



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.pass4lead.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**

Which statement about the 4-port GigabitEthernet card with hardware bypass is true?

- A. Hardware bypass only works with inline interface pairs.
- B. Hardware bypass is only supported on the Cisco IPS 4270 appliance.
- C. Hardware bypass is independent from software bypass.
- D. Hardware bypass is enabled if software bypass is configured to "OFF".
- E. Hardware bypass is supported between any of the four GigabitEthernet ports

Correct Answer: A

QUESTION 2

Which Cisco IPS appliance TCP session tracking mode should be used if packets of the same session are coming to the sensor over different interfaces, but should be treated as a single session?

- A. interface and VLAN
- B. virtual sensor
- C. VLAN only
- D. promiscuous
- E. normalizer

Correct Answer: B

http://www.cisco.com/en/US/docs/security/ips/7.1/configuration/guide/ime/ime_policies.html#wp20_05229

Inline TCP Session Tracking Mode

When you choose to modify packets inline, if the packets from a stream are seen twice by the Normalizer engine, it cannot properly track the stream state and often the stream is dropped. This situation occurs most often when a stream is

routed through multiple VLANs or interfaces that are being monitored by the IPS. A further complication in this situation is the necessity of allowing asymmetric traffic to merge for proper tracking of streams when the traffic for either direction is

received from different VLANs or interfaces.

To deal with this situation, you can set the mode so that streams are perceived as unique if they are received on separate interfaces and/or VLANs (or the subinterface for VLAN pairs).

The following inline TCP session tracking modes apply:

?ninterface and VLAN--All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) and on the



same interface belong to the same session. Packets with the same key but on different VLANs are tracked separately.

?LAN Only--All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) regardless

of the interface belong to the same session. Packets with the same key but on different VLANs are tracked separately.

?irtual Sensor--All packets with the same session key (AaBb) within a virtual sensor belong to the same session. This is the default and almost always the best option to choose.

QUESTION 3

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

The screenshot shows the 'Add Event Action Filter' dialog box with the following fields and values:

- 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 (expanded):
 - Active: Yes No
 - OS Relevance: Not Relevant (selected), Relevant, Unknown
 - Deny Percentage: 100
 - Stop on Match: Yes No
 - Comments: (empty)

Buttons: 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

?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.

QUESTION 4

Which ASA CLI command is used to configure the network parameters for downloading the AIP- SSM recovery image?

- A. hw-module 1 recover boot
- B. hw-module 1 recover configure
- C. sysopt ips recovery configure
- D. sysopt ips recover-location
- E. boot hw-module 1 tftp
- F. boot system tftp

Correct Answer: B

<http://www.cisco.com/en/US/docs/security/ips/5.0/configuration/guide/cli/clissm.html#wp1034193>

QUESTION 5

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



VCE & PDF

Pass4Lead.com

<https://www.pass4lead.com/642-627.html>

2022 Latest pass4lead 642-627 PDF and VCE dumps Download

[642-627 PDF Dumps](#)

[642-627 Practice Test](#)

[642-627 Study Guide](#)



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.pass4lead.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 © pass4lead, All Rights Reserved.