



**642-533**

## **Implementing Cisco Intrusion Prevention Systems**

Q&A

DEMO Version

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website.

## **Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

**QUESTION NO: 1 DRAG DROP**

Drop

Match each sensor characteristic on the left with the sensor placement location on the right.

requires immediate response to alarms	Sensor on the outside
has a higher probability of generating false positives	
does not detect internal attacks	
compliments FW by monitoring for malicious activity	Sensor on the inside
monitors traffic permitted by firewall	
has a lower probability of generating false positives	

CHINATAG

**Answer:**

Match each sensor characteristic on the left with the sensor placement location on the right.

requires immediate response to alarms	Sensor on the outside
has a higher probability of generating false positives	
does not detect internal attacks	
compliments FW by monitoring for malicious activity	Sensor on the inside
monitors traffic permitted by firewall	
has a lower probability of generating false positives	

CHINATAG

**Explanation:**

Match each sensor characteristic on the left with the sensor placement location on the right.

requires immediate response to alarms	Sensor on the outside
has a higher probability of generating false positives	
does not detect internal attacks	
compliments FW by monitoring for malicious activity	Sensor on the inside
monitors traffic permitted by firewall	
has a lower probability of generating false positives	

CHINATAG

**QUESTION NO: 2**

What is the best way to mitigate the risk that executable-code exploits will perform malicious acts such as erasing your hard drive?

- A. assign blocking actions to signatures that are controlled by the State engine
- B. assign deny actions to signatures that are controlled by the Trojan engines
- C. assign the TCP reset action to signatures that are controlled by the Normalizer engine
- D. enable blocking
- E. enable application policy enforcement

**Answer: B**

**QUESTION NO: 3**

Which type of signature engine is best suited for creating custom signatures that inspect data at Layer 5 and above?

- A. Service
- B. AIC
- C. String
- D. Sweep
- E. Flood
- F. ATOMIC

**Answer: A**

**QUESTION NO: 4**

Refer to the exhibit. As an administrator, you need to change the Event Action and Event Count settings for signature 1108 in the sig1 instance. Which of the following should you select to view and change the required parameters?

Sig ID	Subsig ID	Name	Enabled	Severity	Facility Rating	Base RIT	Action
1000	0	IP options-Bad Option List	Yes	Informational	75	18	Produce Alert
1004	0	IP options-Loose Source Route	No	High	100	100	Produce Alert
1006	0	IP options-Strict Source Route	Yes	High	100	100	Produce Alert
1007	0	IPv6 over IPv4	No	Informational	100	25	Produce Alert
1101	0	Unknown IP Protocol	Yes	Informational	75	18	Produce Alert
1102	0	Impossible IP Packet	Yes	High	100	100	Produce Alert
1104	0	IP Localhost Source Spoof	Yes	High	100	100	Produce Alert
1107	0	RFC 1918 Addresses Seen	No	Informational	100	25	Produce Alert
1100	0	IP Packet with Proto 11	Yes	High	100	100	Produce Alert
1109	3	Cisco IOS Interface DoS	No	Medium	75	56	Produce Alert
1109	2	Cisco IOS Interface DoS	No	Medium	75	56	Produce Alert
1109	1	Cisco IOS Interface DoS	No	Medium	75	56	Produce Alert
1109	0	Cisco IOS Interface DoS	No	Medium	75	56	Produce Alert
1200	0	IP Fragmentation Buffer Full	Yes	Informational	100	25	Deny Packet Inline Produce Alert
1201	0	IP Fragment Overlap	No	Informational	100	25	Deny Packet Inline Produce Alert
1202	0	IP Fragment Overrun - Datagram T...	Yes	High	100	100	Deny Packet Inline Produce Alert
1203	0	IP Fragment Overwrite - Data is O...	Yes	High	100	100	Deny Packet Inline Produce Alert
1204	0	IP Fragment Missing Initial Fragment	Yes	Medium	85	63	Log Pair Packets Log Victim Packets
1205	0	IP Fragment Too Many Datagrams	Yes	Informational	100	25	Deny Packet Inline Produce Alert
1206	0	IP Fragment Too Small	Yes	Low	100	50	Deny Packet Inline

- A. Miscellaneous tab
- B. Signature Variables tab
- C. Actions button
- D. Edit button

**Answer: D**

### QUESTION NO: 5

You would like to investigate an incident and have already enabled the Log Pair Packets action on various signatures being triggered. What should you do next?

- A. Use CLI to send the IP log to a PC using TFTP, then open it with Notepad to view and interpret the contents.
- B. Use Cisco IDM to download the IP log to a management station then use a packet analyzer like Ethereal to decode the IP log.
- C. Use the External Product Interface feature to download the IP log to Cisco Security MARS for incident investigation.
- D. Use Cisco Security Manager to retrieve the IP log then use the Cisco Security Manager IPS Manager to decode the IP log.
- E. Use Cisco IEV to retrieve the IP log then use the IEV Generate Reports function to produce a report based on the IP log content.

**Answer: B**

**QUESTION NO: 6**

Which signature action or actions should be selected to cause the attacker's traffic flow to terminate when the Cisco IPS Sensor is operating in promiscuous mode?

- A. deny attacker
- B. reset tcp connection
- C. deny connection
- D. deny packet
- E. deny packet, reset tcp connection
- F. deny connection, reset tcp connection

**Answer: B**

**QUESTION NO: 7**

You are using Cisco IDM. What precaution must you keep in mind when adding, editing, or deleting allowed hosts on a Cisco IPS Sensor?

- A. You must not allow entire subnets to access the Cisco IPS Sensor
- B. You must not delete the IP address used for remote management.
- C. When using access lists to permit remote access, you must specify the direction of allowed communications.
- D. You can only configure the allowed hosts using the CLI.
- E. You must use an inverse mask, such as 10.0.2.0 0.0.0.255, for the specified network mask for the IP address.

**Answer: B**

**QUESTION NO: 8**

Which action does the copy /erase ftp://172.26.26.1/sensor\_config01 current-config command perform?

- A. erases the sensor\_config01 file on the FTP server and replaces it with the current configuration file from the Cisco IPS Sensor
- B. merges the source configuration file with the current configuration
- C. copies and saves the running configuration to the FTP server and replaces it with the source configuration file
- D. overwrites the backup configuration and applies the source configuration file to the system default configuration

**Answer: D**

**QUESTION NO: 9**

Refer to the exhibit. Which interfaces are assigned to an inline VLAN pair?

Virtual Sensor Name: vs0  
 Signature Definition Policy: sig0  
 Event Action Rules Policy: rules0  
 Anomaly Detection Policy: ad0  
 AD Operational Mode: Detect  
 Inline TCP Session Tracking Mode: Virtual Sensor  
 Description: default virtual sensor

Name	Details	Assigned
GigabitEthernet0/1	Promiscuous Interface	No
GigabitEthernet0/2	Promiscuous Interface	Yes
GigabitEthernet0/3	Promiscuous Interface	Yes

Buttons: OK, Cancel, Help, CHINATAG

- A. GigabitEthernet0/1 with GigabitEthernet0/3
- B. None in this virtual sensor
- C. GigabitEthernet0/1 with GigabitEthernet0/2
- D. GigabitEthernet0/2 with GigabitEthernet0/3

**Answer: B**

**QUESTION NO: 10**

Which character must precede a variable to indicate that you are using a variable rather than a string?

- A. percent sign
- B. asterisk
- C. dollar sign
- D. pound sign

E. ampersand

**Answer: C**