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

QUESTION 1

Which global correlation data is sent to the Cisco SensorBase Network with full network participation that is not sent with partial network participation?

A. attack type

B. connecting IP address and port

C. victim IP address and port

D. protocol attributes

E. IPS appliance CPU and memory usage information

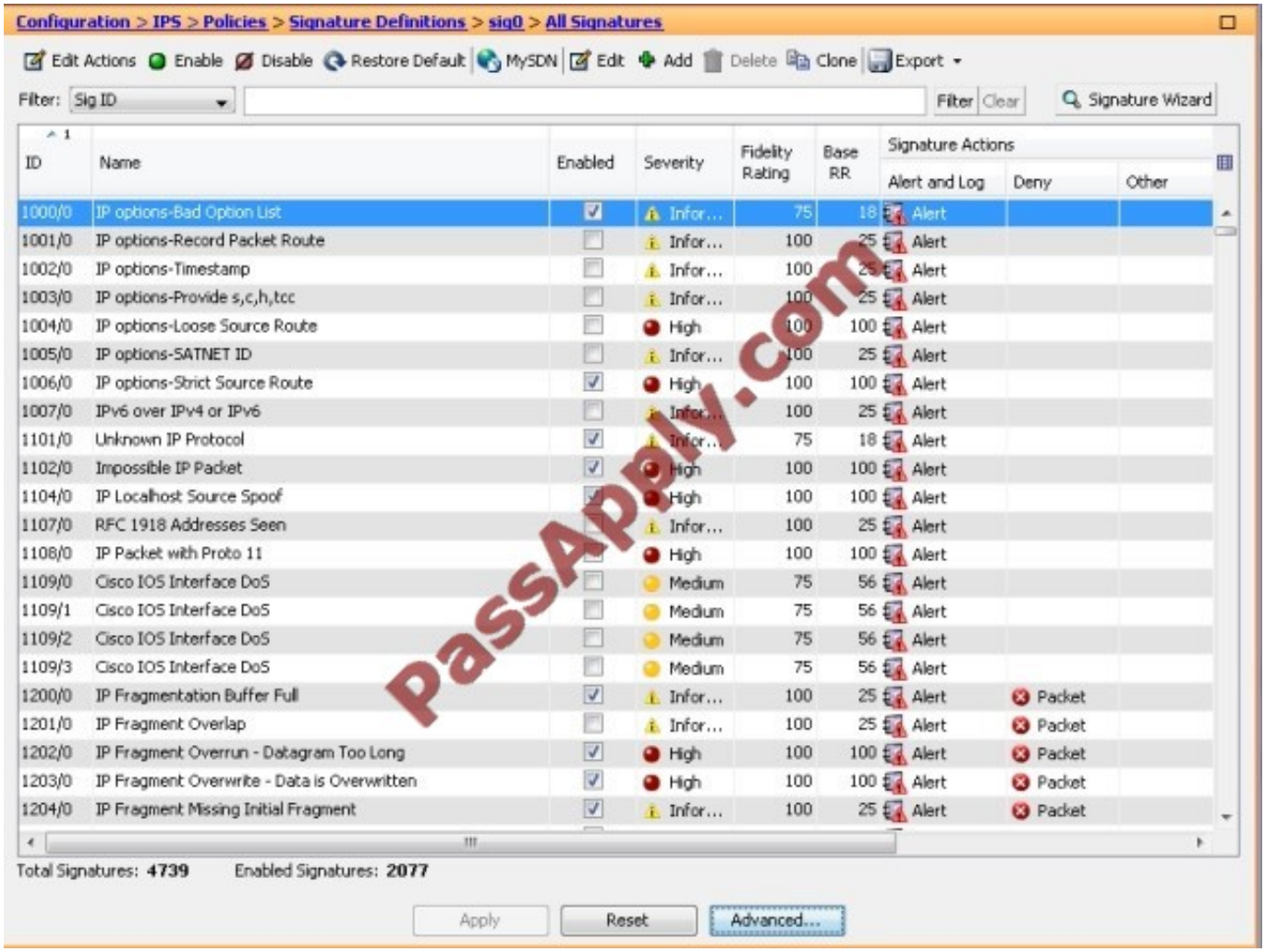
Correct Answer: C

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/idm/idm_collaboration.html# wp1053292

In the Network Participation pane, you can configure the sensor to send data to the SensorBase Network. You can configure the sensor to fully participate and send all data to the SensorBase Network. Or you can configure the sensor to collect the data but to omit potentially sensitive data, such as the destination IP address of trigger packets.

QUESTION 2

Refer to the exhibit.



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

QUESTION 3

Refer to the exhibit.

Which statement is true about the IPS signature shown?

A. To match a string, the regular expression requires zero or more period characters (.) to immediately precede the newline character.

B. A summary alert is sent once during each interval for each unique Summary Key entry.

C. An alert is generated each time the signature triggers.

D. This signature does not fire until three events are seen during 60 minutes with the same attacker and victim IP addresses and ports.

E. This signature does not analyze traffic that is sent from the SMTP server to the client.

Correct Answer: D

QUESTION 4

Which three are global correlation network participation modes? (Choose three.)

A. off

B. partial participation

C. reputation filtering

D. detect

E. full participation

F. learning

Correct Answer: ABE

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

QUESTION 5

Numerous attacks using duplicate packets, changed packets, or out-of-order packets are able to successfully evade and pass through the Cisco IPS appliance when it is operating in inline mode. What could be causing this problem?

A. The IPS Application Inspection and Control is disabled.

B. All the DoS signatures are disabled.

C. All the reconnaissance signatures are disabled.

D. TCP state bypass is enabled.

E. The normalizer is set to asymmetric mode.

Correct Answer: E

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

QUESTION 6

What are four properties of an IPS signature? (Choose four.)

A. reputation rating

B. fidelity rating

C. summarization strategy

D. signature engine

E. global correlation mode

F. signature ID and signature status

Correct Answer: BCDF

http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.1/user/guide/ipsvchap.html#wp1912551 Reputation and correaltion are NOT

QUESTION 7

Which Cisco IPS NME interface is visible to the NME module but not visible in the router configuration and acts as the sensing interface of the NME module?

A. ids-sensor 0/1 interface

B. ids-sensor 1/0 interface

C. gigabitEthernet 0/1

D. gigabitEthernet 1/0

E. management 0/1

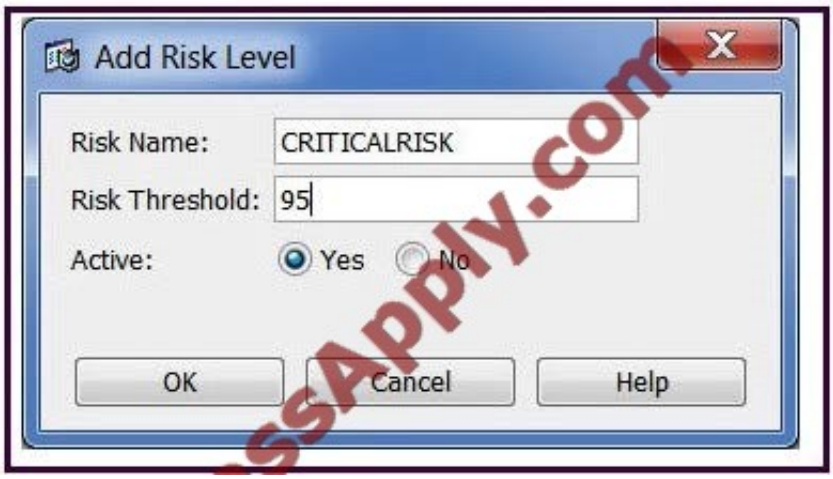
F. management 1/0

Correct Answer: C

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_nme.html#wp1057817

QUESTION 8

Refer to the exhibit. What does the Risk Threshold setting of 95 specify?



A. the low risk rating threshold

B. the low threat rating threshold

C. the low target value rating threshold

D. the high risk rating threshold

E. the high threat rating threshold

F. the high target value rating threshold

Correct Answer: D

HIGHRISK = 90 - 100 - = Red Threat

QUESTION 9

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

A. SDEE

B. global correlation

C. anomaly detection

D. remote blocking

E. virtual sensor

F. OS fingerprinting

Correct Answer: D

http://www.cisco.com/en/US/docs/security/ips/6.1/installation/guide/hw_troubleshooting.html#wpm kr1185768

QUESTION 10

Which Cisco IPS appliance CLI command is used to display information in the IPS Event Store?

A. show config

B. show events

C. show database

D. show sdee

E. show log

F. show event-store

G. show alerts

Correct Answer: B

show events To display the local event log contents, use the show events command in EXEC mode. show events [{alert [informational] [low] [medium] [high] [include-traits traits] [exclude-traits traits] [min-threatrating min-rr] [max-threat-rating max-rr | error [warning] [error] [fatal] | NAC | status}] [hh:mm:ss [month day [year]] | past hh:mm:ss] Syntax Description

alert	Displays alerts. Provides notification of some suspicious activity that may indicate an intrusion attack is in progress or has been attempted. Alert events are generated by the analysis engine whenever an IPS signature is triggered by network activity. If no level is selected (informational, low, medium, high), all alert events are displayed.
include-traits	Displays alerts that have the specified traits.
exclude-traits	Does not display alerts that have the specified traits.
traits	Trait bit position in decimal (0-15).
min-threat-rating	Displays events with a threat rating above or equal to this value. The valid range is 0 to 100. The default is 0.
max-threat-rating	Displays events with a threat rating below or equal to this value. The valid range is 0 to 100. The default is 100.
error	Displays error events. Error events are generated by services when error conditions are encountered. If no level is selected (warning, error, or fatal), all error events are displayed.
NAC	Displays ARC requests (block requests). **Note** Network Access Controller is now known as Attack Response Controller (ARC). Although the service has a new name, the change is not reflected in the Cisco IPS 6.2 and later CLI. You will still see network-access and nac throughout the CLI.
status	Displays status events.
hh:mm:ss	Starts time in hours (24-hour format), minutes, and seconds.
day	Starts day (by date) in the month.
month	Starts month (by name).
year	Starts year (no abbreviation).
past	Displays events starting in the past. The hh:mm:ss specify a time in the past to begin the display.

QUESTION 11

Which parameter is used to configure a signature to fire if the activity it detects happens a certain number of times for the same address set within a specified period of time?

A. event action

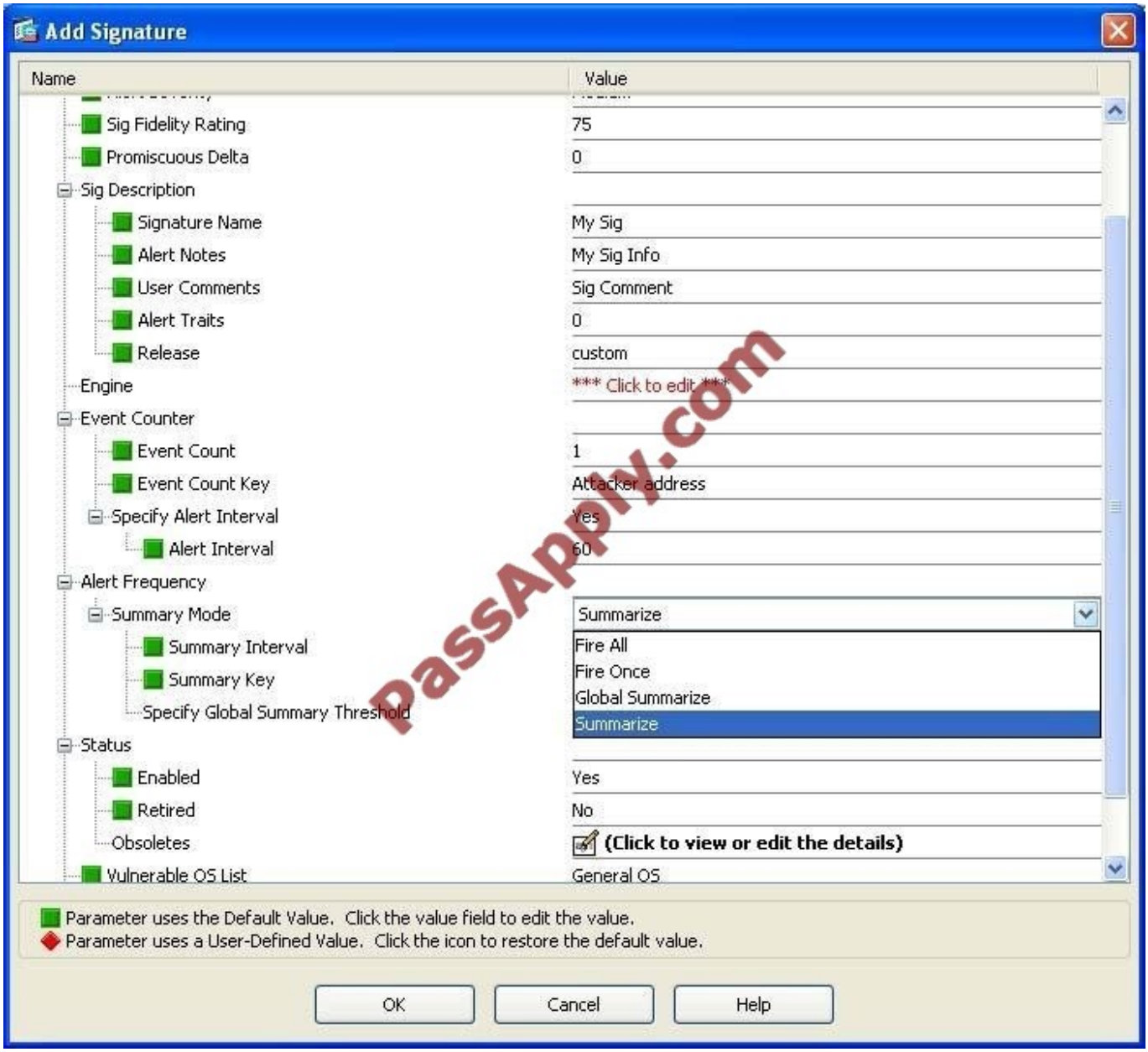
B. event counter

C. summary count

D. summary key

Correct Answer: B

http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.1/user/guide/ipsvchap.pdf



QUESTION 12

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