Manual:Interface/L2TP

From MikroTik Wiki
< Manual:Interface

Applies to RouterOS: v6+

Contents

Summary

Standards: `RFC 2661`

L2TP is a secure tunnel protocol for transporting IP traffic using PPP. L2TP encapsulates PPP in virtual lines that run over IP, Frame Relay and other protocols (that are not currently supported by MikroTik RouterOS). L2TP incorporates PPP and MPPE (Microsoft Point to Point Encryption) to make encrypted links. The purpose of this protocol is to allow the Layer 2 and PPP endpoints to reside on different devices interconnected by a packet-switched network. With L2TP, a user has a Layer 2 connection to an access concentrator - LAC (e.g., modem bank, ADSL DSLAM, etc.), and the concentrator then tunnels individual PPP frames to the Network Access Server - NAS. This allows the actual processing of PPP packets to be separated from the termination of the Layer 2 circuit. From the user's perspective, there is no functional difference between having the L2 circuit terminate in a NAS directly or using L2TP.

It may also be useful to use L2TP just as any other tunneling protocol with or without encryption. The L2TP standard says that the most secure way to encrypt data is using L2TP over IPsec (Note that it is default mode for Microsoft L2TP client) as all L2TP control and data packets for a particular tunnel appear as homogeneous UDP/IP data packets to the IPsec system.

Multilink PPP (MP) is supported in order to provide MRRU (the ability to transmit full-sized 1500 and larger packets) and bridging over PPP links (using Bridge Control Protocol (BCP) that allows to send raw Ethernet frames over PPP links). This way it is possible to setup bridging without EoIP. The bridge should either have an administratively set MAC address or an Ethernet-like interface in it, as PPP links do not have MAC addresses.

L2TP includes PPP authentication and accounting for each L2TP connection. Full authentication and accounting of each connection may be done through a RADIUS client or locally.

MPPE 128bit RC4 encryption is supported.

L2TP traffic uses UDP protocol for both control and data packets. UDP port 1701 is used only for link establishment, further traffic is using any available UDP port (which may or may not be 1701). This means that L2TP can be used with most firewalls and routers (even with NAT) by enabling UDP traffic to be routed through the firewall or router.

L2TP Client

Sub-menu: `/interface l2tp-client`

Properties

Property	Description
`add-default-route` (*yes | no*; Default: **no**)	Whether to add L2TP remote address as a default route.
`allow` (*mschap2 | mschap1 | chap | pap*; Default: **mschap2, mschap1, chap, pap**)	Allowed authentication methods.
`connect-to` (*IP*; Default:)	Remote address of L2TP server
`comment` (*string*; Default:)	Short description of the tunnel.
`default-route-distance` (*byte*; Default:)	Since v6.2, sets distance value applied to auto created default route, if `add-default-route` is also selected
`dial-on-demand` (*yes | no*; Default: **no**)	connects only when outbound traffic is generated. If selected, then route with gateway address from 10.112.112.0/24 network will be added while connection is not established.
`disabled` (*yes | no*; Default: **yes**)	Enables/disables tunnel.
`keepalive-timeout` (*integer [1..4294967295]*; Default: **60s**)	Since v6.0rc13, tunnel keepalive timeout in seconds.
`max-mru` (*integer*; Default: **1460**)	Maximum Receive Unit. Max packet size that L2TP interface will be able to receive without packet fragmentation.
`max-mtu` (*integer*; Default: **1460**)	Maximum Transmission Unit. Max packet size that L2TP interface will be able to send without packet fragmentation.
`mrru` (*disabled | integer*; Default: **disabled**)	Maximum packet size that can be received on the link. If a packet is bigger than tunnel MTU, it will be split into multiple packets, allowing full size IP or Ethernet packets to be sent over the tunnel. `Read more >>`
`name` (*string*; Default:)	Descriptive name of the interface.
`password` (*string*; Default: **""**)	Password used for authentication.
`profile` (*name*; Default: **default-encryption**)	Used PPP profile.
`user` (*string*; Default:)	User name used for authentication.
`use-ipsec` (*yes | no*; Default: **no**)	When this option is enabled, dynamic IPSec peer configuration and policy is added to encapsulate L2TP connection into IPSec tunnel.
`ipsec-secret` (*string*; Default:)	Preshared key used when `use-ipsec` is enabled.

Quick example

This example demonstrates how to set up L2TP client with username "l2tp-hm", password "123" and server 10.1.101.100

```
[admin@dzeltenais_burkaans] /interface l2tp-client>add name=l2tp-hm user=l2tp-hm password=123 \
\... connect-to=10.1.101.100 disabled=no
[admin@dzeltenais_burkaans] /interface l2tp-client> print detail
Flags: X - disabled, R - running
 0    name="l2tp-hm" max-mtu=1460 max-mru=1460 mrru=disabled
      connect-to=10.1.101.100 user="l2tp-hm" password="123"
      profile=default-encryption add-default-route=no dial-on-demand=no
      allow=pap,chap,mschap1,mschap2
```

L2TP Server

Sub-menu: `/interface l2tp-server`

This sub-menu shows interfaces for each connected L2TP clients.

An interface is created for each tunnel established to the given server. There are two types of interfaces in L2TP server's configuration

- Static interfaces are added administratively if there is a need to reference the particular interface name (in firewall rules or elsewhere) created for the particular user.
- Dynamic interfaces are added to this list automatically whenever a user is connected and its username does not match any existing static entry (or in case the entry is active already, as there can not be two separate tunnel interfaces referenced by the same name).

Dynamic interfaces appear when a user connects and disappear once the user disconnects, so it is impossible to reference the tunnel created for that use in router configuration (for example, in firewall), so if you need persistent rules for that user, create a static entry for him/her. Otherwise it is safe to use dynamic configuration.

Note: in both cases PPP users must be configured properly - static entries do not replace PPP configuration.

Server configuration

Sub-menu: `/interface l2tp-server server`

Properties

Property	Description
`authentication` (*pap | chap | mschap1 | mschap2*; Default: **mschap1,mschap2**)	Authentication methods that server will accept.
`default-profile` (*name*; Default: **default-encryption**)	default profile to use
`enabled` (*yes | no*; Default: **no**)	Defines whether L2TP server is enabled or not.
`max-mru` (*integer*; Default: **1460**)	Maximum Receive Unit. Max packet size that L2TP interface will be able to receive without packet fragmentation.
`keepalive-timeout` (*integer*; Default: **30**)	If server during `keepalive-timeout` period does not receive any packets, it will send keepalive packets every second, five times. If the server still does not receive any response from the client, then the client will be disconnected after 5 seconds. Logs will show 5x "LCP missed echo reply" messages and then disconnect. Available starting from v5.22 and v6rc3.
`max-mtu` (*integer*; Default: **1460**)	Maximum Transmission Unit. Max packet size that L2TP interface will be able to send without packet fragmentation.
`use-ipsec` (*no | yes | require*; Default: **no**)	When this option is enabled, dynamic IPSec peer configuration is added to suite most of the L2TP road-warrior setups. When `require` is selected server will accept only those L2TP connection attempts that were encapsulated in the IPSec tunnel.
`ipsec-secret` (*string*; Default:)	Preshared key used when `use-ipsec` is enabled
`mrru` (*disabled | integer*; Default: **disabled**)	Maximum packet size that can be received on the link. If a packet is bigger than tunnel MTU, it will be split into multiple packets, allowing full size IP or Ethernet packets to be sent

	over the tunnel. `Read more >>`

To enable L2TP server:

```
[admin@MikroTik] interface l2tp-server server> set enabled=yes
[admin@MikroTik] interface l2tp-server server> print
          enabled: yes
          max-mtu: 1460
          max-mru: 1460
             mrru: disabled
   authentication: pap,chap,mschap1,mschap2
  default-profile: default-encryption
[admin@MikroTik] interface l2tp-server server>
```

Monitoring

Monitor command can be used to monitor status of the tunnel on both client and server.

```
[admin@dzeltenais_burkaans] /interface l2tp-client> monitor 0
     status: "connected"
     uptime: 7h24m18s
  idle-time: 6h21m4s
   encoding: "MPPE128 stateless"
        mtu: 1460
        mru: 1460

```

Read-only properties

Property	Description
`status` ()	Current L2TP status. Value other than "connected" indicates that there are some problems establishing tunnel. - **dialing** - attempting to make a connection - **verifying password** - connection has been established to the server, password verification in progress - **connected** - tunnel is successfully established - **terminated** - interface is not enabled or the other side will not establish a connection
`uptime` (*time*)	Elapsed time since tunnel was established.
`idle-time` (*time*)	Elapsed time since last activity on the tunnel.
`encoding` ()	Used encryption method
`local-address` (*IP Address*)	IP Address of local interface

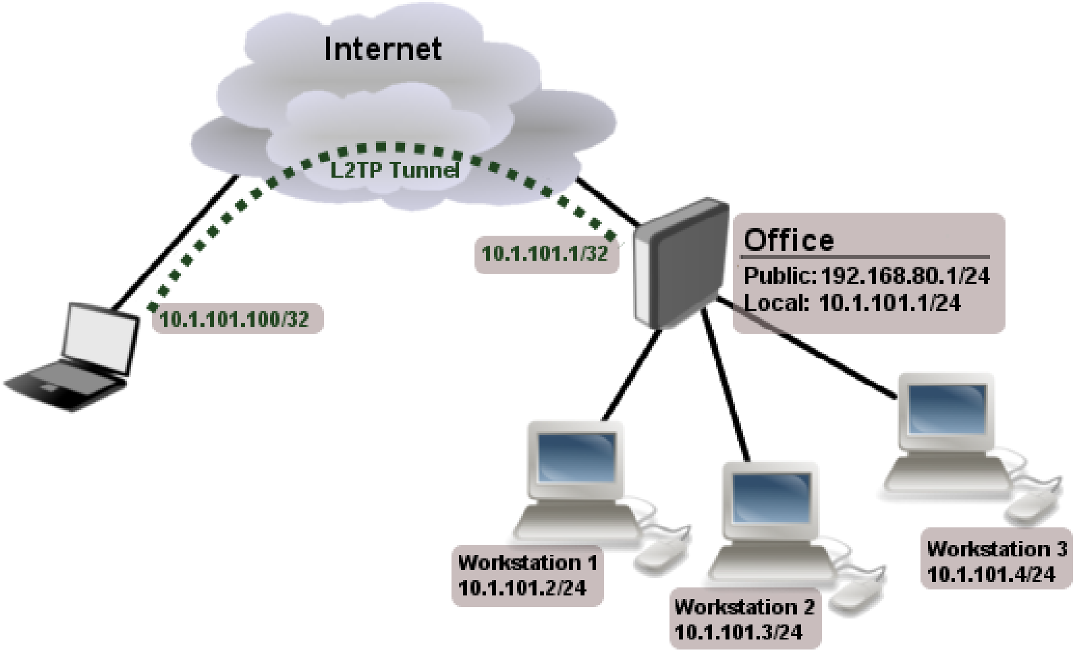
`remote-address` (*IP Address*)	IP Address of remote interface
`mru` (*integer*)	Negotiated and used MRU

Application Examples

Connecting Remote Client

The following example shows how to connect a computer to a remote office network over L2TP encrypted tunnel giving that computer an IP address from the same network as the remote office has (without any need of bridging over EoIP tunnels)

Consider following setup:



Office router is connected to internet through **ether1**. Workstations are connected to **ether2**. Laptop is connected to the internet and can reach Office router's public IP (in our example it is 192.168.80.1).

First step is to create a user

```
[admin@RemoteOffice] /ppp secret> add name=Laptop service=l2tp password=123
local-address=10.1.101.1 remote-address=10.1.101.100
[admin@RemoteOffice] /ppp secret> print detail
Flags: X - disabled
  0   name="Laptop" service=l2tp caller-id="" password="123" profile=default
      local-address=10.1.101.1 remote-address=10.1.101.100

[admin@RemoteOffice] /ppp secret>
```

Notice that L2TP local address is the same as routers address on local interface and remote address is from the same range as local network (10.1.101.0/24).

Next step is to enable L2TP server and L2TP client on the laptop.

```
[admin@RemoteOffice] /interface l2tp-server server> set enabled=yes
[admin@RemoteOffice] /interface l2tp-server server> print
            enabled: yes
            max-mtu: 1460
            max-mru: 1460
               mrru: disabled
     authentication: mschap2
    default-profile: default-encryption
[admin@RemoteOffice] /interface l2tp-server server>
```

L2TP client from the laptop should connect to routers public IP which in our example is 192.168.80.1.
Please, consult the respective manual on how to set up a L2TP client with the software you are using.

