Cisco 642-627

Implementing Cisco Intrusion Prevention System v7.0

Version: 5.1

QUESTION NO: 1

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

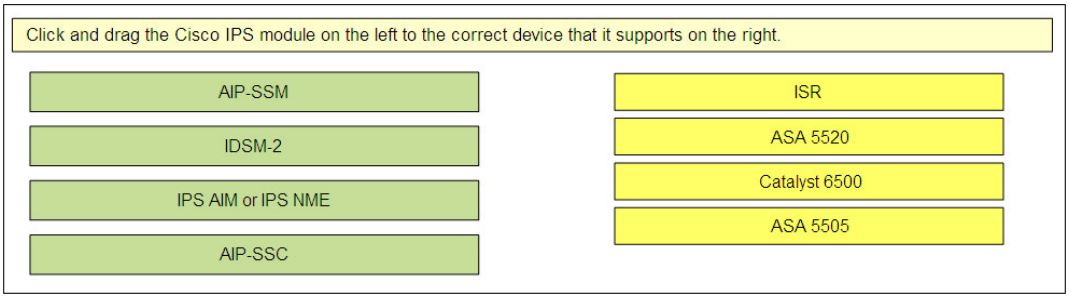
A. off
B. partial participation
C. reputation filtering
D. detect
E. full participation
F. learning

Answer: A,B,E

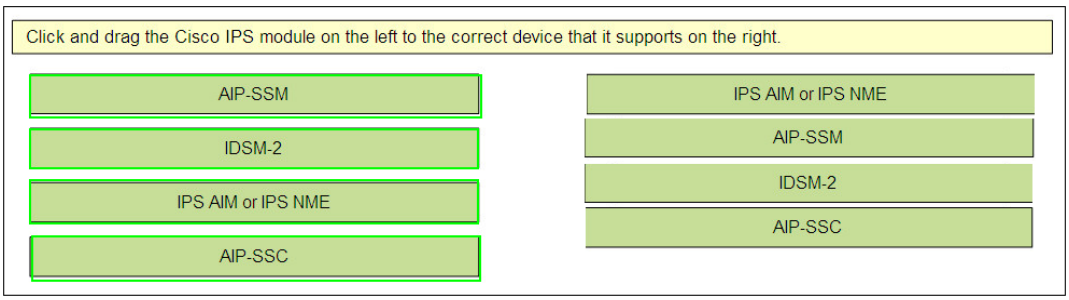
Explanation:

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

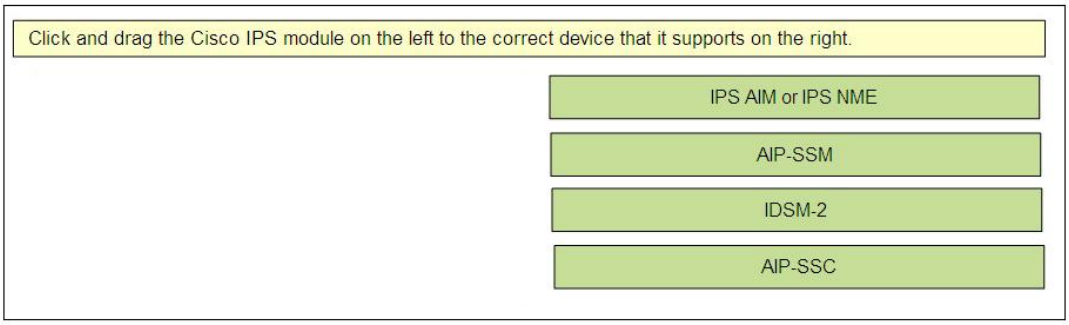
QUESTION NO: 2 DRAG DROP



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?

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

Answer: C

Explanation:

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

QUESTION NO: 7

Which two methods can be used together to configure a Cisco IPS signature set into detection mode when tuning the Cisco IPS appliance to reduce false positives? (Choose two.)

A. Subtract all aggressive actions using event action filters.
B. Enable anomaly detection learning mode.
C. Enable verbose alerts using event action overrides.
D. Decrease the number of events required to trigger the signature.
E. Increase the maximum inter-event interval of the signature.

Answer: A,C

Explanation:

1 > Remove all agressive actions from all signatures using event action filters

2 > Add verbose alerts using event action overrides

3 > Add logging packets between the attacker and the victim using event action overrides

QUESTION NO: 8

In which CLI configuration mode is the Cisco IPS appliance management IP address configured?

