BEC TECHNOLOGIES

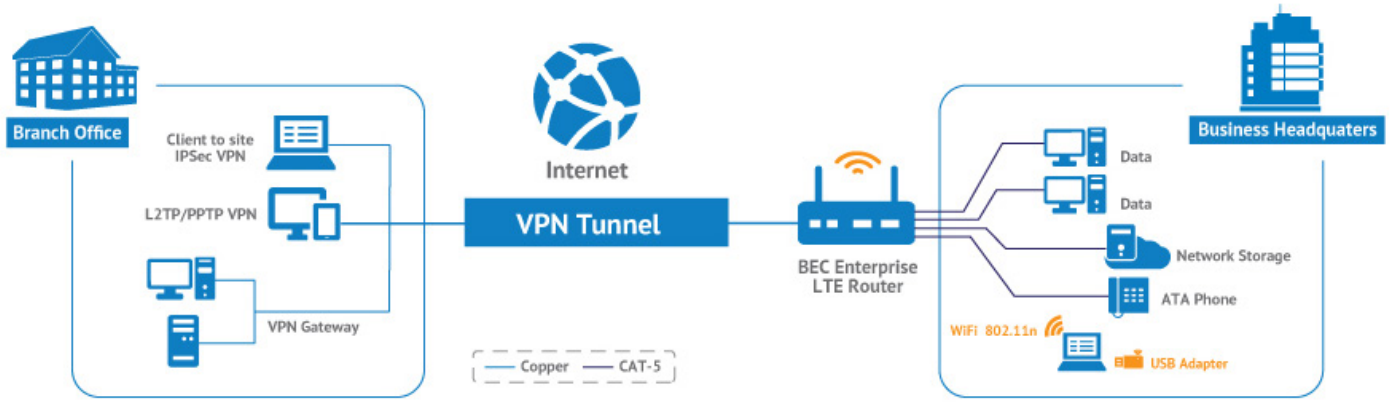
Technical Article

BEC VPN Solutions Guide for MX-200 & MX-1000

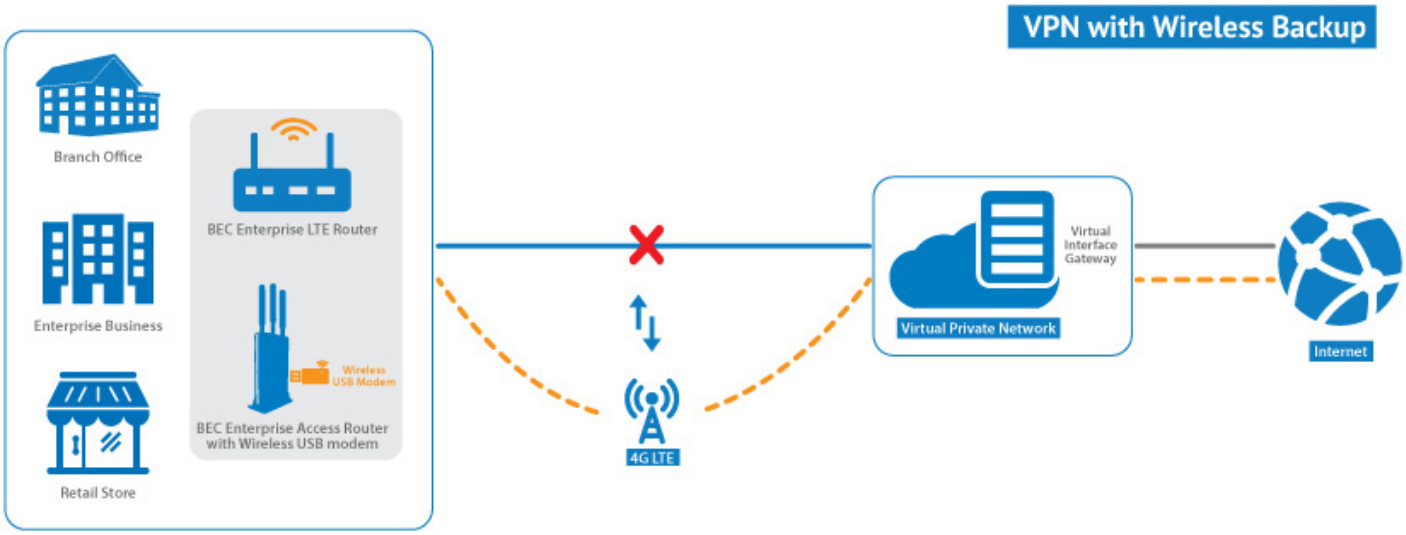
A Virtual Private Network (VPN) creates a secure "tunnel" across the Internet between you and your office, a VPN provider, or your home. Businesses use VPNs to connect remote datacenters, and individuals can use VPNs to get access to network resources when they're not physically on the same LAN, or as a method for securing and encrypting their communications when they're using an untrusted public network.

What is Virtual Private Network (VPN)?

A Virtual Private Network (VPN) creates a secure "tunnel" across the Internet between you and your office, a VPN provider, or your home. Businesses use VPNs to connect remote datacenters, and individuals can use VPNs to get access to network resources when they're not physically on the same LAN, or as a method for securing and encrypting their communications when they're using an untrusted public network.



BEC MX-200 and MX-1000 router comes with VPN features to enable remote access that will free you to have extra devices. Moreover, with BEC MX-200 and MX1000 router you will get full complete VPN solutions with 4G LTE failover & failback in secure and reliable network connectivity.

