

Chapter 4

Applications Configuration Guidelines

You can define application protocols for the stateful firewall and Network Address Translation (NAT) services to use in match condition rules. An application protocol defines application parameters using information from network Layer 3 and above. Examples of such applications are FTP and H.323.

To configure applications that are used with services, you include statements at the [edit applications] hierarchy level of the configuration:

```
[edit applications]
application application-name {
  application-protocol protocol-name;
  destination-port port-number;
  icmp-code value;
  icmp-type value;
  inactivity-timeout value;
  protocol type;
  rpc-program-number number;
  snmp-command command;
  source-port port-number;
  ttl-threshold value;
  uuid hex-value;
}
}
application-set application-set-name {
  [ application application-names ];
}
```

This chapter includes the following sections:

Configuring Application Protocol Properties on page 44

Configuring Application Sets on page 51

JUNOS Default Groups on page 51

Examples: Configuring Applications on page 53

Configuring Application Protocol Properties

To configure application properties, include the application statement at the [edit applications] hierarchy level:

```
[edit applications]
application application-name {
  application-protocol protocol-name;
  destination-port port-number;
  icmp-code value;
  icmp-type value;
  inactivity-timeout value;
  protocol type;
  rpc-program-number number;
  snmp-command command;
  source-port port-number;
  ttl-threshold value;
  uuid hex-value;
}
```

You can group application objects by configuring the application-set statement; for more information, see “Configuring Application Sets” on page 51.

This section includes the following tasks for configuring applications:

- Configuring an Application Protocol on page 44
- Configuring the Network Protocol on page 46
- Configuring the ICMP Code and Type on page 46
- Configuring Source and Destination Ports on page 48
- Configuring the Inactivity Timeout Period on page 50
- Configuring an SNMP Command on page 50
- Configuring an RPC Program Number on page 50
- Configuring the TTL Threshold on page 50
- Configuring a Universal Unique Identifier on page 51

Configuring an Application Protocol

The application-protocol statement allows you to specify which of the supported application protocols to configure and include in an application set for service processing. To configure, include the application-protocol statement at the [edit applications application *application-name*] hierarchy level:

```
[edit applications application application-name]
application-protocol protocol-name;
```

Table 4 shows the list of supported protocols.

Table 4: Application Protocols Supported by Services Interfaces

Protocol Name	CLI value	Comments
BOOTP	bootp	Supports BOOTP and DHCP.
DCE RPC	dce-rpc	Requires the protocol statement to have the value <code>udp</code> or <code>tcp</code> . Requires a <code>uuid</code> value. You cannot specify <code>destination-port</code> or <code>source-port</code> values.
DCE RPC portmap	dce-rpc-portmap	Requires the protocol statement to have the value <code>udp</code> or <code>tcp</code> . Requires a <code>destination-port</code> value.
DNS	dns	Requires the protocol statement to have the value <code>udp</code> . This application protocol closes the DNS flow as soon as the DNS response is received.
Exec	exec	Requires the protocol statement to have the value <code>tcp</code> or to be unspecified. Requires a <code>destination-port</code> value.
FTP	ftp	Requires the protocol statement to have the value <code>tcp</code> or to be unspecified. Requires a <code>destination-port</code> value.
H.323	h323	Requires the protocol statement to have the value <code>tcp</code> or to be unspecified. Requires a <code>destination-port</code> value.
ICMP	icmp	Requires the protocol statement to have the value <code>icmp</code> or to be unspecified.
IIOP TCP	iiop	Requires the protocol statement to have the value <code>tcp</code> or to be unspecified. Requires a <code>destination-port</code> value.
NetBIOS	netbios	Requires the protocol statement to have the value <code>udp</code> or to be unspecified. Requires a <code>destination-port</code> value.
NetShow	netshow	Requires the protocol statement to have the value <code>tcp</code> or to be unspecified. Requires a <code>destination-port</code> value.
RealAudio	realaudio	Requires the protocol statement to have the value <code>tcp</code> or to be unspecified. Requires a <code>destination-port</code> value.
RPC UDP or TCP	rpc	Requires the protocol statement to have the value <code>udp</code> or <code>tcp</code> . Requires a <code>rpc-program-number</code> value. You cannot specify <code>destination-port</code> or <code>source-port</code> values.
RPC portmap	rpc-portmap	Requires the protocol statement to have the value <code>udp</code> or <code>tcp</code> . Requires a <code>destination-port</code> value.
RTSP	rtsp	Requires the protocol statement to have the value <code>tcp</code> or to be unspecified. Requires a <code>destination-port</code> value.
Shell	shell	Requires the protocol statement to have the value <code>tcp</code> or to be unspecified. Requires a <code>destination-port</code> value.
SNMP	snmp	Requires the protocol statement to have the value <code>udp</code> or to be unspecified. Requires a <code>destination-port</code> value.
SQLNet	sqlnet	Requires the protocol statement to have the value <code>tcp</code> or to be unspecified. Requires a <code>destination-port</code> or <code>source-port</code> value.
TFTP	tftp	Requires the protocol statement to have the value <code>udp</code> or to be unspecified. Requires a <code>destination-port</code> value.
Trace route	traceroute	Requires the protocol statement to have the value <code>udp</code> or to be unspecified. Requires a <code>destination-port</code> value.
WinFrame	winframe	Requires the protocol statement to have the value <code>tcp</code> or to be unspecified. Requires a <code>destination-port</code> value.

