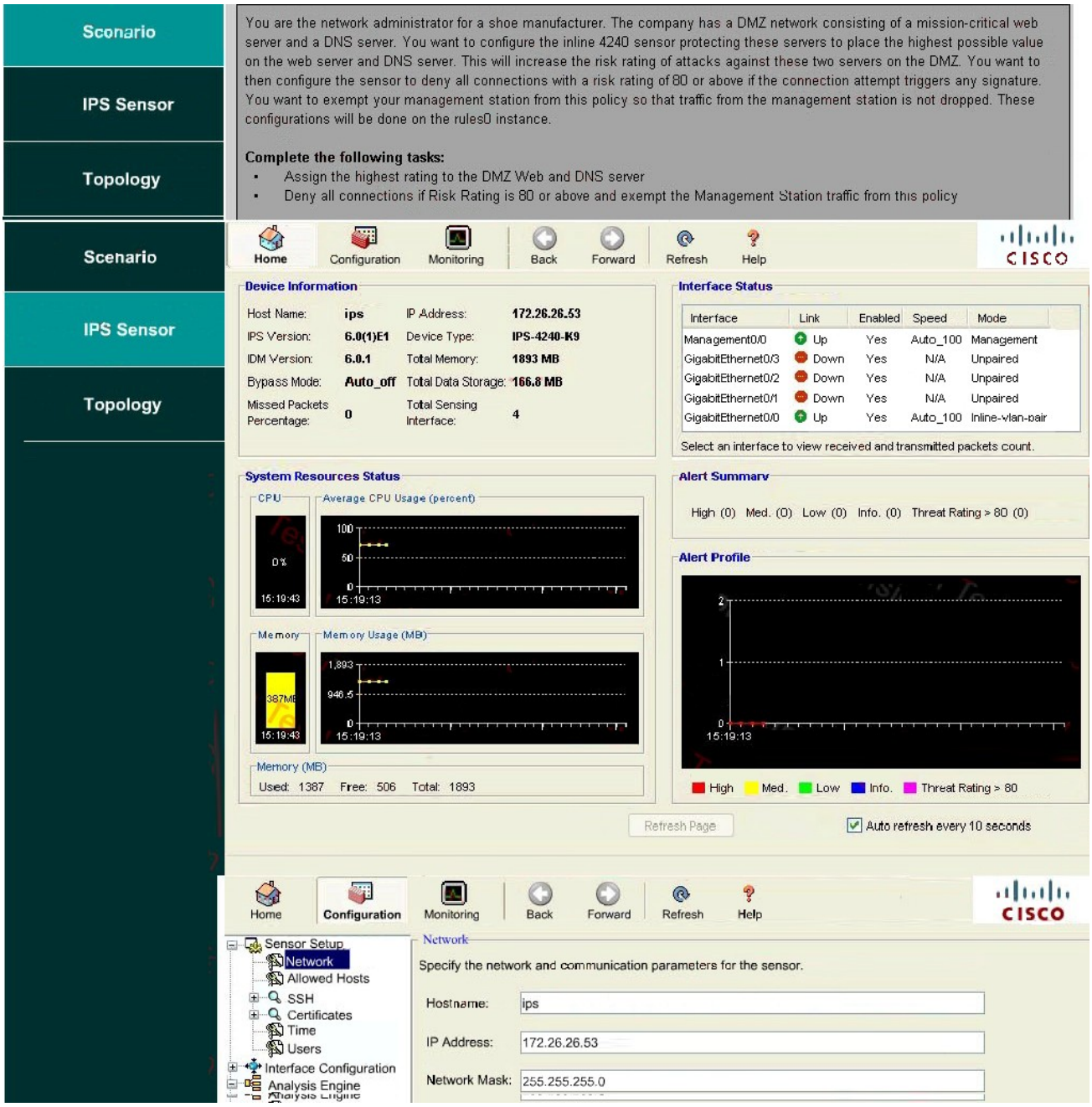
5. LAB

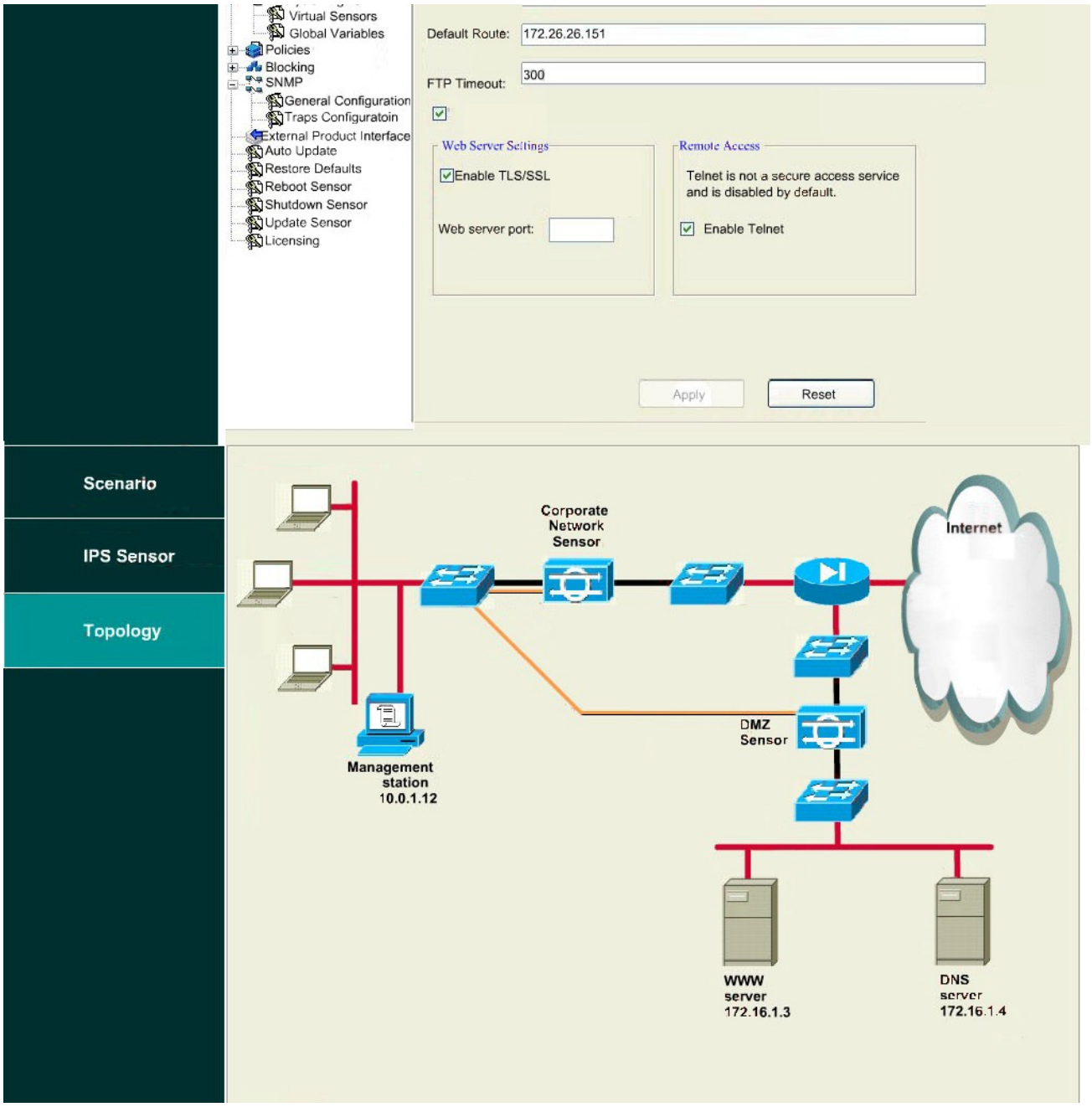


Answer: Sorry , No Correct Answer!

6. LAB

Answer: Sorry , No Correct Answer!


