



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.passapply.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

You are working with Cisco TAC to troubleshoot a software problem on the Cisco IPS appliance. TAC suspects a fault with the ARC software module in the Cisco IPS appliance. In this case, which Cisco IPS appliance operations may be most affected by the ARC software module fault?

- A. SDEE
- B. global correlation
- C. anomaly detection
- D. remote blocking
- E. virtual sensor
- F. OS fingerprinting

Correct Answer: D

http://www.cisco.com/en/US/docs/security/ips/6.1/installation/guide/hw_troubleshooting.html#wpm kr1185768

QUESTION 2

Select and Place:

At right are CLI commands that can be used to direct traffic to the Cisco IPS sensor. Drag the device type from the left to match the corresponding CLI command it supports on the right.

Catalyst 3560E	ips inline fail-open
Catalyst 6500	monitor session 1 filter ip access-group MyFilter
ASA 5520	ids-service-module monitoring inline access-list 101
ISR	vlan access-map MyMap 10

Correct Answer:

At right are CLI commands that can be used to direct traffic to the Cisco IPS sensor. Drag the device type from the left to match the corresponding CLI command it supports on the right.

	ASA 5520
	Catalyst 3560E
	ISR
	Catalyst 6500



QUESTION 3

Which Cisco IPS appliance feature uses profile-based intrusion detection?

- A. profiler
- B. anomaly detection
- C. threat detection
- D. netflow
- E. reputation filter
- F. senderbase

Correct Answer: B

QUESTION 4

The default virtual sensor on all IPS appliances is vs0. Which three components are assigned to vs0 by default? (Choose three.)

- A. sig0
- B. engine0
- C. rules0
- D. ad0
- E. filters0
- F. gc0

Correct Answer: ACD

http://www.cisco.com/en/US/docs/security/ips/7.1/configuration/guide/idm/idm_policies.html

The sensor can receive data inputs from one or many monitored data streams. These monitored data streams can either be physical interface ports or virtual interface ports. For example, a single sensor can monitor traffic from in front of the firewall, from behind the firewall, or from in front of and behind the firewall concurrently. And a single sensor can monitor one or more data streams. In this situation a single sensor policy or configuration is applied to all monitored data streams.

A virtual sensor is a collection of data that is defined by a set of configuration policies. The virtual sensor is applied to a set of packets as defined by interface component. A virtual sensor can monitor multiple segments, and you can apply a different policy or configuration for each virtual sensor within a single physical sensor. You can set up a different policy per monitored segment under analysis. You can also apply the same policy instance, for example, sig0, rules0, or ad0, to different virtual sensors. You can assign interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups to a virtual sensor.

QUESTION 5



Refer to the exhibit.

Configuration > Interfaces > Traffic Flow Notifications

You can configure the sensor to monitor the flow of packets across an interface and send notification if that flow changes during a specified interval. The sensor monitors the percentage of missed packets during a specified notification interval and issues a status event if the percentage of missed packets exceeds the Missed Packets Threshold. The sensor also issues a status event if the interface remains idle and does not receive packets for a specified amount of time.

Missed Packets Threshold: percent

Notification Interval: seconds

Interface Idle Threshold: seconds

PassApply.com

Configuring traffic flow notifications on the Cisco IPS appliance is most useful in what situation?

- A. to determine the IPS throughput rate when using inline mode
- B. to detect IPS performance issues
- C. to enable bypass mode when the Cisco IPS appliance fails
- D. to prevent DoS attacks

Correct Answer: B

<http://www.cisco.com/en/US/docs/security/ips/5.0/configuration/guide/idm/dminter.html#wp103214>

[642-627 VCE Dumps](#)

[642-627 Exam Questions](#)

[642-627 Braindumps](#)



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.passapply.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 © passapply, All Rights Reserved.