Cisco 642-533

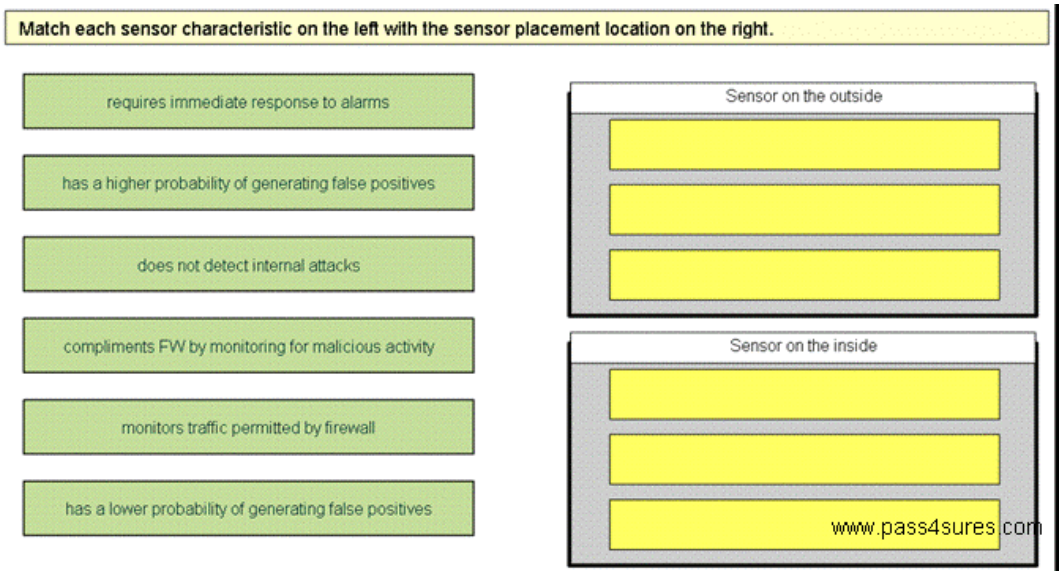
CISCO 642-533 Implementing Cisco Intrusion Prevention System (IPS)

