

Understanding Traffic Anomalies Rulebase IP Actions

If traffic matches a traffic anomalies rule, the IDP appliance can take action against the current connection and 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 1 describes Traffic Anomalies rulebase IP actions.

Table 1: Traffic Anomalies 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.



NOTE: Traffic Anomalies rulebase IP actions are the same IP actions available for IDP rulebase rules.

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

- Understanding the Traffic Anomalies Rulebase

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

- Configuring Traffic Anomalies Rulebase Rules (NSM Procedure)

Published: 2010-01-12