

## Understanding Traffic Anomalies Rulebase Match Conditions

---

We recommend the following settings for Traffic Anomalies rulebase match conditions:

- Source — Any
- Destination — IP addresses for servers you want to protect
- Service — Any (or specify specific services if you are creating an ignore list)



**TIP:** You can use two rules to protect a large number of servers. Configure rule 1 to match services you do not want to detect and set the detection option to **Ignore**. Configure rule 2 to match any traffic and set the detection operation to **Detect**.



**TIP:** In NSM, you can create address objects and service objects to facilitate configuration. One benefit of using objects is that you can configure them once and then use them in multiple rules. For details, see the NSM documentation.



**NOTE:** The Traffic Anomalies rulebase is a terminal rulebase—that is, Traffic Anomalies rules are inherently terminal rules. If a Traffic Anomalies rule matches, IDP does not process subsequent rules.

---

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

- Understanding the Rule-Matching Algorithm
- Understanding the Traffic Anomalies Rulebase

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

- Configuring Traffic Anomalies Rulebase Rules (NSM Procedure)

---

Published: 2010-01-12