

# Chapter 18

## Network Address Translation Overview

Network Address Translation (NAT) is a mechanism for concealing a set of host addresses on a private network behind a pool of public addresses. It can be used as a security measure to protect the host addresses from direct targeting in network attacks.

Traditional NAT, specified in RFC 3022, *Traditional IP Network Address Translator*, is fully supported by JUNOS software. In addition, network address port translation (NAPT) is supported for source addresses.

The AS PIC interfaces support three types of NAT processing: static-source, dynamic-source, and static-destination.

Static-source NAT hides a private network without using NAPT.

Dynamic-source NAT hides a private network using NAPT.

Static-destination NAT makes selected private servers accessible.

You can implement NAT to hide one or many hosts on a private network behind a pool of public IP addresses. The pool can be as small as one IP address, or it can be a multiple of contiguous IP addresses. You can specify a port range to restrict port translation when NAT is configured in dynamic-source mode.

Private address to public address binding can be either static or dynamic. In the basic NAT mode, a NAT rule can force a private IP address to be always bound to a public address; in the NAPT mode, a NAT rule can force a paired private address and private TU port to be mapped to a public IP and public TU port. However, when the address binding is not statically forced by the NAT rules, NAT can dynamically pick an available address or address and TU port pairing when a new session starts.

Like most traditional NAT implementations, the JUNOS implementation of NAT supports sessions initiated from the private side only. Sessions initiated from the public side are supported only when you configure static address binding.

NAT becomes activated only when a packets passes the AS PIC stateful firewall inspection. For this reason, you must configure stateful firewall rules in combination with NAT. A stateful firewall discard packet does not reach NAT even if the packet otherwise matches the NAT rule.