Sconario
IPS Sensor
Topology
You are the network administrator for a shoe manufacturer. The company has a DMZ network consisting of a mission-critical web server and a DNS server. You want to configure the inline 4240 sensor protecting these servers to place the highest possible value on the web server and DNS server. This will increase the risk rating of attacks against these two servers on the DMZ. You want to then configure the sensor to deny all connections with a risk rating of 80 or above if the connection attempt triggers any signature. You want to exempt your management station from this policy so that traffic from the management station is not dropped. These configurations will be done on the rules0 instance.
Complete the following tasks:
Assign the highest rating to the DMZ Web and DNS server
Deny all connections if Risk Rating is 80 or above and exempt the Management Station traffic from this policy
Scenario
IPS Sensor
Topology
Home
Configuration
Monitoring
Back
Forward
Refresh
Help
CISCO
Device Information
Host Name: ips
IP Address: 172.26.26.53
IPS Version: 6.0(1)E1
Device Type: IPS-4240-K9
IDM Version: 6.0.1
Total Memory: 1893 MB
Bypass Mode: Auto_off
Total Data Storage: 166.8 MB
Missed Packets Percentage: 0
Total Sensing Interface: 4
Interface Status
Interface Link Enabled Speed Mode
Management0/0 Up Yes Auto_100 Management
GigabitEthernet0/3 Down Yes N/A Unpaired
GigabitEthernet0/2 Down Yes N/A Unpaired
GigabitEthernet0/1 Down Yes N/A Unpaired
GigabitEthernet0/0 Up Yes Auto_100 Inline-vlan-pair
Select an interface to view received and transmitted packets count.
System Resources Status
CPU
Average CPU Usage (percent)
0%
15:19:43
100
50
0
15:19:13
Memory
Memory Usage (MB)
387MB
15:19:43
1,893
946.5
0
15:19:13
Memory (MB)
Used: 1387 Free: 506 Total: 1893
Alert Summary
High (0) Med. (0) Low (0) Info. (0) Threat Rating > 80 (0)
Alert Profile
2
1
0
15:19:13
High Med. Low Info. Threat Rating > 80
Refresh Page
Auto refresh every 10 seconds
Home
Configuration
Monitoring
Back
Forward
Refresh
Help
CISCO
Sensor Setup
Network
Allowed Hosts
SSH
Certificates
Time
Users
Interface Configuration
Analysis Engine
Network
Specify the network and communication parameters for the sensor.
Hostname: ips
IP Address: 172.26.26.53
Network Mask: 255.255.255.0



7. How can you clear events from the event store?

A. You do not need to clear the event store; it is a circular log file, so once it reaches the maximum size it will be overwritten by new events.

