642-627 Q&As

Implementing Cisco Intrusion Prevention System v7.0

Pass Cisco 642-627 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

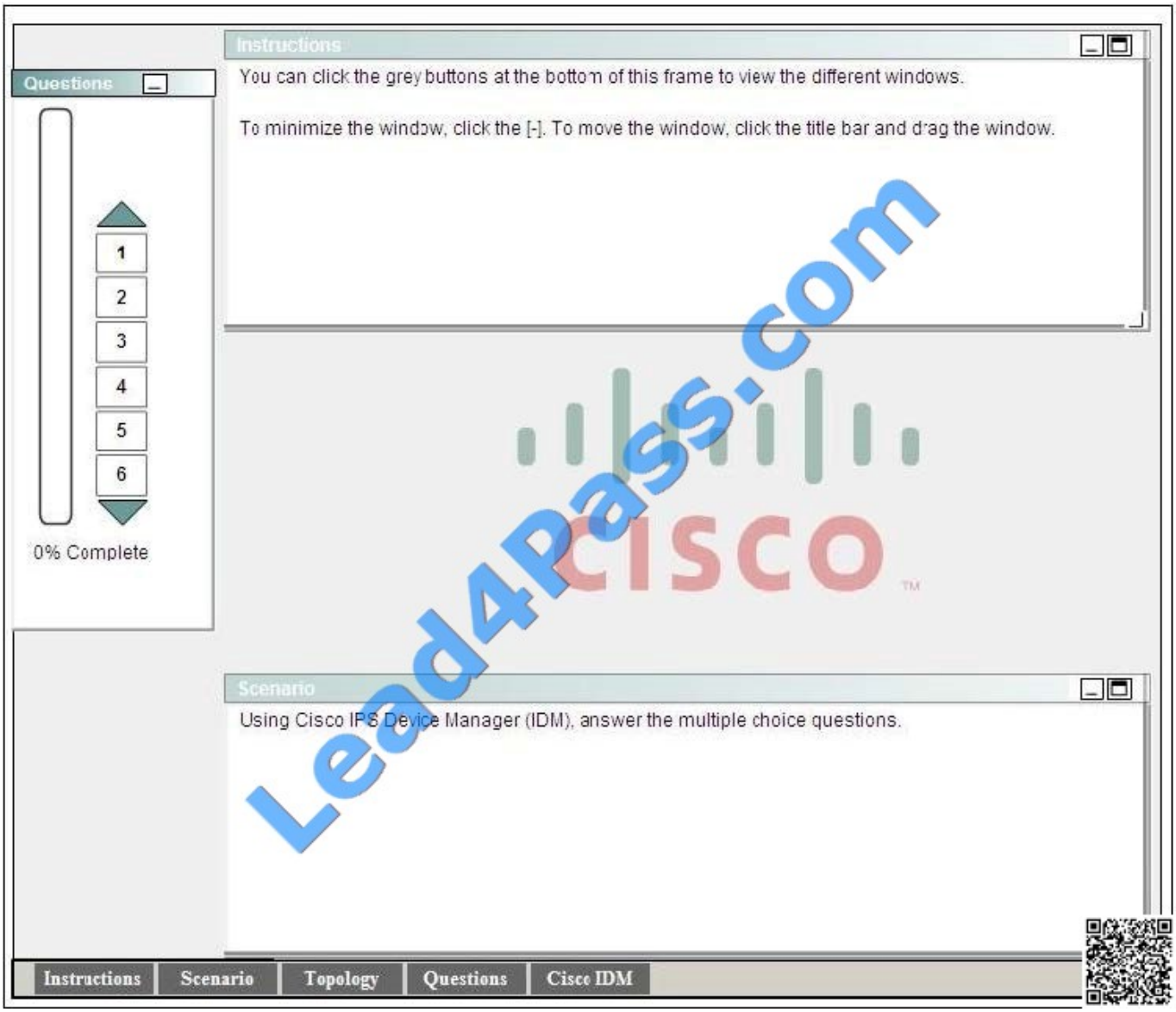
https://www.lead4pass.com/642-627.html