A. global configuration
ips(config)#
B. service network-access
ips(config-net)#
C. service host network-settings
ips(config-hos-net)#

D. service interface
ips(config-int)#

Answer: C

Explanation:

http://www.cisco.com/en/US/docs/security/ips/7.1/configuration/guide/cli/cli_setup.html#wp1031325

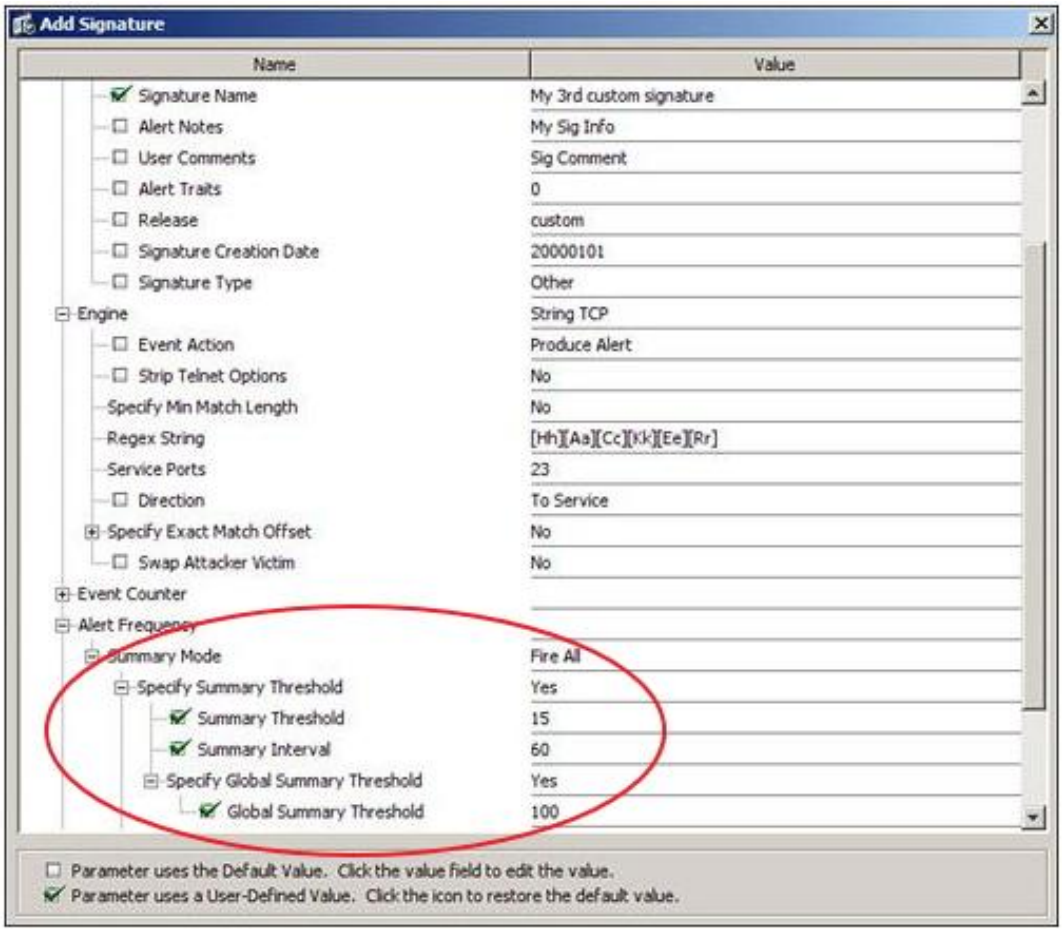
QUESTION NO: 9

Which four parameters are used to configure how often the Cisco IPS appliance generates alerts when a signature is firing? (Choose four.)

A. summary mode
B. summary interval
C. event count key
D. global summary threshold
E. summary key
F. event count
G. summary count
H. event alert mode

Answer: A,B,D,F

Explanation:



NB: Watch for Summary Threshold instead of Event Count

QUESTION NO: 10

Which three Cisco IPS cross-launch capabilities do Cisco Security Manager and Cisco Security MARS support? (Choose three.)

A. Edit IPS signatures in Cisco Security Manager from a Cisco Security MARS query.
B. Create custom signatures in Cisco Security Manager from a Cisco Security MARS query.
C. Create event action filters in Cisco Security Manager from a Cisco Security MARS query.
D. Create a Cisco Security MARS drop rule from Cisco Security Manager policy.
E. Create a Cisco Security MARS user inspection rule from Cisco Security Manager policy.
F. Query Cisco Security MARS from Cisco Security Manager policy.

