Exam Code: 642-533

Exam Name: Implementing Cisco Intrusion Prevention System (IPS)

Vendor: CISCO

Version: DEMO

Part: A

2: 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.
Correct Answers: E

3: 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
Correct Answers: D

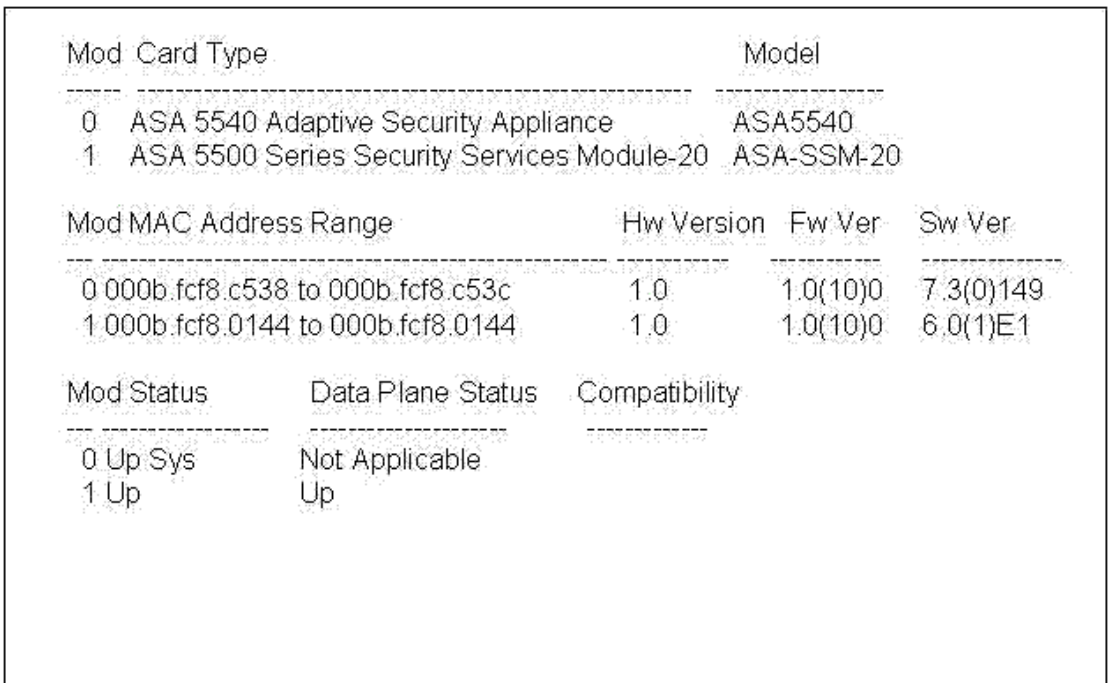
4: Which character must precede a variable to indicate that you are using a variable rather than a string?
A.percent sign
B.dollar sign
C.ampersand
D.pound sign
E.asterisk
Correct Answers: B

5: 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.
Correct Answers: C

6: 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.
Correct Answers: B

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



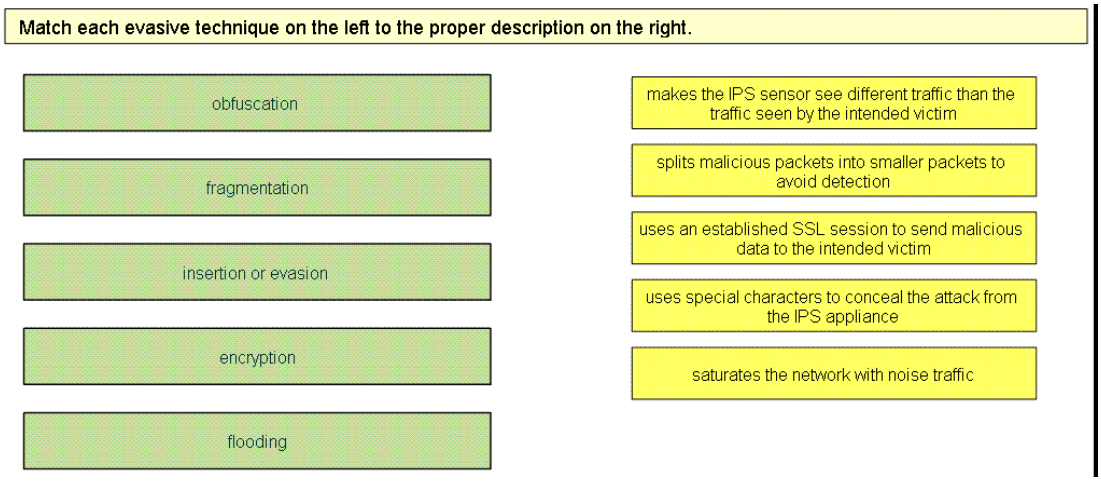
```
Mod  Card Type                                    Model
---- ------------------------------------------- ------------------
 0   ASA 5540 Adaptive Security Appliance        ASA5540
 1   ASA 5500 Series Security Services Module-20 ASA-SSM-20

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.
Correct Answers: D

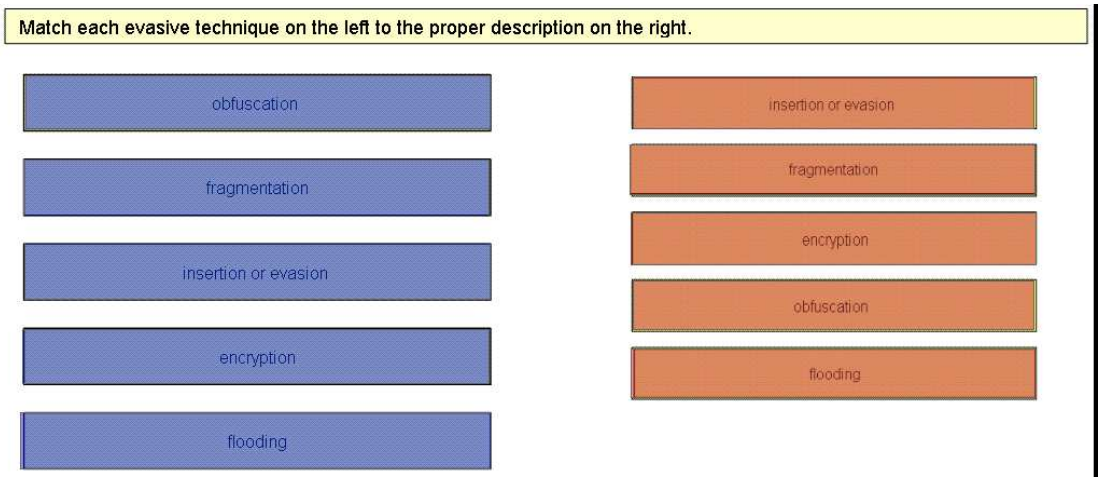
8: Which action does the copy /erase ftp://172.26.26.1/sensor_config01 current-config command perform?

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
Correct Answers: C

9: Drop



Correct Answers:



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
Correct Answers: D