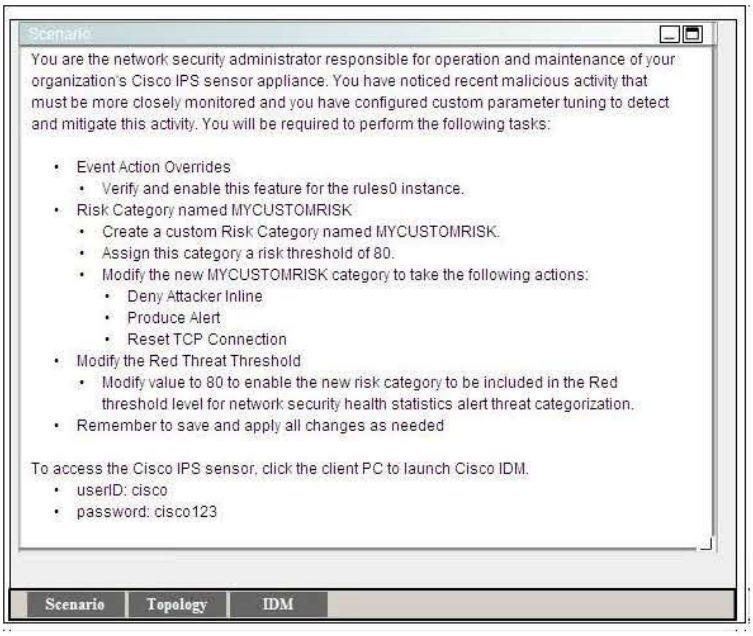
100% Passing Guarantee
100% Money Back Assurance

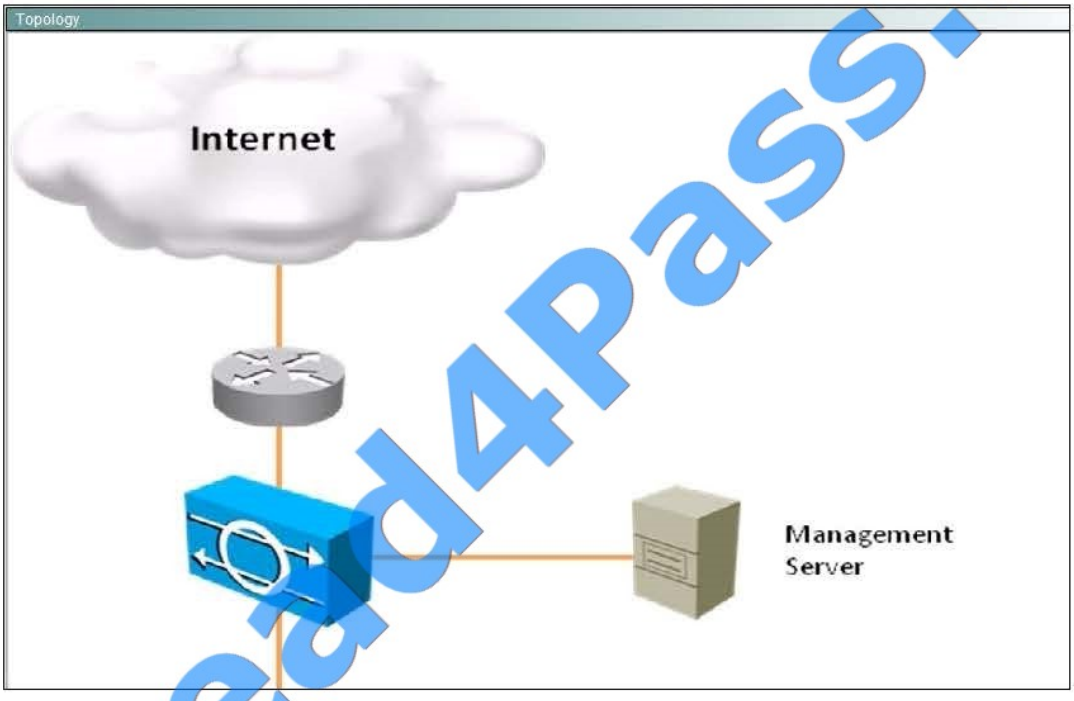
Following Questions and Answers are all new published by Cisco Official Exam Center