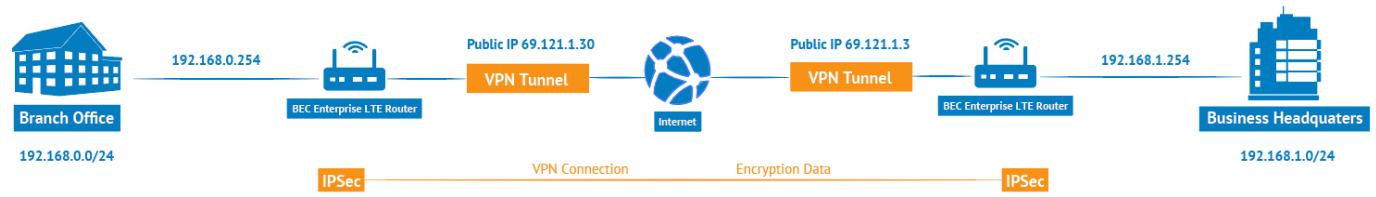


Why BEC's VPN Solutions?

BEC's one device solution will save your money. With BEC's integrated cloud management system software platform, ease the set up process of your VPN solution. (BEC MX-200 left & MX-1000 right)

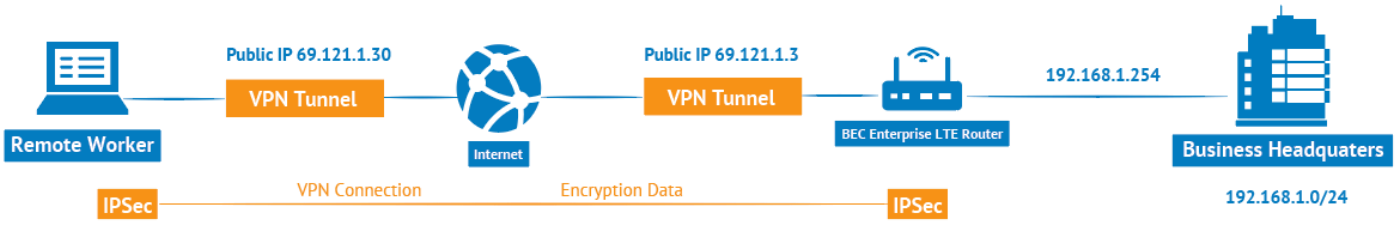
BEC VPN Features:

IPSec -- MX-200/1000 to MX-200/1000 (network to network)



IPSec VPN-LAN to LAN

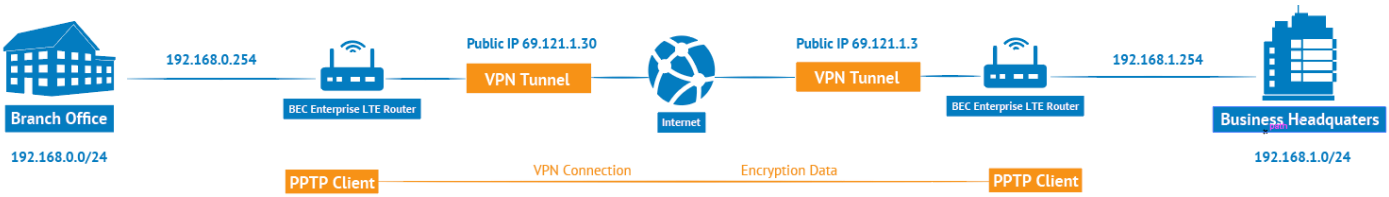
IPSec -- Remote Employee MX-200/1000 Connection



IPSec VPN-Host to LAN

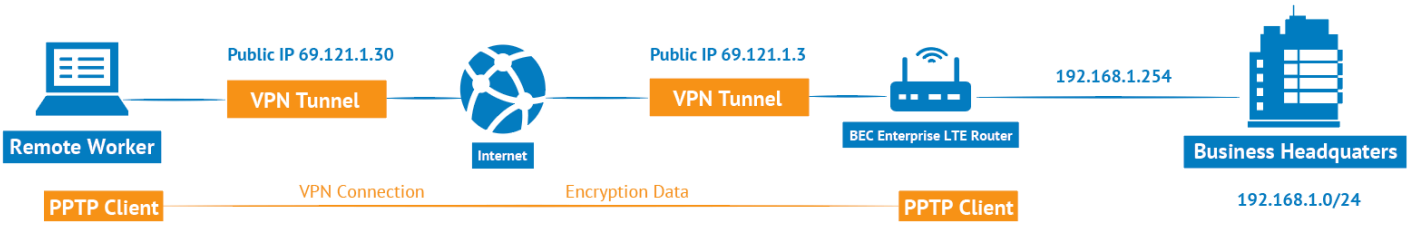
PPTP -- Network to Network Connection

The Point-to-Point Tunneling Protocol (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network.