Practice Test

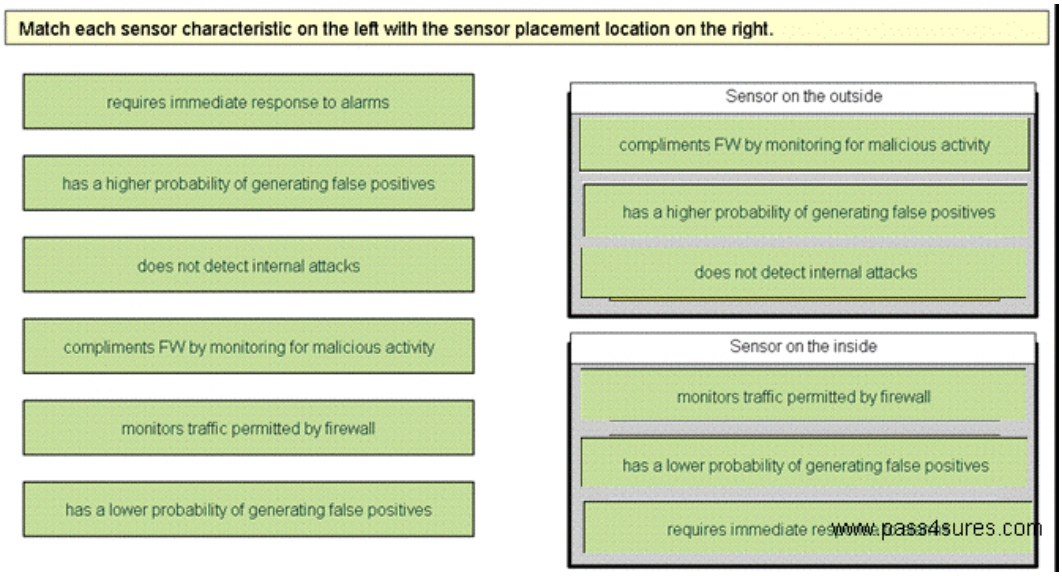
Version 1.9

QUESTION NO: 1 DRAG DROP

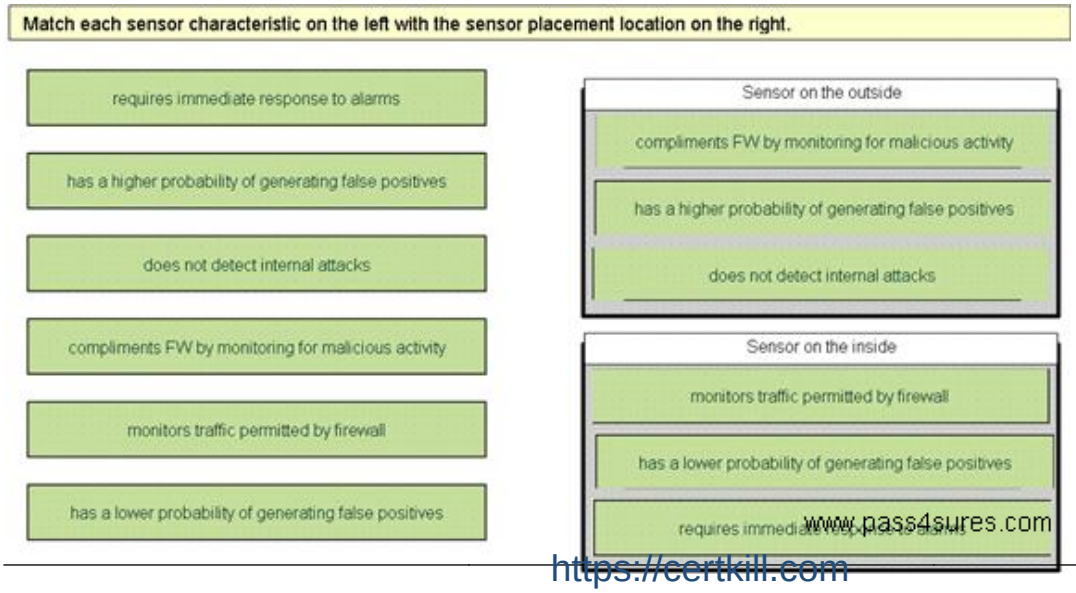
Drop



Answer:



Explanation:



QUESTION NO: 2

What is the best way to mitigate the risk that executable-code exploits will perform malicious acts such as erasing your hard drive?

A. assign blocking actions to signatures that are controlled by the State engine
B. assign deny actions to signatures that are controlled by the Trojan engines
C. assign the TCP reset action to signatures that are controlled by theNormalizer engine
D. enable blocking
E. enable application policy enforcement

Answer: B

QUESTION NO: 3

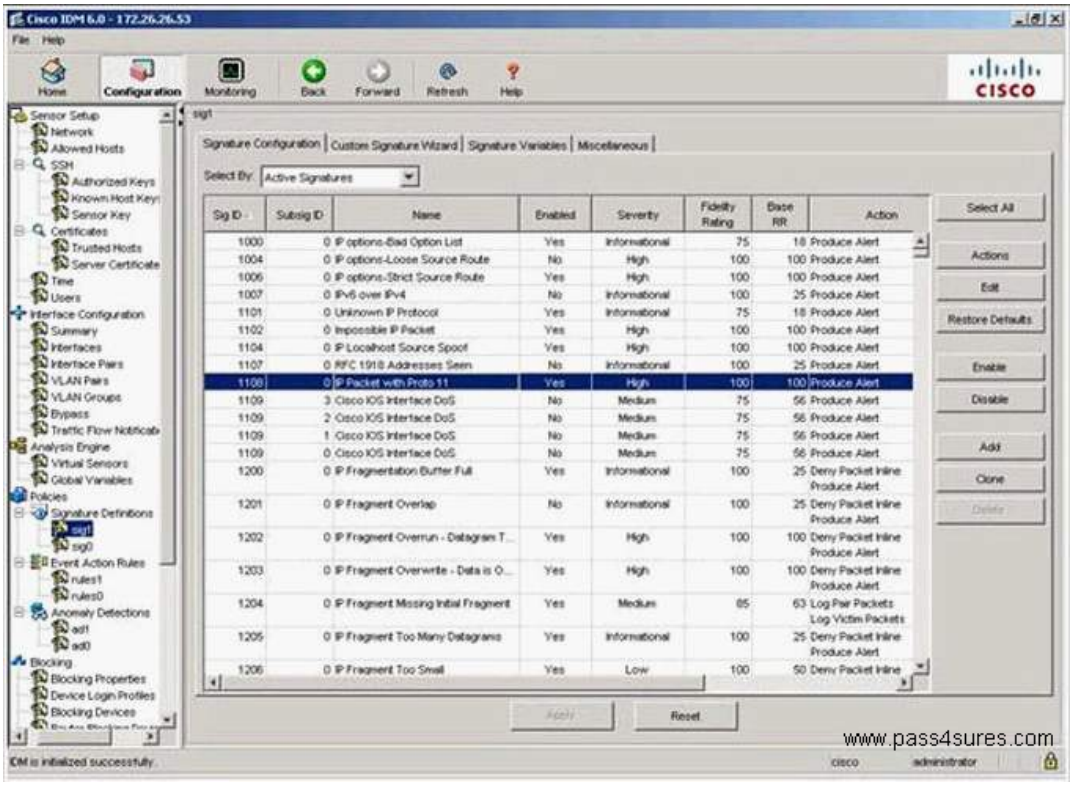
Which type of signature engine is best suited for creating custom signatures that inspect data at Layer 5 and above?

A. Service
B. AIC
C. String
D. Sweep
E. Flood
F. ATOMIC

Answer: A

QUESTION NO: 4

Refer to the exhibit. As an administrator, you need to change the Event Action and Event Count settings for signature 1108 in the sig1 instance. Which of the following should you select to view and change the required parameters?



A. Miscellaneous tab
B. Signature Variables tab
C. Actions button
D. Edit button

Answer: D

QUESTION NO: 5

You would like to investigate an incident and have already enabled the Log Pair Packets action on various signatures being triggered. What should you do next?

A. Use CLI to send the IP log to a PC using TFTP, thenopen it with Notepad to view and interpret the contents.
B. Use Cisco IDM to download the IP log to a management station then use a packet analyzer like Ethereal to decode the IP log.
C. Use the External Product Interface feature to download the IP log to Cisco Security MARS for incident investigation.
D. Use Cisco Security Manager to retrieve the IP log then use the Cisco Security Manager IPS Manager to decode the IP log.
E. Use Cisco IEV to retrieve the IP log then use the IEV Generate Reports function to produce a report based on the IP log content.

Answer: B

QUESTION NO: 6

Which signature action or actions should be selected to cause the attacker's traffic flow to terminate when the Cisco IPS Sensor is operating in promiscuous mode?

A. deny attacker
B. resettcp connection
C. deny connection
D. deny packet
E. deny packet, resettcp connection
F. deny connection, resettcp connection

Answer: B

QUESTION NO: 7

You are using Cisco IDM. What precaution must you keep in mind when adding, editing, or deleting allowed hosts on a Cisco IPS Sensor?

A. You must not allow entire subnets to access the Cisco IPS Sensor
B. You must not delete the IP address used for remote management.
C. When using access lists to permit remote access, you must specify the direction of allowed communications.
D. You can only configure the allowed hosts using the CLI.
E. You must use an inverse mask, such as 10.0.2.0 0.0.0.255, for the specified network mask for the IP address.

