

100% Money Back
Guarantee

Vendor:Cisco

Exam Code:642-627

Exam Name:Implementing Cisco Intrusion Prevention
System v7.0

Version:Demo

QUESTION 1

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

- A. SDEE
- B. global correlation
- C. anomaly detection
- D. remote blocking
- E. virtual sensor
- F. OS fingerprinting

Correct Answer: D

http://www.cisco.com/en/US/docs/security/ips/6.1/installation/guide/hw_troubleshooting.html#wpm kr1185768

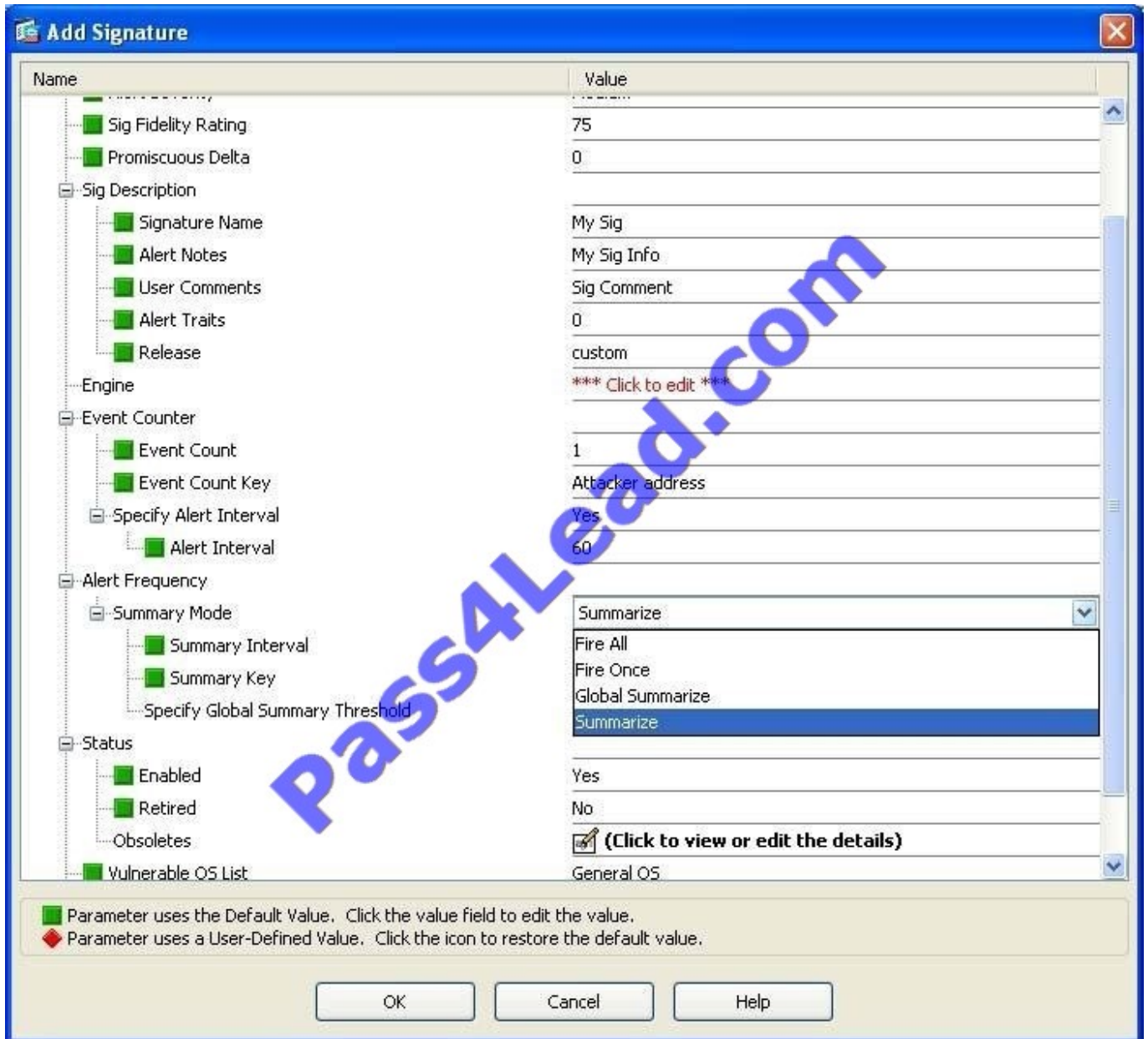
QUESTION 2

Which parameter is used to configure a signature to fire if the activity it detects happens a certain number of times for the same address set within a specified period of time?