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

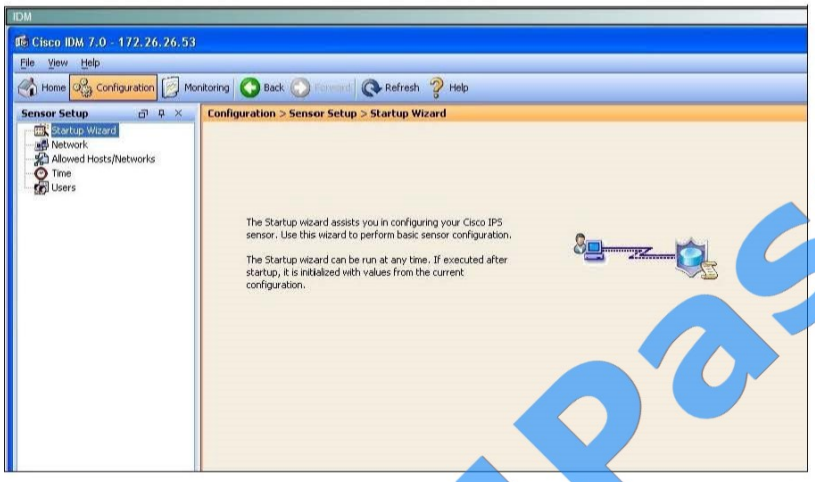

Instructions
Questions
You can click the grey buttons at the bottom of this frame to view the different windows.
To minimize the window, click the [-]. To move the window, click the title bar and drag the window.
1
2
3
4
5
6
0% Complete
Scenario
Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.
Instructions
Scenario
Topology
Questions
Cisco IDM

