VCE & PDF
passapply.com

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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Select and Place:

Click and drag the Cisco IPS module on the left to the correct device that it supports on the right.

AIP-SSM		ISR
IDSM-2		ASA 5520
IPS AIM or IPS NME		Catalyst 6500
AIP-SSC		ASA 5505

Correct Answer:

Click and drag the Cisco IPS module on the left to the correct device that it supports on the right.

		IPS AIM or IPS NME
		AIP-SSM
		IDSM-2
		AIP-SSC

QUESTION 2

Which Cisco IPS appliance feature is best used to detect these two conditions? 1) The network starts becoming congested by worm traffic. 2) A single worm-infected source enters the network and starts scanning for other vulnerable hosts.

A. global correlation

B. anomaly detection

C. reputation filtering

D. custom signature

E. meta signature

F. threat detection

Correct Answer: B

http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security

_manager/4.0/user/guide/ipsanom.html

Anomaly detection identifies worm-infected hosts by their behavior as a scanner. To spread, a worm virus must find new hosts. It finds them by scanning the Internet using TCP, UDP, and other protocols to generate unsuccessful attempts to access different destination IP addresses. A scanner is defined as a source IP address that generates events on the same destination port (in TCP and UDP) for too many destination IP addresses.

QUESTION 3

Refer to the exhibit of a partial Cisco IPS appliance CLI configurations, what is the purpose of the access-list CLI command?

A. to define network objects that are used for IPS policy application

B. to specify which traffic will be analyzed on the sensing interfaces of the IPS sensor

C. to configure manually blocked IP addresses

D. to specify trusted management IP addresses for SSH and HTTPS access to the IPS appliance

Correct Answer: D

QUESTION 4

Which two IPS appliance configuration options are used in conjunction with the attack relevance rating feature? (Choose two.)

A. OS mappings

B. OS risk category levels

C. passive OS fingerprinting

D. OS target value rating

E. OS event action filter

F. OS event action override

Correct Answer: AC

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper09
00aecd80191021.html

QUESTION 5

Select and Place:

Click and drag the rating or weight on the left to the correct description on the right.

SFR	indicates how accurately the signature detects the event
ASR	associated with the relevancy of the targeted OS
TVR	associated with the severity of a successful exploit of the vulnerability
ARR	associated with the perceived value of the target
PD	value subtracted from the overall RR
WLR	associated with the Management Center for Cisco Security Agent

Correct Answer:

Click and drag the rating or weight on the left to the correct description on the right.   5 / 6

	SFR
	ARR
	ASR
	TVR
	PD
	WLR

To Read the Whole Q&As, please purchase the Complete Version from Our website.
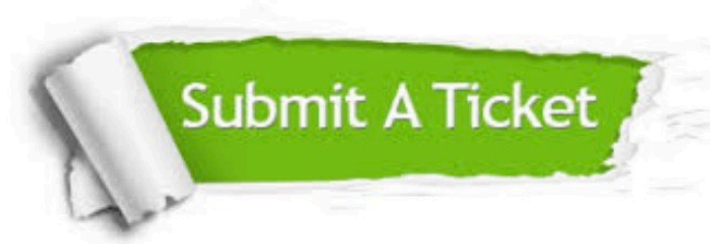
Try our product !

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:

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.