

Configuring Unimax HSUPA for establishing maXvpn connection

In this week's blog, we'll provide you with information on how to configure Unimax HSUPA router with maXvpn authentication details. The setup will allow Unimax router to establish a maXvpn session allowing monitoring of your devices on maXwan network. (For further information on maXwan and maXvpn network please refer to the IP WAN services page on maxon website http://www.maxon.com.au/menu_ipwanservices.php)

To apply maXvpn configurations, open the web interface of Unimax and under **Advanced** click on **VPN**. Select Mode as **VPN Client (L2TP/IPSec)** and apply the following settings:

| | | |
|-----------------------|-------------------|------------------------------------|
| Pre-Shared key (PSK): | ***** | <i>provided by Maxon Australia</i> |
| Authentication: | CHAP | |
| Username: | ***** | <i>provided by Maxon Australia</i> |
| Password: | ***** | <i>provided by Maxon Australia</i> |
| Server Address: | 202.130.219.30 | |
| NAT-T | Enabled | |
| IPSec Type | Tunnel | |
| Key Exchange | IKE | |
| Key Life | 14400 seconds | |
| ISAKMP SA: | 3DES MD5 MODP1024 | |
| IPSec Auth: | None | |
| PFS: | Disabled | |

Following is the screen capture of VPN page taken from the Web Interface of Unimax:

| | |
|----------------------|--|
| Mode : | <input type="text" value="VPN Client (L2TP/IPSec)"/> |
| | Gateway - Unimax Router acts as a VPN server. Client - Unimax Router connects to a remote VPN server. |
| Pre Shared Key : | <input type="text" value="....."/> |
| | Enter Pre Shared Key used by remote VPN server (client mode) or PSK to be used by clients connecting to Unimax Router in Gateway mode. |
| Authentication : | <input type="text" value="CHAP"/> |
| | Select PAP/CHAP/None Authentication method supported by remote VPN server. None - Follows the Authentication Supported by the VPN server. Select None when using Unimax Router as client connecting to another Unimax Router as VPN server. |
| User Name: | <input type="text" value="demovpn"/> |
| Password: | <input type="text" value="....."/> |
| Server Address : | <input type="text" value="202.130.219.30"/> |
| Server Subnet Mask : | <input type="text"/> |
| | Server IP address of the remote VPN server Unimax Router will connect to in client mode. |
| NAT-T : | <input type="text" value="Enable"/> |
| IPsec Type : | <input type="text" value="Tunnel"/> |
| Key Exchange : | <input type="text" value="IKE"/> |
| Key Life : | <input type="text" value="14400"/> Seconds |
| ISAKMP SA : | <input type="text" value="3DES"/> <input type="text" value="MD5"/> <input type="text" value="MODP1024"/> |
| IPsec Auth : | <input type="text" value="None"/> |
| IPsec SA : | <input type="text" value="3DES"/> <input type="text" value="HMAC MD5"/> |
| PFS : | <input type="text" value="Disable"/> |

The above settings can only be applied if your Unimax router is running on the latest firmware. For a copy of the latest firmware, please contact Maxon Technical support team on +61 2 8707 3000 or email support@maxon.com.au.