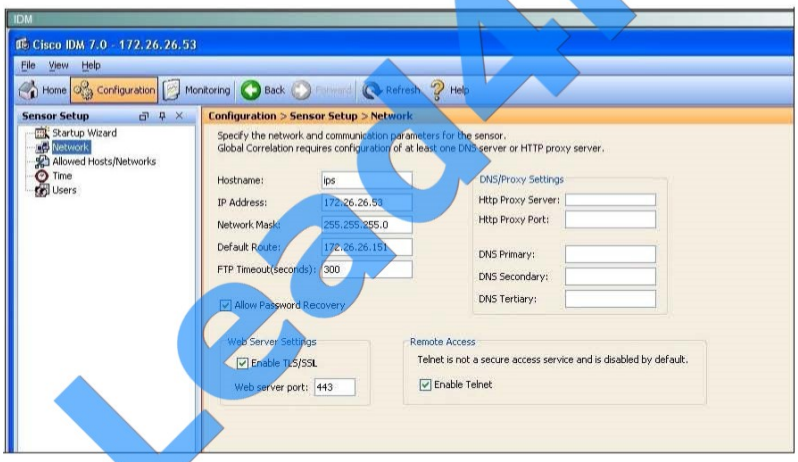


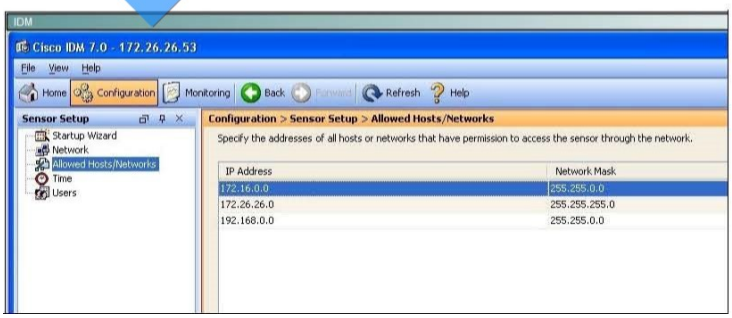


Lead4Pass.co


IDM
Cisco IDM 7.0 - 172.26.26.53
File View Help
Home Configuration Monitoring Back Forward Refresh Help
Home
Health Dashboard
Add Gadgets Add Das
Sensor Information - sensor
Updated 11:37:35 AM
Host Name: ips
IP Address: 172.26.26.53
IPS Version: 7.0(2)E3
Device Type: IPS-4240-K9
In Bypass: No
Total Memory: 1984 MB
Total Sensing Interfaces: 4
Total Data Storage: 788 MB
Analysis Engine Status: Running Normally
Sensor Health - sensor
Sensor Health
Network Security Health
Details
Critical
Normal
CPU, Memory, & Load - sensor
Inspection Load
CPU Usage
CPU 0%
Memory Usage
System 71%
Analysis Engine 23%
Disk Usage
boot 61%
system 44%
application-log 24%
application-data 28%
Licensing - sensor
License Status: No License
Signature Version: 425.0
Released On: Aug 16, 2009 8:00:00 PM EDT
Applied On: Oct 15, 2009 3:43:54 PM EDT
Auto Update Status: Not Checked


IDM
Cisco IDM 7.0 - 172.26.26.53
File View Help
Home Configuration Monitoring Back Forward Refresh Help
Sensor Setup
Startup Wizard
Network
Allowed Hosts/Networks
Time
Users
Configuration > Sensor Setup > Startup Wizard
The Startup wizard assists you in configuring your Cisco IPS sensor. Use this wizard to perform basic sensor configuration.
The Startup wizard can be run at any time. If executed after startup, it is initialized with values from the current configuration.


IDM
Cisco IDM 7.0 - 172.26.26.53
File View Help
Home Configuration Monitoring Back Forward Refresh Help
Sensor Setup
Startup Wizard
Network
Allowed Hosts/Networks
Time
Users
Configuration > Sensor Setup > Network
Specify the network and communication parameters for the sensor.
Global Correlation requires configuration of at least one DNS server or HTTP proxy server.
Hostname: ips
IP Address: 172.26.26.53
Network Mask: 255.255.255.0
Default Route: 172.26.26.151
FTP Timeout(seconds): 300
Allow Password Recovery
DNS/Proxy Settings
Http Proxy Server:
Http Proxy Port:
DNS Primary:
DNS Secondary:
DNS Tertiary:
Web Server Settings
Enable TLS/SSL
Web server port: 443
Remote Access
Telnet is not a secure access service and is disabled by default.
Enable Telnet


IDM
Cisco IDM 7.0 - 172.26.26.53
File View Help
Home Configuration Monitoring Back Forward Refresh Help
Sensor Setup
Startup Wizard
Network
Allowed Hosts/Networks
Time
Users
Configuration > Sensor Setup > Allowed Hosts/Networks
Specify the addresses of all hosts or networks that have permission to access the sensor through the network.
IP Address
Network Mask
172.16.0.0
255.255.0.0
172.26.26.0
255.255.255.0
192.168.0.0
255.255.0.0

Lead4Pass

What action will the sensortake regarding IP addresses listed as known bad hosts in the Cisco SensorBase network?

A. Global correlation is configured in Audit mode for testing the feature without actually denying any hosts.

B. Global correlation is configured in Aggressive mode, which has a very aggressive effect on deny actions.

C. It will not adjust risk rating values based on the known bad hosts list.

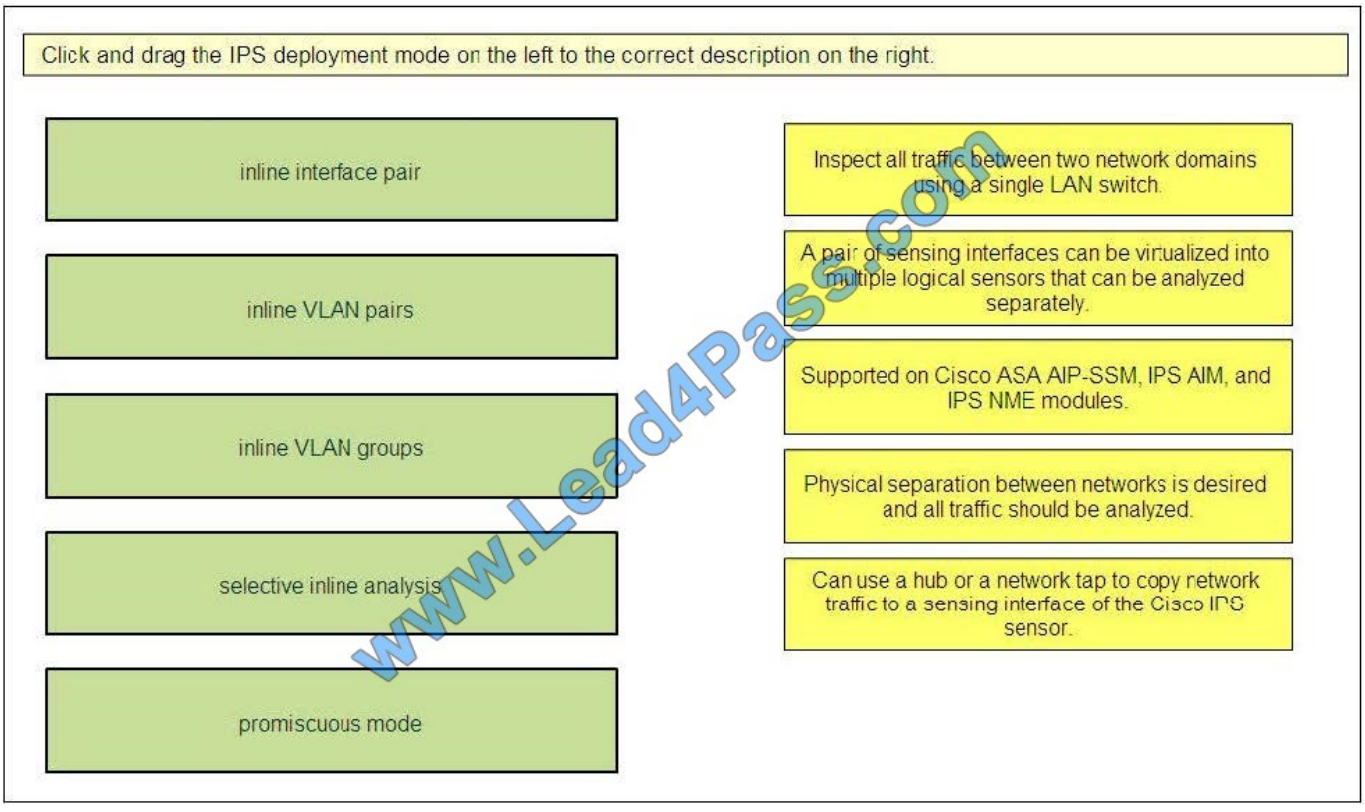
D. Reputation filtering is disabled.

Correct Answer: D

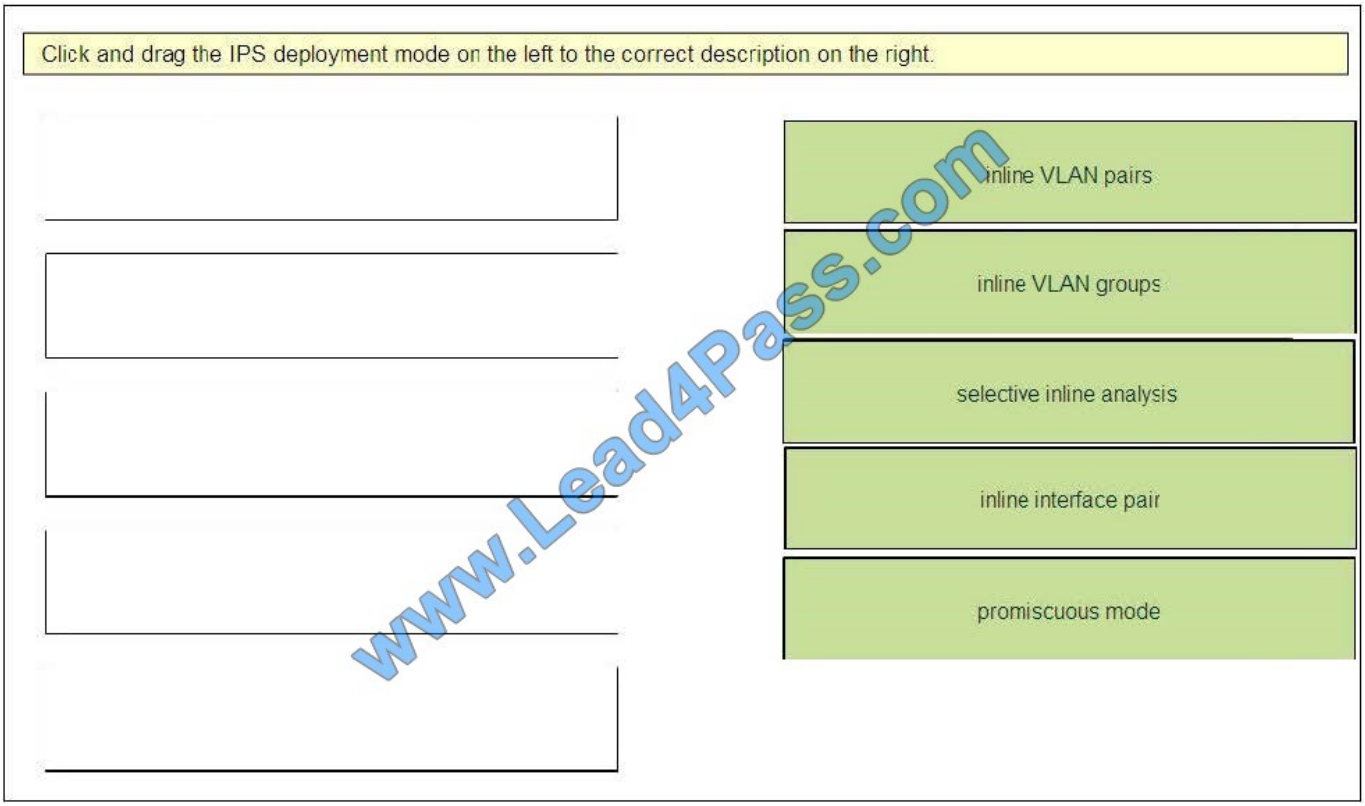
http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/idm/idm_collaboration.html# wp1054333

