

Chapter 11

Summary of Intrusion Detection Services Configuration Statements

The following sections explain each of the intrusion detection services (IDS) statements. The statements are organized alphabetically.

aggregation

Syntax	aggregation { destination-prefix <i>prefix-number</i> ; source-prefix <i>prefix-number</i> ; }
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then]
Description	Specify the type of data to be aggregated.
Options	The remaining statements are explained separately.
Usage Guidelines	See “Configuring IDS Actions” on page 98.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

application-sets

Syntax	application-sets [<i>set-names</i>];
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i> from]
Description	Define one or more target application sets.
Options	<i>set-name</i> —Name of the target application set.
Usage Guidelines	See “Configuring IDS Match Conditions” on page 97.
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-names</i>];</code>
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i> from]
Description	Define one or more applications to which IDS applies.
Options	<i>application-name</i> —Name of the target application.
Usage Guidelines	See “Configuring IDS Match Conditions” on page 97.
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 ids rule <i>rule-name</i> term <i>term-name</i> from]
Description	Specify the destination address for rule matching.
Options	<i>address</i> —Destination IP address.
Usage Guidelines	See “Configuring IDS Match Conditions” on page 97.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

destination-prefix

Syntax	<code>destination-prefix <i>prefix-number</i>;</code>
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then aggregation]
Description	Specify the prefix value for destination IP address aggregation.
Options	<i>prefix-number</i> —Integer value. Range: 1 through 32
Usage Guidelines	See “Configuring IDS Actions” on page 98.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

force-entry

Syntax	(force-entry ignore-entry);
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then]
Description	Specify handling of entries in the IDS events cache: <p>force-entry—Ensure that the entry has a permanent place in the IDS cache after one event is registered.</p> <p>ignore-entry—Ensure that all IDS events are ignored.</p>
Usage Guidelines	See “Configuring IDS Actions” on page 98.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

from

Syntax	from { <p>applications [<i>application-names</i>];</p> <p>application-sets [<i>set-names</i>];</p> <p>destination-address <i>address</i>;</p> <p>source-address <i>address</i>;</p> <p>}</p>
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i>]
Description	Specify input conditions for the IDS term.
Options	For information on match conditions, see the description of firewall filter match conditions in the <i>JUNOS Policy Framework Configuration Guide</i> . <p>The remaining statements are explained separately.</p>
Usage Guidelines	See “Configuring IDS Match Conditions” on page 97.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

ignore-entry

See force-entry on page 103

logging

Syntax	logging { syslog; threshold <i>rate</i> ; }
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then]
Description	Set logging values for this IDS term.
Options	The remaining statements are explained separately.
Usage Guidelines	See “Configuring IDS Actions” on page 98.
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 ids rule <i>rule-name</i>]
Description	Specify the direction in which the rule match is applied.
Options	input—Apply the rule match on input. output—Apply the rule match on output. input-output—Apply the rule match bidirectionally.
Usage Guidelines	See “Configuring IDS Match Conditions” on page 97.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

mss

Syntax	mss <i>value</i> ;
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then syn-cookie]
Description	Specify the maximum sequence selection (MSS) value used in TCP delayed binding.
Options	<i>value</i> —MSS value. Default: 1500 Range: 128 through 8192
Usage Guidelines	See “Configuring IDS Actions” on page 98.
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 {
            aggregation {
                destination-prefix prefix-number;
                source-prefix prefix-number;
            }
            (force-entry | ignore-entry);
            logging {
                syslog;
                threshold rate;
            }
            syn-cookie {
                mss value;
                threshold rate;
            }
        }
    }
}

```

Hierarchy Level [edit services ids],
[edit services ids 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.

Usage Guidelines See “Configuring IDS Rule Content” on page 95.

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

rule-set

Syntax	<code>rule-set <i>rule-set-name</i> { [rule <i>rule-names</i>]; }</code>
Hierarchy Level	[edit services ids]
Description	Specify the rule set the router uses when applying this service.
Options	<i>rule-set-name</i> —Identifier for the collection of rules that constitute this rule set.
Usage Guidelines	See “Configuring the IDS Rule Set” on page 95.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

services

Syntax	<code>services ids { ... }</code>
Hierarchy Level	[edit]
Description	Define the service rules to be applied to traffic.
Options	<i>ids</i> —Identifies the IDS set of rules statements.
Usage Guidelines	See “Configuring Intrusion Detection Properties” on page 95.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

source-address

Syntax	<code>source-address <i>address</i>;</code>
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i> from]
Description	Specify the source address for rule matching.
Options	<i>address</i> —Source IP address.
Usage Guidelines	See “Configuring IDS Match Conditions” on page 97.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

source-prefix

Syntax	source-prefix <i>prefix-number</i> ;
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then aggregation]
Description	Specify the prefix value for source IP address aggregation.
Options	<i>prefix-number</i> —Integer value. Range: 1 through 32
Usage Guidelines	See “Configuring IDS Actions” on page 98.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

syn-cookie

Syntax	syn-cookie { mss <i>value</i> ; threshold <i>rate</i> ; }
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then]
Description	Enable syn-cookie defenses against SYN attacks. By default, syn-cookie techniques are not applied.
Options	The remaining statements are described separately.
Usage Guidelines	See “Configuring IDS Actions” on page 98.
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 ids rule <i>rule-name</i> term <i>term-name</i> then logging]
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.
Usage Guidelines	See “Configuring IDS Actions” on page 98.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

term

```

Syntax term term-name {
    from {
        applications [ application-names ];
        application-sets [ set-names ];
        destination-address address;
        source-address address;
    }
    then {
        aggregation {
            destination-prefix prefix-number;
            source-prefix prefix-number;
        }
        (force-entry | ignore-entry);
        logging {
            syslog;
            threshold rate;
        }
        syn-cookie {
            mss value;
            threshold rate;
        }
    }
}

```

Hierarchy Level [edit services ids rule *rule-name*]

Description Define the IDS term properties.

Options *term-name*—Identifier for the term.

Usage Guidelines See “Configuring IDS Rule Content” on page 95.

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

then

Syntax	<pre> then { aggregation { destination-prefix <i>prefix-number</i>; source-prefix <i>prefix-number</i>; } (force-entry ignore-entry); logging { syslog; threshold <i>rate</i>; } syn-cookie { mss <i>value</i>; threshold <i>rate</i>; } } </pre>
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i>]
Description	Define the IDS term actions.
Options	The remaining statements are explained separately.
Usage Guidelines	See “Configuring IDS Rule Content” on page 95.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

threshold

Syntax	threshold <i>rate</i> ;
Hierarchy Level	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then logging], [edit services ids rule <i>rule-name</i> term <i>term-name</i> then syn-cookie]
Description	Specify the threshold for logging or applying syn-cookie defenses.
Options	<i>rate</i> —Logging threshold number of events per second. <i>rate</i> —Syn-cookie defense number of SYN attacks per second.
Usage Guidelines	See “Configuring IDS Actions” on page 98.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

