NetTunnel Operational Concept

**OfficePC**

We have a PC at an office that is a member of a LAN and it is inaccessible from the internet due to a firewall and the lack of any inbound rules. We have no ability to alter or otherwise configure the firewall. No inbound connections are allowed.

**HomePC**

We have a PC at home which is also on a LAN, but we have access to the router/firewall and can port-forward.

**Scenario**

We need to be able to RDP to the PC **OfficePC** from the PC **HomePC**. This is not typically not possible since **OfficePC** is firewalled.

With NetTunnel, we can install an EndPoint client on **OfficePC** and install another instance on **HomePC**. We then configure the firewall at home to forward port 40565 from the internet to the **HomePC** local LAN IP address of the **OfficePC** instance.

We then open the NetTunnel UI on the **OfficePC** instance and “add an endpoint”. Here we enter the IP/host of the **HomePC**’s external IP address and the username/password that is needed to login to NetTunnel. Note that we have to establish the connection from the **OfficePC** because the connection needs to be “outbound” from the **OfficePC** network since it is firewalled.

Once the connection is established, from either side (**HomePC** or **OfficePC**) we can right-click on the newly added endpoint and select “add tunnel”.

We would select that we want to listen on port 403389 at the **HomePC** and terminate at **OfficePC** to the IP address 127.0.0.1 port 3389.

With this configuration, when a connection is made to the **HomePC’s** local port 403389, the NetTunnel endpoint will accept the connection and ask the **OfficePC’**s instance of NetTunnel to connect to its configured tunnel destination address:port and will forward all bi-directional traffic over the initially configured endpoint connection.