

Understanding the Rule-Matching Algorithm

The IDP process engine processes rulebases in the following order:

1. Application Policy Enforcement (APE) rulebase (terminal)
2. Traffic Anomalies rulebase (terminal)
3. SYN Protector rulebase (terminal)
4. Network Honeypot rulebase (terminal)
5. IDP rulebase (nonterminal)
6. Exempt rulebase (nonterminal)
7. Backdoor rulebase (terminal)

For terminal rulebases, the IDP rule-matching algorithm evaluates rules according to the ordered list to identify matches. As soon as the algorithm identifies a match, it applies the rule and terminates rule matching. For example, if a terminal rule 1 matches, it is applied, and rule 2 is not consulted.

For nonterminal rulebases, the IDP rule-matching algorithm also evaluates rules according to the ordered list to identify matches. However, even if it finds a match, it continues down the list to identify additional matches.

The IDP rulebase includes the option to mark a rule as a terminal rule. When a terminal rule matches source, destination, and service, IDP applies the rule and terminates rule matching. It does not matter whether the traffic matches the attack objects.

In the IDP rulebase, you can set the terminal rule flag for the following purposes:

- To disregard traffic that originates from a particular trusted source (however, an Exempt rulebase rule might be a better choice).
- To exit rule processing when you want a particular match to always trigger a particular action and no other, such as a drop connection action.
- To exit rule processing when your rule specifies precise destination addresses and precise services, and you know that the subsequent rules do not apply.

Use caution when specifying the terminal flag. You can inadvertently leave your network open to attacks by creating an inappropriate terminal rule. Be particularly careful about terminal rules using the value **Any** for both the source and destination. Terminal rules should appear near the top of the rulebase, before other rules that would match the same traffic.

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

- Understanding the Components of an IDP Security Policy
- Example: Fine-Tuning a Security Policy
- Understanding APE Rulebase Match Conditions

- Understanding IDP Rulebase Rule Match Settings
- Understanding Backdoor Rulebase Match Settings
- Understanding SYN Protector Rulebase Match Settings
- Understanding Traffic Anomalies Rulebase Match Conditions
- Understanding Network Honeypot Rulebase Match Settings

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

- Developing Security Policies Task Summary

Published: 2010-01-12