Answer: B

QUESTION NO: 8

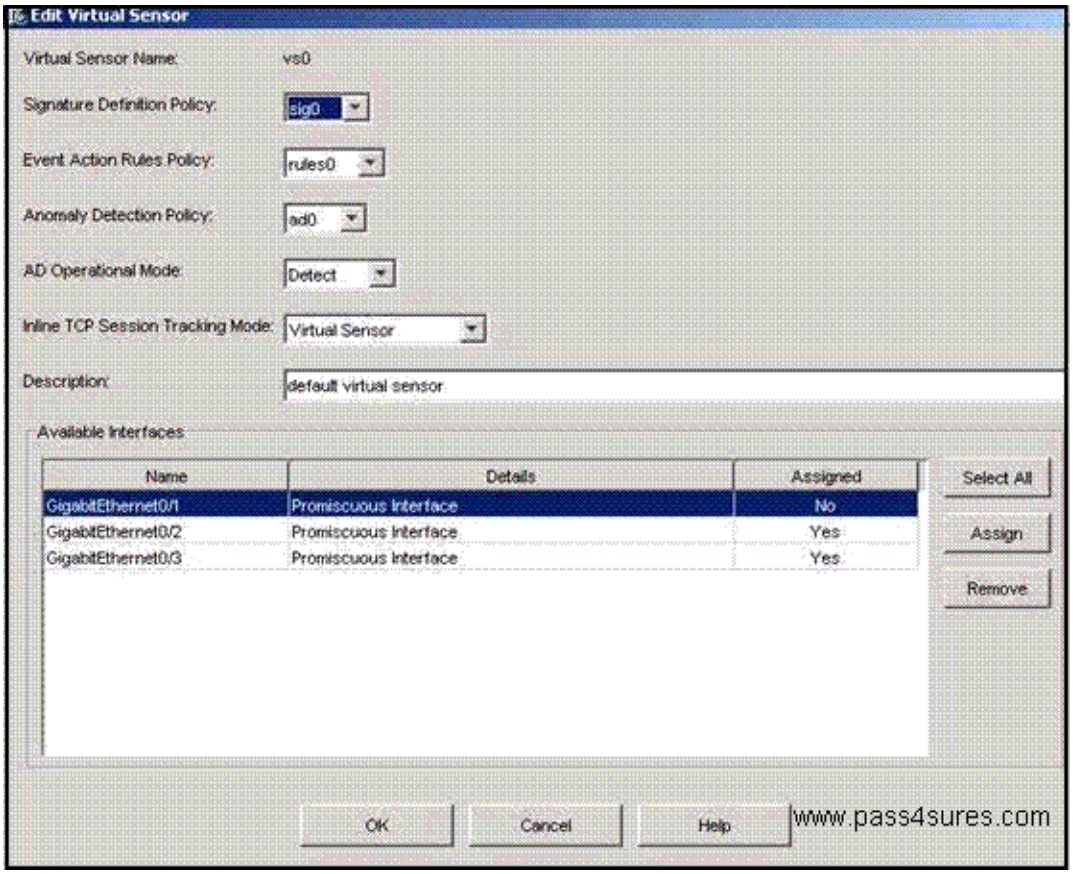
Which action does the copy /erase ftp://172.26.26.1/sensor_config01 current-config command perform?

A. erases the sensor_config01 file on the FTP server and replaces it with the current configuration file from the Cisco IPS Sensor
B. merges the source configuration file with the current configuration
C. copies and saves the running configuration to the FTP server and replaces it with the source configuration file
D. overwrites the backup configuration and applies the source configuration file to the system default configuration

Answer: D

QUESTION NO: 9

Refer to the exhibit. Which interfaces are assigned to an inline VLAN pair?



A. GigabitEthernet0/1 with GigabitEthernet0/3
B. None in this virtual sensor
C. GigabitEthernet0/1 with GigabitEthernet0/2
D. GigabitEthernet0/2 with GigabitEthernet0/3

Answer: B

QUESTION NO: 10

Which character must precede a variable to indicate that you are using a variable rather than a string?

