

## Chapter 11

# Summary of Intrusion Detection Services Configuration Statements

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

### aggregation

---

<b>Syntax</b>	aggregation { destination-prefix <i>prefix-number</i> ; source-prefix <i>prefix-number</i> ; }
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then]
<b>Description</b>	Specify the type of data to be aggregated.
<b>Options</b>	The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configure IDS Actions” on page 92.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

### application-sets

---

<b>Syntax</b>	application-sets [ <i>set-names</i> ];
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> from]
<b>Description</b>	Define one or more target application sets.
<b>Options</b>	<i>set-name</i> —Name of the target application set.
<b>Usage Guidelines</b>	See “Configure IDS Match Conditions” on page 91.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## applications

---

<b>Syntax</b>	<code>applications [ <i>application-names</i> ];</code>
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> from]
<b>Description</b>	Define one or more applications to which the intrusion detection services apply.
<b>Options</b>	<i>application-name</i> —Name of the target application.
<b>Usage Guidelines</b>	See “Configure IDS Match Conditions” on page 91.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## destination-address

---

<b>Syntax</b>	<code>destination-address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> from]
<b>Description</b>	Destination address for rule matching.
<b>Options</b>	<i>address</i> —Destination IP address.
<b>Usage Guidelines</b>	See “Configure IDS Match Conditions” on page 91.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## destination-prefix

---

<b>Syntax</b>	<code>destination-prefix <i>prefix-number</i>;</code>
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then aggregation]
<b>Description</b>	Prefix value for destination IP address aggregation.
<b>Options</b>	<i>prefix-number</i> —Integer value. <b>Range:</b> 1 through 32
<b>Usage Guidelines</b>	See “Configure IDS Actions” on page 92.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## force-entry

---

<b>Syntax</b>	(force-entry   ignore-entry);
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then]
<b>Description</b>	force-entry—Ensure that the entry has a permanent place in the IDS cache after one event is registered.  ignore-entry—Ensure that all IDS events are ignored.
<b>Usage Guidelines</b>	See “Configure IDS Actions” on page 92.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## from

---

<b>Syntax</b>	from { applications [ <i>application-names</i> ]; application-sets [ <i>set-names</i> ]; destination-address <i>address</i> ; source-address <i>address</i> ; }
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> ]
<b>Description</b>	Specify input conditions for the DS term.
<b>Options</b>	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.
<b>Usage Guidelines</b>	See “Configure IDS Match Conditions” on page 91.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## ignore-entry

---

See force-entry on page 97

## logging

---

<b>Syntax</b>	logging { syslog; threshold <i>rate</i> ; }
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then]
<b>Description</b>	Set logging values for this IDS term.
<b>Options</b>	The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configure IDS Actions” on page 92.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## match-direction

---

<b>Syntax</b>	match-direction (input   output   input-output);
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> ]
<b>Description</b>	Specify the direction in which the rule match is applied.
<b>Options</b>	input—Apply the rule match on input.  output—Apply the rule match on output.  input-output—Apply the rule match bidirectionally.
<b>Usage Guidelines</b>	See “Configure IDS Match Conditions” on page 91.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## mss

---

<b>Syntax</b>	mss <i>value</i> ;
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then syn-cookie]
<b>Description</b>	Specify the maximum sequence selection (MSS) value used in TCP delayed binding.
<b>Options</b>	<i>value</i> —MSS value. <b>Default:</b> 1500 <b>Range:</b> 128 through 8192
<b>Usage Guidelines</b>	See “Configure IDS Actions” on page 92.
<b>Required Privilege Level</b>	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 “Configure IDS Rule Content” on page 89.

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

## rule-set

---

<b>Syntax</b>	<code>rule-set <i>rule-set-name</i> {     [ rule <i>rule-names</i> ]; }</code>
<b>Hierarchy Level</b>	[edit services ids]
<b>Description</b>	Specify the rule set the router uses when applying this service.
<b>Options</b>	<i>rule-set-name</i> —Identifier for the collection of rules that constitute this rule set.
<b>Usage Guidelines</b>	See “Configure the IDS Rule Set” on page 89.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## services

---

<b>Syntax</b>	<code>services ids { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Description</b>	Define the service rules to be applied to traffic.
<b>Options</b>	<i>ids</i> —Identifies the Intrusion Detection Services set of rules statements.
<b>Usage Guidelines</b>	See “Configure Intrusion Detection Properties” on page 89.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## source-address

---

<b>Syntax</b>	<code>source-address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> from]
<b>Description</b>	Source address for rule matching.
<b>Options</b>	<i>address</i> —Source IP address.
<b>Usage Guidelines</b>	See “Configure IDS Match Conditions” on page 91.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## source-prefix

---

<b>Syntax</b>	source-prefix <i>prefix-number</i> ;
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then aggregation]
<b>Description</b>	Prefix value for source IP address aggregation.
<b>Options</b>	<i>prefix-number</i> —Integer value. <b>Range:</b> 1 through 32
<b>Usage Guidelines</b>	See “Configure IDS Actions” on page 92.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## syn-cookie

---

<b>Syntax</b>	syn-cookie { mss <i>value</i> ; threshold <i>rate</i> ; }
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then]
<b>Description</b>	Enable syn-cookie defenses against SYN attacks. By default, syn-cookie techniques are not applied.
<b>Options</b>	The remaining statements are described separately.
<b>Usage Guidelines</b>	See “Configure IDS Actions” on page 92.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## syslog

---

<b>Syntax</b>	syslog;
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> then logging]
<b>Description</b>	Enable system logging. The system log information of the Adaptive Services PIC is passed to the kernel for logging in the /var/log directory.
<b>Usage Guidelines</b>	See “Configure IDS Actions” on page 92.
<b>Required Privilege Level</b>	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 “Configure IDS Rule Content” on page 89.

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

## then

---

<b>Syntax</b>	<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>
<b>Hierarchy Level</b>	[edit services ids rule <i>rule-name</i> term <i>term-name</i> ]
<b>Description</b>	Define the IDS term actions.
<b>Options</b>	The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configure IDS Rule Content” on page 89.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## threshold

---

<b>Syntax</b>	threshold <i>rate</i> ;
<b>Hierarchy Level</b>	[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]
<b>Description</b>	Specify the threshold for logging or applying syn-cookie defenses.
<b>Options</b>	<i>rate</i> —Logging: threshold number of events per second. <i>rate</i> —Syn-cookie defense: number of SYN attacks per second.
<b>Usage Guidelines</b>	See “Configure IDS Actions” on page 92.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

