



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.pass4itsure.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

Select and Place:

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

false positive	A security control did not act because no malicious activity occurred.
false negative	A security control did not act when malicious activity occurred.
true positive	A security control acted when malicious activity occurred.
true negative	A security control acted when malicious activity did not occur.

Correct Answer:

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

	true negative
	false negative
	true positive
	false positive

QUESTION 2

Which three statements about the Cisco IPS appliance Event Store are true? (Choose three.)

- A. The Event Store is accessible through the CLI, Cisco IDM, Cisco ASDM, or SDEE.
- B. The Event Store is a circular, first-in first-out buffer.
- C. The Event Store can be configured to be located on a remote server.
- D. The size of the Event Store depends on the Cisco IPS appliance platform.



E. Each virtual sensor has its own Event Store.

F. If the Event Store is full, the Cisco IPS appliance performs an automatic graceful shutdown.

Correct Answer: ABD

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_system_architecture.html


QUESTION 3



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.



Questions

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

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:

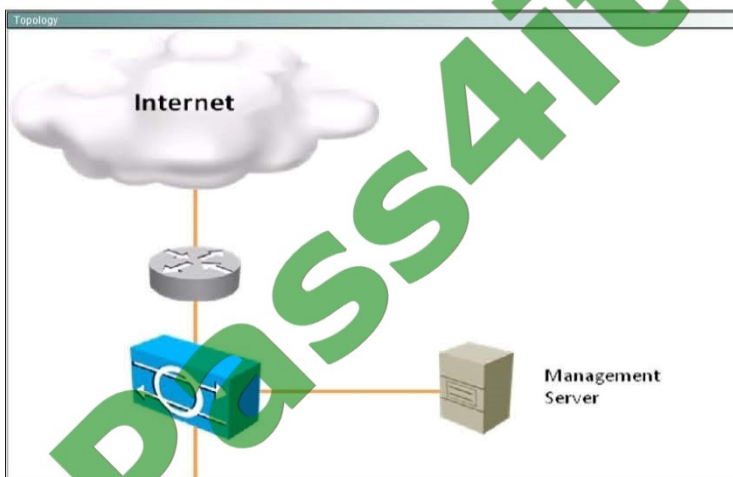
- Event Action Overrides
 - Verify and enable this feature for the rules0 instance.
- Risk Category named MYCUSTOMRISK
 - Create a custom Risk Category named MYCUSTOMRISK.
 - Assign this category a risk threshold of 80.
- Modify the new MYCUSTOMRISK category to take the following actions:
 - Deny Attacker 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.

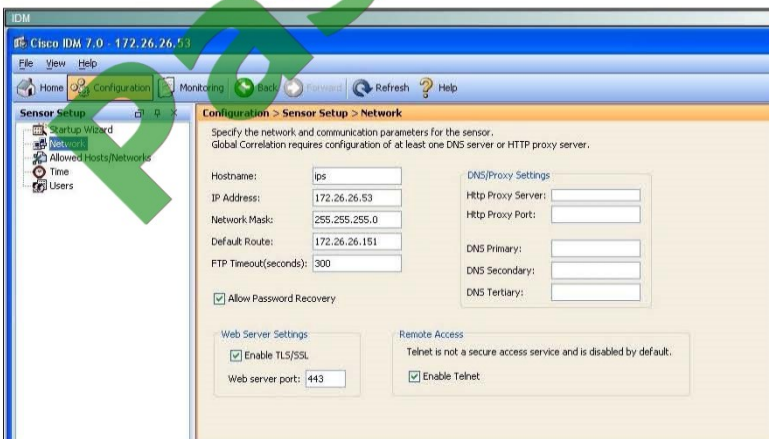
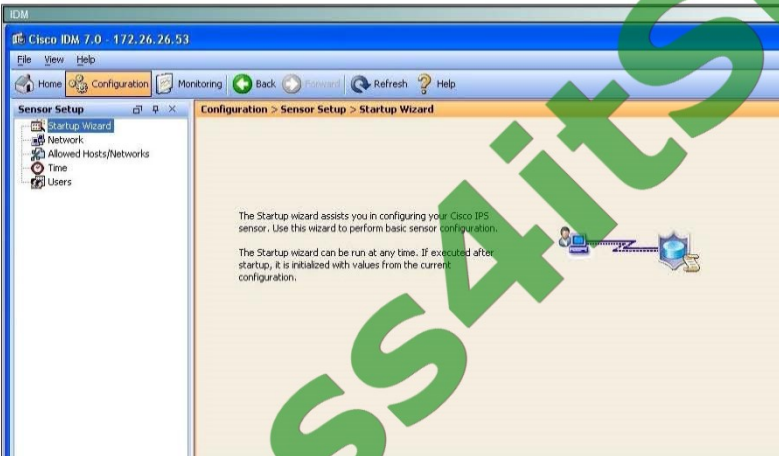
Remember to save and apply all changes as needed

