

Chapter 10

Policer Overview

Policing, or rate limiting, enables you to limit the amount of traffic that passes into or out of an interface. It is an essential component of firewall filters that is designed to thwart denial-of-service (DoS) attacks. Policing applies two types of rate limits on the traffic:

Bandwidth—The number of bits per second permitted, on average.

Maximum burst size—The maximum size permitted for bursts of data that exceed the given bandwidth limit.

Policing uses the *token-bucket algorithm*, which enforces a limit on average bandwidth while allowing bursts up to a specified maximum value. It offers more flexibility than the *leaky bucket algorithm* (see the *JUNOS Internet Software Network Interfaces and Class of Service Configuration Guide*) in allowing a certain amount of bursty traffic before it starts discarding packets.

You can define specific classes of traffic on an interface and apply a set of rate limits to each. You can use a policer in one of two ways: as part of a filter configuration or as an individual policer statement that applies to each family on an interface.

After you have defined and named a policer, it is stored as a template. You can later use the same policer name to provide the same policer configuration each time you wish to use it. This eliminates the need to define the same policer values more than once.

