



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

The screenshot displays a web-based exam interface. On the left, a 'Questions' sidebar contains a vertical list of question numbers 1 through 6, with a progress indicator showing '0% Complete'. The main area features two windows: 'Instructions' and 'Scenario'. The 'Instructions' window contains text about window controls. The 'Scenario' window contains text about using Cisco IPS Device Manager (IDM). A large 'Lead4Pass.com' watermark is overlaid on the interface, and a QR code is located in the bottom right corner. A navigation bar at the bottom includes tabs for 'Instructions', 'Scenario', 'Topology', 'Questions', and 'Cisco IDM'.

Instructions

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.

Scenario

Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.


0% Complete

1
2
3
4
5
6

Instructions Scenario Topology Questions Cisco IDM

Lead4Pass.com

CISCO





Scenario

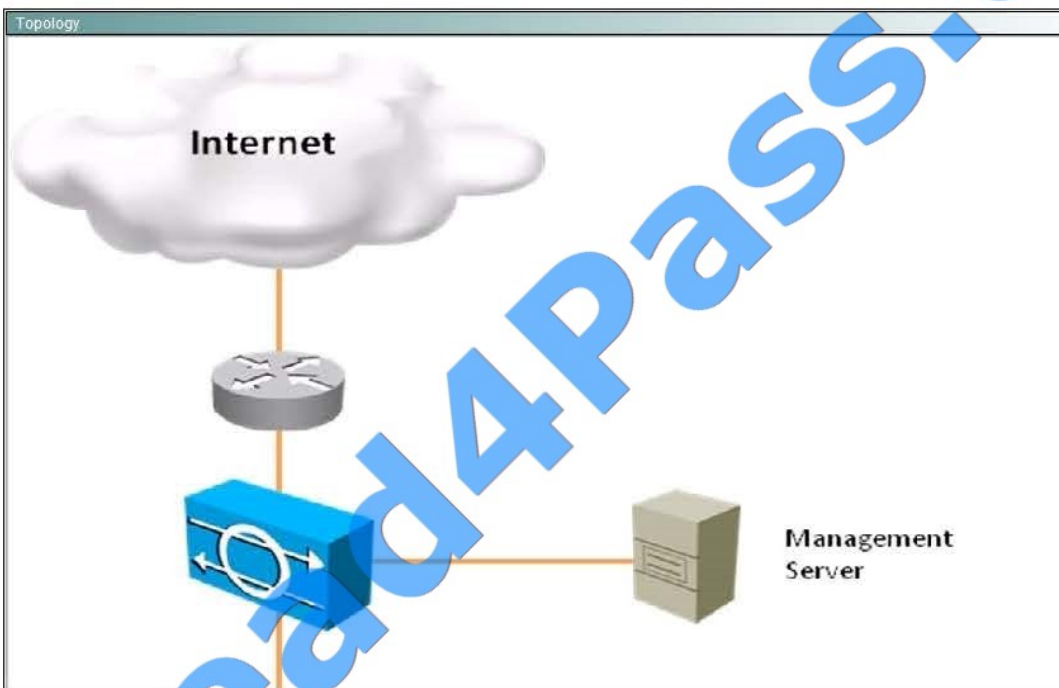
You are the network security administrator responsible for operation and maintenance of your organization's Cisco IPS sensor appliance. You have noticed recent malicious activity that must be more closely monitored and you have configured custom parameter tuning to detect and mitigate this activity. You will be required to perform the following tasks:

- Event Action Overrides
 - Verify and enable this feature for the rules0 instance.
- Risk Category named MYCUSTOMRISK
 - Create a custom Risk Category named MYCUSTOMRISK.
 - Assign this category a risk threshold of 80.
 - Modify the new MYCUSTOMRISK category to take the following actions:
 - Deny Attacker Inline
 - Produce Alert
 - Reset TCP Connection
- Modify the Red Threat Threshold
 - Modify value to 80 to enable the new risk category to be included in the Red threshold level for network: security health statistics alert threat categorization.
- Remember to save and apply all changes as needed

To access the Cisco IPS sensor, click the client PC to launch Cisco IDM.