A. percent sign
B. asterisk
C. dollar sign
D. pound sign

E. ampersand

Answer: C

QUESTION NO: 11

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

A. It can generate an alert when it detects traffic that matches a set of rules that pertain to typical intrusion activity.
B. It permits or denies traffic into the protected network based on access lists that you create on the sensor.
C. It uses a blend of intrusion detection technologies to detect malicious network activity.
D. 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.
E. It can take a variety of actions when it detects traffic that matches a set of rules that pertain to typical intrusion activity.
F. It uses anomaly detection technology to prevent evasive techniques such as obfuscation, fragmentation, and encryption.

Answer: A,C,E

QUESTION NO: 12

Which CLI mode allows you to tune signatures?

A. setup
B. global configuration
C. service signature-definition
D. privileged exec
E. service analysis-engine
F. virtual-sensor-configuration

Answer: C

QUESTION NO: 13

Select the two correct general Cisco IPS Sensor tuning recommendations if the environment consists exclusively of Windows servers. (Choose two.)

A. enable all IIS signatures
B. enable all NFS signatures
C. enable all RPC signatures
D. use "NT" IP fragment reassembly mode
E. disable deobfuscation for all HTTP signatures
F. use "Windows" TCP stream reassembly mode

Answer: A,D

QUESTION NO: 14

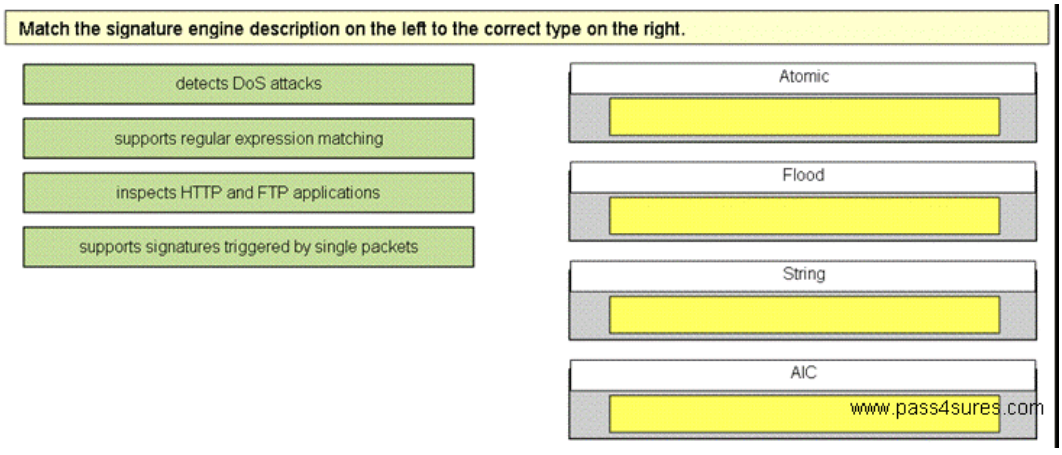
Which two management access methods are enabled by default on a Cisco IPS Sensor? (Choose two.)

