

Chapter 12

Summary of Firewall Filter and Policer Configuration Statements

The following descriptions explain each of the firewall filter and policer configuration statements. The statements are organized alphabetically.

accounting-profile

Syntax	accounting-profile <i>name</i> ;
Hierarchy Level	[edit firewall family <i>family-name</i> filter <i>filter-name</i>]
Description	Enable collection of accounting data for the specified filter.
Options	<i>name</i> —Name assigned to the accounting profile.
Usage Guidelines	See “Configure a Firewall Filter Accounting Profile” on page 187.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

family

Syntax family *family-name* {
 filter *filter-name* {
 accounting-profile *name*;
 interface-specific;
 }
 prefix-action *name* {
 count;
 destination-prefix-length *prefix-length*;
 policer *policer-name*;
 source-prefix-length *prefix-length*;
 subnet-prefix-length *prefix-length*;
 }
 }

Hierarchy Level [edit firewall]

Description Configure a firewall filter for Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) traffic.

Options *family-name*—Version of addressing protocol:

inet—IPv4 addressing protocol.

inet6—IPv6 addressing protocol.

mpls—Multiprotocol Label Switching (MPLS) protocol.

The remaining statements are explained separately.

Usage Guidelines See “Configure the Family Address Type” on page 155.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

filter

Syntax filter *filter-name* {
 accounting-profile *name*;
 interface-specific;
 term *term-name* {
 from {
 match-conditions;
 }
 then {
 action;
 action-modifiers;
 }
 }
 }

Hierarchy Level [edit firewall family *family-name*]

Description Configure firewall filters.

Options *filter-name*—Name that identifies the filter. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" ").

The remaining statements are explained separately.

Usage Guidelines See “Configure Firewall Filters” on page 155.

Required Privilege Level firewall—To view this statement in the configuration.
 firewall-control—To add this statement to the configuration.

filter-specific

Syntax filter-specific;

Hierarchy Level [edit firewall policer *policer-name*]

Description Configure a policer to act as a filter-specific policer. If this statement is not specified, then the policer defaults to a term-specific policer.

Usage Guidelines See “Configure Filter-Specific Policers” on page 203.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

firewall

Syntax	firewall { ... }
Hierarchy Level	[edit]
Description	Configure firewall filters. The statements are explained separately.
Usage Guidelines	See “Firewall Filter Configuration” on page 153.
Required Privilege Level	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.

if-exceeding

Syntax	if-exceeding { bandwidth-limit <i>bps</i> ; bandwidth-percent <i>number</i> ; burst-size-limit <i>bytes</i> ; }
Hierarchy Level	[edit firewall policer <i>policer-name</i>]
Description	Configure policer rate limits.
Options	<p>bandwidth-limit <i>bps</i>—Traffic rate, in bits per second (bps). There is no minimum value, but any value below 61,040 bps results in an effective rate of 30,520 bps. Range: 32,000 through 32,000,000,000 bps Default: None</p> <p>bandwidth-percent <i>number</i>—Port speed, in decimal percentage number. Range: 1 through 100 Default: None</p> <p>burst-size-limit <i>bytes</i>—Maximum burst size, in bytes. The minimum recommended value is the maximum transmission unit (MTU) of the IP packets being policed. Range: 1500 through 100,000,000 bytes Default: None</p>
Usage Guidelines	See “Configure Rate Limiting” on page 201.
Required Privilege Level	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.

interface-specific

Syntax	interface-specific;
Hierarchy Level	[edit firewall family <i>family-name</i> filter <i>filter-name</i>]
Description	Configure interface-specific names for firewall counters.
Usage Guidelines	See “Configure Interface-Specific Counters” on page 184.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

policer

Syntax	<pre>policer <i>policer-name</i> { filter-specific; if-exceeding { bandwidth-limit <i>bps</i>; bandwidth-percent <i>number</i>; burst-size-limit <i>bytes</i>; } then { <i>policer-action</i>; } }</pre>
Hierarchy Level	[edit firewall]
Description	Configure policer rate limits and actions. When included at the [edit firewall] hierarchy level, it creates a template, and you do not have to configure a policer individually for every firewall filter or interface. To activate a policer, you must include the policer action modifier in the then statement in a firewall filter term or on an interface.
Options	<p><i>policer-action</i>—One or more actions to take:</p> <ul style="list-style-type: none"> discard—Discard traffic that exceeds the rate limits. forwarding-class <i>class-name</i>—Specify the particular forwarding class. loss-priority—Set the packet loss priority (PLP) to low or high. <p><i>policer-name</i>—Name that identifies the policer. The name can contain letters, numbers, and hyphens (-), and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (“ ”).</p> <p>then—Actions to take on matching packets.</p> <p>The remaining statements are explained separately.</p>

Usage Guidelines See “Configure Policers” on page 200.

Required Privilege Level firewall—To view this statement in the configuration.
 firewall-control—To add this statement to the configuration.

prefix-action

Syntax prefix-action *name* {
 count;
 destination-prefix-length *prefix-length*;
 policer *policer-name*;
 source-prefix-length *prefix-length*;
 subnet-prefix-length *prefix-length*;
 }

Hierarchy Level [edit firewall family inet]

Description Configure prefix-specific action.

Options count—Enable counter.

destination-prefix-length *prefix-length*—Destination prefix length.
Range: 0 through 32

policer *policer-name*—Policer name.

source-prefix-length *prefix-length*—Source prefix length.
Range: 0 through 32

subnet-prefix-length *prefix-length*—Subnet prefix length.
Range: 0 through 32

Usage Guidelines See “Configure Prefix-Specific Actions” on page 204.

Required Privilege Level firewall—To view this statement in the configuration.
 firewall-control—To add this statement to the configuration.

service-filter

Syntax `service-filter filter-name {
 term term-name {
 from {
 match-conditions;
 }
 then {
 action;
 action-modifiers;
 }
 }
}`

Hierarchy Level [edit firewall family inet]

Description Configure service filters.

Options *filter-name*—Name that identifies the service filter. The name can contain letters, numbers, and hyphens (-), and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" ").

The remaining statements are explained separately.

Usage Guidelines See “Configure Service Filters” on page 182.

Required Privilege Level `firewall`—To view this statement in the configuration.
`firewall-control`—To add this statement to the configuration

term

Syntax	<pre> term <i>term-name</i> { from { <i>match-conditions</i>; } then { <i>actions</i>; <i>action-modifiers</i>; } } </pre>
Hierarchy Level	[edit firewall family <i>family-name</i> filter <i>filter-name</i>]
Description	Define a firewall filter term.
Options	<p><i>actions</i>—(Optional) An action to take if conditions match. If you do not specify an action, the packets that match the conditions in the from statement are accepted. The actions are described in Table 22 on page 158.</p> <p><i>action-modifiers</i>—(Optional) One or more actions to perform on a packet. The action modifiers are described in Table 22 on page 158.</p> <p><i>from</i>—(Optional) Match packet fields to values. If not included, all packets are considered to match and the actions and action modifiers in the then statement are taken.</p> <p><i>match-conditions</i>—One or more conditions to use to make a match. The conditions are described in Table 23 on page 163, Table 24 on page 166, Table 25 on page 169, and Table 26 on page 173.</p> <p><i>term-name</i>—Name that identifies the term. The name can contain letters, numbers, and hyphens (-), and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" ").</p> <p><i>then</i>—(Optional) Actions to take on matching packets. If not included and a packet matches all the conditions in the from statement, the packet is accepted.</p>
Usage Guidelines	See “Configure Firewall Filters” on page 155.
Required Privilege Level	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>