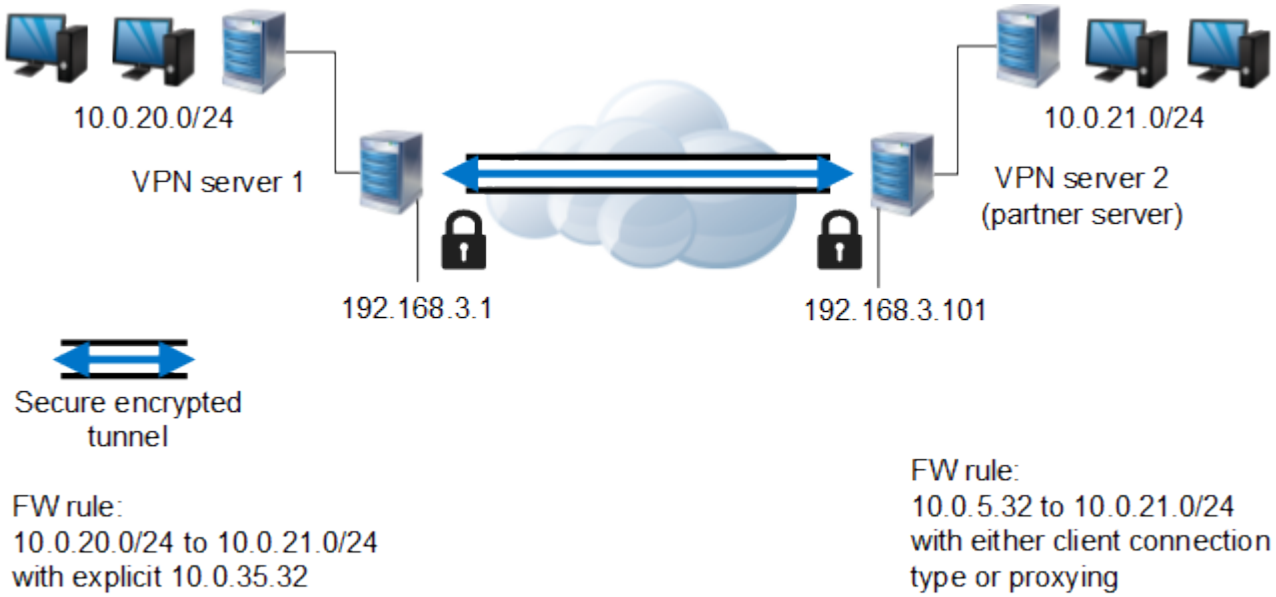
Stealth VPN Tunnel Setup

https://campus.barracuda.com/doc/41116246/

In a stealth or half-side transparent tunnel, only a local network is granted access to a partner network; the partner network cannot access the local network. The internal IP structure of the local network is hidden from the partner network. In such a setup, it is crucial that you correctly configure the firewall rules that handle traffic in the VPN tunnel.

The following figure illustrates a stealth VPN tunnel setup where the network for VPN server 1 is hidden from the network for VPN server 2. In the example setup, only one IP address (*10.0.35.32*) is explicitly directed into the tunnel. This article provides example settings for creating a site-to-site TINA VPN tunnel for this environment.



VPN Server 1 Settings

Tab	Setting	Value	Comment
Basic	**Transport**	UDP&TCP (or whatever is needed)	-
	Encryption	AES (or whatever is needed)	May be unencrypted for intranet connections only aiming at routing assistance.

Advanced	**Tunnel Timeout**	• For intranet: 10 • For Internet-like connections: 30	-
Local Networks	**Call Direction**	Active or Passive	Converse to the partner's configuration.
Local	**IP Address or Interface Used for Tunnel Address**	10.0.35.32	Only this IP address is directed into the tunnel.
Remote Networks	**Remote Network**	10.0.21.0/24	-
Remote	**Remote Peer IP Addresses**	192.168.3.101	-

Firewall Rule for VPN server 1

When creating a Pass firewall rule for VPN server 1 to redirect traffic into the tunnel, explicitly specify the **Connection Type** as **Explicit: *10.0.35.32***.

VPN Server 2 Settings

Tab	Setting	Value	Comment
Basic	**Encryption**	Same value as on the local side	-
Advanced	**Tunnel Timeout**	• For intranet: 10 • For Internet-like connections: 30	-
Local Networks	**Call Direction**	Active or Passive	Converse to the partner's configuration.
	Network Address	10.0.21.0/24	-
Local	**IP Address or Interface Used for Tunnel Address**	Dynamic (via routing)	Only one IP address is assumed on the outside interface.
Remote Networks	**Remote Network**	10.0.35.32	-
Remote	**Remote Peer IP Addresses**	192.168.3.1	-

Firewall Rule for VPN Server 2

Because the tunnel terminates at a point located previous to the firewall engine, create a Pass firewall rule that allows the 10.0.35.32 IP address into the local network.

Further Remarks

The proxy address may be chosen without restrictions. Half-side transparent tunneling is suitable as an alternative to personal VPN access. The local network IP address is then derived from the personal VPN networks. Stealth mode tunnels may as well be operated without personal access configuration. Because the tunnels are not fully transparent, there is no need to set up network routes, proxy ARPs, etc.

Optionally, a local IP address (e.g. 10.0.21.156) may be defined as the tunnel endpoint. In this case, the VPN server must request traffic being directed to this address. You can either introduce this IP address as a personal access network or create a standalone proxy ARP for it.

Figures

1. stealth_tunnel.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.