Matching NAT rules on Firewall rules

This document accompanies the “NAT rulebase flowchart” Visio diagram.

Note that this is a first-match process, unless the service of NAT rule is “***any***”, and then this is a multi-match process!!!

**Match process bypass scenarios**

The NAT rule matching on firewall rule is aborted in the following scenarios:

* The destination of firewall rule is “***any***”
* The firewall rule is a cleanup rule
* Disabled NAT rule
* Section 4 NAT rule (“***all\_internal***”)
* Mirrored NAT (static) rule
* Network object NAT dynamic rule
* Manual NAT dynamic rule
* Twice NAT rule where source = translated source and destination = translated destination

In all other scenarios the process continues until there is a match.

**Service Match**

After there is a match by source and destination, as described in the diagram, a service match is performed.

If the service of NAT rule is “***any***”, all firewall rules in sub-policy are searched for match, not just the first-matched firewall rule. In this case the service of firewall rule is used for the new rule.

If the service of firewall rule is “***any***”, the match is successful, and the translated service of NAT rule is used for the new rule.

If neither of services is “***any***”:

First, the NAT service name is compared to firewall services list. If matched, the translated service of NAT rule is used for the new rule.

If the name doesn’t match, service port ranges are checked – NAT rule service port/range must be a subset of firewall service port ranges. If matched, the translated service of NAT rule is used for the new rule.