- userID: cisco
- password: cisco123

Scenario | Topology | IDM



IDM

Cisco ASDM-IDM Launcher v1.5(37)

Cisco ASDM-IDM Launcher CISCO

Device IP Address / Name: 172.26.26.53

Username:

Password:

Run in Demo Mode

OK Close





The Health Dashboard shows the following sensor information:

- 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
- CPU, Memory, & Load - sensor** (Updated 11:37:35 AM):
 - CPU Usage: 0%
 - Memory Usage: System (71%), Analysis Engine (23%)
 - Disk Usage: boot (61%), system (44%), application-log (24%), application-data (28%)
- Sensor Health - sensor** (Updated 11:37:35 AM):
 - Sensor Health: Critical
 - Network Security Health: Normal
- Licensing - sensor** (Updated 11:37:35 AM):
 - 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

The Startup Wizard page provides instructions for configuring the Cisco IPS sensor. It states that the wizard assists in performing basic sensor configuration and can be run at any time. A large blue watermark 'Lead4Pass' is overlaid on the page.

The Network configuration page allows specifying network and communication parameters. The following fields are visible:

- Hostname: ips
- IP Address: 172.26.26.53
- Network Mask: 255.255.255.0
- Default Route: 172.26.26.151
- FTP Timeout(Seconds): 300
- Web Server Settings: Web server port: 443
- Remote Access: Enable Telnet (checked)
- DNS/Proxy Settings: Http Proxy Server, Http Proxy Port, DNS Primary, DNS Secondary, DNS Tertiary

The Allowed Hosts/Networks page shows a table of permitted IP addresses and network masks:

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





What action will the sensor take 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](http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/idm/idm_collaboration.html#wp1054333)

QUESTION 2

Select and Place:

Click and drag the IPS deployment mode on the left to the correct description on the right.

inline interface pair	Inspect all traffic between two network domains using a single LAN switch.
inline VLAN pairs	A pair of sensing interfaces can be virtualized into multiple logical sensors that can be analyzed separately.
inline VLAN groups	Supported on Cisco ASA AIP-SSM, IPS AIM, and IPS NME modules.
selective inline analysis	Physical separation between networks is desired and all traffic should be analyzed.
promiscuous mode	Can use a hub or a network tap to copy network traffic to a sensing interface of the Cisco IPS sensor.

Correct Answer:



Click and drag the IPS deployment mode on the left to the correct description on the right.

	inline VLAN pairs
	inline VLAN groups
	selective inline analysis
	inline interface pair
	promiscuous mode

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:

Click and drag the Cisco IPS module on the left to the correct device that it supports on the right.

AIP-SSM	ISR
IDSM-2	ASA 5520
IPS AIM or IPS NME	Catalyst 6500
AIP-SSC	ASA 5505

Correct Answer:



Click and drag the Cisco IPS module on the left to the correct device that it supports on the right.

	IPS AIM or IPS NME
	AIP-SSM
	IDSM-2
	AIP-SSC

QUESTION 5

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



Add Event Action Filter

Name: MY-FILTER

Enabled: Yes No

Signature ID: 2100

Subsignature ID: 0-255

Attacker IPv4 Address: 10.2.1.1

Attacker IPv6 Address: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Attacker Port: 0-65535

Victim IPv4 Address: 0.0.0.0-255.255.255.255

Victim IPv6 Address: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Victim Port: 0-65535

Risk Rating: 0 to 100

Actions to Subtract: Produce Alert

More Options

Active: Yes No

OS Relevance: **Relevant** (dropdown menu showing Not Relevant, Relevant, Unknown)

Deny Percentage: 100

Stop on Match: Yes No

Comments:

OK Cancel Help

- 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

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



VCE & PDF

Lead4Pass.com

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

2021 Latest lead4pass 642-627 PDF and VCE dumps Download

[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 !

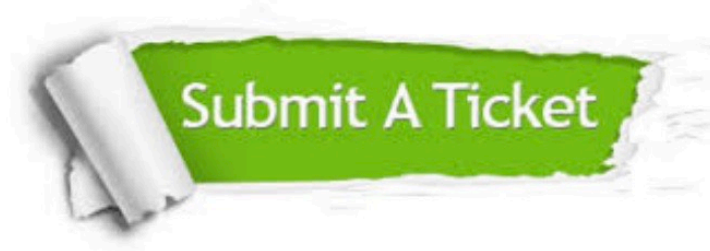
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#),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



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

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.