

## Overview of Traffic Classification for Firewall Exceptions and NAT Rules

---

You can create for a subscriber a list of application objects that can be used to classify the traffic affected by a firewall exception to a stateful firewall or by a NAT rule. These application objects are based on application protocols—protocols that are categorized in the application layer of the TCP/IP reference model—or IP protocols that the JUNOS routing platform supports. Subordinate subscribers inherit application objects configured for parent subscribers.

An application protocol defines how a client and a server communicate during a *conversation*—a particular activity between the client and the server, such as an FTP session. A conversation in the application layer consists of multiple *flows*. A flow is one element of the conversation; for example, in an FTP session, the initial TCP control connection or a subsequent UDP traffic connection. You can apply a NAT rule or a firewall exception to the initial flow in a conversation by defining an application object. The NAT rule or firewall exception then applies to all subsequent flows in that conversation.

In the FTP example, the client may create a TCP connection to the server and send the server a UDP port number in the initial flow. The server may then start sending UDP traffic to the UDP port specified in the initial flow. If the initial flow matches a defined application object that a firewall allows, the firewall will allow the UDP traffic in the second flow and in all subsequent flows in the conversation.

Certain application protocols, such as FTP, are supported explicitly, and you can select them for your application object. These application protocols usually have an associated IP protocol that the portal selects automatically. If you want to create an application object for an application protocol that is not explicitly supported, such as HTTP, you can create an application object based on an IP protocol only. For example, you could create an application object called HTTP, specify no application protocol, and select TCP as the IP protocol. You can then specify 8080 for the source and destination ports in the application protocol to identify the HTTP traffic.

