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.certbus.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 with respect to the AIP-SSC? (Choose two.)

A. The AIP-SSC is a module for the ASA 5510.

B. The AIP-SSC supports a maximum of two virtual sensors.

C. The AIP-SSC supports custom signatures.

D. The AIP-SSC supports fail open.

E. The AIP-SSC supports both promiscuous and inline analysis.

Correct Answer: DE

https://docs.google.com/viewer?a=vandq=cache:xcV24pCOF4MJ:www.cisco.com/en/US/docs/security/ips/6.2/configuration/guide/cli/cli_ssc.pdf+cisco+asa+aip+ssc+failopenand hl=enandgl=usandpid=blandsrcid=ADGEESi0RHlzQEpHH8Uu4c_jbwGBNqpMmZsVkjsfy6phll2Z0C5uZe QXUErbeYB-mLNlzyPb2FkNp9CrNqTJ70P-rjxrka68y6lzM9wGKpB76k-A38s8q70NsLgU_D3QAei23fVql53andsig=AHIEtbQ5ENt7hynvXatqPIccq8paHRyuJQ

QUESTION 2

In which three ways can you achieve better Cisco IPS appliance performance? (Choose three.)

A. Place the Cisco IPS appliance behind a firewall.

B. Disable unneeded signatures.

C. Enable unidirectional capture.

D. Have multiple Cisco IPS appliances in the path and configure them to detect different types of events

E. Enable selective packet capture using VLAN ACL on the Cisco IPS 4200 Series appliance.

F. Enable all anti-evasive measures to reduce noise.

Correct Answer: ABD

A. Placing the IPS behind a firewall will reduce traffic which will help improve performance - Confirmed Correct

B. Disable unneeded signatures will reduce processing over head which will help improve performance - Unconfirmed Correct

C. Enabling unidirectional capture would improve device performance but it would also result in poor IPS performance - Unconfirmed Incorrect

D. Having multiple Cisco IPS devices in the path each detecting a different type of traffic would balance the load resulting in increased performance on each device - Confirmed correct E. VACL selective packet capture is enabled on the switch, not the device. - Confirmed incorrect F. Enabling all anti-evasive measures would force all traffic through the device likely causing an increase in noice (not a reduction) and the increased traffic would cause increased load on the device resulting in decrease performance. - Confirmed Incorrect

http://my.safaribooksonline.com/book/certification/ccnp/9780132372107/deploying-cisco-ips-for- highavailability-and-high-performance/499#

QUESTION 3

Which two interface modes can be implemented with a single physical sensing interface on the Cisco IPS 4200 Series appliance? (Choose two.)

A. inline interface pair

B. inline VLAN groups

C. inline VLAN pair

D. promiscuous

E. hardware bypass

Correct Answer: CD

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

QUESTION 4

The Cisco IPS appliance risk category is used with which other feature?

A. anomaly detection

B. event action overrides

C. global correlation

D. reputation filter

Correct Answer: B

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/idm/idm_event_action_rules. html#wp2068398

QUESTION 5

Passive operating system fingerprinting can be used to determine which aspect of the event risk rating?

A. target value rating

B. watch list rating

C. signature fidelity rating

D. attack severity rating

E. promiscuous delta

F. attack relevancy rating

Correct Answer: F

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd806e7299.html

QUESTION 6

When upgrading a Cisco IPS AIM or IPS NME using manual upgrade, what must be performed before installing the upgrade?

A. Disable the heartbeat reset on the router.

B. Enable fail-open IPS mode.

C. Enable the Router Blade Configuration Protocol.

D. Gracefully halt the operating system on the Cisco IPS AIM or IPS NME.

Correct Answer: A

http://www.cisco.com/en/US/docs/security/ips/7.0/release/notes/18483_01.html Using manual upgrade:

if you want to manually update your sensor, copy the 7.0(1)E3 update files to the directory on the server that your sensor polls for updates.

when you upgrade the AIM IPS or the NME IPS using manual upgrade, you must disable heartbeat reset on the router before installing the upgrade. You can reenable heartbeat reset after you complete the upgrade. If you do not disable

heartbeat reset, the upgrade can fail and leave the AIM IPS or the NME IPS in an unknown state, which can require a system reimage to recover.

