Fast2Test
FIRST TEST, FIRST PASS!

Fast2Test

We're not the only ones **happy** about Fast2test Practice Materials ...

62316+ customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

https://kr.fast2test.com

유효한 시험자료,최고의 적중율을 자랑하는 시험대비 덤프

Exam : **642-627**

Title : Implementing Cisco Intrusion Prevention System v7.0

Vendors : Cisco

Version : DEMO

NO.1 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
Answer: B
Explanation:
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

NO.2 Which two statements accurately describe virtual sensor operations on the Cisco IPS appliance? (Choose two.)
A. You must create a new instance of a signature set for each new virtual sensor.
B. The packet processing policy is virtualized.
C. Creating a new virtual sensor creates a "virtual" machine on the Cisco IPS appliance.
D. vs0 can be cloned then deleted.
E. Each virtual sensor can have its own unique event action rules.
Answer: B,E
Explanation:
http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/cli/cli_virtual_sensors.html # wp1029979

NO.3 When setting up a Cisco IPS appliance in promiscuous mode, which Cisco Catalyst switch CLI command is used to configure SPAN on the switch?
A. span source in interface configuration mode
B. span session in global configuration mode
C. monitor destination in interface configuration mode
D. monitor session in global configuration mode
E. mirror session in global configuration mode
Answer: D
Explanation:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612. shtml

NO.4 Which Cisco IPS appliance TCP session tracking mode should be used if packets of the same session are coming to the sensor over different interfaces, but should be treated as a single session?
A. interface and VLAN
B. virtual sensor
C. VLAN only

D. promiscuous
E. normalizer
Answer: B
Explanation:
http://www.cisco.com/en/US/docs/security/ips/7.1/configuration/guide/ime/ime_policies.html#wp20
Inline TCP Session Tracking Mode When you choose to modify packets inline, if the packets from a stream are seen twice by the Normalizer engine, it cannot properly track the stream state and often the stream is dropped. This situation occurs most often when a stream is routed through multiple VLANs or interfaces that are being monitored by the IPS. A further complication in this situation is the necessity of allowing asymmetric traffic to merge for proper tracking of streams when the traffic for either direction is received from different VLANs or interfaces.
To deal with this situation, you can set the mode so that streams are perceived as unique if they are received on separate interfaces and/or VLANs (or the subinterface for VLAN pairs). The following inline TCP session tracking modes apply:
Interface and VLAN-All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) and on the same interface belong to the same session. Packets with the same key but on different VLANs are tracked separately.
VLAN Only-All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) regardless of the interface belong to the same session. Packets with the same key but on different VLANs are tracked separately.
Virtual Sensor-All packets with the same session key (AaBb) within a virtual sensor belong to the same session. This is the default and almost always the best option to choose.

NO.5 The Cisco IPS appliance global correlation and reputation filtering features depend on which two of these? (Choose two.)
A. anomaly detection
B. OS fingerprinting
C. Cisco SensorBase
D. watch list ratings
E. event action overrides
F. DNS
Answer: C,F
Explanation:
http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.1/user/guide/ipsglobe.html

NO.6 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.
Answer: A,B,C,E

NO.7 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
Answer: A,B,E
Explanation:
http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/idm/idm_collaboration.html