# Architecture



# Tunnel establishment

A tunnel is established between the PFSENSE and the FORCEPOINT firewall:

|  |  |
| --- | --- |
| PFSENSE | FORCEPOINT |
| Traffic end | Tunnel end | Tunnel end | Traffic end |
| 10.10.10.0/24 | 195.101.36.9 | 217.108.170.60 | 10.56.210.16 |

The configuration of the tunnel is up and running, the IP packets are carried out inside the enc0 interface that is a virtual interface used in BSD

# NAT configuration

The 10.10.10.30 uses NAT on the em0 interface (Port Forward) to be reachable from the 10.56.210.16 throughout the virtual IP 12.0.0.2. The NAT presence is mandatory as the customer network uses à 10.0.0.0 / 8 IP network.

# Status

The flow comes from the 10.56.210.16 to the 12.0.0.2 IP address of the PFSENSE : it answers to the ping

The NAT rule matches only TCP and UDP protocols.

When 10.56.210.16 tries to open a SSH or HTTPS session (TCP) on 12.0.0.2, then the NAT rule is matched. The flow goes to the 10.10.10.30 device, with 10.56.210.16 IP source which is correct.

The 10.10.10.30 device answers to the 10.56.210.16. When PFSENSE receives the TCP packets, then the NAT works also, but the IP packet is routed to the em1 interface (WAN) and does not matches the tunnel policy. Its look like a tunnel process error handling (we can assume that the tunnel is prior to the NAT, and then the tunnel rule could not be matched).