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

QUESTION 1

Which two Cisco IPS modules support sensor virtualization? (Choose two.)

A. AIP-SSM

B. AIP-SSC

C. IPS AIM

D. IPS NME

E. IDSM-2

Correct Answer: AE

http://my.safaribooksonline.com/book/certification/ccnp/9780132372107/using-cisco-ips-virtual- sensors/ch20lev1sec5

QUESTION 2

What is a best practice to follow before tuning a Cisco IPS signature?

A. Disable all the alert actions on the signature to be tuned.

B. Disable the signature to be tuned.

C. Create a clone of the signature to be tuned.

D. Increase the number of events required to trigger the signature to be tuned.

E. Decrease the attention span (maximum inter-event interval) of the signature to be tuned

Correct Answer: C

http://www.cisco.com/web/about/security/intelligence/ips_custom_sigs_pdf.pdf, specifically:

Cloning a Signature

Administrators often find the need to modify a signature to meet the needs of a specific network, such as to reduce false positives or false negatives.

In such cases, the first approach should be to fine tune signature parameters such as event action filters and override policies. If these tunings are not sufficient, the last action that is available is to modify a signature. By default, signature

parameters such as the regular expression cannot be modified.

The signature must first be cloned in order to modify such signature parameters. The original signature can be retired or disabled if it is determined that it is no longer required.

ORIGINAL FROM CHIP:

Still Doubt here. 100% certain C is wrong.

A is best answer with B also possible.

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd8066d265.html

Official Guide - Chapter 13 Quiz - When tuning signatures it is recommended Answer: By removing harmful actions during the tuning phase we can have visibility.....without interfering with normal traffic "Do no harm" approach.

QUESTION 3

Which statement about inline VLAN pair deployment with the Cisco IPS 4200 Series appliance is true?

A. The sensing interface acts as an 802.1q trunk port, and the Cisco IPS appliance performs VLAN translation between pairs of VLANs.

B. The Cisco IPS appliance connects to two physically distinct switches using two paired physical interfaces.

C. Two sensing interfaces connect to the same switch that forwards traffic between two VLANs.

D. The pair of sensing interfaces can be selectively divided (virtualized) into multiple logical "wires" by VLANs that can be analyzed separately

Correct Answer: A

QUESTION 4

Which protocol or protocols does the Cisco Security Manager use to communicate with the Cisco IPS appliance?

A. HTTPS only

B. SSH only

C. SNMPv3 only

D. HTTPS and SNMPv3

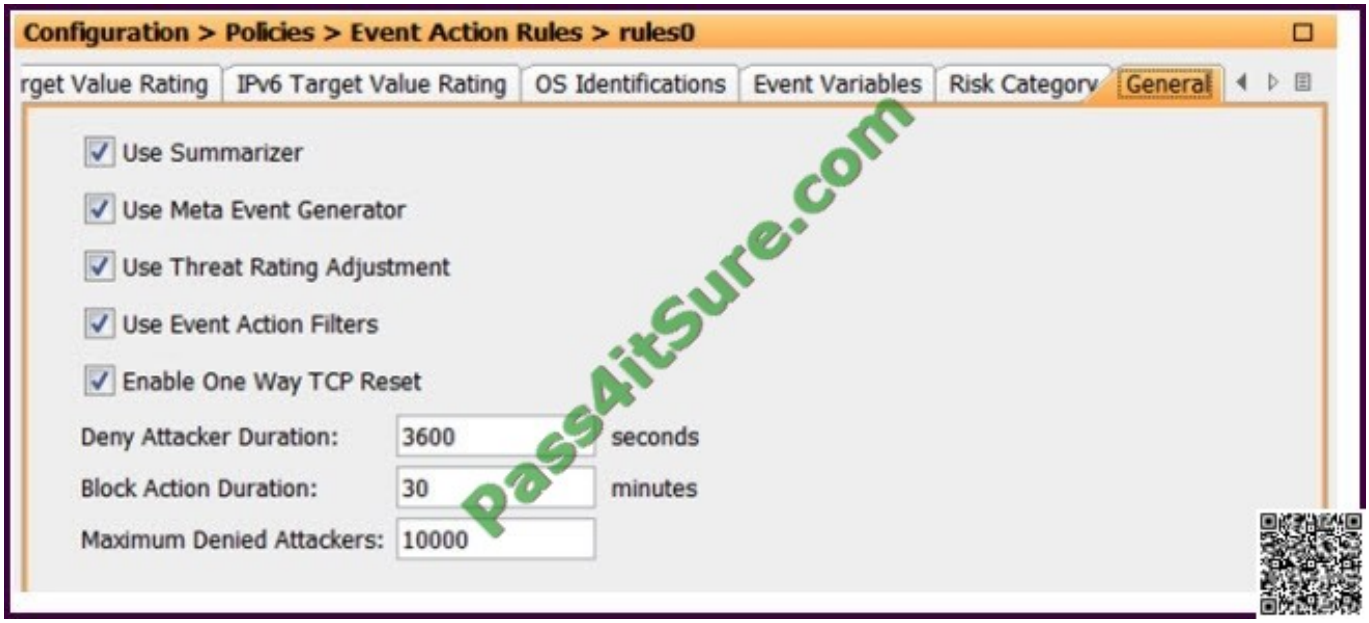
E. HTTPS and SSH

F. HTTPS, SSH, and SNMPv3

Correct Answer: A

QUESTION 5

Refer to the exhibit.



Which three statements are true? (Choose three.)

A. Triggered inline blocks will last for 1 hour while triggered requests for external systems to block will last for 30 minutes.

B. Triggered inline blocks will last for 30 minutes while triggered requests for external systems to block will last for 1 hour.

C. TCP Resets will only be sent to the victim IP address.

D. TCP Resets will only be sent to the attacker IP address.

E. The IPS appliance can be configured to ignore scanning events sourced from the organization network management system.

F. An alert risk rating will be calculated from the base value of the threat rating reduced by a value corresponding to the preventative actions taken by the IPS appliance.

Correct Answer: ACE

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: