

Understanding Network Honeypot Rulebase IP Actions

If traffic matches a Network Honeypot 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 Network Honeypot rulebase IP actions.

Table 1: Network Honeypot Rulebase IP Actions

IP Action	Description
IP Block	<p>IDP blocks the matching connection and future connections that match combinations of the following properties you specify:</p> <ul style="list-style-type: none">■ Source IP address■ Source subnet■ Protocol■ Destination IP address■ Destination subnet■ Destination port■ From zone
IP Close	<p>IDP closes the matching connection and future connections that match combinations of the following properties you specify:</p> <ul style="list-style-type: none">■ Source IP address■ Source subnet■ Protocol■ Destination IP address■ Destination subnet■ Destination port■ From zone <p>NOTE: The IP Close action might not work as expected for MPLS traffic. When the IDP engine processes MPLS traffic, it stores the MPLS label information for traffic in each direction. In the case of an IP action, the IDP engine is programmed to take a server-to-client action before the traffic has reached the server. In these cases, the IDP engine does not have server-to-client MPLS label information. Therefore, the TCP reset packet does not include an MPLS label. Some MPLS routers can add packets without a label to an existing MPLS tunnel; others drop such packets.</p>
IP Notify	IDP does not take any action against future traffic but logs the event or sends an alert.



NOTE: Network Honeypot 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 Network Honeypot Rulebase

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

- Configuring Network Honeypot Rulebase Rules (NSM Procedure)

Published: 2010-01-12