IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

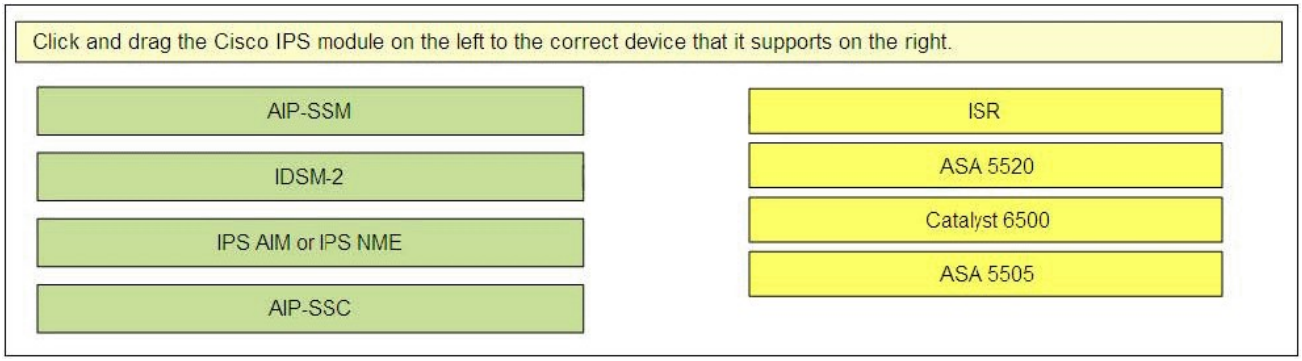
Exam : **642-627**

Title : Implementing Cisco Intrusion Prevention System v7.0

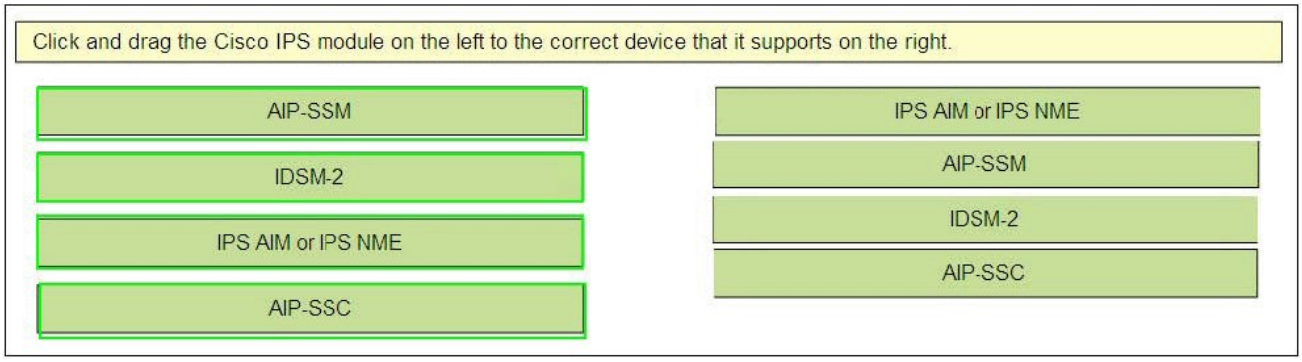
Version : DEMO

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

2.DRAG DROP



Answer:



