

Understanding Backdoor Rulebase Match Settings

Backdoor rulebase rules are triggered when source, destination, and service for the traffic match the rule.

To detect incoming interactive traffic, set the source to **Any** and the destination to the IP address of network device you want to protect.

To detect outgoing interactive traffic, set the source to the IP address of the network device you want to protect and the destination to **Any**.

Specify not only the services on the network device you want to protect but also interactive services that can be installed and used by attackers.



NOTE: Including Telnet, SSH, RSH, NetMeeting, or VNC as services can result in false positives because these services are used to legitimately control a remote system. We recommend that you not include these services in your service 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 Operation to **Ignore**. Configure rule 2 to match any traffic and set 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 Backdoor rulebase is a terminal rulebase—that is, Backdoor rules are inherently terminal rules. If a Backdoor rule matches, the IDP engine 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 Backdoor Rulebase

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

- Configuring Backdoor Rulebase Rules (NSM Procedure)