Configuring the Network Protocol

The protocol statement allows you to specify which of the supported network protocols to match in an application definition. To configure, include the protocol statement at the [edit applications application *application-name*] hierarchy level:

```
[edit applications application application-name]
  protocol type;
```

You specify the protocol type as a numeric value; for the more commonly used protocols, text names are also supported in the command-line interface (CLI). Table 5 shows the list of the supported protocols.

Table 5: Network Protocols Supported by Services Interfaces

Network Protocol Type	CLI Value	Comments
IPSec AH	ah	
EGP	egp	
IPSec ESP	esp	
GRE	gre	
ICMP	icmp	Requires an application-protocol value of icmp.
IGMP	igmp	
IP in IP	ipip	
IPv6 in IP	ipv6	
OSPF	ospf	
PIM	pim	
RSVP	rsvp	
TCP	tcp	Requires a destination-port or source-port value unless you specify application-protocol rcp or dce-rcp.
UDP	udp	Requires a destination-port or source-port value unless you specify application-protocol rcp or dce-rcp.
VRRP	vrrp	

For a complete list of possible numeric values, see RFC 1700, *Assigned Number s* (for the Internet Protocol Suite).

Configuring the ICMP Code and Type

The Internet Control Message Protocol (ICMP) code and type provide additional specification, in conjunction with the network protocol, for packet matching in an application definition. To configure, include the icmp-code and icmp-type statements at the [edit applications application *application-name*] hierarchy level:

```
[edit applications application application-name]
  icmp-code value;
  icmp-type value;
```

You can include only one ICMP code and type value. The application-protocol statement must have the value icmp. Table 6 shows the list of supported ICMP values.

Table 6: ICMP Codes and Types Supported by Services Interfaces

CLI Statement	Description
icmp-code	<p>This value or keyword provides more specific information than icmp-type. Because the value's meaning depends upon the associated icmp-type value, you must specify icmp-type along with icmp-code. For more information, see the <i>JUNOS Policy Framework Configuration Guide</i>.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed). The keywords are grouped by the ICMP type with which they are associated:</p> <p>parameter-problem: ip-header-bad (0), required-option-missing (1)</p> <p>redirect: redirect-for-host (1), redirect-for-network (0), redirect-for-tos-and-host (3), redirect-for-tos-and-net (2)</p> <p>time-exceeded: ttl-eq-zero-during-reassembly (1), ttl-eq-zero-during-transit (0)</p> <p>unreachable: communication-prohibited-by-filtering (13), destination-host-prohibited (10), destination-host-unknown (7), destination-network-prohibited (9), destination-network-unknown (6), fragmentation-needed (4), host-precedence-violation (14), host-unreachable (1), host-unreachable-for-TOS (12), network-unreachable (0), network-unreachable-for-TOS (11), port-unreachable (3), precedence-cutoff-in-effect (15), protocol-unreachable (2), source-host-isolated (8), source-route-failed (5)</p>
icmp-type	<p>Normally, you specify this match in conjunction with the protocol match statement to determine which protocol is being used on the port. For more information, see the <i>JUNOS Policy Framework Configuration Guide</i>.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): echo-reply (0), echo-request (8), info-reply (16), info-request (15), mask-request (17), mask-reply (18), parameter-problem (12), redirect (5), router-advertisement (9), router-solicit (10), source-quench (4), time-exceeded (11), timestamp (13), timestamp-reply (14), or unreachable (3).</p>



NOTE: If you configure an interface with an input firewall filter that includes a reject action and with a service set that includes stateful firewall rules, the router executes the input firewall filter before the stateful firewall rules are run on the packet. As a result, when the Packet Forwarding Engine sends an ICMP error message out through the interface, the stateful firewall rules might drop the packet because it was not seen in the input direction.