Answer: A,C,F

Explanation:

"...MARS creates queries that include a launch point for CSM. When CSM is launched, you can carry out the following (cross-connected actions):

Edit an IPS Signature
Add an event action filter to an IPS configuration in Cisco Security Manager and when you use CSM to cross-launch MARS, you can query events that were originated by the signatures in CSM."
http://my.safaribooksonline.com/book/certification/ccnp/9780132372107/integrating-cisco-ips-with-csm-andcisco-security-mars/435#

QUESTION NO: 11

Which statement about inline VLAN pair deployment with the Cisco IPS 4200 Series appliance is true?

A. The sensing interface acts as an 802.1q trunk port, and the Cisco IPS appliance performs VLAN translation between pairs of VLANs.
B. The Cisco IPS appliance connects to two physically distinct switches using two paired physical interfaces.
C. Two sensing interfaces connect to the same switch that forwards traffic between two VLANs.
D. The pair of sensing interfaces can be selectively divided (virtualized) into multiple logical "wires" by VLANs that can be analyzed separately

Answer: A
Explanation:

QUESTION NO: 12

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
Explanation:

QUESTION NO: 13

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

A. SNMP
B. IDM or IME
C. global correlation
D. remote blocking
E. anomaly detection
F. SDEE

Answer: A
Explanation:
http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_system_architecture.html#wp1009053

NotificationApp allows the sensor to send alerts and system error messages as SNMP traps. It subscribes to events in the Event Store and translates them into SNMP MIBs and sends them to destinations through a public-domain SNMP agent. NotificationApp supports sending sets and gets. The SNMP GETs provide information about basic sensor health.

QUESTION NO: 14

Which two switching-based mechanisms are used to deploy high availability IPS using multiple Cisco IPS appliances? (Choose two.)

A. Spanning Tree-based HA
B. HSRP-basedHA
C. EtherChannel-based HA
D. VRRP-basedHA

Answer: A,C
Explanation:
When network switches are used to provide High Availability you have two options

EtherChannel based HA

STP based HA

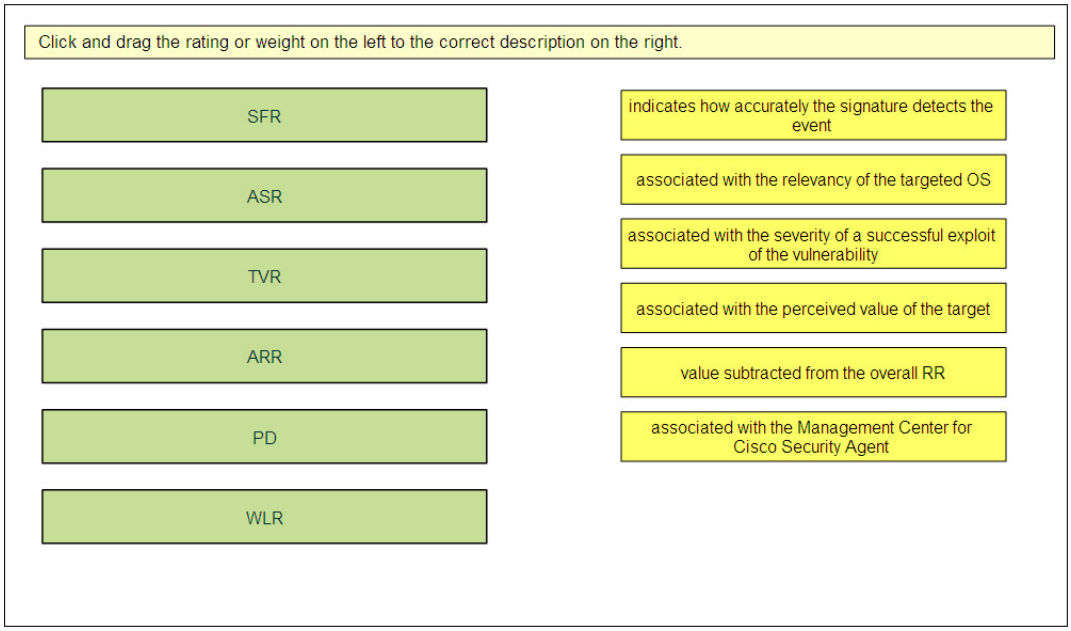
QUESTION NO: 15

Which statement about the 4-port GigabitEthernet card with hardware bypass is true?

A. Hardware bypass only works with inline interface pairs.
B. Hardware bypass is only supported on the Cisco IPS 4270 appliance.
C. Hardware bypass is independent from software bypass.
D. Hardware bypass is enabled if software bypass is configured to "OFF".
E. Hardware bypass is supported between any of the four GigabitEthernet ports

Answer: A
Explanation:

QUESTION NO: 16 DRAG DROP



Answer: