

## 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

---

<b>Syntax</b>	accounting-profile <i>name</i> ;
<b>Hierarchy Level</b>	[edit firewall family <i>family-name</i> filter <i>filter-name</i> ]
<b>Description</b>	Enable collection of accounting data for the specified filter.
<b>Options</b>	<i>name</i> —Name assigned to the accounting profile.
<b>Usage Guidelines</b>	See “Configuring a Firewall Filter Accounting Profile” on page 192.
<b>Required Privilege Level</b>	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 IP version 4 (IPv4) or IP 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 “Configuring the Family Address Type” on page 159.

**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 “Configuring Firewall Filters” on page 159.

**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 “Configuring Filter-Specific Policers” on page 207.

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

## firewall

---

<b>Syntax</b>	firewall { ... }
<b>Hierarchy Level</b>	[edit]
<b>Description</b>	Configure firewall filters.  The statements are explained separately.
<b>Usage Guidelines</b>	See “Firewall Filter Configuration” on page 157.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.

## if-exceeding

---

<b>Syntax</b>	if-exceeding { bandwidth-limit <i>bps</i> ; bandwidth-percent <i>number</i> ; burst-size-limit <i>bytes</i> ; }
<b>Hierarchy Level</b>	[edit firewall policer <i>policer-name</i> ]
<b>Description</b>	Configure policer rate limits.
<b>Options</b>	<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. <b>Range:</b> 32,000 through 32,000,000,000 bps <b>Default:</b> None</p> <p>bandwidth-percent <i>number</i>—Port speed, in decimal percentage number. <b>Range:</b> 1 through 100 <b>Default:</b> 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. <b>Range:</b> 1500 through 100,000,000 bytes <b>Default:</b> None</p>
<b>Usage Guidelines</b>	See “Configuring Rate Limiting” on page 205.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.

## interface-set

---

<b>Syntax</b>	interface-set <i>interface-set-name</i> { [ <i>interface-names</i> ]; }
<b>Hierarchy Level</b>	[edit firewall]
<b>Description</b>	Configure an interface set.
<b>Options</b>	<i>interface-names</i> —Names of interfaces to include in the interface set. You must specify more than one name.
<b>Usage Guidelines</b>	See “Configuring an Interface Set” on page 213.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.

## interface-specific

---

<b>Syntax</b>	interface-specific;
<b>Hierarchy Level</b>	[edit firewall family <i>family-name</i> filter <i>filter-name</i> ]
<b>Description</b>	Configure interface-specific names for firewall counters.
<b>Usage Guidelines</b>	See “Configuring Interface-Specific Counters” on page 188.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## load-balance-group

---

<b>Syntax</b>	load-balance-group <i>group-name</i> { next-hop-group [ <i>group-names</i> ]; }
<b>Hierarchy Level</b>	[edit firewall]
<b>Description</b>	Configure a load-balance group.
<b>Options</b>	<i>group-name</i> —Name of load-balance group.  <i>group-names</i> —Name of next-hop groups to include in the load-balance group set.
<b>Usage Guidelines</b>	See “Configuring a Load-Balance Group” on page 215.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.

## policer

---

**Syntax** `policer policer-name {  
 filter-specific;  
 if-exceeding {  
 bandwidth-limit bps;  
 bandwidth-percent number;  
 burst-size-limit bytes;  
 }  
 then {  
policer-action;  
 }  
 }`

**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** *policer-action*—One or more actions to take:

discard—Discard traffic that exceeds the rate limits.

forwarding-class *class-name*—Specify the particular forwarding class.

loss-priority—Set the packet loss priority (PLP) to low or high.

*policer-name*—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 (" ").

then—Actions to take on matching packets.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring Policers” on page 205.

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

## prefix-action

---

<b>Syntax</b>	<pre> prefix-action <i>name</i> {     count;     destination-prefix-length <i>prefix-length</i>;     policer <i>policer-name</i>;     source-prefix-length <i>prefix-length</i>;     subnet-prefix-length <i>prefix-length</i>; } </pre>
<b>Hierarchy Level</b>	[edit firewall family inet]
<b>Description</b>	Configure prefix-specific action.
<b>Options</b>	<p>count—Enable counter.</p> <p>destination-prefix-length <i>prefix-length</i>—Destination prefix length.  <b>Range:</b> 0 through 32</p> <p>policer <i>policer-name</i>—Policer name.</p> <p>source-prefix-length <i>prefix-length</i>—Source prefix length.  <b>Range:</b> 0 through 32</p> <p>subnet-prefix-length <i>prefix-length</i>—Subnet prefix length.  <b>Range:</b> 0 through 32</p>
<b>Usage Guidelines</b>	See “Configuring Prefix-Specific Actions” on page 208.
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>

## 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 “Configuring Service Filters” on page 187.

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

## term

```

Syntax term term-name {
    from {
        match-conditions;
    }
    then {
        actions;
        action-modifiers;
    }
}

```

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

**Description** Define a firewall filter term.

**Options** *actions*—(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 163.

*action-modifiers*—(Optional) One or more actions to perform on a packet. The action modifiers are described in Table 22 on page 163.

*from*—(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.

*match-conditions*—One or more conditions to use to make a match. The conditions are described in Table 23 on page 167, Table 24 on page 170, Table 25 on page 173, and Table 26 on page 177.

*term-name*—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 (" ").

*then*—(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.

**Usage Guidelines** See “Configuring Firewall Filters” on page 159.

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

