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

QUESTION 1

Which IPS alert action is available only in inline mode?

A. produce verbose alert

B. request rate limit

C. reset TCP connection

D. log attacker/victim pair packets

E. deny-packet-inline

F. request block connection

Correct Answer: E

http://www.cisco.com/web/about/security/intelligence/ipsmit.html

Inline Mode Event Actions

The following actions require the device to be deployed in Inline mode and are in affect for a user- configurable default time of 3600 seconds (60 minutes). Deny attacker inline: This action is the most severe and effectively blocks all

communication from the attacking host that passes through the IPS for a specified period of time. Because this event action is severe, administrators are advised to use this only when the probability of false alarms or spoofing is minimal.

Deny attacker service pair inline: This action prevents communication between the attacker IP address and the protected network on the port in which the event was detected. However, the attacker would be able to communicate on another

port that has hosts on the protected network. This event action works well for worms that attack many hosts on the same service port. If an attack occurred on the same host but on another port, this communication would be allowed. This

event action is appropriate when the likelihood of a false alarm or spoofing is minimal. Deny attacker victim pair inline: This action prevents the attacker from communicating with the victim on any port. However, the attacker could

communicate with other hosts, making this action better suited for exploits that target a specific host. This event action is appropriate when the likelihood of a false alarm or spoofing is minimal.

Deny connection inline: This action prevents further communication for the specific TCP flow. This action is appropriate when there is the potential for a false alarm or spoofing and when an administrator wants to prevent the action but not

deny further communication. Deny packet inline: This action prevents the specific offending packet from reaching its intended destination.

Other communication between the attacker and victim or victim network may still exist. This action is appropriate when there is the potential for a false alarm or spoofing. Note that for this action, the default time has no effect.

Modify packet inline: This action enables the IPS device to modify the offending part of the packet. However, it forwards the modified packet to the destination. This action is appropriate for packet normalization and other anomalies, such as

TCP segmentation and IP fragmentation re-ordering.

QUESTION 2

Which configuration is required when setting up the initial configuration on the Cisco ASA 5505 to support the Cisco ASA AIP-SSC?

A. Configure a VLAN interface as a management interface to access the Cisco ASA AIP-SSC.

B. Using MPF, configure which virtual sensor to use.

C. Configure a management access rule to allow Cisco ASDM access from the Cisco ASA AIP- SSC management interface IP address.

D. Configure a management access rule to allow SSH access from the Cisco ASA AIP-SSC management interface IP address.

Correct Answer: A

http://www.cisco.com/en/US/docs/security/asa/quick_start/ips/ips_qsg.html

2 Connecting Management Interface Cables

?SA 5505--The ASA 5505 does not have a dedicated management interface. You must use an ASA VLAN to access an internal management IP address over the backplane. Connect the management PC to one of the following ports:

Ethernet 0/1 through 0/7. These ports are assigned to VLAN 1 using the 192.168.1.1/24 address. The internal IPS management address is 192.168.1.2/24.

QUESTION 3

Which three statements are true with respect to IPS false positives? (Choose three.)

A. An example of a false positive is when the IPS appliance produces an alert in response to the normal activities of the company\\'s network management system.

B. Increasing the set of TCP ports that a signature matches on may reduce false positives.

C. False positives may be reduced by disabling certain signatures.

D. Event action filters can be implemented to reduce false positives.

E. An example of a false positive is the IPS not reacting to a successful denial of service attack.

Correct Answer: ACD

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/cli/cli_signature_definitions.h tml#wp1094231

Understanding Signatures

Attacks or other misuses of network resources can be defined as network intrusions. Sensors that use a signature-based technology can detect network intrusions. A signature is a set of rules that your sensor uses to detect typical intrusive

activity, such as DoS attacks. As sensors scan network packets, they use signatures to detect known attacks and respond with actions that you define. The sensor compares the list of signatures with network activity. When a match is found,

the sensor takes an action, such as logging the event or sending an alert. Sensors let you modify existing signatures and define new ones.

Signature-based intrusion detection can produce false positives because certain normal network activity can be misinterpreted as malicious activity. For example, some network applications or operating systems may send out numerous ICMP

messages, which a signature-based detection system might interpret as an attempt by an attacker to map out a network segment. You can minimize false positives by tuning your signatures.

To configure a sensor to monitor network traffic for a particular signature, you must enable the signature. By default, the most critical signatures are enabled when you install the signature update. When an attack is detected that matches an

enabled signature, the sensor generates an alert, which is stored in the Event Store of the sensor. The alerts, as well as other events, may be retrieved from the Event Store by web-based clients. By default the sensor logs all Informational

alerts or higher.

