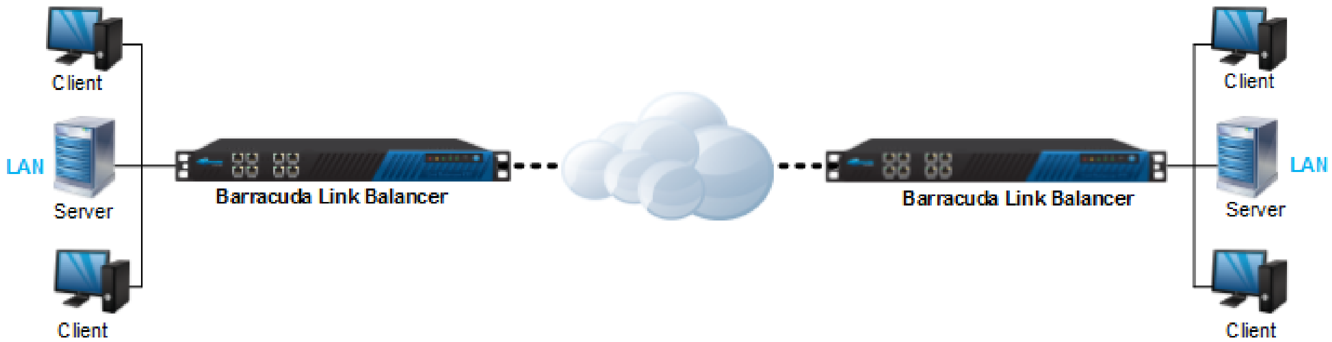
Site-to-Site VPN Overview

https://campus.barracuda.com/doc/3692/

The Barracuda Link Balancer can act as an endpoint in a site-to-site VPN tunnel. The following sections describe the VPN capabilities and explain the configuration steps.

Site-to-Site VPN Tunnels

You can create a site-to-site VPN tunnel between two Barracuda Link Balancers or between a Barracuda Link Balancer and another device that supports IPsec. Networks connected via a tunnel will communicate as if they are on the same network, even though they are separated by the Internet.



The **Services > VPN** page displays all tunnels and their status. You can add, disable, edit or delete a tunnel from this page.

Creating VPN Tunnels

When creating a tunnel, make sure that the relevant tunnel parameters on both ends are in sync. If needed, record the settings on the other endpoint and compare them to the local endpoint. If the settings of the tunnel endpoints do not match, you may fail to establish a tunnel successfully. Many tunnel security parameters are advanced settings and have been given reasonable defaults. If both endpoints are Barracuda Link Balancers, use the defaults provided unless you have a specific reason for changing these settings.
For testing purposes, you may choose to start with a shared secret on both endpoints, but using SSL certificates is recommended in a production environment. On the **ADVANCED > Certificates** page, upload the local and remote certificates.

Creating a VPN in a NAT'd Environment

If either the Barracuda Link Balancer or the remote endpoint is behind a device such as a firewall which is NAT'ing traffic, you must enable the NAT-Traversal (NAT-T) option when creating the VPN tunnel. NAT-T is required to make IPsec and NAT work together. If the option is not enabled, packets will be dropped on the receiving end. If the remote endpoint for the VPN is behind a NAT'ing device, enter the IP address for the remote endpoint in the Remote NAT-T IP field. In this case, the Primary Remote Gateway IP address is the NAT'ing device. If only the local Barracuda Link Balancer is behind a NAT'ing device, the Primary Remote Gateway IP address is the remote endpoint and the Remote NAT-T IP field should be left blank.
In order for NAT-T to work, open UDP port 4500 on the firewall.The VPN log (on the **LOGS > VPN Log** page) will display which VPN endpoint is NAT'd.

Failover and Failback

When configuring a tunnel you can specify a primary and a backup link. If the primary link fails, the tunnel will be re-established using the backup link. When the primary link is restored, the tunnel will automatically fail back to using the primary link.

To configure VPN failover:

- In **New/Edit VPN Tunnel**, select a working secondary WAN link in the **Backup Local Link** field. This WAN link must not be identical with the **Primary Local Link**.
- Enter a hostname or external IP address of a secondary WAN link on the remote VPN gateway into the **Backup Remote Gateway** field.

> Note that just as the backup local link, the backup remote link must be an independent second Internet connection on the remote gateway. VPN failover will not work if either endpoint uses the same WAN link for primary and backup.

VPN Tunnel as Failover Link for a Broken Site-to-Site WAN Link

A VPN tunnel can be configured as a failover link replacing a temporarily broken WAN link. To make use of this feature, you must have Barracuda Link Balancer with disabled firewall in each network which are connected through the failover tunnel. Both Barracuda Link Balancers need to be configured to act as failover WAN endpoints. To activate the WAN failover, you must select the respective option in the VPN Status configuration item of a VPN connection on each Barracuda Link Balancer in order to enable the failover tunnel for WAN1 (or, respectively, one of the other interfaces). If the WAN link fails, the VPN connection will then be activated. When the WAN link is restored, the

VPN connection will no longer be used.

External firewalls must be configured properly to allow the VPN failover tunnel.

To make use this feature, please perform the following configuration tasks:

- Add an IP/APP rule to send all site-to-site traffic via the WAN link and use the VPN as failover for this traffic.
- Add an IP/APP rule to send all remaining traffic via any WAN link but do not expect this traffic to failover to the VPN.

IP/APP rules should be configured as described below to allow this to happen:

- IP/APP rule #1: Src 192.168.17.0/24, App *, Dst 172.16.1.0/24, LB No, use MPLS, no Backup, no NAT
- IP/APP rule #2: Src 192.168.17.0/24, App Ping, Dst 172.16.1.0/24, LB No, use MPLS, no Backup, no NAT
- IP/APP rule #3: Src 0.0.0.0/0, App *, Dst 0.0.0.0/0, LB No, use DSL, no Backup, NAT yes
- IP/APP rule #4: Src 0.0.0.0/0, App Ping, Dst 0.0.0.0/0, LB No, use DSL, no Backup, NAT yes

Troubleshooting a VPN Tunnel

If the Barracuda Link Balancer is unable to establish a tunnel then you may discover the problem by doing the following:

- On the **LOGS > VPN Log** page, check the **VPN Log** to see if anything has been logged about the cause of failure.
- On the **SERVICES > VPN** page, click **Edit** next to the tunnel entry to view the tunnel parameters. Check that the security and authentication values match the tunnel parameters of the other end of the tunnel.
- Check the link status using the **BASIC > Status** page.

External firewalls must be configured properly to allow the VPN failover tunnel.

- Use the tools on the **Advanced > Troubleshooting** page to ping the remote gateway and perform other diagnostics on the network connection. (For more information, see Troubleshooting.)

Figures