

Understanding the IDP Rulebase

The IDP rulebase employs an attack object database to support two robust detection methods: stateful signatures and protocol anomalies.

A *stateful signature* combines an attack pattern with service, context, and other properties into a signature attack object. As a result, IDP does not need to expend resources inspecting huge sections of network traffic where attacks cannot possibly be, and IDP produces very few false positives.

A *protocol anomaly* is a deviation from protocol standards established by the Internet Engineering Taskforce (IETF) Request for Comment (RFC) process. Traffic that does not adhere to these standards is suspicious because most legitimate applications adhere to the standards, and anomalies can fairly be regarded as purposeful attempts to evade an intrusion detection system (IDS). IDP protocol-anomaly attack objects find traffic that deviates from IETF RFC standards.

When you create rules for the IDP rulebase, you specify:

- A source/destination/service match condition
- Attack objects
- Action
- Notification options

For complete procedures on configuring IDP rulebase rules, see the *IDP Administration Guide*.

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

- Understanding IDP Rulebase Rule Match Settings
- Using Application Identification
- Using Attack Objects
- Understanding IDP Rulebase Actions
- Understanding IDP Rulebase Notification Options
- IDP Rulebase Example: Using Application Identification
- IDP Rulebase Example: Specifying the Default Service
- IDP Rulebase Example: Using Recommended Attack Objects
- IDP Rulebase Example: Using Recommended Actions
- Example: Fine-Tuning a Security Policy

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

- Modifying IDP Rulebase Rules (NSM Procedure)

Published: 2010-01-12