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

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

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

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

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,E

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

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

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: C,E,F

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

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

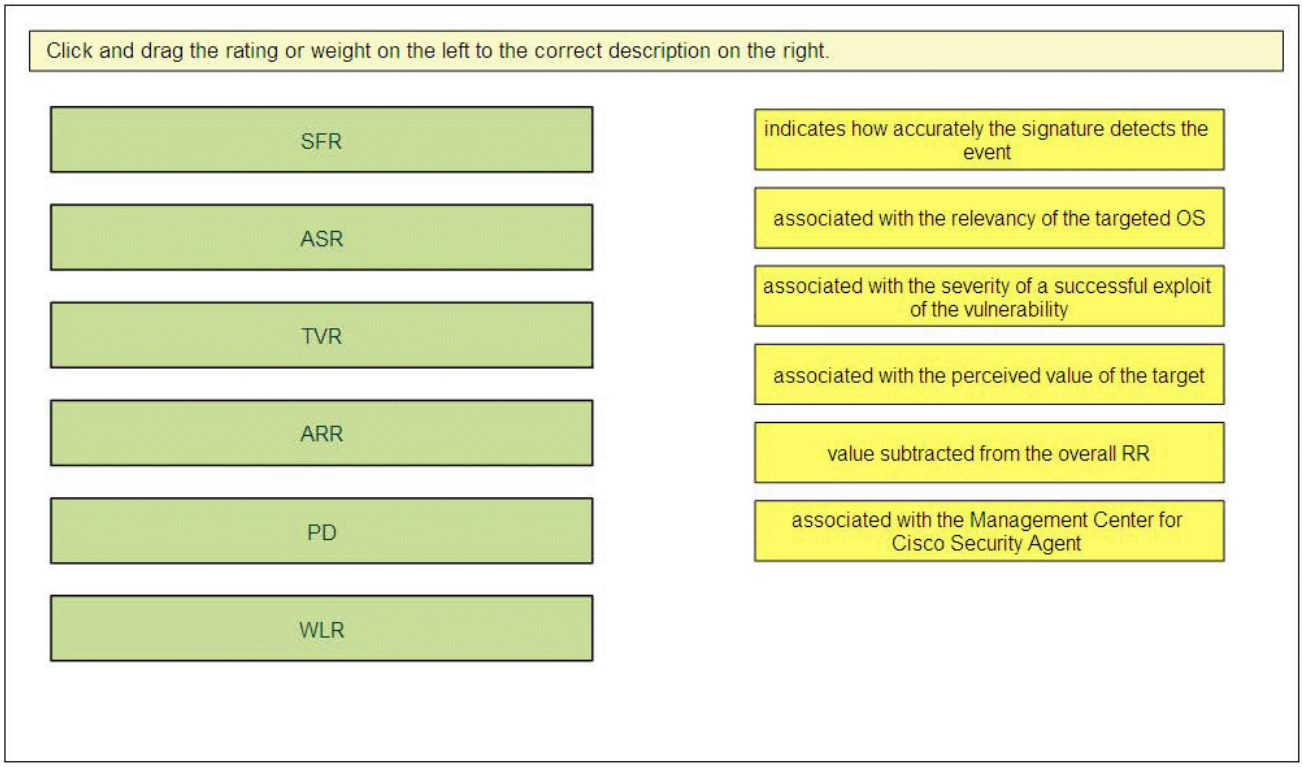
13.You are working with Cisco TAC to troubleshoot a software problem on the Cisco IPS appliance. TAC suspects a fault with the NotificationApp software module in the Cisco IPS appliance. In this case, which Cisco IPS appliance operations may be most affected by the NotificationApp software module fault?
A. SNMP
B. IDM or IME
C. global correlation
D. remote blocking

E. anomaly detection
F. SDEE
Answer: A

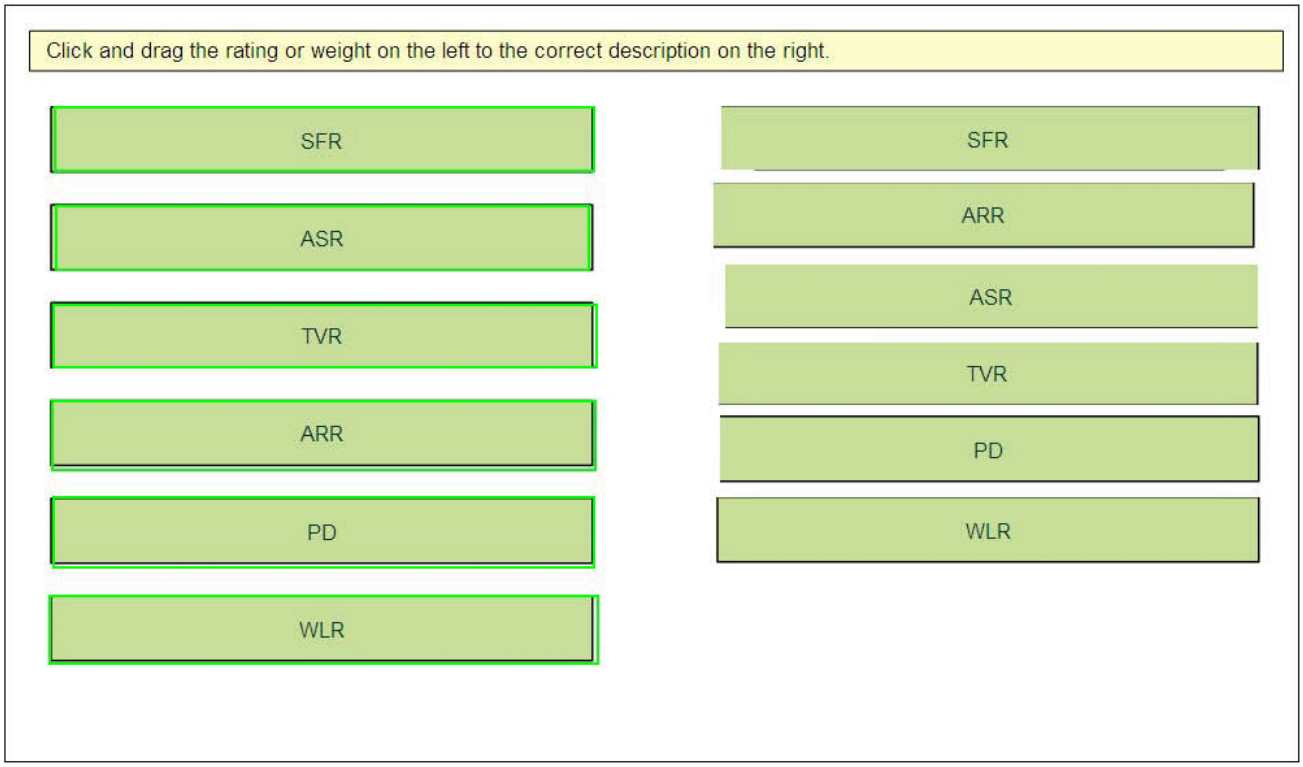
14.Which two switching-based mechanisms are used to deploy high availability IPS using multiple Cisco IPS appliances? (Choose two.)
A. Spanning Tree-based HA
B. HSRP-basedHA
C. EtherChannel-based HA
D. VRRP-basedHA
Answer: A,C