- A. event action
- B. event counter
- C. summary count
- D. summary key

Correct Answer: B

http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.1/user/guide/ipsvchap.pdf



QUESTION 3

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.

Correct Answer: A

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 4

Select and Place:

Drag the Cisco IPS sensor model on the left to the appropriate password recovery method on the right

IPS 4200 Series appliance	clear the password from the boot-loader
IPS AIM	download the image through the maintenance partition
AIP-SSM	GRUB prompt or ROMMON
IDSM-2	ASA CLI command

Correct Answer:

Drag the Cisco IPS sensor model on the left to the appropriate password recovery method on the right

	IPS AIM
	IDSM-2
	IPS 4200 Series appliance
	AIP-SSM

QUESTION 5

What is the maximum number of virtual sensors that a Cisco IPS 4200 Series appliance can support?

- A. depends on the Cisco IPS 4200 Series appliance model
- B. 2
- C. 3
- D. 4
- E. 5

F. 6

Correct Answer: D

[http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_virtual_sensors.html# wp1035356](http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_virtual_sensors.html#wp1035356) It states you can create four virtual sensors.

QUESTION 6

Which two statements are true with respect to IPS false negatives? (Choose two.)

- A. A false negative is the failure of the IPS to create an alert on malicious activity.
- B. Increasing event count thresholds can lead to false negatives.
- C. A false negative results in an IPS alert that is associated with an unsuccessful denial of service attack.
- D. Disabling anti-evasion features of the IPS can reduce false negatives.
- E. False negatives can only occur when an IPS sensor is in promiscuous mode.

Correct Answer: AB

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd805c389a.html

QUESTION 7

Select and Place:

Drag the internal Cisco IPS appliance architectural component on the left to the appropriate function on the right.

ARC	send SNMP traps
NotificationApp	IDM
CollaborationApp	global correlation
SensorApp	traffic analysis
Web Server	control remote blocking

www.Pass4Lead.com

Correct Answer:

Drag the internal Cisco IPS appliance architectural component on the left to the appropriate function on the right.

	NotificationApp
	Web Server
	CollaborationApp
	SensorApp
	ARC

QUESTION 8

D and D matching users with their capabilities

Select and Place:

Tune signatures, and users and assign passwords, Manage Routers, Assign physical sensing interfaces to a virtual

Tune signatures, Manage Routers, Modify passwords, Assign configuration to a virtual sensor

View configuration, Modify their own passwords

Used for support and troubleshooting

Viewer

Approver

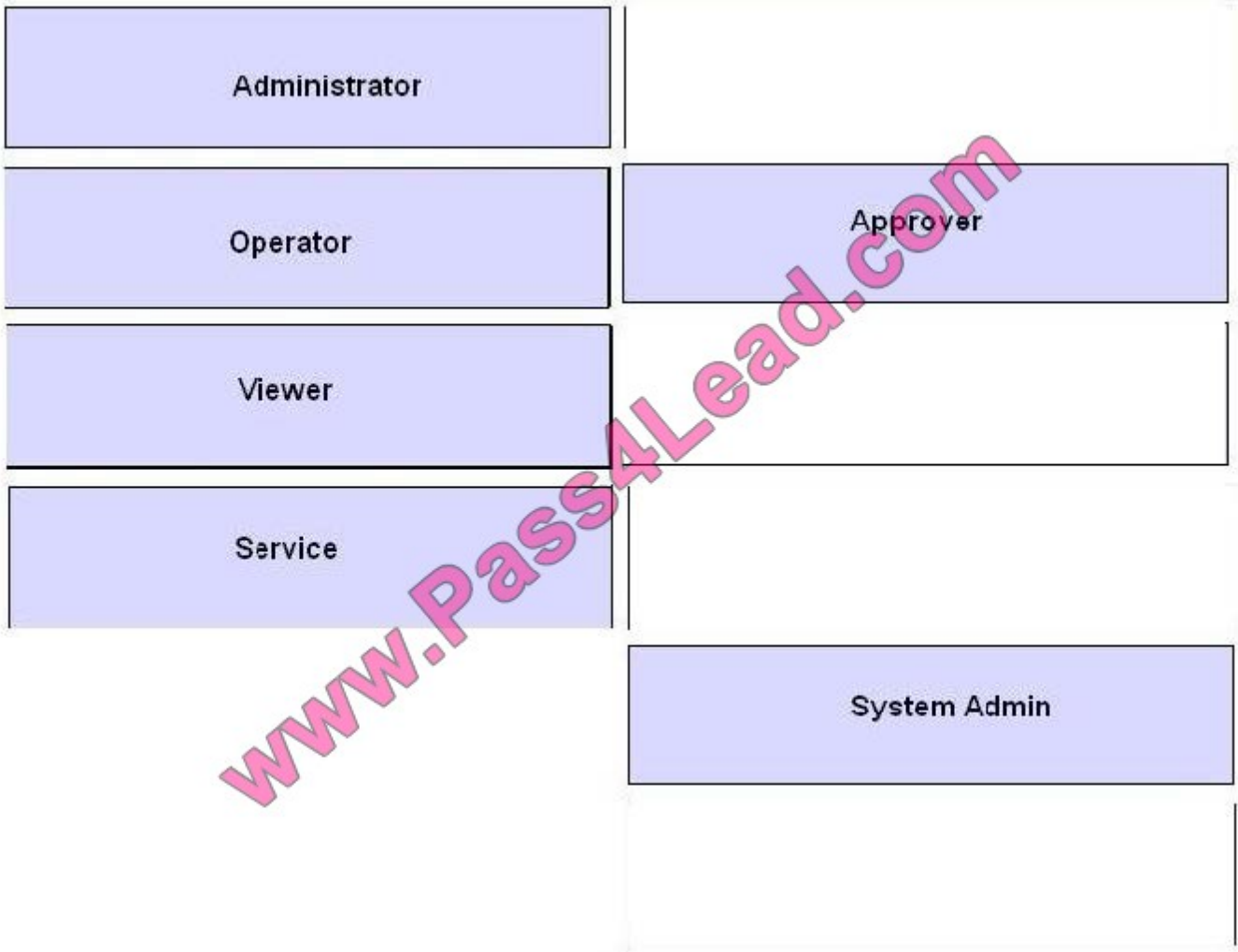
Service

Operator

System Admin

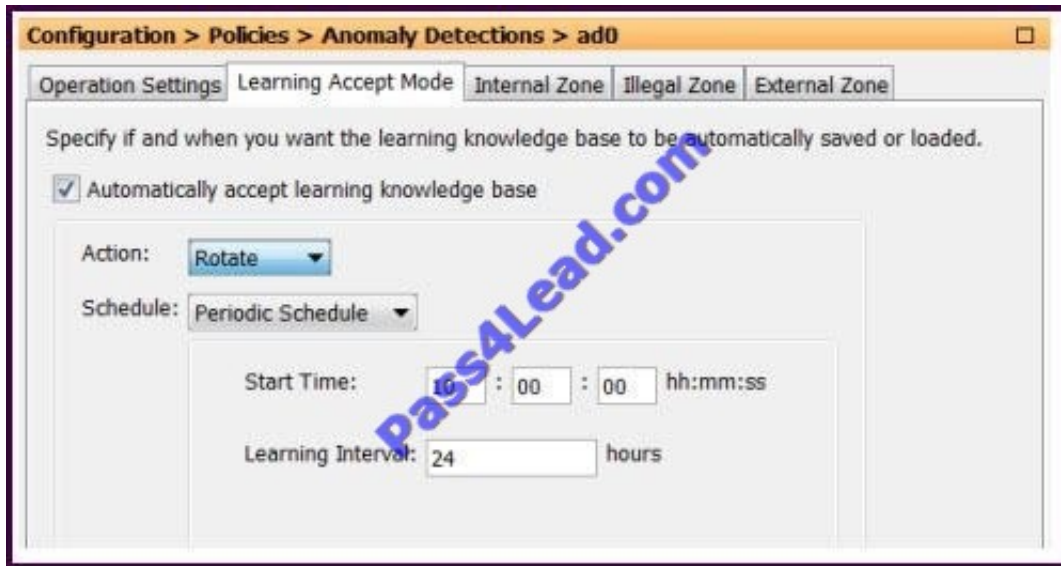
Administrator

Correct Answer:



QUESTION 9

Refer to the exhibit.



What does an action of Rotate indicate?

- A. A new knowledge base is created, but is not loaded. You can view it to decide if you want to load it.
- B. A new knowledge base is created and loaded.
- C. The knowledge base is rolled back to the previous version.
- D. The knowledge base is rotated on a periodic schedule using the different existing knowledge bases.

Correct Answer: B

QUESTION 10

Select and Place:

At right are CLI commands that can be used to direct traffic to the Cisco IPS sensor. Drag the device type from the left to match the corresponding CLI command it supports on the right.

Catalyst 3560E	ips inline fail-open
Catalyst 6500	monitor session 1 filter ip access-group MyFilter
ASA 5520	ids-service-module monitoring inline access-list 101
ISR	vlan access-map MyMap 10

Correct Answer:

At right are CLI commands that can be used to direct traffic to the Cisco IPS sensor. Drag the device type from the left to match the corresponding CLI command it supports on the right.

- ASA 5520
- Catalyst 3560E
- ISR
- Catalyst 6500

QUESTION 11

Select and Place:

Click and drag the rating or weight on the left to the correct description on the right.