Some signatures have subsignatures, that is, the signature is divided into subcategories. When you configure a subsignature, changes made to the parameters of one subsignature apply only to that subsignature. For example, if you edit

signature 3050 subsignature 1 and change the severity, the severity change applies to only subsignature 1 and not to 3050 2, 3050 3, and 3050 4.

Cisco IPS 6.1 contains over 10,000 built-in default signatures. You cannot rename or delete signatures from the list of built-in signatures, but you can retire signatures to remove them from the sensing engine. You can later activate retired

signatures; however, this process requires the sensing engines to rebuild their configuration, which takes time and could delay the processing of traffic. You can tune built-in signatures by adjusting several signature parameters. Built-in

signatures that have been modified are called tuned signatures.

QUESTION 4

Which Cisco IPS signature parameter can be tuned to reduce the volume of the alerts that are written to the event store?

A. alert action

B. alert frequency

C. alert fidelity rating

D. alert severity

E. alert firing mode

F. alert logging

Correct Answer: B

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/cli/cli_signature_definitions.h tml#wp1094231

Configuring Alert Frequency

Use the alert-frequency command in signature definition submode to configure the alert frequency for a signature. The alert-frequency command specifies how often the sensor alerts you when this signature is firing.

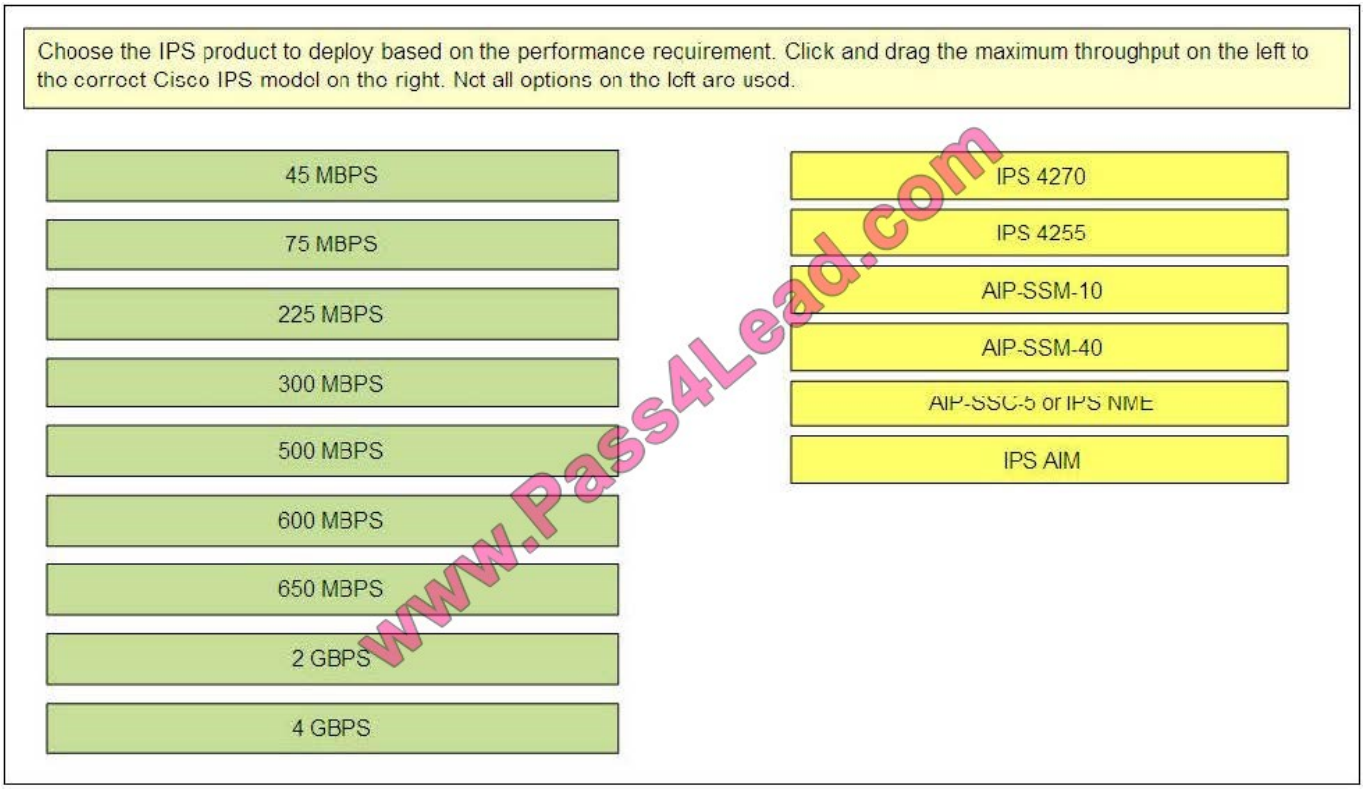
The following options apply:

?ig_id--Identifies the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature. The value is 1000 to 65000. ?ubsig_id--Identifies the unique numerical value assigned to this subsignature. A

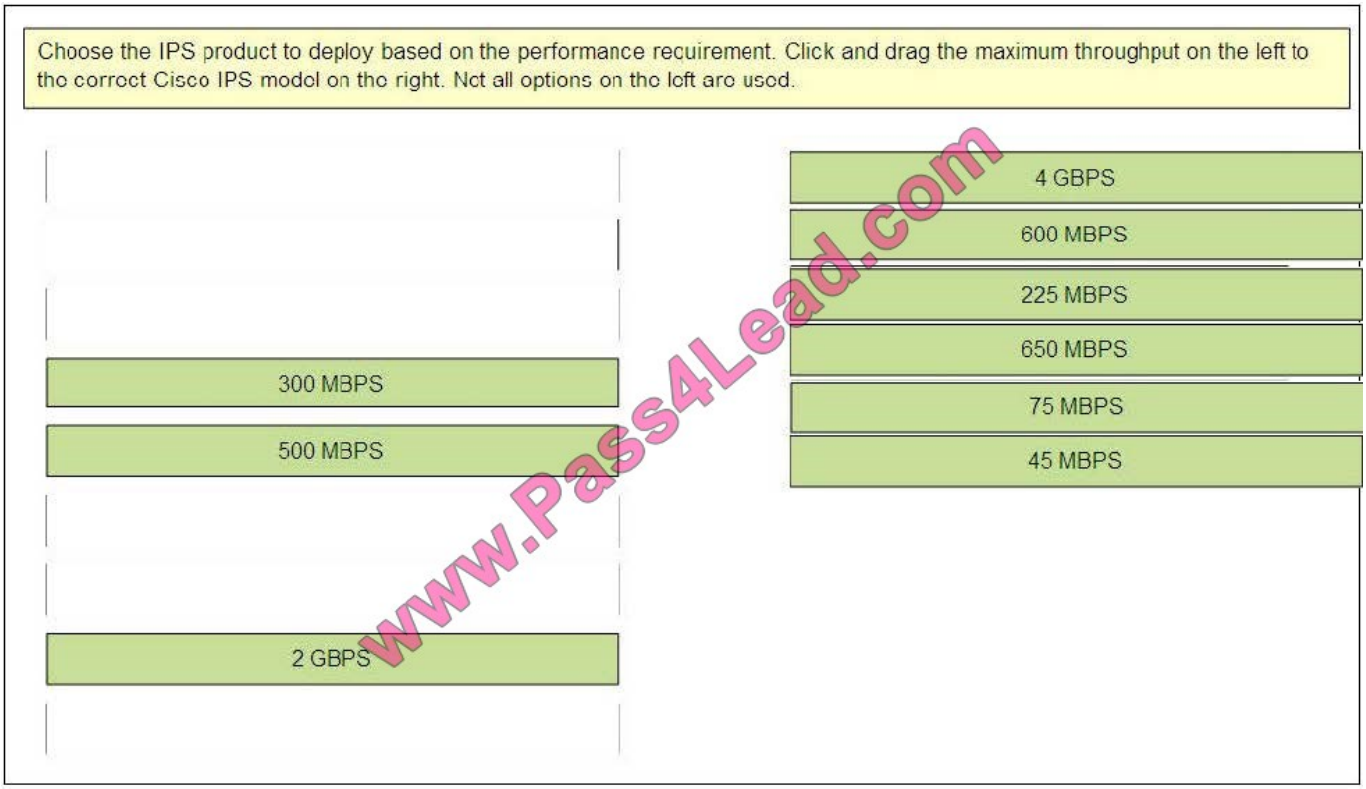
subsignature ID is used to identify a more granular version of a broad signature. The value is 0 to 255.

QUESTION 5

Select and Place:



Correct Answer:



[Latest 642-627 Dumps](#) [642-627 PDF Dumps](#) [642-627 Exam Questions](#)

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: