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

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

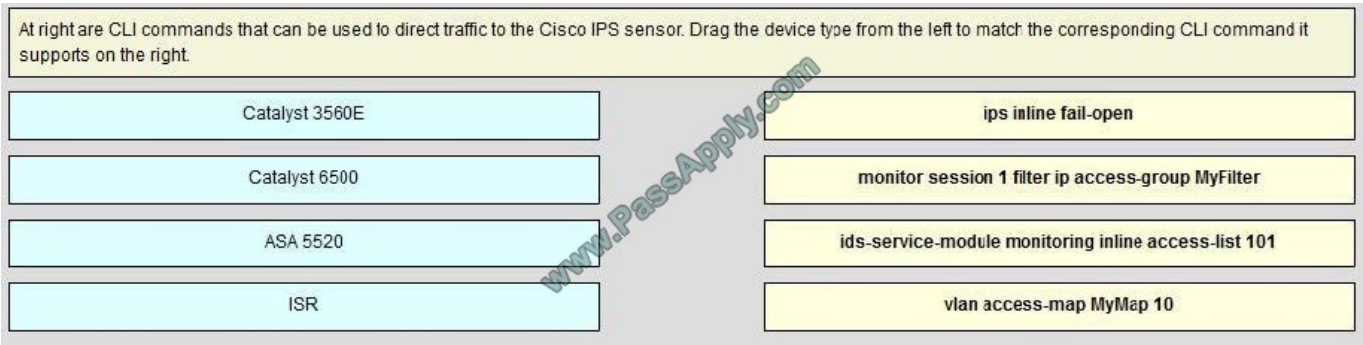
F. OS fingerprinting

Correct Answer: D

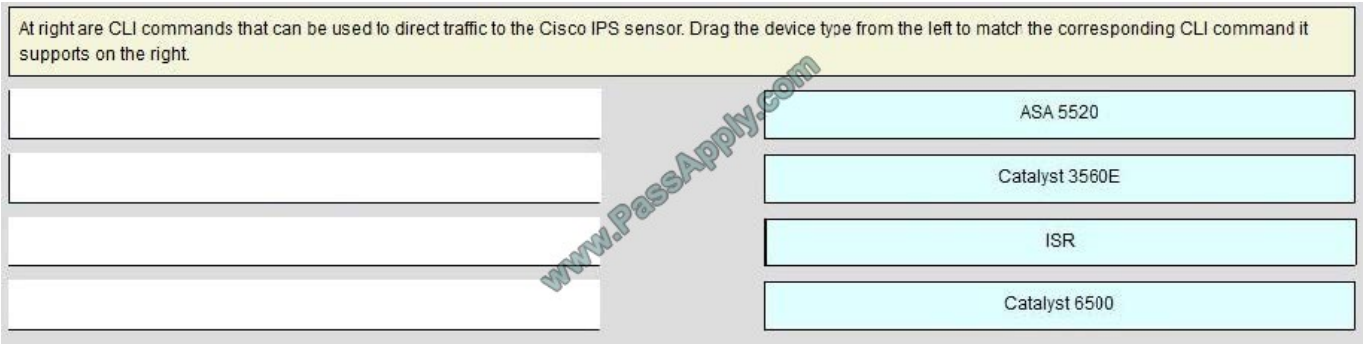
http://www.cisco.com/en/US/docs/security/ips/6.1/installation/guide/hw_troubleshooting.html#wpm kr1185768

QUESTION 2

Select and Place:



Correct Answer:



QUESTION 3

Which Cisco IPS appliance feature uses profile-based intrusion detection?

A. profiler

B. anomaly detection

C. threat detection

D. netflow

E. reputation filter

F. senderbase

Correct Answer: B

QUESTION 4

The default virtual sensor on all IPS appliances is vs0. Which three components are assigned to vs0 by default? (Choose three.)

A. sig0

B. engine0

C. rules0

D. ad0

E. filters0

F. gc0

Correct Answer: ACD

http://www.cisco.com/en/US/docs/security/ips/7.1/configuration/guide/idm/idm_policies.html

The sensor can receive data inputs from one or many monitored data streams. These monitored data streams can either be physical interface ports or virtual interface ports. For example, a single sensor can monitor traffic from in front of the firewall, from behind the firewall, or from in front of and behind the firewall concurrently. And a single sensor can monitor one or more data streams. In this situation a single sensor policy or configuration is applied to all monitored data streams.

A virtual sensor is a collection of data that is defined by a set of configuration policies. The virtual sensor is applied to a set of packets as defined by interface component. A virtual sensor can monitor multiple segments, and you can apply a different policy or configuration for each virtual sensor within a single physical sensor. You can set up a different policy per monitored segment under analysis. You can also apply the same policy instance, for example, sig0, rules0, or ad0, to different virtual sensors. You can assign interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups to a virtual sensor.

QUESTION 5

Refer to the exhibit.

Configuring traffic flow notifications on the Cisco IPS appliance is most useful in what situation?

A. to determine the IPS throughput rate when using inline mode

B. to detect IPS performance issues

C. to enable bypass mode when the Cisco IPS appliance fails

D. to prevent DoS attacks

Correct Answer: B

http://www.cisco.com/en/US/docs/security/ips/5.0/configuration/guide/idm/dminter.html#wp103214