Connection Objects

https://campus.barracuda.com/doc/46209019/

A connection object defines the egress interface and source (NAT) IP address for traffic matching the access rule. If a source IP address is specified, the appropriate link will be used based on the routing table. If an interface is specified, the appropriate source IP address will be used based on the routing table. You can use the predefined connection objects or you can create new connection objects.

Connection Objects

- **Dynamic SNAT** – The firewall uses the routing table to find a suitable interface for routing the packet and uses the IP address of the relevant interface as the new source IP address.
- **No SNAT** – The original source IP address of the packet is not changed.
- **SNAT with 3G IP** – Source NAT is using the first IP address on the ppp5 device.
- **SNAT with DHCP IP** – Source NAT is using the first IP address on the dhcp device.
- **SNAT with DSL IP** – Source NAT is using the first IP address on the ppp1 device.
- **Custom Connection Objects (explicit-conn)** – Create your own custom connection objects, to define the explicit source address for this connection.
  - **NAT Tables** – NAT Table are a expanded type of source NAT for a network or IP address range.

For more information, see How to Create a Custom Connection Object and How to Create NAT Tables (Translation Maps).

Failover and Link Load Balancing

For every custom connection objects you create a failover and link/load balancing can be defined. The load balancing settings are also used for firewall-assisted multipath routing when multiple paths are used to route traffic through a single target network.

For more information, see How to Configure Link Balancing and Failover for Multiple WAN Connections.