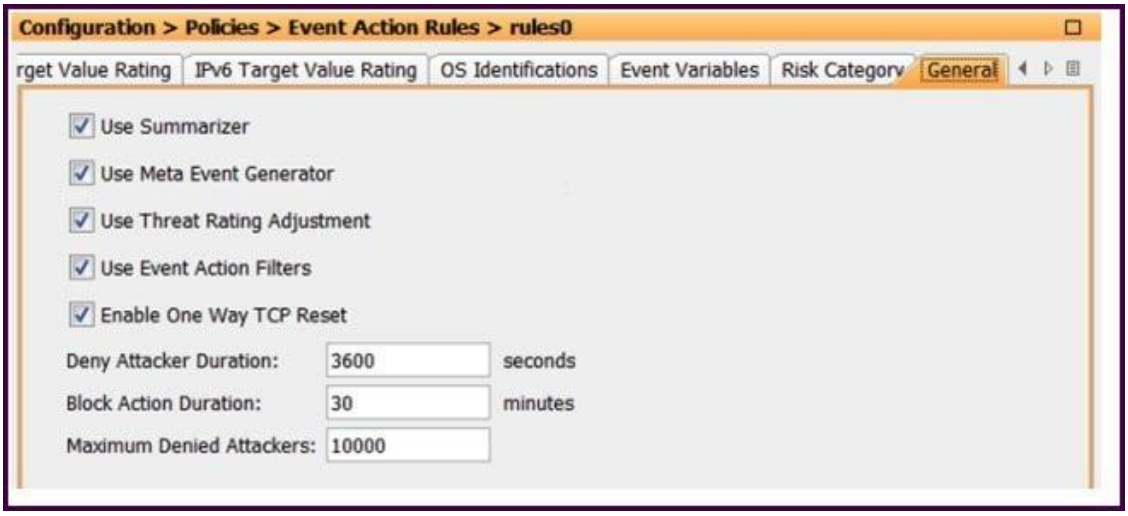
Vendor: Cisco

Exam Code: 642-627

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

Version: DEMO

QUESTION 1
Refer to the exhibit. Which three statements are true? (Choose three.)



A. Triggered inline blocks will last for 1 hour while triggered requests for external systems to block will last for 30 minutes.
B. Triggered inline blocks will last for 30 minutes while triggered requests for external systems to block will last for 1 hour.
C. TCP Resets will only be sent to the victim IP address.
D. TCP Resets will only be sent to the attacker IP address.
E. The IPS appliance can be configured to ignore scanning events sourced from the organization network management system.
F. An alert risk rating will be calculated from the base value of the threat rating reduced by a value corresponding to the preventative actions taken by the IPS appliance.

Answer: ACE

QUESTION 2
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

Answer: ACD

QUESTION 3
Which three statements about the Cisco IPS appliance anomaly detection feature are true? (Choose three.)

A. The scanner threshold is used to detect a single scanner.

B. Once the multiple scanners alert is triggered, the learning period will begin.
C. The histogram is used to detect multiple scanners.
D. Once a scanner threshold is violated, an alert is triggered for the multiple scanner signature.
E. The illegal zone should contain non-allocated internal IP addresses.
F. The traffic anomaly signature engine contains only two anomaly detection signatures (signature ID 13000 and 13001).

Answer: ACE

QUESTION 4
Which four data strings will match the regular expression c[a-z]*sc[0-4]+? (Choose four.)

A. Cisc0
B. Francisc0123456789
C. Ciscocisc0
D. SanFrancisco44
E. SanFranciscosc00L
F. csc0123456780

Answer: BCEF

QUESTION 5
The Cisco IDM Custom Signature Wizard asks you to select between the protocol types IP, ICMP, UDP, and TCP under which circumstance?

A. when you specify the String engine
B. when you specify the Service engine
C. when you specify the Atomic engine
D. when you specify the String or Service engine
E. when you do not select a specific engine

Answer: E

QUESTION 6
Regarding the Cisco IPS NME, when should the heartbeat reset be disabled on the ISR?

A. when performing an upgrade on the ISR
B. when the NME is used in inline mode
C. when the NME is used in promiscuous mode
D. when the NME is used in fail-open mode
E. when the NME is used in fail-closed open mode
F. when performing an upgrade on the NME

Answer: F

QUESTION 7
Which three IPS alert actions are available in promiscuous mode? (Choose three.)

A. reset tcp connection
B. request block host
C. deny packet
D. deny connection
E. send snmp inform
F. log pair packets

Answer: ABF

QUESTION 8
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

Answer: B

QUESTION 9
Which two statements are true regarding the Cisco IPS appliance traffic normalizer? (Choose two.)

A. It only operates in inline mode.
B. It operates in one of three modes: symmetric, loose, or asymmetric.
C. It can help prevent false negatives that are caused by evasions.
D. It can help ensure that Layer 7 traffic conforms to its protocol specifications.
E. It will not modify fragmented IP traffic.

Answer: AC

QUESTION 10
Numerous attacks using duplicate packets, changed packets, or out-of-order packets are able to successfully evade and pass through the Cisco IPS appliance when it is operating in inline mode. What could be causing this problem?

A. The IPS Application Inspection and Control is disabled.
B. All the DoS signatures are disabled.
C. All the reconnaissance signatures are disabled.
D. TCP state bypass is enabled.
E. The normalizer is set to asymmetric mode.

Answer: E

Ensurepass.com Members Features:

1. Verified Answers researched by industry experts.
2. Q&As are downloadable in PDF and VCE format.
3. 98% success Guarantee and **Money Back** Guarantee.
4. Free updates for **180** Days.

View list of All Exam provided:
http://www.ensurepass.com/certfications?index=A

To purchase Lifetime Full Access Membership click here:
http://www.ensurepass.com/user/register

Valid Discount Code for 2014: SFOH-FZA0-7Q2S

To purchase the HOT Exams:

Cisco		CompTIA		Oracle	VMWare	IBM
100-101	640-554	220-801	LX0-101	1Z0-051	VCAD510	C2170-011
200-120	640-802	220-802	N10-005	1Z0-052	VCP510	C2180-319
300-206	640-816	BR0-002	SG0-001	1Z0-053	VCP550	C4030-670
300-207	640-822	CAS-001	SG1-001	1Z0-060	VCAC510	C4040-221
300-208	640-864	CLO-001	SK0-002	1Z0-474	VCP5-DCV	RedHat
350-018	642-467	ISS-001	SK0-003	1Z0-482	VCP510PSE	EX200
352-001	642-813	JK0-010	SY0-101	1Z0-485		EX300
400-101	642-902	JK0-801	SY0-301	1Z0-580		
640-461	700-302			1Z0-820