

## Understanding the Exempt Rulebase

---

The Exempt rulebase enhances manageability of the IDP solution by enabling you to categorically exempt traffic segments you know to be safe from processing by the IDP rulebase.

A *false positive*, also known as a false alert, is a situation in which benign traffic causes an intrusion detection system (IDS) to generate an alert. Too many false positives can degrade performance and produce oversized log files.

The IDP engine reduces false positives by using stateful signatures to detect known attacks. A stateful signature knows the pattern and location of the attack, and produces fewer false positives than regular attack signatures because it does not inspect network traffic that cannot contain the attack.

To further increase detection accuracy and reduce false positives, the IDP engine uses:

- Flow tracking to correlate multiple TCP/UDP connections into a single flow to determine the validity of the traffic.
- IP defragmentation and TCP reassembly to reconstruct fragmented traffic.
- Protocol normalization to normalize traffic to a common format for analysis.

Still, a few false positives from your IDS are normal, especially when you are testing new security policies. You can use the Exempt rulebase to manage these cases.

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

- A source/destination/service match condition
- At least one attack object



**NOTE:** The Exempt rulebase is a non-terminal rulebase. That is, the IDP process engine processes all rules in the rulebase.

---

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

- Understanding the Components of an IDP Security Policy
- Understanding the Rule-Matching Algorithm
- Understanding the IDP Rulebase
- Exempt Rulebase Example: Exempting a Source Destination Pair
- Exempt Rulebase Example: Exempting an Attack Object

The following related topics are included in the *IDP Administration Guide*.

- Configuring Exempt Rulebase Rules (NSM Procedure)

---

Published: 2010-01-12