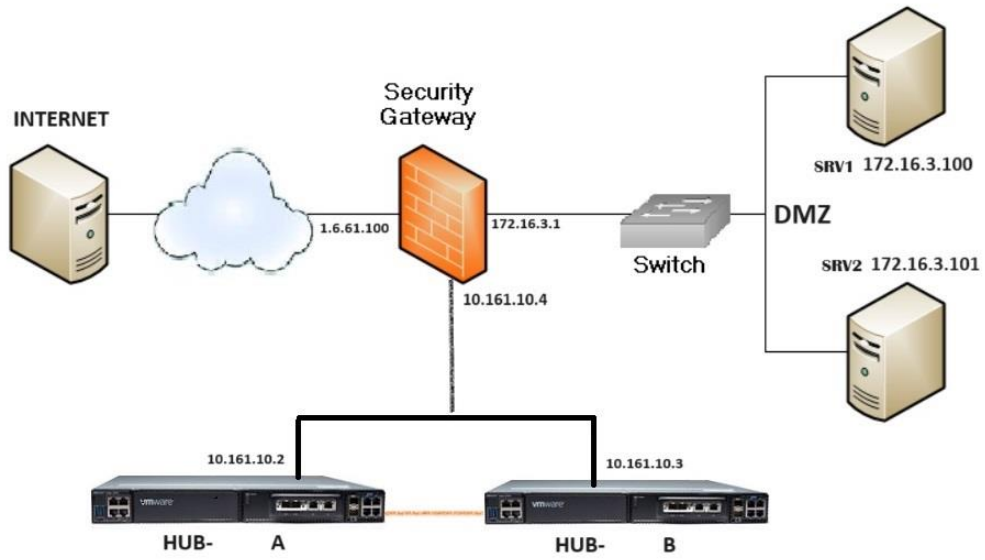
configure NAT U-Turn (Loopback / Hairpin NAT / NAT Reflection) on Check Point Security Gateway



Connection flow from VCC on internal network to the VCO:

VCC sends a request packet with a Source IP address 172.16.3.101 to a Destination IP address 1.6.61.100 (on TCP port 80/443) to request some web resource:

Source / Destination	IP Address
Source IP address	172.16.3.101
Destination IP address	1.6.61.100

Since the Destination IP address 1.6.61.100 is not on a directly connected network, VCC sends the request to its Default Gateway - the Security Gateway.

The Security Gateway performs NAT on the packet and changes the Destination IP address from 1.6.61.100 to VCO private IP address 172.16.3.100 (the source IP address 172.16.3.101 is not changed):

IP Address	IP Address Before NAT	IP Address After NAT
Source IP address	172.16.3.101	172.16.3.101
Destination IP address	1.6.61.100	172.16.3.100

The VCO creates a reply packet with a Source IP address 172.16.3.100 and Destination IP address 172.16.3.101

Source / Destination	IP Address
Source IP address	172.16.3.100
Destination IP address	172.16.3.101

Since the Destination IP address 172.16.3.101 is on a directly connected network, the VCO does not send the reply packet back to the Security Gateway, but sends it back directly to 172.16.3.100

VCC receives the reply packet but discards it because it expects a packet back from IP address 1.6.61.100, and not from IP address 172.16.3.100.

As far as the client is concerned, the reply packet is invalid and not related to any connection the client previously attempted to establish.

To resolve the issue with the traffic flow between VCC on an internal network and the VCO, an additional NAT rule needs to be added on the Security Gateway to perform NAT on this traffic as on the traffic between Any on the public network and the VCO.

The following NAT rules will perform the required NAT

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On
1	Host object with VCC Private IP 172.16.3.101	Host object with VCO Public IP 1.6.61.100	`http` `https`	Host object with Security Gateway's Private IP 172.16.3.1	Host object with Web Server's Private IP 172.16.3.100	`= Original`	Security Gateway object
2	Host object with VCO Private IP 172.16.3.100	Host object with VCC Private IP 172.16.3.101	`http` `https`	Host object with VCO Public IP 1.6.61.100	`= Original`	`= Original`	Security Gateway object

This is called - among other terms - Hairpin NAT because the traffic flow from internal clients enters and leaves the Security Gateway through the same interface.

Ref: How to configure NAT Loopback (Hairpin NAT / NAT Reflection) on Check Point Security Gateway