QUESTION 2

Select and Place:



Correct Answer:



QUESTION 3

Which IPS alert action is available only in inline mode?

A. produce verbose alert

B. request rate limit

C. reset TCP connection

D. log attacker/victim pair packets

E. deny-packet-inline

F. request block connection

Correct Answer: E

http://www.cisco.com/web/about/security/intelligence/ipsmit.html

Inline Mode Event Actions

The following actions require the device to be deployed in Inline mode and are in affect for a user- configurable default time of 3600 seconds (60 minutes). Deny attacker inline: This action is the most severe and effectively blocks all

communication from the attacking host that passes through the IPS for a specified period of time. Because this event action is severe, administrators are advised to use this only when the probability of false alarms or spoofing is minimal.

Deny attacker service pair inline: This action prevents communication between the attacker IP address and the protected network on the port in which the event was detected. However, the attacker would be able to communicate on another

port that has hosts on the protected network. This event action works well for worms that attack many hosts on the same service port. If an attack occurred on the same host but on another port, this communication would be allowed. This

event action is appropriate when the likelihood of a false alarm or spoofing is minimal. Deny attacker victim pair inline: This action prevents the attacker from communicating with the victim on any port. However, the attacker could

communicate with other hosts, making this action better suited for exploits that target a specific host. This event action is appropriate when the likelihood of a false alarm or spoofing is minimal.

Deny connection inline: This action prevents further communication for the specific TCP flow. This action is appropriate when there is the potential for a false alarm or spoofing and when an administrator wants to prevent the action but not

deny further communication. Deny packet inline: This action prevents the specific offending packet from reaching its intended destination.