QUESTION 7

Which four statements about Cisco IPS appliance anomaly detection histograms are true? (Choose four.)

A. Histograms are learned or configured manually.

B. Destination IP address row is the same for all histograms.

C. Source IP address row can be learned or configured.

D. Anomaly detection only builds a single histogram for all services in a zone.

E. You can enable a separate histogram and scanner threshold for specific services, or use the default one for all other services

F. Anomaly detection histograms only track source (attacker) IP addresses.

Correct Answer: ABCE

QUESTION 8

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

A. SNMP

B. IDM or IME

C. global correlation

D. remote blocking

E. anomaly detection

F. SDEE

Correct Answer: A

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_system_architecture.ht ml#wp1009053

NotificationApp allows the sensor to send alerts and system error messages as SNMP traps. It subscribes to events in the Event Store and translates them into SNMP MIBs and sends them to destinations through a public-domain SNMP agent. NotificationApp supports sending sets and gets. The SNMP GETs provide information about basic sensor health.

QUESTION 9

Which of these depicts the correct process order of the Cisco IPS reputation filters and global correlation operations?

A. IPS reputation filters > signature inspection > global correlation

B. IPS reputation filters > global correlation > signature inspection

C. global correlation > IPS reputation filters > signature inspection

D. signature inspection > IPS reputation filters > global correlation

Correct Answer: A

http://www.cisco.com/en/US/prod/collateral/modules/ps2641/solution_overview_cisco_ips_aim.ht ml

QUESTION 10

Which protocol is used by Encapsulated Remote SPAN?

A. ESP

B. GRE

C. TLS

D. STP

E. VTI

F. 802.1Q

Correct Answer: B

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/span.html#wp1059482

ERSPAN Overview

ERSPAN supports source ports, source VLANs, and destination ports on different switches, which provides remote monitoring of multiple switches across your network (see Figure 52-3). ERSPAN consists of an ERSPAN source session,

routable ERSPAN GRE-encapsulated traffic, and an ERSPAN destination session. You separately configure ERSPAN source sessions and destination sessions on different switches.

To configure an ERSPAN source session on one switch, you associate a set of source ports or VLANs with a destination IP address, ERSPAN ID number, and optionally with a VRF name. To configure an ERSPAN destination session on

another switch, you associate the destination ports with the source IP address, ERSPAN ID number, and optionally with a VRF name.

ERSPAN source sessions do not copy locally sourced RSPAN VLAN traffic from source trunk ports that carry RSPAN VLANs. ERSPAN source sessions do not copy locally sourced ERSPAN GRE-encapsulated traffic from source ports.

Each ERSPAN source session can have either ports or VLANs as sources, but not both. The ERSPAN source session copies traffic from the source ports or source VLANs and forwards the traffic using routable GRE-encapsulated packets to

the ERSPAN destination session. The ERSPAN destination session switches the traffic to the destination ports.

QUESTION 11

Which Cisco IPS signature parameter cannot be edited using IDM?

A. signature name

B. signature engine type

C. signature type

D. vulnerable OS list

E. event count key

Correct Answer: B

http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.0.1/user/guide/ipsvchap.html

QUESTION 12

Which two statements are true with respect to IPS false negatives? (Choose two.)

A. A false negative is the failure of the IPS to create an alert on malicious activity.

B. Increasing event count thresholds can lead to false negatives.

C. A false negative results in an IPS alert that is associated with an unsuccessful denial of service attack.

D. Disabling anti-evasion features of the IPS can reduce false negatives.

E. False negatives can only occur when an IPS sensor is in promiscuous mode.

Correct Answer: AB

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd805c389a.html

642-627 PDF 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 !

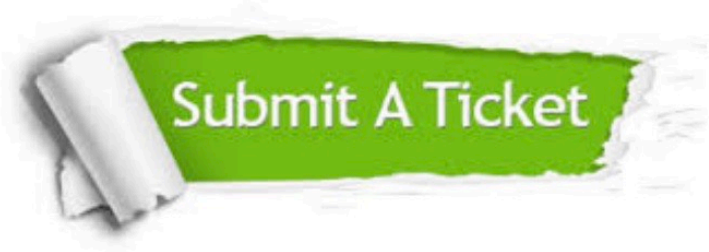
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.certbus.com/allproducts

Need Help

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



Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © certbus, All Rights Reserved.