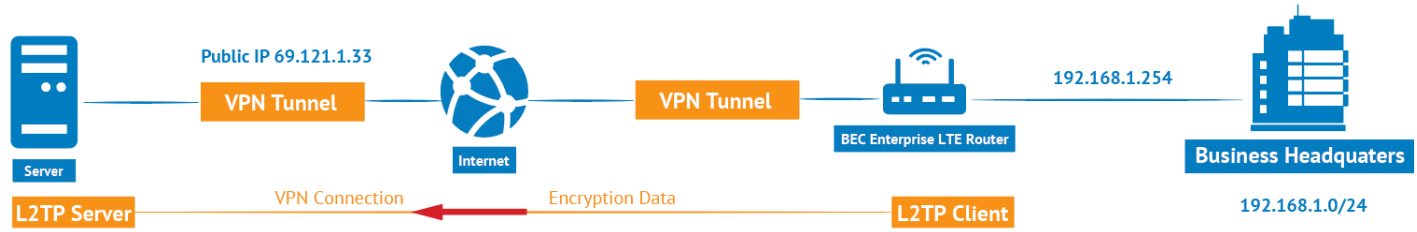
PPTP VPN-LAN to LAN

PPTP -- Network to Network Connection



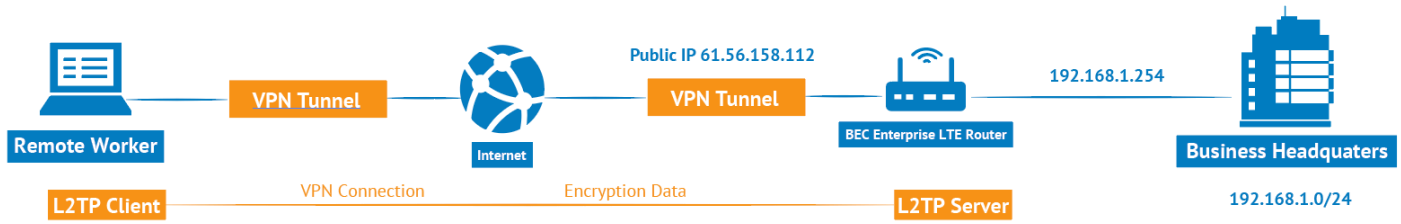
PPTP VPN-Remote Access (Dial-in)

L2TP VPN – MX-200/MX-1000 Dial-out to a Server



L2TP VPN-Remote Access (Dial-out)

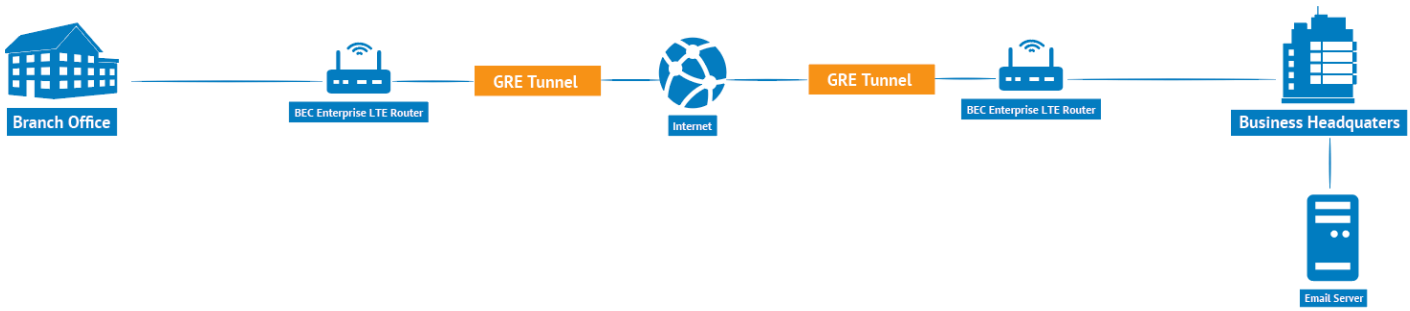
L2TP VPN – Remote Employee Dial-in to MX-200/MX-1000



L2TP VPN-Remote Access (Dial-in)

GRE Tunnel (Up to 8 tunnels)

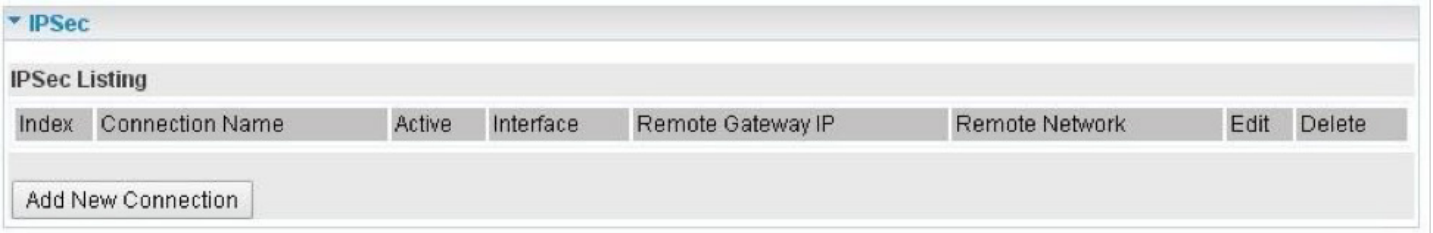
Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocol packets inside virtual point-to-point links over an IP network.



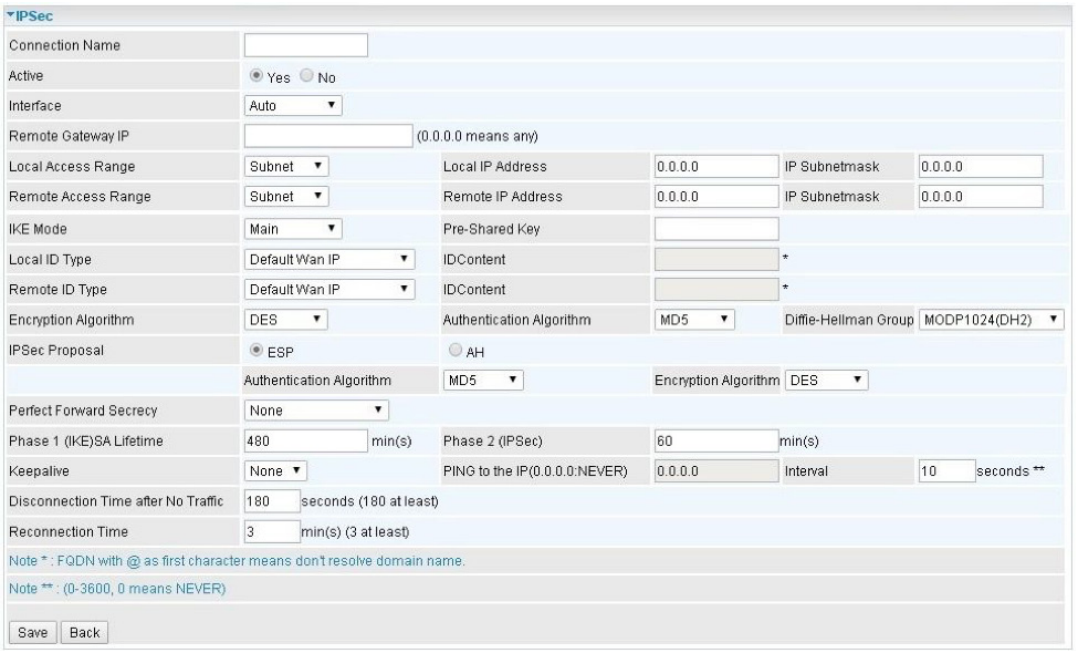
Configuration:

Configuring IPsec VPN

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. A total of 8 IPsec tunnels can be added in MX-200 and MX-1000.



1.Add New Connection to create an IPsec connection.



2.**Connection Name:** Assign a name for this connection. Example: connection to office.
3.**Active: Yes,** to activate the connection.
4.**Interface:** Select the set used interface for the IPsec connection, when you select 3G/4G-LTE interface, the IPsec tunnel would via this interface to connect to the remote peer.
5.**Remote Gateway IP:** The WAN IP address of the remote VPN gateway that is to be connected, establishing a VPN tunnel.
6.**Local Access Range:** Set the IP address or subnet of the local network.

A. **Single IP:** The IP address of the local host, for establishing an IPsec connection between a security gateway and a host (network-to-host).
B. **Subnet:** The subnet of the local network, for establishing an IPsec tunnel between a pair of security gateways (network-to-network)

7.**Remote Access Range:** Set the IP address or subnet of the remote network.

A. **Single IP:** The IP address of the local host, for establishing an IPsec connection between a security gateway and a host (network-to-host). If the remote peer is a host, select Single Address.
B. **Subnet:** The subnet of the local network, for establishing an IPsec tunnel between a pair of security gateways (network-to-network), if the remote peer is a network, select Subnet.

8.**IKE Mode:** IKE, Internet Key Exchange, is the mechanism to negotiate and exchange parameters and keys between IPsec peers to establish security associations (SA). Select Main or Aggressive mode.
9.**Pre-Shared Key:** This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPsec) that require a key. Before any IPsec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).
10.**Local ID Type and Remote ID Type:** When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs.
11.**IDContent:** Enter IDContent the name you want to identify when the Local and Remote Type are Domain Name; Enter IDContent IP address you want to identify when the Local and Remote Type are IP addresses (IPv4 and IPv6 supported).
12.**Encryption Algorithm:** Select the encryption algorithm from the drop-down menu. There are several options: DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

A. **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
B. **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
C. **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

13.**Authentication Algorithm:** Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

A.**MD5:** A one-way hashing algorithm that produces a 128–bit hash.
B.**SHA1:** A one-way hashing algorithm that produces a 160–bit hash.

14.**Diffle-Hellman Group:** It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.
15.**IPSec Proposal:** Select the IPSec security method. There are two methods of verifying the authentication information, AH (Authentication Header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and the data origin be authenticated but using AH data origin will only be authenticated but not encrypted.
16.**Authentication Algorithm:** Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash

Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

A. **MD5:** A one-way hashing algorithm that produces a 128–bit hash.
B. **SHA1:** A one-way hashing algorithm that produces a 160–bit hash.

17.**Encryption Algorithm:** Select the encryption algorithm from the drop-down menu. There are several options: DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

A. **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
B. **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
C. **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

18.**Perfect Forward Secrecy:** It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

19.**SA Lifetime:** Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, and IKE SA is used by IKE.

A. **Phase 1 (IKE):** To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 480 minutes.
B. **Phase 2 (IPSec):** To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes. A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

20.**Keep Alive:**

A. **None:** Disable. The system will not detect remote IPSec peer is still alive or lost. The remote peer will get disconnected after the interval, in seconds, is up.
B. **PING:** This mode will detect the remote IPSec peer has lost or not by pinging specify IP address.
C. **DPD:** Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be detected lively when the connection between the router and a remote IPSec peer has lost. Please be noted, it must be enabled on the both sites.

21.**PING to the IP:** It is being able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Reestablish of this connection is required. Default setting is 0.0.0.0 which disables the function.

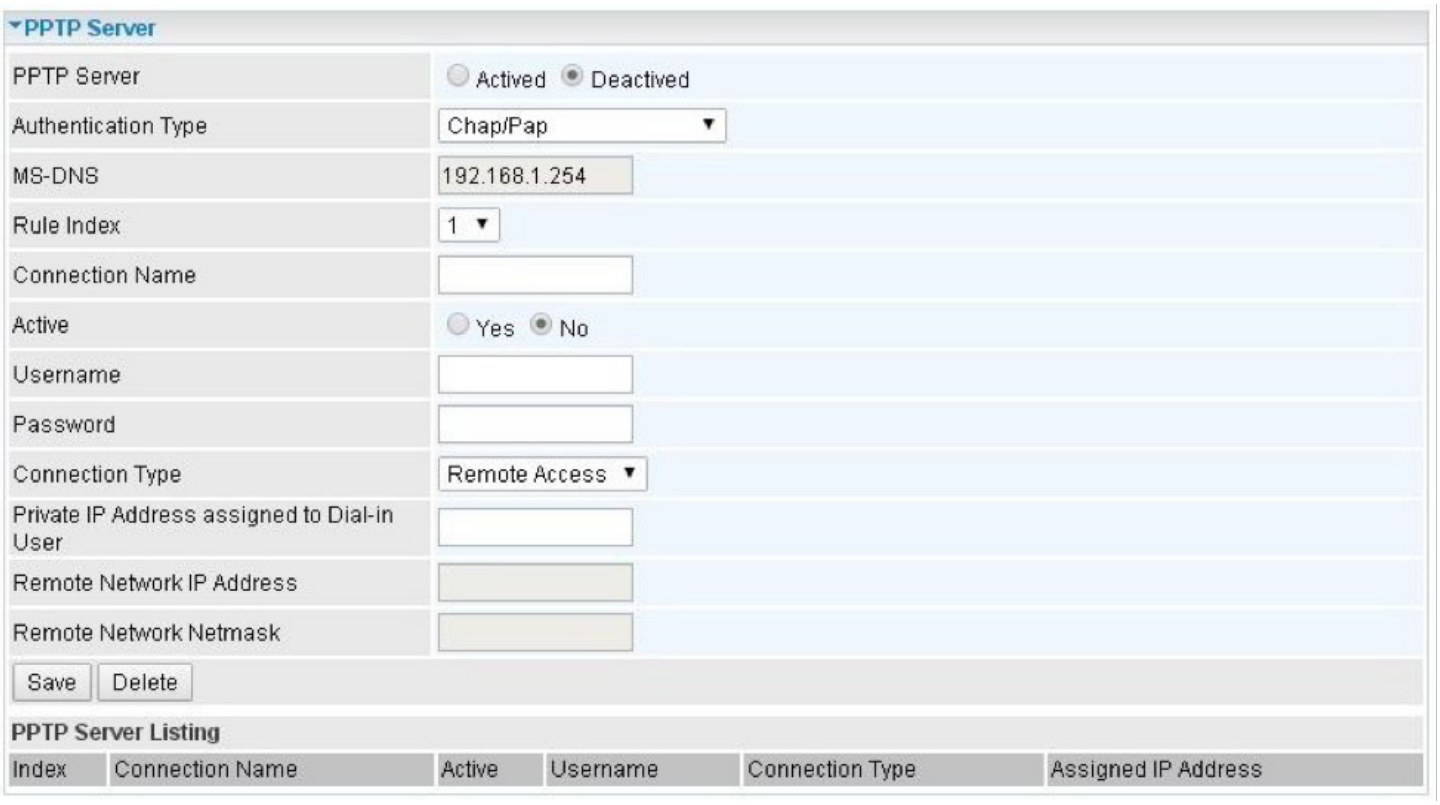
22.**Interval:** This sets the time interval between Pings to the IP function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second, 0 second disables the function.

23.**Disconnection Time after No Traffic:** It is the NO Response time clock. When no traffic stage time is beyond the Disconnection time set, Router will automatically halt the tunnel connection and re-establish it base on the Reconnection Time set. 180 seconds is minimum time interval for this function.

24.**Reconnection Time:** It is the reconnecting time interval after NO TRAFFIC is initiated. 3 minutes is minimum time interval for this function.

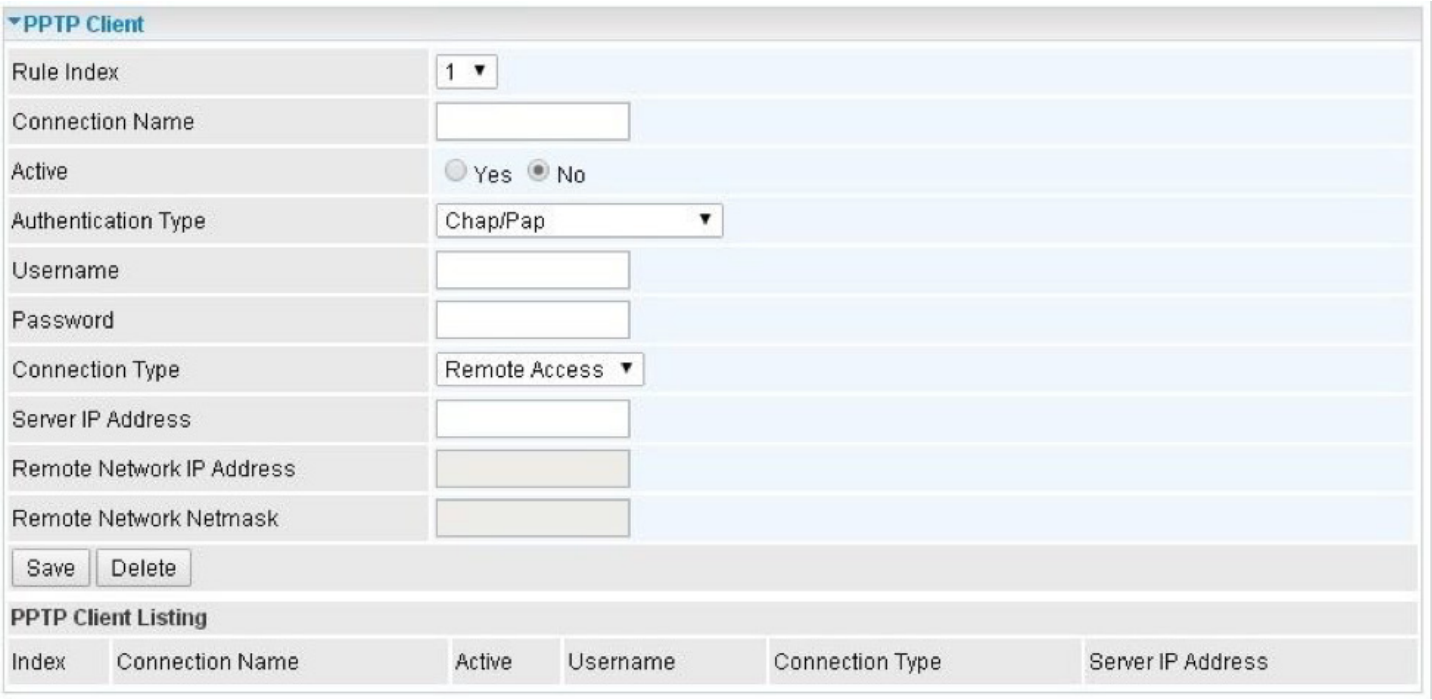
25.**Click Save to apply the settings.**

PPTP Server Configuration



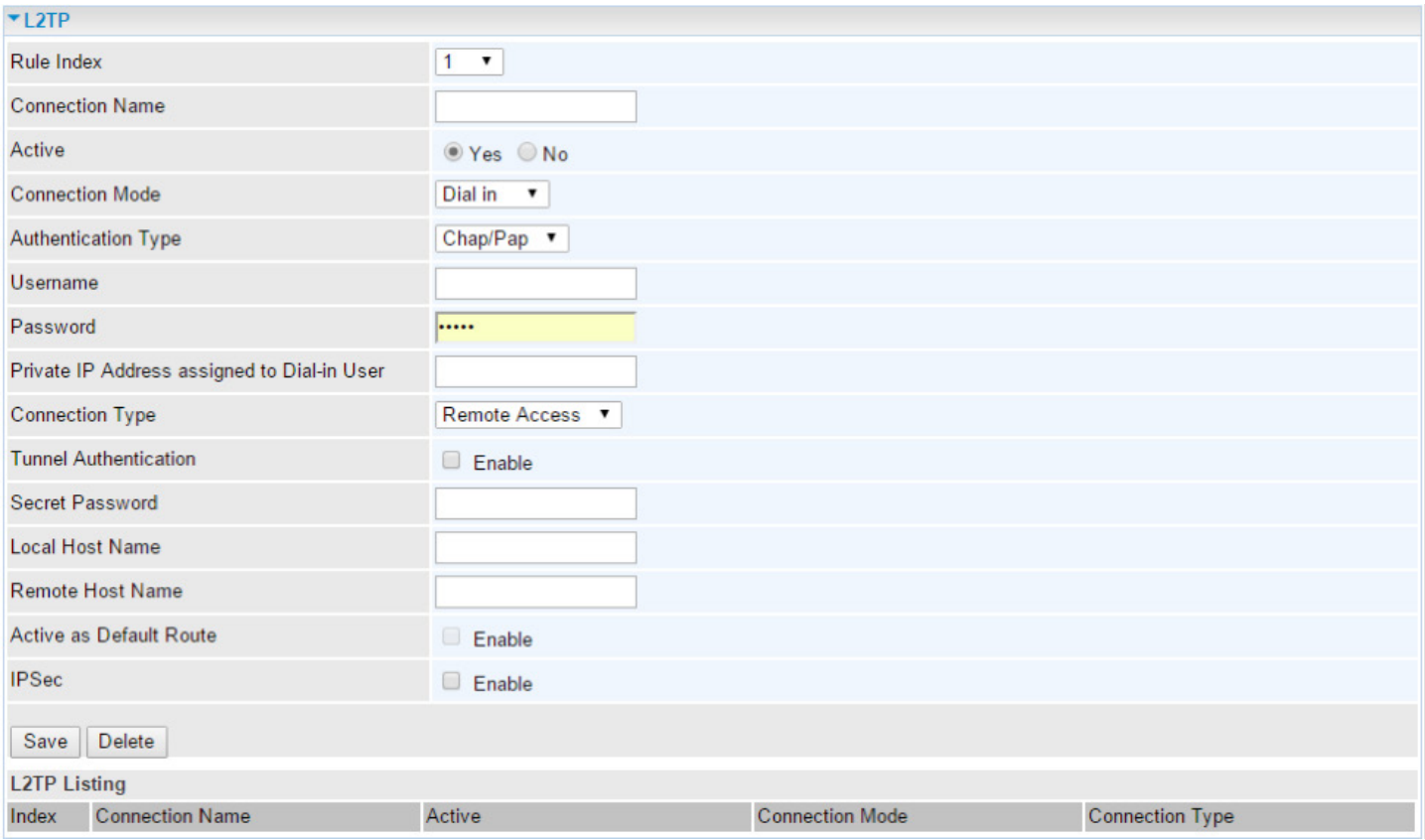
1.**PPTP Server:** Select Activate to enable PPTP Server. Deactivate to disable the PPTP Server.
2.**Authentication Type:** The authentication type, Pap or Chap, and MPPE 128bit Encryption. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.
3.**MS-DNS:** Assign a DNS server or use router default IP address to be the MS-DNS server IP address.
4.**Rule Index:** The numeric rule indicator for PPTP server. The maximum entry is up to 4.
5.**Connection Name:** User-defined name for the PPTP connection.
6.**Active:** Yes, to activate the account. PPTP server is waiting for the client to connect to this account.
7.**Username:** Please input the username for this account.
8.**Password:** Please input the password for this account.
9.**Connection Type:** Select Remote Access for single user, Select LAN to LAN for remote gateway.
10.**Private IP Address Assigned to Dial-in User:** Specify the private IP address to be assigned to dial-in clients, and the IP should be in the same subnet as local LAN, but not occupied.
11.**Remote Network IP Address:** Please input the subnet IP for remote network.
12.**Remote Network Netmask:** Please input the Netmask for remote network.
13.Click **Save** to apply your settings.

PPTP Client Configuration



1.**Rule Index:** The numeric rule indicator for PPTP client. The maximum entry is up to 4.
2.**Connection Name:** User-defined name for the PPTP connection.
3.**Active:** Yes, to activate the account. PPTP server is waiting for the client to connect to this account.
4.**Authentication Type:** The authentication type, Pap or Chap, and MPPE 128bit Encryption. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.
5.**Username:** Please input the username for this account.
6.**Password:** Please input the password for this account.
7.**Connection Type:** Select Remote Access for single user, Select LAN to LAN for remote gateway.
8.**Server Address:** Enter the WAN IP address of the PPTP server.
9.**Remote Network IP Address:** Please input the subnet IP for remote network.
10.**Remote Network Netmask:** Please input the Netmask for remote network.
11.Click **Save** to apply the settings.

L2TP Configuration



1.**Rule Index:** The numeric rule indicator for L2TP. The maximum entry is up to 8.
2.**Connection Name:** User-defined name for the connection.
3.Active: To enable or disable the tunnel.
4.**Connection Mode:**

4.1 Select **Dial In** to operate as a L2TP server.

a.**Authentication Type:** Default is Chap/Pap(CHAP, Challenge Handshake Authentication Protocol. PAP, Password Authentication Protocol.) If you want the router to determine the authentication type to use, or else manually specify PAP if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server).

b.**Username:** Please input the username for this account.

c.**Password:** Please input the password for this account.

d.**Private IP Address Assigned to Dial-in User:** The private IP to be assigned to dial-in user by L2TP server. The IP should be in the same subnet as local LAN, and should not be occupied.

4.2**Connection Mode:** Choose **Dial Out** if you want your router to operate as a client (connecting to a remote L2TP Server, e.g., your office server).

a.**Server IP Address:** Enter the IP address of your VPN Server.

b.**Authentication Type:** Default is Chap/Pap(CHAP, Challenge Handshake Authentication Protocol. PAP, Password Authentication Protocol.) If you want the router to determine the authentication type to use, or else manually specify PAP if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server).

c.**Username:** Please input the username for this account.

d.**Password:** Please input the password for this account.

5.**Connection Type:**

A. **Remote Access:** From a single user.

B. **LAN to LAN:** Enter the peer network information, such as network address and Netmask.

6.**Tunnel Authentication:** This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

7.**Secret Password:** The secure password length should be 16 characters which may include numbers and characters.

8.**Local Host Name:** Enter hostname of Local VPN device that is connected / establishes a VPN tunnel.

9.**Remote Host Name:** Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

10.**Active as Default Route:** Enabled to let the tunnel to be the default route for traffic, under this circumstance, all packets will be forwarded to this tunnel and routed to the next hop.

11.**IPsec Enable:**

A. **IPSec:** Enable to activate L2TP over IPSec. When enabled, the L2TP tunnel authentication will be based on the IPSec authentication system.