- SFR
- ASR
- TVR
- ARR
- PD
- WLR

- indicates how accurately the signature detects the event
- associated with the relevancy of the targeted OS
- associated with the severity of a successful exploit of the vulnerability
- associated with the perceived value of the target
- value subtracted from the overall RR
- associated with the Management Center for Cisco Security Agent

Correct Answer:

Click and drag the rating or weight on the left to the correct description on the right.

	SFR
	ARR
	ASR
	TVR
	PD
	WLR

www.Pass4Lead.com

QUESTION 12

Which Cisco IDM pane is used to add the public keys of all the SSH clients that are allowed to connect to the IPS appliance SSH server using RSA authentication?

- A. Configuration > Sensor Management > SSH > Authorized Keys
- B. Configuration > Sensor Management > SSH > Known Host Keys
- C. Configuration > Sensor Management > SSH > Sensor key
- D. Configuration > Sensor Management > Certificates > Trusted Hosts
- E. Configuration > Sensor Management > Certificates > Server Certificate
- F. Configuration > Sensor Management > Certificates > Known Host Keys

Correct Answer: A

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

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average **99.9%** Success Rate

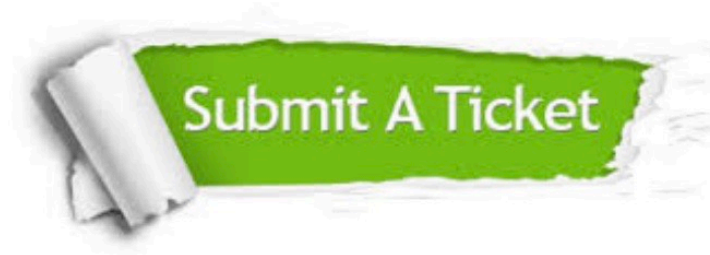
More than **800,000** Satisfied Customers Worldwide

Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.