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

16.DRAG DROP



Answer:



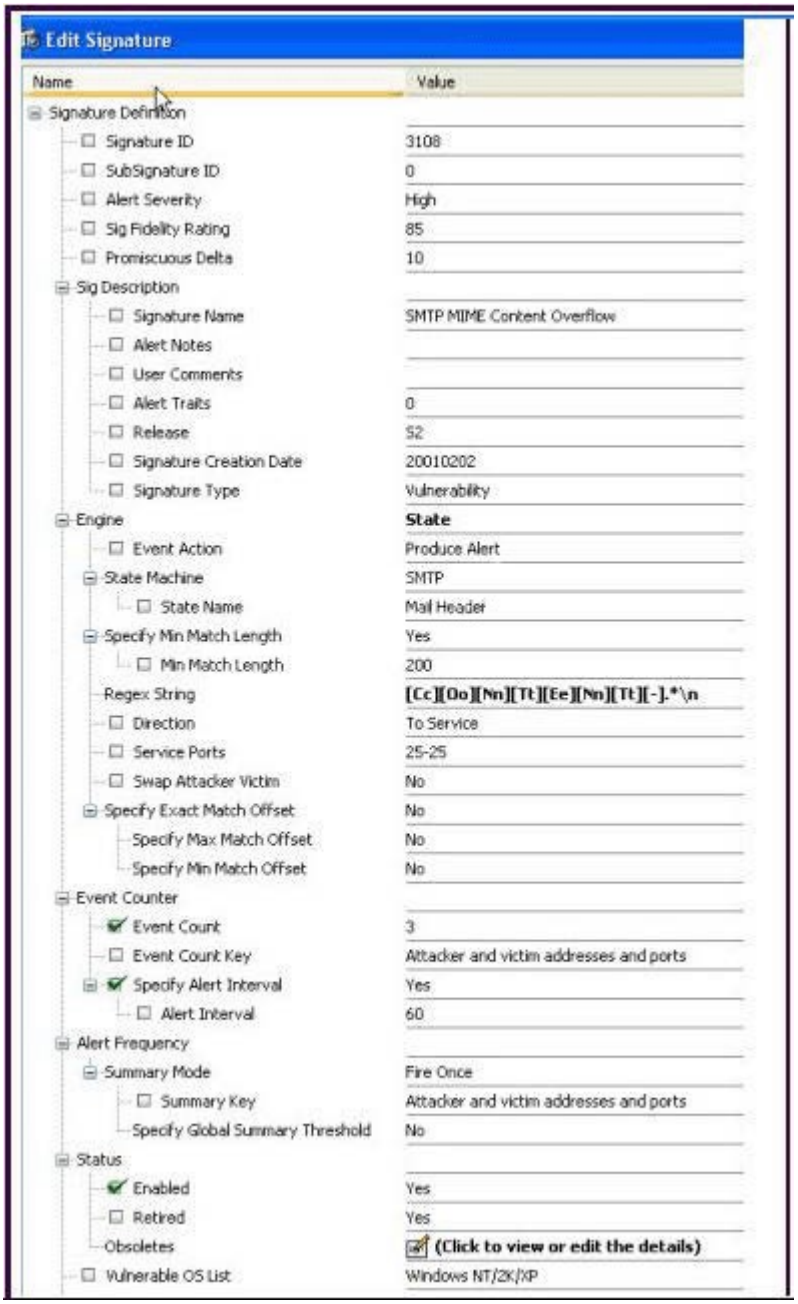
17.What is the correct regular expression to match a URI request equal to /test.exe?
A. /test.exe
B. Vtest\.exe
C. /test\.exe
D. */test\.exe
E. */test\.exe
F. */test.exe
Answer: C

18.Which four types of interface modes are available on the Cisco IPS 4200 Series appliance? (Choose four.)
A. promiscuous
B. inline TAP
C. inline interface
D. inline VLAN pair
E. VLAN groups
F. bypass
Answer: A,C,D,E

19.Which option is best to use to capture only a subset of traffic (capturing traffic per-IP-address, per-protocol, or per-application) off the switch backplane and copy it to the Cisco IPS appliance?
A. SPAN
B. PBR
C. VACL

D. MPF
E. STP
Answer: C

20.Refer to the exhibit.



Which statement is true?
A. A summary alert is sent once during each interval for each unique Summary Key entry.
B. An alert is generated each time the signature triggers.
C. This signature does not fire until three events are seen during 60 seconds with the same attacker and victim IP addresses and ports
D. This signature is disabled by default.
E. When this signature triggers, the Cisco IPS appliance sends an SNMP trap for this event.

Answer: C