How to Configure IP Tunneling

https://campus.barracuda.com/doc/48203185/

In most cases it is better to use Site-to-Site VPN tunnels instead of IP tunnels.

You can introduce simple point-to-point tunnels with generic routing (GRE) or plain IP in IP encapsulation. IP tunnels are established at the box level and do not support peer authentication or encryption.

Configure an IP tunnel

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. In the left menu, expand **Configuration Mode** and click **Switch to Advanced**.
3. In the left menu, click **IP Tunneling**.
4. Click **Lock**.
5. In the **Tunnel Configuration** table, click **+** to add an IP tunnel.
6. Enter a **Name**.
7. Click **OK**. The **Tunnel Configuration** window opens.
8. Enter the IP tunnel settings. For more information on the settings, see the IP Tunnel Settings section below.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

IP tunnel settings

Setting	Description
Encapsulation Mode	The encapsulation mode for the tunnel. You can select: • **GRE(47)** – Default mode. Generic routing encapsulation. • **IPinIP(4)** – Plain IP in IP encapsulation.
Tunnel TTL	(Optional) The TTL for encapsulated tunnel traffic. To use the standard behavior of TTL inherit and Nopmtudisc (no path MTU discovery), leave this field blank.
Set Multicast Flag	To set the multicast flag for the tunnel interface, select **yes**.
Source IP Type	The source IP type. You can select: • **ServerIP** – The source IP address is provided by a server. • **BoxIP** – A local source IP address is used. You must specify the local source IP address in the following **Source IP** field. Without a local source IP address, the system cannot use the tunnel for local traffic.

Source IP	If you selected **BoxIP** from the **Source IP Type** list, enter a local source IP address in this field. Specify a routable source IP address if the box itself will use the tunnel. The IP address is activated on the tunnel interface. In combination of with the **Source Mask** this is the network inside the IP tunnel.
Source Mask	The netmask for the source IP address. A non-zero mask specifies a local network.
Route Metric	If more than two routes exist for a target, enter a preference number for the route if one of the following scenarios also applies: • You do not want to use policy routing for tunneling. Thus, the respective tunnel routes go either into the main or default table (whenever the target network must be 0.0.0.0/0). • You want to use policy routing but plan to assign the routes to an existing table. It is not a good idea to introduce redundant routes to a target network with a direct route being the preferred path.
Remote End IP	The IP address of the remote tunnel end. Make sure that this IP address can be accessed from the local tunnel end that is specified in the following **Local End IP** field. If you are connecting over the Internet this would be the public IP address of the remote router/firewall.
Check Reachability	To check the reachability of the remote tunnel end from the local tunnel end, select **yes**. If this check fails, the tunnel is not introduced. If verification is active already, you will not be able to send configuration changes. To disable this check, select **no**. Disable this check when the remote tunnel end is only accessible via a VPN route.
Local End IP	The IP address of the local tunnel end. Make sure that you have already introduced this IP address in the network configuration of the system. If you are connecting over the Internet this would be the public IP address of the firewall.
Trust Level	Specifies the IP address type that is counted by the firewall for traffic on this interface. You can classify the interface as one of the following: • **Unclassified** • **Trusted** • **DMZ** • **Untrusted** • **Internal01** • **Internal02**
Target Networks	In this table, specify target networks that must be accessible through the tunnel. Use IP/mask notation. Add the target networks of routes that rely on the tunnel interface. Each specified target will rely on a corresponding direct route.
Advertise Route	To advertise this route via dynamic routing protocols when the OSPF/RIP/BGP service is used, select **yes**.
Use Policy Routing	To specify a routing table for tunnel routes from specific source networks, select **yes**. You can then configure the following policy routing settings: **Table Placement**, **Use Table**, and **Source Networks**.

Table Placement	If you are using policy routing, specify where the table should be placed. You can select **postmain** (default), **premain**, or **existing**. Select **existing** if you want to use an existing table and specify the table in the following **Use Table** field. The rule preference of this table will be inherited.
Use Table	If you selected **existing** from the **Table Placement** list, specify the policy routing table in this field. Do not specify the local, main, or default tables. For each source network defined, an appropriate rule pointing to this table (with the table's original preference) is also appended.
Source Networks	If the route from a network or single host must be looked up in the policy routing table specified in the **Table Placement** setting, add it to this table. By default, the policy routing table uses the same name as the one that you entered for the tunnel configuration entry. However, you may assign the routes to another table. Use IP/mask notation. For a single host, you must enter 32 as the netmask.