How to Create a Site-to-Site VPN Tunnel

https://campus.barracuda.com/doc/39818629/

You can create a VPN tunnel between two Barracuda Link Balancers or between a Barracuda Link Balancer and another device that supports IPsec. When creating the tunnel or modifying its parameters, ensure that the settings are correct and in sync on both ends. If possible, display the configuration settings of the remote endpoint in another browser window so that you can ensure that you enter them correctly here.

Related Article

- Site-to-Site VPN Overview

Step 1. Create the VPN Tunnel

To configure the VPN tunnel settings on the Barracuda Link Balancer,

1. Log into the Barracuda Link Balancer web interface.
2. Go to the **SERVICES > VPN** page.
3. To create a new VPN tunnel, click **ADD New VPN Tunnel**.
4. Enter a descriptive **Name** for the tunnel. (The tunnel name does not have to match the name of the endpoint.)
5. From the **Primary Local Link** list, select the link that this tunnel will use.
6. From the **Backup Local Link** list, select a backup link. If the primary link fails, the tunnel will be reestablished using the backup link on both ends. Thus, you must specify a backup link on both ends of the tunnel.
7. In the **Primary Remote Gateway** field, enter the hostname or IP address for the remote gateway.
8. In the **Backup Remote Gateway** field, enter the hostname or IP address for the backup remote gateway. If there is a failover, this remote gateway will be used.
9. If either this Barracuda Link Balancer or the remote endpoint is behind a device such as a firewall which is NATting traffic, set **Enable NAT-Traversal** to *Yes* and enter the IP address of the remote endpoint in the **Remote NAT-T IP** field.
10. In the **Local Network** section, select the local subnets that can communicate using this VPN. This list includes the subnet local to the Barracuda Link Balancer and the static routes listed on

the **Advanced > Advanced Networking** page.

11. In the **Remote Network** field, enter the network addresses and subnet masks of any remote subnets you want accessible to local clients.
    These addresses must exactly match the addresses specified on the remote endpoint. If the remote endpoint is a Barracuda Link Balancer, the local subnets must be listed on this same page in the the remote endpoint Local Network list. You do not need to include all possible remote subnets in this list.
12. Set **Enable VPN** to *Yes* to open the tunnel. (*No* closes the tunnel.)

Step 2. Specify the Security Policies

For testing purposes, start with a shared secret on both endpoints. In a production environment, you should use certificates.

1. In the **Security Policies** section, select the **IPsec Keying Mode** used for encrypting data:
   If you choose **Shared Secret**, enter a password in the **Shared Secret** field. Be sure to enter this same password on the device on the other end of the tunnel.
   If you choose **Trusted Certificates** to use SSL certificates for authentication, proceed as follows:
   1. If you have not already uploaded the local and remote certificates to the Barracuda Link Balancer using the **Advanced > VPN Certificates** page:
      1. Save your changes here first.
      2. Navigate to the **Advanced > VPN Certificates** page.
      3. Upload local and remote certificates.
      4. Navigate back to this page.
   2. Uploaded signed certificates appear in the **Local Certificate** list. Select the correct one.
      1. Saved CA certificates appear in the **Remote Certificate** list. Select the uploaded certificate for the remote endpoint.
      2. Enter the distinguished name (e.g. *my.domain.com*) for the remote endpoint.

Step 3. Verify the IPsec Key Exchange Policy

IPsec Key Exchange is a protocol that allows devices to exchange information required for secure communication. If the endpoint is also a Barracuda Link Balancer, then unless you have a specific reason for changing these settings, use the defaults provided. Otherwise, make sure the settings here are in sync with those on the other end of the tunnel. *Any* matches whatever the endpoint uses.

If you choose one of the other options, make sure the endpoint is using the same options. Do not choose *Any* on both endpoints for any of the values here because the negotiation required slows the creation of the tunnel.

Specify the following settings for **Phase 1** and **Phase 2**:

1. In the **Encryption and Authentication** field, choose the encryption and authentication algorithms.
2. Select the Diffie-Hellman group to use from the **DH Group** list. Recommended: DH **Group 2** (1,024 bits of keying strength). DH **Group 5** uses 1536-bit encryption. DH **Group 14** (2,048 bits of keying strength) may be used for maximum security.
3. In the **Lifetime** fields, enter how long, in seconds, this key exchange policy exists before it needs to be renegotiated.

Perfect Forward Secrecy or PFS (IPsec Key Exchange Policy Phase 2 only) ensures that even if your current private key is compromised, all past and future communication cannot be decrypted with this private key. This setting must match the PFS setting on the remote endpoint.