ISLEVER

642-627

Implementing Cisco Intrusion Prevention System v7.0 - (IPS v7.0)

DEMO

https://www.islever.com/642-627.html

https://www.islever.com/cisco.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

QUESTION NO: 1

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

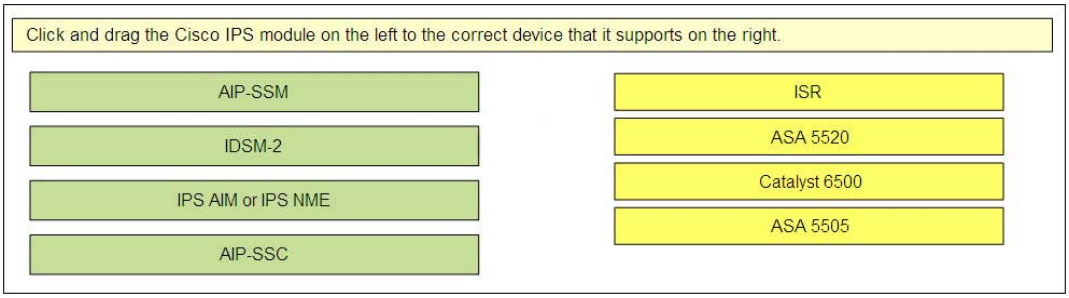
A. off
B. partial participation
C. reputation filtering
D. detect
E. full participation
F. learning

Answer: A,B,E

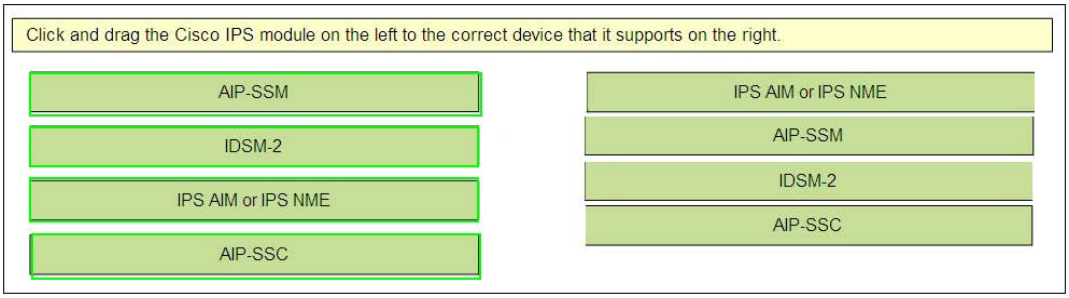
Explanation:

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

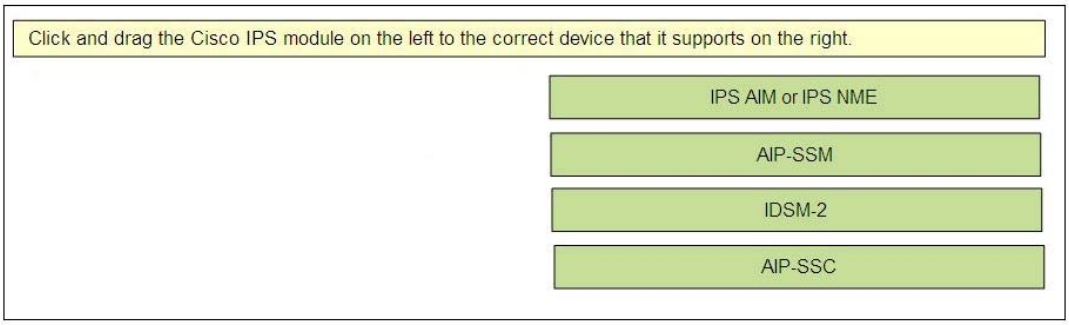
QUESTION NO: 2 DRAG DROP



Answer:



Explanation:



QUESTION NO: 3

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

Answer: B,C,D,F
Explanation:
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 NO: 4

The custom signature ID of a Cisco IPS appliance has which range of values?

A. 10000 to 19999
B. 20000 to 29999
C. 50000 to 59999
D. 60000 to 65000
E. 80000 to 90000
F. 1 to 20000

Answer: D

Explanation:

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

Signature Identification Field Definitions

The following fields and buttons are found in the Signature Identification window of the Custom Signature Wizard.

Field Descriptions:

•Signature ID—Identifies the unique numerical value assigned to this signature.

The signature ID lets the sensor identify a particular signature. The signature ID is reported to the Event Viewer when an alert is generated. The valid range is between 60000 and 65000.

QUESTION NO: 5

When upgrading a Cisco IPS AIM or IPS NME using manual upgrade, what must be performed before installing the upgrade?

A. Disable the heartbeat reset on the router.
B. Enable fail-open IPS mode.
C. Enable the Router Blade Configuration Protocol.
D. Gracefully halt the operating system on the Cisco IPS AIM or IPS NME.

Answer: A

Explanation:

http://www.cisco.com/en/US/docs/security/ips/7.0/release/notes/18483_01.html

Using manual upgrade:

–If you want to manually update your sensor, copy the 7.0(1)E3 update files to the directory on the server that your sensor polls for updates.

–When you upgrade the AIM IPS or the NME IPS using manual upgrade, you must disable heartbeat reset on the router before installing the upgrade. You can reenable heartbeat reset after you complete the upgrade. If you do not disable heartbeat reset, the upgrade can fail and leave the AIM IPS or the NME IPS in an unknown state, which can require a system reimage to recover.

QUESTION NO: 6

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?