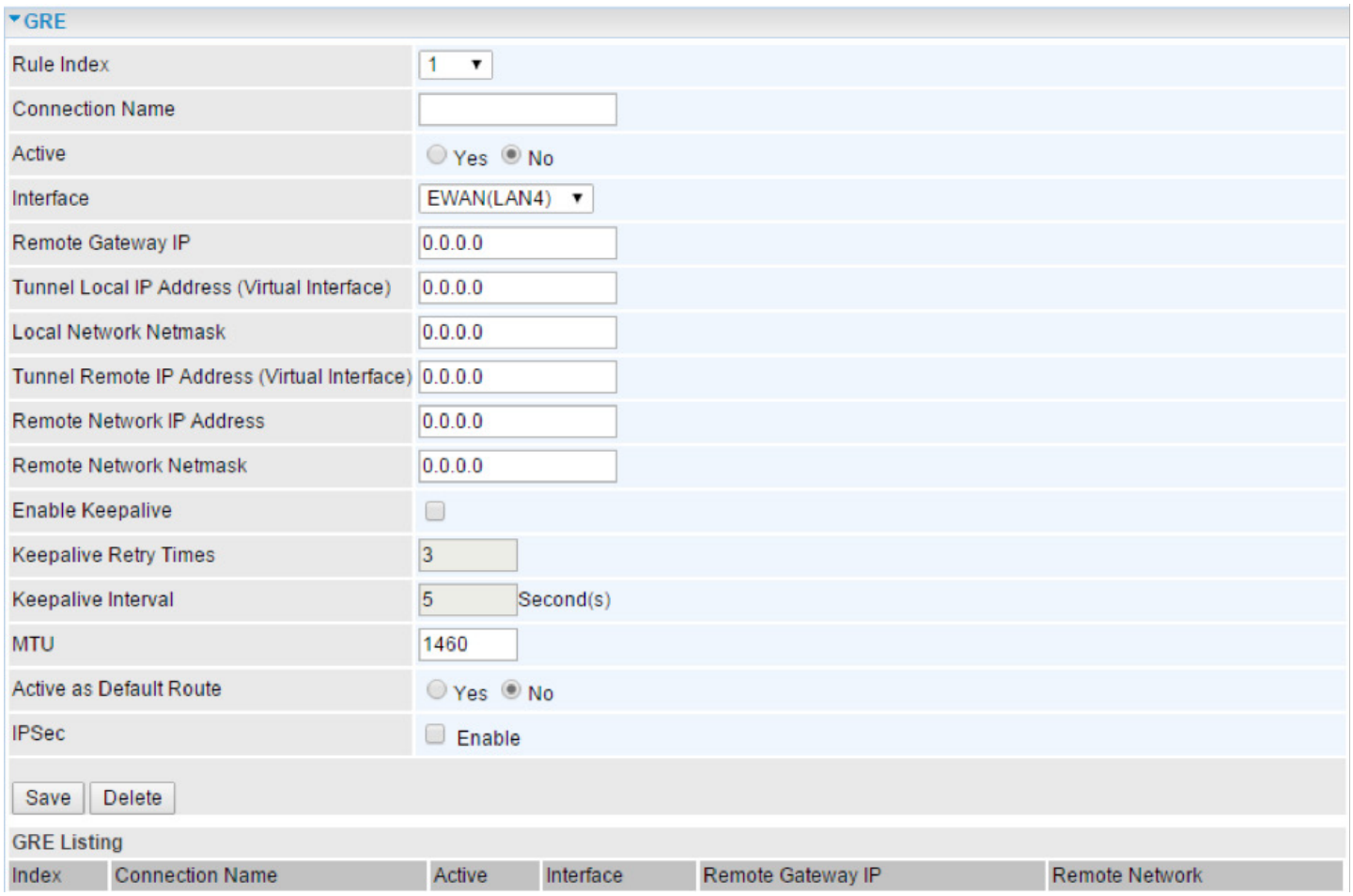
B. **IKE Mode:** IKE, Internet Key Exchange, is the mechanism to negotiate and exchange parameters and keys between IPSec peers to establish security associations(SA). Select Main or Aggressive mode.

C. **IKE(IPSec) Local ID/Remote ID:** When the mode of IPSec phase 1 is aggressive, Local and Remote peers can be identified by other IDs.

D. **IKE(IPSec) Pre-Shared Key:** This is for the Internet Key Exchange (IKE) protocol, a string from 1 to 32 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

12.Click **Save** to apply the settings

GRE Tunnel Configuration



1.**Rule Index:** The numeric rule indicator for GRE. The maximum entry is up to 8.
2.**Connection Name:** User-defined name for the connection.
3.**Active:** Select Yes to activate the GRE tunnel.
4.**Interface:** Select the exact WAN interface configured for the tunnel as the local IP.
5.**Remote Gateway:** The remote GRE gateway IP.
6.**Tunnel Local IP:** Please set the source IP for the local tunnel.
7.**Tunnel Local Netmask:** Please set the Netmask for the local tunnel.
8.**Tunnel Remote IP Address:** Set the peer IP address of the tunnel.
9.**Remote Network IP Address:** Please set the subnet IP for remote network.
10.**Remote Network Netmask:** Please set the Netmask for remote network.
11.**Enable Keep-alive:** Normally, the tunnel interface is always up. Enable keep-alive to determine when the tunnel interface is to be closed. The local router sends keep-alive packets to the peer router, if keep-alive response is not received from peer router within the allowed time ('retry time' multiply 'interval', based on default settings, the time interval can be 30 seconds), the local router will shut up its tunnel interface.
12.**Keep-alive Retry Times:** Set the keep-alive retry times, default is 3.
13.**Keep-alive Interval:** Set the keep-alive Interval, unit in seconds. Default is 5 seconds.
14.**MTU:** Maximum Transmission Unit.
15.**Active as Default Route:** Select if to set the GRE tunnel as the default route.
16.**IPSec:** Enable to activate GRE over IPSec. When enabled, the GRE tunnel authentication will be based on the IPSec authentication system.

17.**IKE(IPSec) Local ID/Remote ID:** When the mode of IPSec phase 1 is aggressive, Local and Remote peers can be identified by other IDs.
18.**IKE(IPSec) Pre-Shared Key:** This is for the Internet Key Exchange (IKE) protocol, a string from 1 to 32 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).
19.Click **Save** to apply the settings.