B. You must use the CLI clear events command.

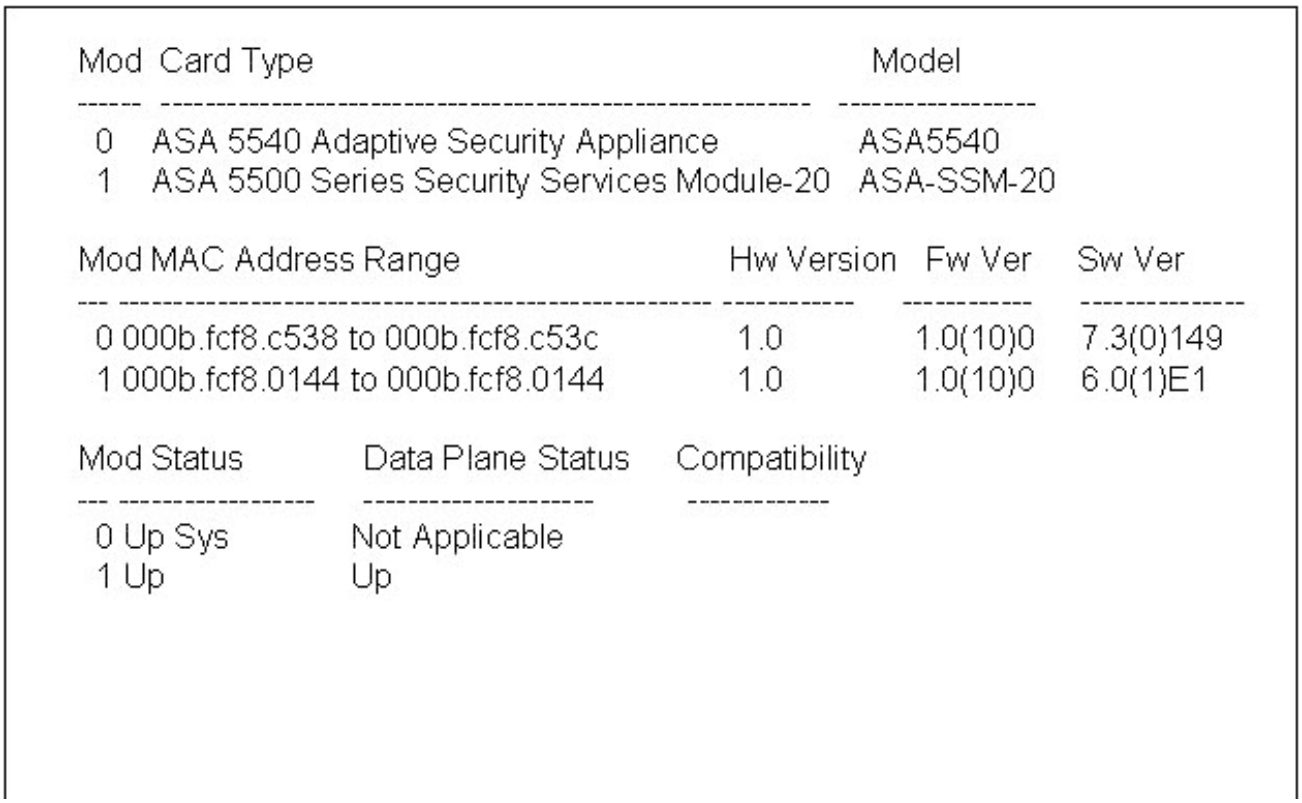
C. If you have Administrator privileges, you can do this by selecting Monitoring > Events > Reset button in Cisco IDM.

D. You should select File > Clear IDM Cache in Cisco IDM.

E. You cannot clear events from the event store; they must be moved off the system using the copy command.

Answer: B

8. Refer to the exhibit. Based on the partial output shown, which of these statements is true?



```
Mod  Card Type                                    Model
---  -------------------------------------------  ------------------
 0   ASA 5540 Adaptive Security Appliance         ASA5540
 1   ASA 5500 Series Security Services Module-20  ASA-SSM-20

Mod MAC Address Range                 Hw Version   Fw Ver      Sw Ver
--- --------------------------------- -----------  ----------  --------------
 0 000b.fcf8.c538 to 000b.fcf8.c53c   1.0          1.0(10)0    7.3(0)149
 1 000b.fcf8.0144 to 000b.fcf8.0144   1.0          1.0(10)0    6.0(1)E1

Mod Status          Data Plane Status    Compatibility
--- --------------- -------------------- -------------
 0 Up Sys           Not Applicable
 1 Up               Up
```

A. The module installed in slot 1 needs to be a type 5540 module to be compatible with the ASA 5540 Adaptive Security Appliance module type.
B. The module installed in slot 1 needs to be upgraded to the same software revision as module 0 or it will not be recognized.
C. Module 0 system services are not running.
D. There is a Cisco IPS security services module installed.
Answer: D

9. Which action does the copy /erase ftp://172.26.26.1/sensor_config01 current-config command perform?
A. erases the sensor_config01 file on the FTP server and replaces it with the current configuration file from the Cisco IPS Sensor
B. copies and saves the running configuration to the FTP server and replaces it with the source configuration file
C. overwrites the backup configuration and applies the source configuration file to the system default configuration
D. merges the source configuration file with the current configuration
Answer: C

10. Which of the following is a valid file name for a Cisco IPS 6.0 system image?
A. IPS-K9-pkg-6.0-sys_img.sys
B. IPS-4240-K9-img-6.0-sys.sys
C. IPS-K9-cd-11-a-6.0-1-E1.img

D. IPS-4240-K9-sys-1.1-a-6.0-1-E1.img
Answer: D