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

- userID: cisco
- password: cisco123

Scenario Topology IDM







The screenshot shows the Cisco IDM 7.0 web interface. The browser address bar displays "Cisco IDM 7.0 - 172.26.26.53". The navigation menu includes "File", "View", and "Help". The main content area is titled "Configuration > Sensor Setup > Allowed Hosts/Networks". Below the title, there is a table with two columns: "IP Address" and "Network Mask". The table contains three rows of data:

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

A QR code is visible in the bottom right corner of the interface.

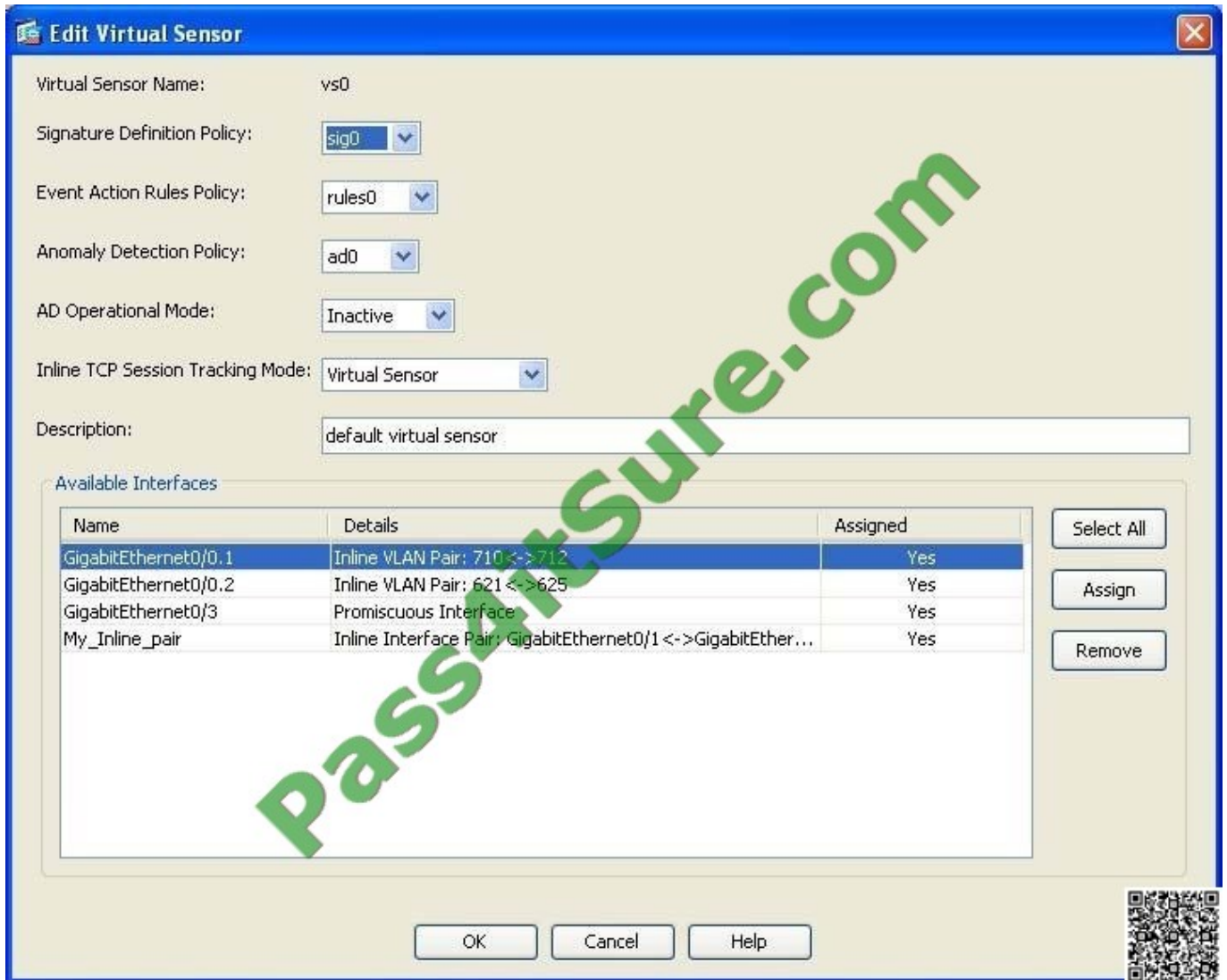
Which signature definition is virtual sensor 0 assigned to use?

