

Forum:[Hack Forums](#)

Thread: [Reverse Socks5 Proxy using .net TCP Sockets](#)

0x0_ - September 15, 2018, 7:27 am

Im quite interested in a solution to open a reverse proxy using .net TCP Sockets in the example Client/Server where the client will run a proxy server and the server can use the client as proxy without the client have to open a port in his router or disable his firewall. i have seen some solutions such as quasarRAT already but i didnt manage to get it to work outside from quasar RAT. Help would be much apreciated.

ppaida - September 15, 2018, 7:44 am

You're not looking for a reverse proxy. A reverse proxy provides a common gateway to retrieve data based on rules.

What you want is NAT punching/traversal. STUN/TURN/ICE are some options. Basically, the "server" communicates to the "client" and the firewall tracks that connection in its state table and allows forwarding without explicitly opening ports.

Zephyros - September 23, 2018, 3:22 am

One way to do it is like this:

The server opens a port for the client(s) to connect to, with some auth and verification preferably. For each new connection from a victim, the server opens a new free port. On that port the server implements the negotiation and auth phase of the SOCKS5 protocol (

<https://en.wikipedia.org/wiki/SOCKS>)

After succesfully authenticating itself, the server tunnels the following traffic to and fro that specific port back to the assigned client. The client implements the rest of the socks5 protocol that establishes the connection to the requested domain and makes the outgoing connection. Then the client tunnels all of the traffic from that connection to the server which relays it over the proxy port to the user that made the request.