

Understanding the Backdoor Rulebase

The Backdoor rulebase detects the kind of interactive traffic produced during backdoor attacks.

A *backdoor* is a mechanism installed on a host computer that facilitates unauthorized access to the system. Attackers who have already compromised a system can install a backdoor to make future attacks easier. When attackers type commands to control a backdoor, they generate interactive traffic.

Unlike antivirus software, which scans for known backdoor files or executable files on the host system, the IDP engine detects the interactive traffic that is produced when backdoors are used. Interactive programs often transmit several short IP packets containing individual keystrokes and their echoes, reflecting the real-time actions of a user (or an attacker).

When detection is enabled, the IDP engine detects traffic that exceeds the interactive traffic thresholds you set as runtime parameters. Figure 1 shows the backdoor detection settings in the NSM Device Manager configuration editor.

Figure 1: NSM Device Manager: Sensor Settings > Run-Time Parameters

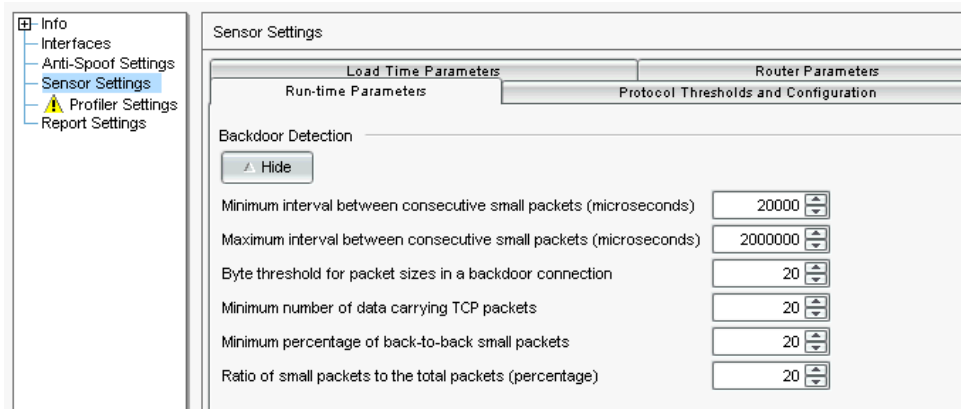


Table 1 shows the defaults for backdoor detection runtime parameters. You can tune these parameters if safe traffic in your network triggers false positives.

Table 1: Backdoor Detection Runtime Parameters

Parameter	Default
Minimum interval between consecutive small packets (microseconds)	20,000
Maximum interval between consecutive small packets (microseconds)	2,000,000
Byte threshold for packet sizes in a backdoor connection (bytes)	20
Minimum number of data carrying TCP packets (number)	20

Table 1: Backdoor Detection Runtime Parameters (continued)

Parameter	Default
Minimum percentage of back-to-back small packets (percentage)	20
Ratio of small packets to the total packets (percentage)	20

Detecting the signs of interactive traffic ensures that the IDP device can detect all backdoors, both known and unknown. If the IDP device detects interactive traffic, it can perform actions against the connection to prevent the attacker from further compromising your network.

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

- A source/destination/service match condition
- Operation
- Action
- Notification options

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

- Understanding the Components of an IDP Security Policy
- Understanding Backdoor Rulebase Match Settings
- Understanding the Backdoor Rulebase Operation Setting
- Understanding Backdoor Rulebase Actions
- Understanding Backdoor Rulebase Notification Options
- Backdoor Rulebase Example: netcat

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

- Configuring Backdoor Rulebase Rules (NSM Procedure)
- Modifying the IDP Device Configuration

Published: 2010-01-12