

Understanding Backdoor Rulebase Actions

By default, Backdoor rulebase rules accept and log traffic that matches the rule. If you choose, you can set a different action. Table 1 describes the actions you can set for Backdoor rulebase rules.

Table 1: Backdoor Rulebase Actions

Action	Description
Accept	Accepts the interactive traffic.
Drop Connection	Drops the interactive 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.
Close Client and Server	Closes the connection and sends an RST packet to both the client and the server. Logs generated for traffic that match this rule display Close . 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.
Close Client	Closes the interactive connection to the client but not to the server.
Close Server	Closes the interactive connection to the server but not to the client.

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

- Understanding the Backdoor Rulebase

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

- Configuring Backdoor Rulebase Rules (NSM Procedure)

Published: 2010-01-12