

Understanding IDP Rulebase Actions

Actions are responses to sessions that match the source/destination/service condition and the attack object. Actions are what protect your network from attacks.

If a packet triggers multiple rule actions, the IDP appliance takes the most severe action. For example, if the rules dictate that a packet receive a DiffServ marking and be dropped, the IDP appliance will take the more severe action, which is dropping the packet.

Predefined attack objects include a recommended action. The recommended action is generally related to attack severity, but other factors are considered. Table 1 lists the recommended actions by attack severity.

Table 1: Recommended Action by Attack Severity

Severity	Description	Recommended Action
Critical	Attacks attempt to evade an intrusion prevention system, crash a machine, or gain system-level privileges.	Drop Packet, Drop Connection
Major	Attacks attempt to crash a service, perform a denial of service, install or use a Trojan, or gain user-level access to a host.	Drop Packet, Drop Connection
Minor	Attacks attempt to obtain critical information through directory traversal or information leaks.	None
Warning	Attacks are obsolete or attempt to obtain noncritical information or scan the network.	None
Info	Attacks are normal, harmless traffic containing URLs, DNS lookup failures, and SNMP public community strings. You can use informational attack objects to obtain information about your network.	None

If you choose, you can set a different action. Table 2 describes the actions you can set for IDP rulebase rules.

Table 2: IDP Rulebase Actions

Action	Description
None	Inspects for attacks but takes no action against the connection if an attack is found.
Ignore	Does not take action and ignores the remainder of the session.
Diffserv Marking	Assigns the indicated service-differentiation value to the packet, and then passes it on normally. Set the service-differentiation value in the dialog box that appears when you select this action in the rulebase. NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. Therefore, this action has no effect in sniffer mode.

Table 2: IDP Rulebase Actions (continued)

Action	Description
Drop Packet	<p>Drops a matching packet before it can reach its destination but does not close the connection. Use this action in rules focused on traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a DoS that prevents you from receiving traffic from a legitimate source address.</p> <p>NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. Therefore, this action has no effect in sniffer mode.</p>
Drop Connection	<p>Drops the connection without sending an RST packet to the sender, preventing the traffic from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.</p> <p>NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. Therefore, this action has no effect in sniffer mode.</p>
Close Client and Server	<p>Closes the connection and sends an RST packet to both the client and the server.</p> <p>NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. However, if you use ACM to configure a sniffer mode reset interface, the IDP device can send an RST packet to both the client and server but does not close the connection.</p>
Close Client	<p>Closes the connection to the client but not to the server.</p> <p>NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. However, if you use ACM to configure a sniffer mode reset interface, the IDP device can send an RST packet to both the client and server but does not close the connection.</p> <p>NOTE: In VLAN tagged MPLS traffic, the Close Client action drops the connection instead of closing it.</p>
Close Server	<p>Closes the connection to the server but not to the client.</p> <p>NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. However, if you use ACM to configure a sniffer mode reset interface, the IDP device can send an RST packet to both the client and server but does not close the connection.</p>

If the IDP engine matches an attack, it can take action not only against the current session but also against subsequent network traffic from the same IP address. Such actions are called *IP actions*. By default, the specified IP action is permanent (timeout = 0). If you prefer, you can set a timeout.

Table 3 describes IDP rulebase IP actions.

Table 3: IDP Rulebase IP Actions

IP Action	Description
IP Block	IDP blocks the matching connection and future connections that match combinations of the following properties you specify: <ul style="list-style-type: none">■ Source IP address■ Source subnet■ Protocol■ Destination IP address■ Destination subnet■ Destination port■ From zone
IP Close	IDP closes the matching connection and future connections that match combinations of the following properties you specify: <ul style="list-style-type: none">■ Source IP address■ Source subnet■ Protocol■ Destination IP address■ Destination subnet■ Destination port■ From zone
IP Notify	IDP does not take any action against future traffic but logs the event or sends an alert.

Related Topics The following related topic is included in the *IDP Concepts and Examples Guide*:

- Understanding the IDP Rulebase
- IDP Rulebase Example: Using Recommended Actions

The following related topic is included in the *IDP Administration Guide*:

- Specifying Rule Session Action (NSM Procedure)

Published: 2010-01-12