NAT rules creation and ordering

Preliminary: “*Non-NAT rules*”

A NAT real or mapped interface is called “*leads to internet*”, if it has routes (subnets) defined and there is a default route (subnet: 0.0.0.0, 0.0.0.0). For example –

*interface TenGigabitEthernet0/8*

*nameif inside*

*security-level 100*

*ip address 10.10.10.1 255.255.255.248*

*…*

*route inside 0.0.0.0 0.0.0.0 158.164.226.121 1*

*…*

*nat (inside,outside) source dynamic svr-10.103.29.222 nat-171.72.158.20 destination static svr-171.72.159.23-vir svr-206.209.34.1*

For network object (automatic) NAT rules, if the mapped interface leads to internet, then the rule is marked as a non-NAT rule.

For manual and twice NAT rules, if a real or mapped interface leads to internet, then the rule is marked as a non-NAT rule.

NAT rule creation important notes

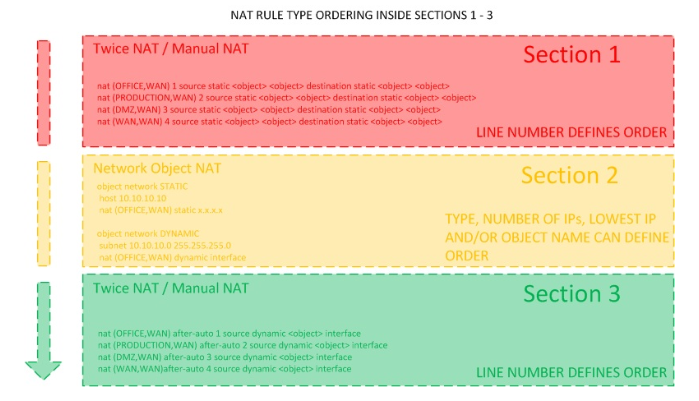
Many times Cisco users create a network group that contains only one member object (network or host). In this case, we extract and use that member object instead of the network object.

Check Point NAT rule’s translated field (source/destination) cannot be a network group!!!

If the source of static NAT rule is network group or network object and the translated source is a host object, we create a dynamic (hide) Check Point NAT rule.

Sections Creation

NAT rules are segmented and ordered into 3 or 7 sections –



**Section 1:**

Manual and twice NAT rules, in the order they appear in the configuration.

**Section 2:**

Network object (automatic) NAT rules – first static rules and then dynamic rules, in the order they appear in the configuration.

There is NO further ordering between rules (currently this is an acceptable limitation).

**Section 3:**

*Auto-After* manual and twice NAT rules, in the order they appear in the configuration.

**If there are non-NAT rules, sections 4-7 are also created**

**Section 4:**

A single NAT rule is generated automatically above interfaces that lead to the internet –

*source: all\_internal*

*destination: all\_internal*

*method: static*

**Section 5:**

Non-NAT section 1 rules

**Section 6:**

Non-NAT section 2 rules

**Section 7:**

Non-NAT section 3 rules