Possible workarounds are to include a forwarding-table filter to perform the reject action, because this type of filter is executed after the stateful firewall in the input direction, or to include an output service filter to prevent the locally generated ICMP packets from going to the stateful firewall service.

Configuring Source and Destination Ports

The Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port provide additional specification, in conjunction with the network protocol, for packet matching in an application definition. To configure, include the destination-port and source-port statements at the [edit applications application *application-name*] hierarchy level:

```
[edit applications application application-name]
destination-port value;
source-port value;
```

You must define one source or destination port. Normally, you specify this match in conjunction with the protocol match statement to determine which protocol is being used on the port; for constraints, see Table 4 on page 45.

You can specify either a numeric value or one of the text synonyms listed in Table 7.

Table 7: Port Names Supported by Services Interfaces

Port Name	Corresponding Port Number
afs	1483
bgp	179
biff	512
bootpc	68
bootps	67
cmd	514
cvspserver	2401
dhcp	67
domain	53
eklogin	2105
ekshell	2106
exec	512
finger	79

Port Name	Corresponding Port Number
ftp	21
ftp-data	20
http	80
https	443
ident	113
imap	143
kerberos-sec	88
klogin	543
kpasswd	761
krb-prop	754
krbupdate	760
kshell	544
ldap	389
login	513
mobileip-agent	434
mobileip-mn	435
msdp	639
netbios-dgm	138
netbios-ns	137
netbios-ssn	139
nfsd	2049
nntp	119
ntalk	518
ntp	123
pop3	110
pptp	1723
printer	515
radacct	1813
radius	1812
rip	520
rkinit	2108
sntp	25
snmp	161
snmptrap	162
snpp	444
socks	1080
ssh	22
sunrpc	111
syslog	514
tacacs-ds	65

Port Name	Corresponding Port Number
talk	517
telnet	23
tftp	69
timed	525
who	513
xdmcp	177
zephyr-clt	2103
zephyr-hm	2104

For more information on matching criteria, see the *JUNOS Policy Framework Configuration Guide*.

Configuring the Inactivity Timeout Period

You can specify a timeout period for application inactivity. If the software has not detected any activity during the duration, the flow becomes invalid when the timer expires. To configure, include the `inactivity-timeout` statement at the [edit applications application *application-name*] hierarchy level:

```
[edit applications application application-name]
  inactivity-timeout seconds;
```

The default value is 30 seconds. The value you configure for an application overrides any global value configured at the [edit interfaces *interface-name* service-options] hierarchy level; for more information, see “Configuring Default Timeout Settings” on page 266.

Configuring an SNMP Command

You can specify a Simple Network Management Protocol (SNMP) command setting for packet matching. To configure, include the `snmp-command` statement at the [edit applications application *application-name*] hierarchy level:

```
[edit applications application application-name]
  snmp-command value;
```

The supported values are `get`, `get-next`, `set`, and `trap`. You can configure only one value for matching. The `application-protocol` statement must have the value `snmp`.

Configuring an RPC Program Number

You can specify a Remote Procedure Call (RPC) program number for packet matching. To configure, include the `rpc-program-number` statement at the [edit applications application *application-name*] hierarchy level:

```
[edit applications application application-name]
  rpc-program-number number;
```

The range of values used for DCE or RPC is from 100,000 through 400,000. The `application-protocol` statement must have the value `rpc`.

Configuring the TTL Threshold

You can specify a trace route time-to-live (TTL) threshold value, which controls the acceptable level of network penetration for trace routing. To configure, include the `ttl-threshold` statement at the [edit applications application *application-name*] hierarchy level:

```
[edit applications application application-name]
ttl-threshold value;
```

The application-protocol statement must have the value `traceroute`.

