Vendor: CISCO

Exam Code: 642-627

Exam Name: Implementing Cisco Intrusion Prevention System v7.0
**QUESTION 1**

Simlet - which area will you need to work in to get the answers for the simlet?

A. Home > Dashboard
B. Configuration > Policies > Rule 0
C. Configuration > Sensor Setup
D. Configuration > Policies > virtual sensor

**Answer:** B

**QUESTION 2**

Which four networking tools does Cisco IME include that can be invoked for specific events, to learn more about attackers and victims using basic network reconnaissance? (Choose four.)

A. ping
B. traceroute
C. packet tracer
D. nslookup
QUESTION 3
In a centralized Cisco IPS appliance deployment, it may not be possible to connect an IPS appliance to every switch or segment in the network. So, an IPS appliance can be deployed to inspect traffic on ports that are located on multiple remote network switches. In this case, which two configurations required? (Choose two.)

A. IPS promiscuous mode operations
B. in-line IPS operations
C. RSPAN
D. SPAN
E. HSRP
F. SLB

Answer: AC

QUESTION 4
Which value is not used by the Cisco IPS appliance in the risk rating calculation?

A. attack severity rating
B. target value rating
C. signature fidelity rating
D. promiscuous delta
E. threat rating adjustment
F. watch list rating

Answer: E

QUESTION 5
Which two Cisco IPS appliance features are implemented using input data from the Cisco SensorBase? (Choose two.)

A. global correlation
B. anomaly detection
C. reputation filters
D. botnet traffic filters
E. OS fingerprinting
F. threat detection

Answer: AC

QUESTION 6
On the Cisco IPS appliance, the anomaly detection knowledge base is used to store which two types of information for each service? (Choose two.)

A. scanner threshold
B. packet per second rate limit
C. anomaly detection mode
D. histogram
E. total bytes transferred

Answer: AD

QUESTION 7
Which four statements about the blocking capabilities of the Cisco IPS appliance are true? (Choose four.)

A. The three types of blocks are: host, connection, and network.
B. Host and connection blocks can be initiated manually or automatically when a signature is triggered.
C. Network blocks can only be initiated manually.
D. The Device Login Profiles pane is used to configure the profiles that the network devices use when logging into the Cisco IPS appliance
E. Multiple Cisco IPS appliances can forward their blocking requests to the master blocking sensor.
F. Pre-Block and Post-Block ACLs are applicable for blocking or rate limiting.

Answer: ABCE

QUESTION 8
What must be configured to enable Cisco IPS appliance reputation filtering and global correlation?

A. DNS server(s) IP address
B. full sensor based network participation
C. trusted hosts settings
D. external product interfaces settings

Answer: A

QUESTION 9
On the Cisco IPS appliance, each virtual sensor can have its own instance of which three parameters? (Choose three.)

A. signature-definition
B. event-action-rules
C. global-correlation-rules
D. anomaly-detection
E. reputation-filters
F. external-product-interfaces

Answer: ABD

QUESTION 10
Threat rating calculation is performed based on which factors?
A. risk rating and adjustment based on the prevention actions taken
B. threat rating and event action overrides
C. event action overrides and event action filters
D. risk rating and target value rating
E. alert severity and alert actions

Answer: A

**QUESTION 11**
Which configuration is required when setting up the initial configuration on the Cisco ASA 5505 to support the Cisco ASA AIP-SSC?

A. Configure a VLAN interface as a management interface to access the Cisco ASA AIP-SSC.
B. Using MPF, configure which virtual sensor to use.
C. Configure a management access rule to allow Cisco ASDM access from the Cisco ASA AIP-SSC management interface IP address.
D. Configure a management access rule to allow SSH access from the Cisco ASA AIP-SSC management interface IP address.

Answer: A

**QUESTION 12**
From which three sources does the Cisco IPS appliance obtain OS mapping information? (Choose three.)

A. from manually configured OS mappings
B. imported OS mappings from Management Center for Cisco Security Agent
C. imported OS mappings from Cisco Security Manager
D. learned OS mappings from passive OS fingerprinting
E. learned OS mappings from CiscoSensorBase input
F. from Cisco IPS signature updates

Answer: ABD
QUESTION 13
A Cisco Catalyst switch is experiencing packet drops on a SPAN destination port that is connected to an Cisco IPS appliance. Which three configurations should be considered to resolve the packet drops issue? (Choose three.)

A. Configure an additional SPAN session to a different Cisco IPS appliance interface connected to the same virtual sensor.
B. Configure an EtherChannel bundle as the SPAN destination port.
C. Configure RSPAN.
D. Configure VACL capture.
E. Configure the Cisco IPS appliance to inline mode.

Answer: AD

QUESTION 14
What are the three anomaly detection modes? (Choose three.)

A. detect
B. active
C. inactive
D. learn
E. full
F. partial

Answer: ACD

QUESTION 15
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
QUESTION 16
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: ABCE

QUESTION 17
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: ABDF
QUESTION 18
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

QUESTION 19
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

QUESTION 20
Which signature action should be selected to cause the attacker’s traffic flow to terminate when the Cisco IPS appliance is operating in promiscuous mode?

A. deny connection
B. deny attacker
C. reset TCP connection
D. deny packet, reset TCP connection
E. deny connection, reset TCP connection

Answer: C