

## Classifying Traffic

To create an application protocol:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber to whom you want to assign the application object.
2. Click the **Applications** tab.

The Applications page appears. This page displays the application protocols that the subscriber inherits from parent subscribers and application protocols configured explicitly for the subscriber.

**Figure 1: Applications Page**

default

▶

local

▶

Acme

▶

Boca

▶

Primary

▶

Bandwidth & VPNs	Applications	Firewall	Addresses	NAT	Schedules	Managers
Name	Application Protocol	IP Protocol	Details			
bootp_boca_primary	bootp	udp	Inactivity timeout: 25 Destination port: 8067	<div>EditDelete</div>		
ftp_boca_primary	ftp	tcp	Inactivity timeout: 30 Destination port: 8098	<div>EditDelete</div>		
<div>Create Application</div>						

3. Click **Create Application**.

The Create Application page appears.

4. Using the following field descriptions, specify details for the application protocol.

Some fields are available only for certain applications. When a field is unavailable, the box in which you enter information is dimmed, and you cannot enter information in it.

5. Click **Apply**.

## ***Traffic Classification Fields in Enterprise Manager Portal***

Use the fields in this topic to classify traffic for firewall exceptions and NAT rules.

### ***Application Name***

- Name for this application protocol.
- Value—Text string
- Default—No value
- Example—bootp-boston

### ***Application Protocol***

- Application protocol.
- Value—Type of application protocol or None
- Guidelines—Select a protocol from the menu to specify that the application uses a particular application protocol. Depending on the application protocol you choose, some fields in the application object are irrelevant (and disabled) or restricted to specific values. If the application protocol you want is not available, you can select the option **None** and base the application object on an IP protocol. If you select this option, the NAT rule or firewall exception affects only the first flow in a conversation. Consequently, you can deny or discard a conversation, but you cannot allow a complete conversation.
- Default—Any
- Example—bootp

### ***IP Protocol***

- IP protocol.
- Value—Type of IP protocol or number of IP protocol in the range 0–255
- Guidelines—The names of the allowed IP protocols are shown in the tool tips for this field. The portal automatically selects an IP protocol for certain application protocols.
- Default—No value
- Example—tcp

### ***Source Port***

- Source TCP/UDP ports (as contained in the IP packets) of traffic for this application object.
- Value—Integer in the range 0–65535
- Guidelines—Enter either a single port number or a range of port numbers separated by two dots (..). To specify all ports, leave this field empty.
- Default—No value
- Example—25..35

### ***Destination Port***

- Destination TCP/UDP ports (as contained in the IP packets) of traffic for this application object.
- Value—Integer in the range 0–65535
- Guidelines—Enter either a single port number or a range of port numbers separated by two dots (..). To specify all ports, leave this field empty.
- Default—No value
- Example—25..35

### ***SNMP Command***

- Type of command for Simple Network Management Protocol (SNMP).
- Value—Type of SNMP command
- Guidelines—Select a type of command from the menu.
- Default—Any
- Example—get-next

### ***ICMP Type***

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message
- Guidelines—Select a type of message from the menu.
- Default—Any
- Example—info-reply

### ***ICMP Code***

- Code for ICMP.
- Value—Type of ICMP code
- Guidelines—Select a type of code from the menu.
- Default—Any
- Example—host-precedence-violation

### ***TTL Threshold***

- Depth of network penetration for the traceroute application protocol.
- Value—Integer in the range 0–255 or unspecified

- Unspecified—Allows traceroutes up to a depth of 255.
- Default—Unspecified
- Example—5

### ***RPC Program Number***

- Program number for the remote procedure call (RPC) application protocol.
- Value—A single program number or range of program numbers separated by two dots (.). Program numbers are integers in the range 100000–400000.
- Guidelines—Specify the RPC program numbers to which the NAT rule or firewall exception applies. To specify all RPC program numbers, leave this field empty.
- Default—No value
- Example—7..12

### ***UUID***

- Universal unique identifier (UUID) for the Distributed Computing Environment (DCE) RPC application protocol.
- Value—Hexadecimal number in the format  
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
- Guidelines—Specify a number of a specific DCE RPC object to which the NAT rule or firewall exception applies. To specify all DCE RPC objects, leave this field empty.
- Default—No value
- Example—1f356a25-ce67-73ad-2187-631ec8ae1bd6

### ***Inactivity Timeout***

- Time for which a conversation associated with the identified application protocol can be inactive before the JUNOS routing platform terminates the conversation.
- Value—Number of seconds in the range 0–2147483647
- Guidelines—Specify a time, or leave this field empty to use the default setting.
- Default—30 seconds
- Example—45