A. HTTPS
B. SSH
C. IPsec
D. HTTP
E. Telnet

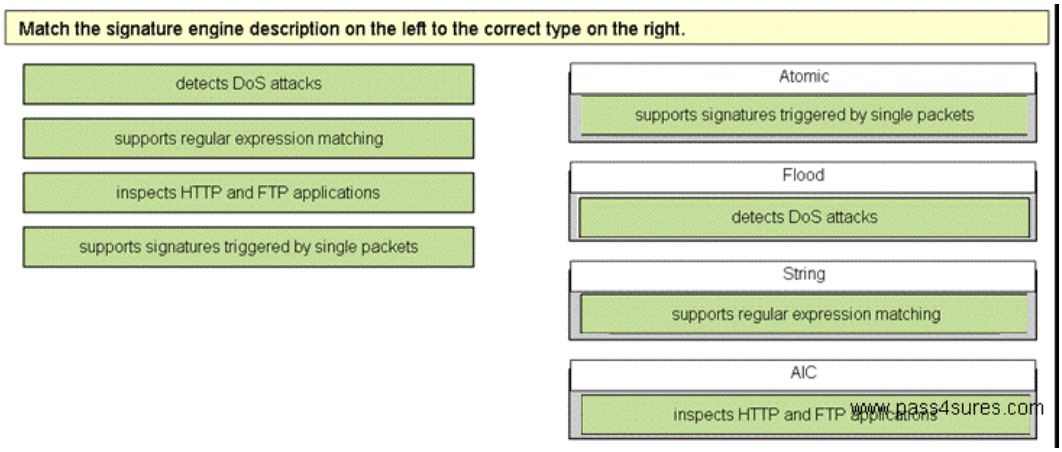
Answer: A,B

QUESTION NO: 15 DRAG DROP

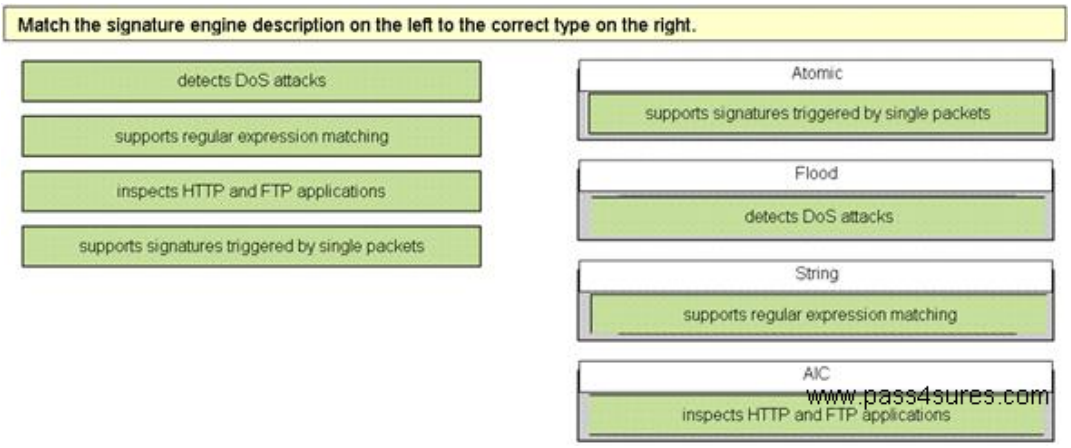
Drop



Answer:

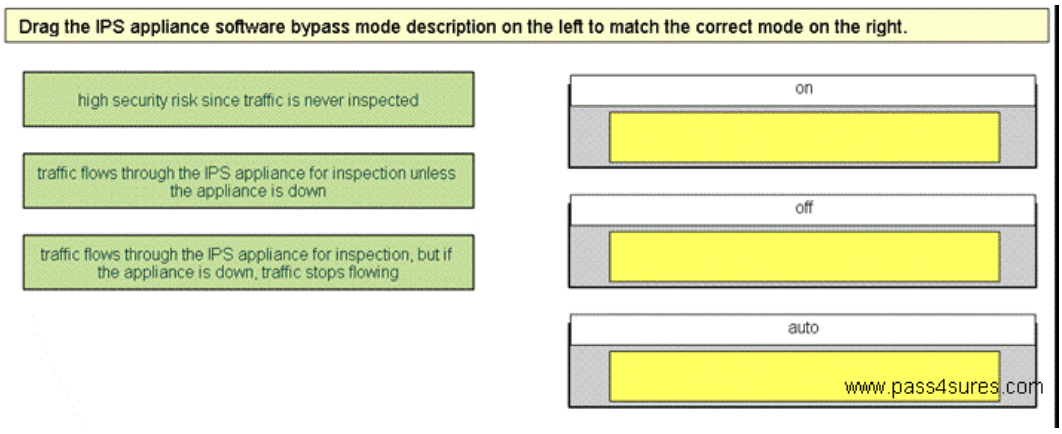


Explanation:

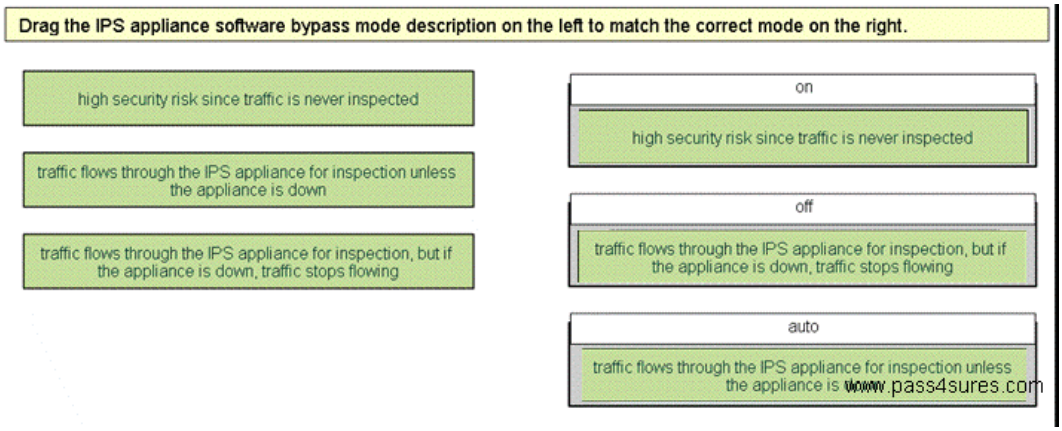


QUESTION NO: 16 DRAG DROP

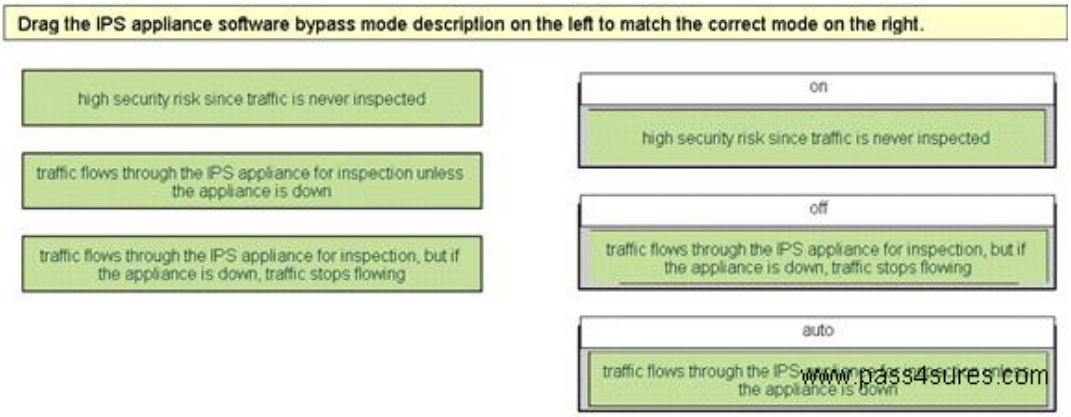
Drop



Answer:



Explanation:



QUESTION NO: 17

In which three of these ways can you achieve better Cisco IPS Sensor performance? (Choose three.)

A. enable selective packet capture using VLAN ACL on the Cisco IPS 4200 Series Sensors
B. alwaysenable unidirectional capture
C. have multiple Cisco IPS Sensors in the path and configure them to detect different types of events
D. disable unneeded signatures
E. place the Cisco IPS Sensor behind a firewall
F. enable all anti-evasive measures to reduce noise

Answer: C,D,E

QUESTION NO: 18

You have been made aware of new and unwanted traffic on your network. You want to create a signature to monitor and perform an action against that traffic when certain thresholds are reached. What would be the best way to configure this new signature?