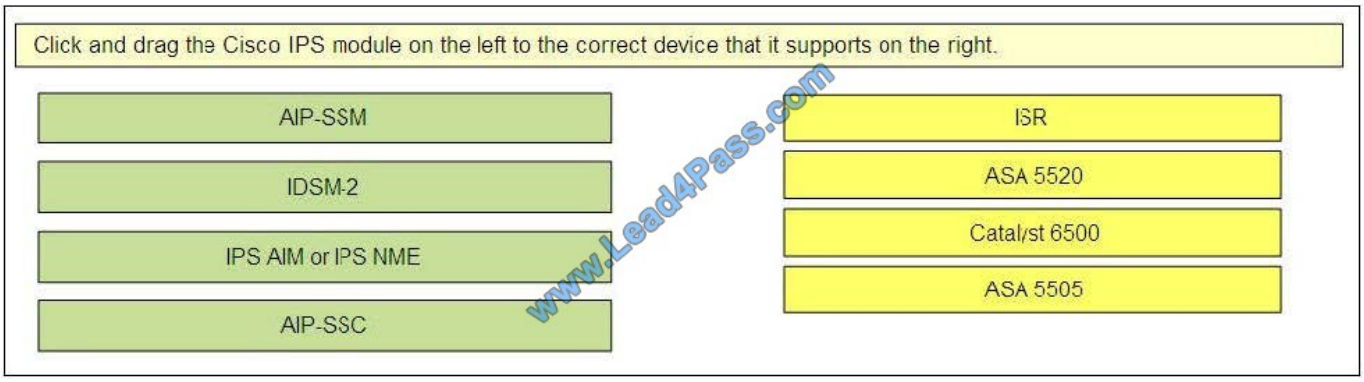
Other communication between the attacker and victim or victim network may still exist. This action is appropriate when there is the potential for a false alarm or spoofing. Note that for this action, the default time has no effect.

Modify packet inline: This action enables the IPS device to modify the offending part of the packet. However, it forwards the modified packet to the destination. This action is appropriate for packet normalization and other anomalies, such as

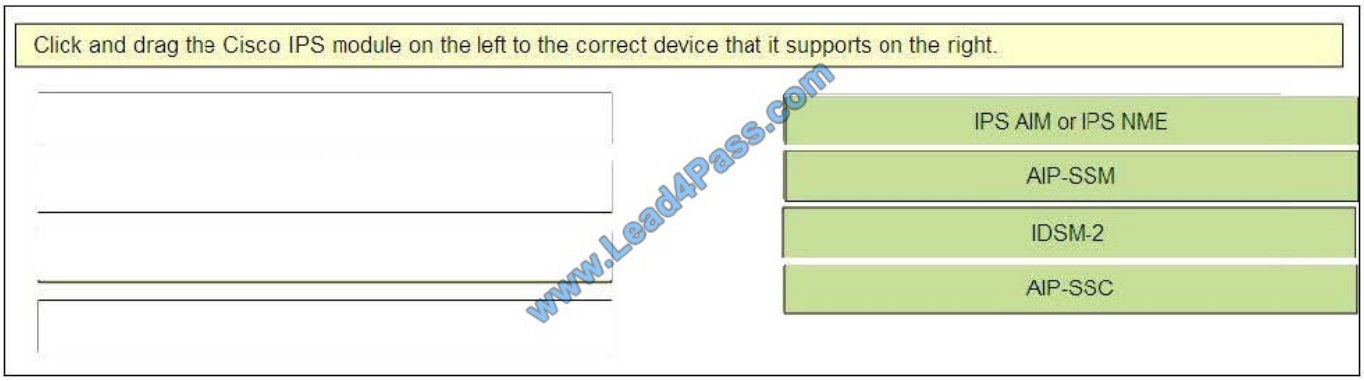
TCP segmentation and IP fragmentation re-ordering.

QUESTION 4

Select and Place:

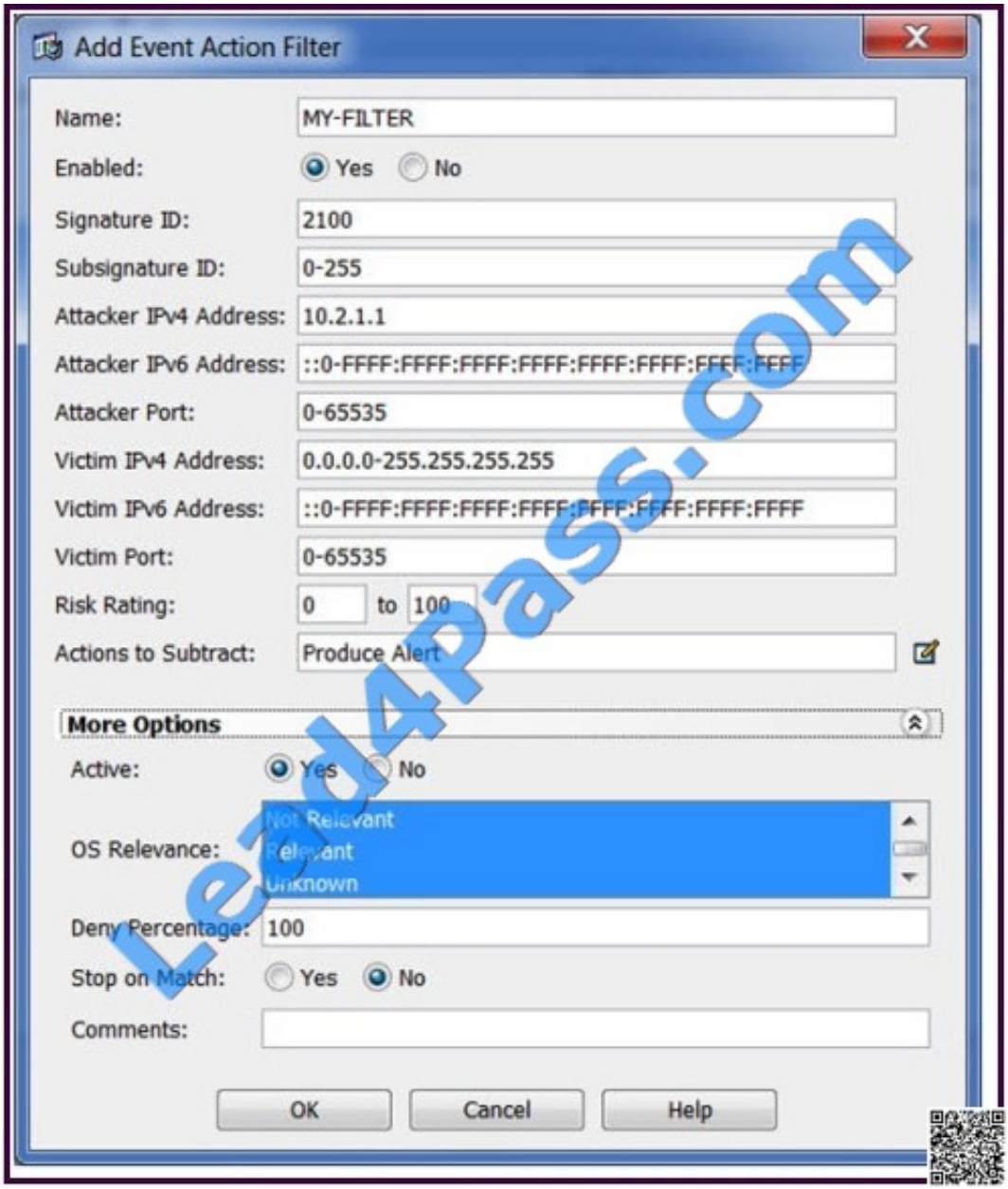


Correct Answer:



QUESTION 5

Refer to the exhibit. What does the Deny Percentage setting affect?



A. the percentage of the signatures to be tuned by the event action filter

B. the percentage of the Risk Rating value to be tuned by the event action filter

C. the percentage of packets to be denied for the deny attacker actions

D. the percentage of the signatures to be tuned by the event action overrides

Correct Answer: C

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/idm/idm_event_action_rules.

html#wp2032330

?eny Percentage--Determines the percentage of packets to deny for deny attacker features. The valid range is 0 to 100. The default is 100 percent.

Latest 642-627 Dumps 642-627 VCE Dumps 642-627 Exam Questions

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

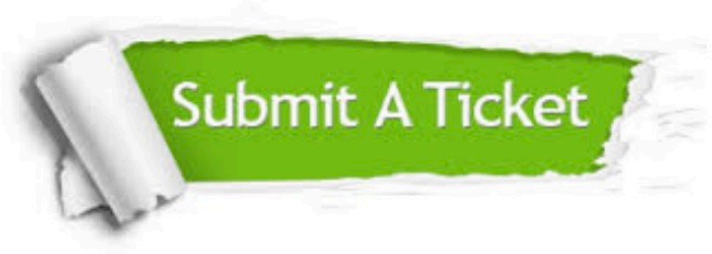
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.lead4pass.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © lead4pass, All Rights Reserved.