- A. rules0
- B. vs0
- C. sig0
- D. ad0
- E. ad1
- F. sigl

Correct Answer: B

Default signature http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/idm/idm_signature_definitions.html

You can create multiple security policies and apply them to individual virtual sensors. A security policy is made up of a signature definition policy, an event action rules policy, and an anomaly detection policy. Cisco IPS contains a default signature definition policy called sig0, a default event action rules policy called rules0, and a default anomaly detection policy called ad0. You can assign the default policies to a virtual sensor or you can create new policies.



QUESTION 4

Which two operations would put an inline Cisco IPS sensor in detection mode? (Choose two.)

- A. subtract all aggressive actions using event action filters
- B. decrease the event count using event action filters
- C. increase the maximum inter-event interval using event action overrides
- D. remove the default event action override, which drops traffic with a risk rating of 90 to 100
- E. enable anomaly detection in detection mode only

Correct Answer: AD

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/cli/cli_anomaly_detection.html#wp1041433

Not sure of this answer yet - 9/25/12 - DD but seems to be another Cisco classif question, meaning that once a



signature is tuned it is ready for prime time i.e. detection mode After the signatures are tuned, remove the event action filters that removed the aggressive actions, and remove the event action overrides that produced the verbose alerts.

QUESTION 5

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

- A. deny connection
- B. deny attacker
- C. reset TCP connection
- D. deny packet, reset TCP connection
- E. deny connection, reset TCP connection

Correct Answer: C

Deny attacker is only available in inline mode! <http://www.cisco.com/web/about/security/intelligence/ipsmit.html#7>

Promiscuous Mode Event Actions The following event actions can be deployed in Promiscuous mode. These actions are in affect for a userconfigurable default time of 30 minutes. Because the IPS sensor must send the request to another device or craft a packet, latency is associated with these actions and could allow some attacks to be successful. Blocking through usage of the Attack Response Controller (ARC) has the potential benefit of being able to perform to the network edge or at multiple places within the network.

Request block host: This event action will send an ARC request to block the host for a specified time frame, preventing any further communication. This is a severe action that is most appropriate when there is minimal chance of a false alarm or spoofing. **Request block connection:** This action will send an ARC response to block the specific connection. This action is appropriate when there is potential for false alarms or spoofing. **Reset TCP connection:** This action is TCP specific, and in instances where the attack requires several TCP packets, this can be a successful action. However, in some cases where the attack only needs one packet it may not work as well. Additionally, TCP resets are not very effective with protocols such as SMTP that consistently try to establish new connections, nor are they effective if the reset cannot reach the destination host in time.

Event actions can be specified on a per signature basis, or as an event action override (based on risk rating values ?event action override only). In the case of event action override, specific event actions are performed when specific risk rating value conditions are met. Event action overrides offer consistent and simplified management. IPS version 6.0 contains a default event action override with a deny-packet-inline action for events with a risk rating between 90 and 100. For this action to occur, the device must be deployed in Inline mode.

[Latest 642-627 Dumps](#)

[642-627 Study Guide](#)

[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.pass4itsure.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 © pass4itsure, All Rights Reserved.