Configuring a Universal Unique Identifier

You can specify a Universal Unique Identifier (UUID) for DCE RPC objects. To configure, include the `uuid` statement at the [edit applications application *application-name*] hierarchy level:

```
[edit applications application application-name]
uuid hex-value;
```

The `uuid` value is in hexadecimal notation. The application-protocol statement must have the value `dce-rpc`. For more information on UUID numbers, see <http://www.opengroup.org/onlinepubs/9629399/apdx.htm>.

Configuring Application Sets

You can group the applications you have defined into a named object by including the `application-set` statement at the [edit applications] hierarchy level:

```
[edit applications]
application-set application-set-name {
  application application1;
  application application2;
}
```

For an example of a typical application set, see “Examples: Configuring Applications” on page 53.

JUNOS Default Groups

The JUNOS software provides a default, hidden configuration group called `junos-defaults` that is automatically applied to the configuration of your routing platform. The `junos-defaults` group contains preconfigured statements that contain predefined values for common applications. Some of the statements must be referenced to take effect, such as applications like File Transfer Protocol (FTP) or telnet. Other statements are applied automatically, such as terminal settings. All of the preconfigured statements begin with the reserved name `junos-`.



NOTE: You can override the JUNOS default configuration values, but you cannot delete or edit them. If you delete a configuration, the defaults return when a new configuration is added.

You cannot use the `apply-groups` statement with the JUNOS defaults group.

To view the full set of available preset statements from the JUNOS default group, issue the `show groups junos-defaults` configuration mode command. The following example displays a partial list of junos default groups.

```

user@host> show groups junos-defaults
groups {
  junos-defaults {
    applications {
      #
      # File Transfer Protocol
      #
      application junos-ftp {
        application-protocol ftp;
        protocol tcp;
        destination-port 21;
      }
      #
      # Trivial File Transfer Protocol
      #
      application junos-tftp {
        application-protocol tftp;
        protocol udp;
        destination-port 69;
      }
      #
      # RPC portmapper on TCP
      #
      application junos-rpc-portmap-tcp {
        application-protocol rpc-portmap;
        protocol tcp;
        destination-port 111;
      }
      #
      # RPC portmapper on UDP
      #
      application junos-rpc-portmap-udp {
        application-protocol rpc-portmap;
        protocol udp;
        destination-port 111;
      }
    }
  }
}

```

To reference statements available from the `junos-defaults` group, include the selected `junos-default-name` statement at the applicable hierarchy level.

Example: Referencing the Preset Statement from the JUNOS Default Group

The following example is a preset statement from the JUNOS default groups that is available for FTP in a stateful firewall:

```
[edit]
groups {
  junos-defaults {
    applications {
      application junos-ftp {           # Use FTP default configuration
        application-protocol ftp;
        protocol tcp;
        destination-port 21;
      }
    }
  }
}
```

To reference a preset JUNOS default statement from the JUNOS default groups, include the `junos-default-name` statement at the applicable hierarchy level. For example, to reference the JUNOS default statement for FTP in a stateful firewall, include the `junos-ftp` statement at the `[edit services stateful-firewall rule rule-name term term-name from applications]` hierarchy level.

```
[edit]
services {
  stateful-firewall {
    rule my-rule {
      term my-term {
        from {
          applications junos-ftp; #Reference predefined statement, junos-ftp,
                                #for FTP in the stateful firewall configuration
        }
      }
    }
  }
}
```

Examples: Configuring Applications

The following example shows an application protocol definition describing a special FTP application running on port 78:

```
[edit applications]
application my-ftp-app {
  application-protocol ftp;
  protocol tcp;
  destination-port 78;
  timeout 100; # inactivity timeout for ftp service
}
```

The following example shows a special ICMP protocol (application-protocol icmp) of type 8 (ICMP echo):

```
[edit applications]
application icmp-app {
  application-protocol icmp;
  protocol icmp;
  icmp-type icmp-echo;
}
```

The following example shows a possible application set:

```
[edit applications]
application-set basic {
  http;
  ftp;
  telnet;
  nfs;
  icmp;
}
```

The software includes a predefined set of well-known application protocols. The set includes applications for which the TCP and UDP destination ports are already recognized by stateless firewall filters.

