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.geekcert.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 two statements are true regarding the Cisco IPS appliance traffic normalizer? (Choose two.)

A. It only operates in inline mode.

B. It operates in one of three modes: symmetric, loose, or asymmetric.

C. It can help prevent false negatives that are caused by evasions.

D. It can help ensure that Layer 7 traffic conforms to its protocol specifications.

E. It will not modify fragmented IP traffic.

Correct Answer: AC

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/white_paper_c11- 459025.html

QUESTION 2

All signatures in the Cisco IPS signature set include which three parameters that can be tuned according to the environment? (Choose three.)

A. vulnerable OS list

B. alert severity rating

C. inline mode delta

D. signature fidelity rating

E. threat rating

Correct Answer: ABD

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/white_paper_c11_54 9300.html

After configuring Cisco IOS IPS on your router, you should adjust the staging router\\'s signature configuration. The IOS IPS `basic\\' and `advanced\\' signature categories include a set of signatures that detect and mitigate a broad range of traffic that could potentially exploit various types of software vulnerabilities in server and workstation hosts, as well as network devices; other signature categories may hold some appeal for your environment, but will likely require tuning to fit into the router\\'s available memory. You will need to be sure that IOS IPS is configured to enable signatures that specifically address the requirements of your environment. Additionally, while some signatures may offer some benefit for vulnerabilities that your network presents, IPS may recognize traffic that is not an exploit as unwanted traffic, thus affecting a "false positive". False positives must be dealt with in a manner that suits the nature of the vulnerability. If a very high-risk vulnerability must be mitigated by IPS, operational tools and staff must be able to distinguish between traffic that comprises a false positive and that which comprises a live exploit. Otherwise, signatures addressing low-risk vulnerabilities might be tuned to generate less response, or disabled entirely, to avoid the additional operational burden of dealing with the false positives. Other reasons for tuning the signature database are to reduce memory or CPU footprint, or to add custom IPS signatures that you have developed to address the security requirements of your environment.

QUESTION 3

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 4

Which two statements are true with respect to the AIP-SSM? (Choose two.)

A. The hosting ASA will always bypass the AIP-SSM if the AIP-SSM fails.

B. The AIP-SSM supports up to four virtual sensors.

C. Initial setup of the AIP-SSM is configured through its external console port.

D. The AIP-SSM supports both promiscuous and inline analysis.

E. The AIP-SSM must be managed by the IPS Device Manager.

Correct Answer: BD

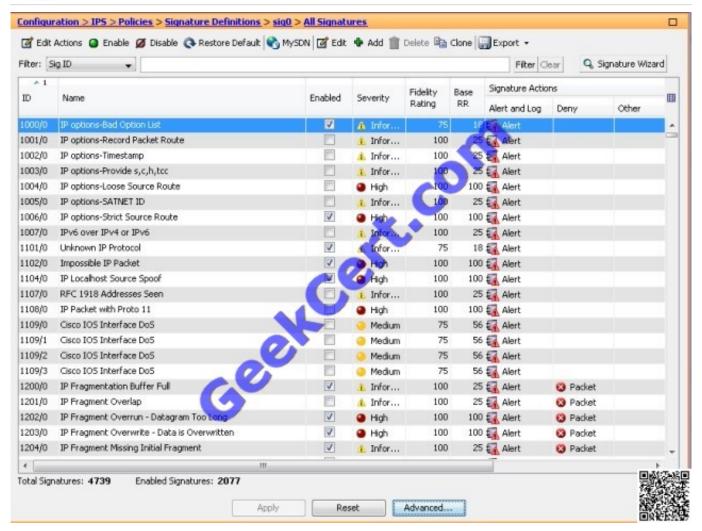http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/ssm.html

QUESTION 5

Refer to the exhibit.

Configuration > IPS > Policies > Signature Definitions > sig0 > All Signatures

Edit Actions ● Enable ⊘ Disable ↻ Restore Default MySDN Edit ✚ Add 🗑 Delete Clone Export ▾

Filter: Sig ID ▾ [   ] Filter | Clear 🔍 Signature Wizard

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions		
						Alert and Log	Deny	Other
1000/0	IP options-Bad Option List	☑	⚠ Infor...	75	18	Alert		
1001/0	IP options-Record Packet Route	☐	ⓘ Infor...	100	25	Alert		
1002/0	IP options-Timestamp	☐	ⓘ Infor...	100	25	Alert		
1003/0	IP options-Provide s,c,h,tcc	☐	ⓘ Infor...	100	25	Alert		
1004/0	IP options-Loose Source Route	☐	● High	100	100	Alert		
1005/0	IP options-SATNET ID	☐	ⓘ Infor...	100	25	Alert		
1006/0	IP options-Strict Source Route	☑	● High	100	100	Alert		
1007/0	IPv6 over IPv4 or IPv6	☐	ⓘ Infor...	100	25	Alert		
1101/0	Unknown IP Protocol	☑	Infor...	75	18	Alert		
1102/0	Impossible IP Packet	☑	High	100	100	Alert		
1104/0	IP Localhost Source Spoof	☑	High	100	100	Alert		
1107/0	RFC 1918 Addresses Seen	☐	ⓘ Infor...	100	25	Alert		
1108/0	IP Packet with Proto 11	☐	● High	100	100	Alert		
1109/0	Cisco IOS Interface DoS	☐	● Medium	75	56	Alert		
1109/1	Cisco IOS Interface DoS	☐	● Medium	75	56	Alert		
1109/2	Cisco IOS Interface DoS	☐	● Medium	75	56	Alert		
1109/3	Cisco IOS Interface DoS	☐	● Medium	75	56	Alert		
1200/0	IP Fragmentation Buffer Full	☑	⚠ Infor...	100	25	Alert	⊗ Packet	
1201/0	IP Fragment Overlap	☐	ⓘ Infor...	100	25	Alert	⊗ Packet	
1202/0	IP Fragment Overrun - Datagram Too Long	☑	● High	100	100	Alert	⊗ Packet	
1203/0	IP Fragment Overwrite - Data is Overwritten	☑	● High	100	100	Alert	⊗ Packet	
1204/0	IP Fragment Missing Initial Fragment	☑	⚠ Infor...	100	25	Alert	⊗ Packet	

Total Signatures: 4739   Enabled Signatures: 2077

[Apply]   [Reset]   [Advanced...]

When viewing the All Signatures pane, clicking on the Advanced option can be used to enable which two IPS configurations? (Choose two.)

A. normalizer mode

B. signature variables

C. HTTP and FTP AIC

D. network participation mode

E. event action overrides

F. event action filters

Correct Answer: BC

http://www.cisco.com/en/US/docs/security/ips/7.1/configuration/guide/idm/idm_signature_definition s.html#wp1224787

642-627 Practice Test   **642-627 Study Guide**   **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.geekcert.com/allproducts

Need Help

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

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.

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.

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.