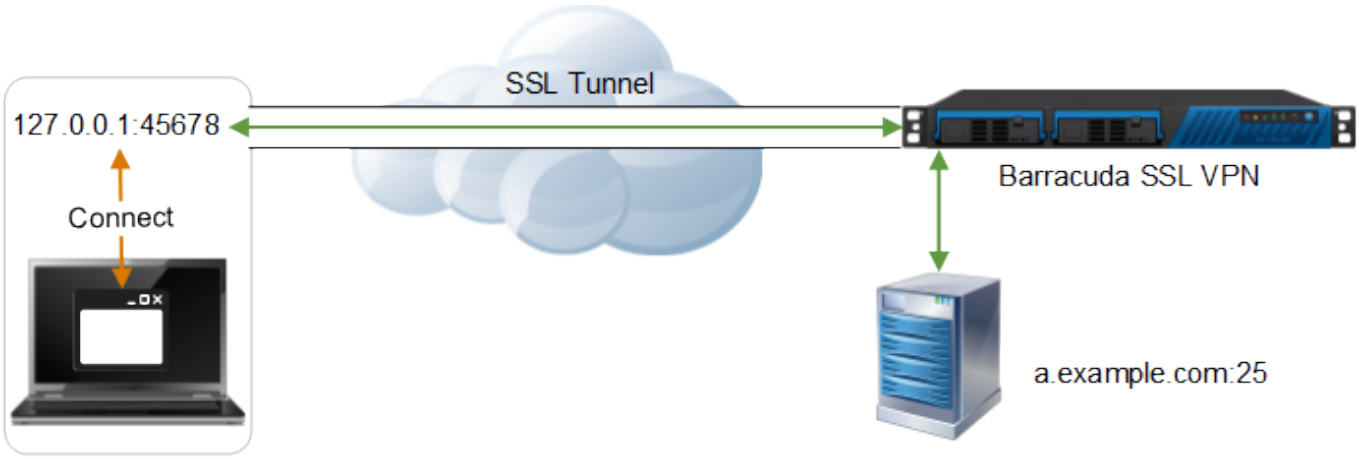
SSL Tunnels

https://campus.barracuda.com/doc/39813241/

SSL Tunnels are used to encrypt data for client/server applications which normally do not use encryption. The tunnel is created by the SSL VPN Agent and terminated at the Barracuda SSL VPN (local tunnel). The remote user does not connect directly to the remote resource as in a VPN, but to a Port on the 127.0.0.1 interface. The SSL VPN Agent accepts the local connection and forwards the traffic through the SSL tunnel. The Barracuda SSL VPN forwards the traffic to the destination IP and Port defined in the SSL tunnel configuration. The traffic from the Barracuda SSL VPN to the destination IP in the network is not encrypted anymore.



SSL tunnels can be configured to only allow local connections or to allow connections directly to the remote network. It is also possible to define the source IP address of the SSL tunnel, so that clients in the same remote network can share a SSL tunnel. The tunnel is terminated when the session is closed or timed out.

Next steps

To create a SSL Tunnel complete the following instructions: How to Create an SSL Tunnel.

Figures

1. SSLTunnel.png