

Understanding the Network Honeypot Rulebase

The Network Honeypot rulebase is a method to detect reconnaissance activities.

A *network honeypot* is an apparently vulnerable system that draws the attention and action of attackers. In an IDP network honeypot, the IDP appliance impersonates ports on protected servers.

When you create rules for the Network Honeypot rulebase, you specify:

- A destination/service match condition
- Operation mode
- Response options
- Notification options



NOTE: The IDP appliance drops MPLS traffic that matches a Network Honeypot rule. When the IDP engine processes MPLS traffic, it stores the MPLS label information. It stores separate labels for client-to-server and server-to-client communication. In the case of traffic that matches Network Honeypot rules, there is no genuine server-to-client communication, so the IDP engine does not have server-to-client MPLS label information. Therefore, the impersonation operation cannot be supported for MPLS traffic.

Related Topics The following related topics are included in the *IDP Concepts and Examples Guide*:

- Understanding Network Honeypot Rulebase Match Settings
- Understanding Network Honeypot Operation Setting
- Understanding Network Honeypot Rulebase IP Actions
- Understanding Network Honeypot Rulebase Notification Options
- Understanding the Components of an IDP Security Policy

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

- Configuring Network Honeypot Rulebase Rules (NSM Procedure)

Published: 2010-01-12