

Chapter 7

Summary of Stateful Firewall Configuration Statements

The following sections explain each of the stateful firewall services statements. The statements are organized alphabetically.

allow-ip-option

Syntax	allow-ip-option [<i>values</i>];																		
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> then]																		
Description	Configures how the stateful firewall handles IP header information. This statement is optional.																		
Options	<i>value</i> —Can be a set or range of numeric values, or one or more of the following predefined option types. You can enter either the option name or its numeric equivalent.																		
	<table border="1"><thead><tr><th>Option Name</th><th>Numeric Value</th></tr></thead><tbody><tr><td>any</td><td>0</td></tr><tr><td>ip-security</td><td>130</td></tr><tr><td>ip-stream</td><td>8</td></tr><tr><td>loose-source-route</td><td>3</td></tr><tr><td>route-record</td><td>7</td></tr><tr><td>router-alert</td><td>148</td></tr><tr><td>strict-source-route</td><td>9</td></tr><tr><td>timestamp</td><td>4</td></tr></tbody></table>	Option Name	Numeric Value	any	0	ip-security	130	ip-stream	8	loose-source-route	3	route-record	7	router-alert	148	strict-source-route	9	timestamp	4
Option Name	Numeric Value																		
any	0																		
ip-security	130																		
ip-stream	8																		
loose-source-route	3																		
route-record	7																		
router-alert	148																		
strict-source-route	9																		
timestamp	4																		
Usage Guidelines	See “Configure Stateful Firewall Actions” on page 60.																		
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.																		

application-sets

Syntax	<code>application-sets [<i>set-name</i>];</code>
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]
Description	Defines one or more target application sets.
Options	<i>set-name</i> —Name of the target application set.
Usage Guidelines	See “Configure Stateful Firewall Match Conditions” on page 59.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

applications

Syntax	<code>applications [<i>application-name</i>];</code>
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]
Description	Defines one or more applications to which the stateful firewall services apply.
Options	<i>application-name</i> —Name of the target application.
Usage Guidelines	See “Configure Stateful Firewall Match Conditions” on page 59.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

destination-address

Syntax	<code>destination-address <i>address</i>;</code>
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]
Description	Destination address for rule matching.
Options	<i>address</i> —Destination IP address. A valid wildcard is any-unicast, which denotes matching all unicast addresses.
Usage Guidelines	See “Configure Stateful Firewall Match Conditions” on page 59.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

from

Syntax	from { applications [<i>application-names</i>]; application-sets [<i>set-names</i>]; destination-address <i>address</i> ; source-address <i>address</i> ; }
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i>]
Description	Specify input conditions for a stateful firewall term.
Options	For information on match conditions, see the description of firewall filter match conditions in the <i>JUNOS Internet Software Policy Framework Configuration Guide</i> . The remaining statements are explained separately.
Usage Guidelines	See “Configure Stateful Firewall Rule Content” on page 58.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

match-direction

Syntax	match-direction (input output input-output);
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i>]
Description	Specify the direction in which the rule match is applied.
Options	input—Apply the rule match on the input side of the interface. output—Apply the rule match on the output side of the interface. input-output—Apply the rule match bidirectionally.
Usage Guidelines	See “Configure Stateful Firewall Rule Content” on page 58.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

rule

Syntax `rule rule-name {
 match-direction (input | output | input-output);
 term term-name {
 from {
 applications [application-names];
 application-sets [set-names];
 destination-address address;
 source-address address;
 }
 then {
 (accept | discard | reject);
 syslog;
 }
 }
}`

Hierarchy Level [edit services stateful-firewall],
 [edit services stateful-firewall rule-set *rule-set-name*]

Description Specify the rule the router uses when applying this service.

Options *rule-name*—Identifier for the collection of terms that constitute this rule.

The remaining statements are explained separately.

Usage Guidelines See “Configure Stateful Firewall Rule Content” on page 58.

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

rule-set

Syntax `rule-set rule-set-name {
 [rule rule-name];
}`

Hierarchy Level [edit services stateful-firewall]

Description Specify the rule set the router uses when applying this service.

Options *rule-set-name*—Identifier for the collection of rules that constitute this rule set.

Usage Guidelines See “Configure the Stateful Firewall Rule Set” on page 58.

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

services

Syntax	services stateful-firewall { ... }
Hierarchy Level	[edit]
Description	Define the service rules to be applied to traffic.
Options	stateful-firewall—Identifies the stateful firewall set of rules statements.
Usage Guidelines	See “Configure Stateful Firewall Properties” on page 57.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

source-address

Syntax	source-address <i>address</i> ;
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]
Description	Source address for rule matching.
Options	<i>address</i> —Source IP address.
Usage Guidelines	See “Configure Stateful Firewall Match Conditions” on page 59.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

syslog

Syntax	syslog;
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> then]
Description	Enable system logging. The system log information of the Adaptive Services PIC is passed to the kernel for logging in the /var/log directory. This setting overrides any syslog statement setting included in the service set or interface default configuration.
Usage Guidelines	See “Configure Stateful Firewall Actions” on page 60.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

term

Syntax	<pre>term <i>term-name</i> { from { applications [<i>application-names</i>]; application-sets [<i>set-names</i>]; destination-address <i>address</i>; source-address <i>address</i>; } then { (accept discard reject); syslog; } }</pre>
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i>]
Description	Define the stateful firewall term properties.
Options	<p><i>term-name</i>—Identifier for the term.</p> <p>The remaining statements are explained separately.</p>
Usage Guidelines	See “Configure Stateful Firewall Rule Content” on page 58.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

then

Syntax	<pre>then { (accept discard reject); syslog; }</pre>
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i>]
Description	Define the stateful firewall term actions. You can configure the router to accept, discard, or reject the targeted traffic. The other actions are optional.
Options	<p>accept—Accept the traffic and send it on to its destination.</p> <p>discard—Do not accept traffic or process it further.</p> <p>reject—Do not accept the traffic and return a rejection message. Rejected traffic can be logged or sampled.</p> <p>The remaining statement is explained separately.</p>
Usage Guidelines	See “Configure Stateful Firewall Actions” on page 60.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
See Also	<i>JUNOS Internet Software Policy Framework Configuration Guide</i>