Note: By default Windows sets up L2TP with IPsec. To disable IpSec, registry modifications are required. `Read more >>`

At this point (when L2TP client is successfully connected) if you will try to ping any workstation from the laptop, ping will time out, because Laptop is unable to get ARPs from workstations. Solution is to set up `proxy-arp` on local interface

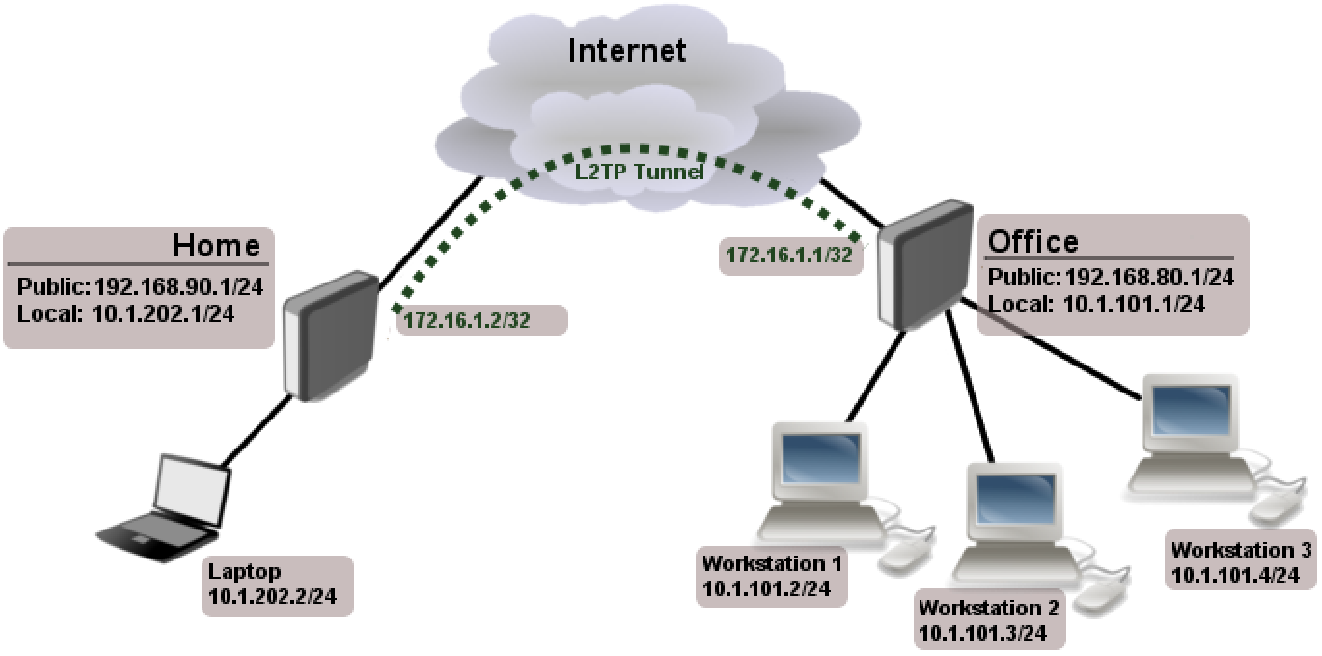
```
[admin@RemoteOffice] interface ethernet> set ether2 arp=proxy-arp
[admin@RemoteOffice] interface ethernet> print
Flags: X - disabled, R - running
  #    NAME                 MTU   MAC-ADDRESS         ARP
  0  R ether1              1500  00:30:4F:0B:7B:C1 enabled
  1  R ether2              1500  00:30:4F:06:62:12 proxy-arp
[admin@RemoteOffice] interface ethernet>
```

After `proxy-arp` is enabled client can now successfully reach all workstations in local network behind the router.

Site-to-Site L2TP

The following is an example of connecting two Intranets using a L2TP tunnel over the Internet.

Consider following setup:



Office and Home routers are connected to internet through **ether1**, workstations and laptops are connected to **ether2**. Both local networks are routed through L2TP client, thus they are not in the same broadcast domain. If both networks should be in the same broadcast domain then you need to use BCP and bridge L2TP tunnel with local interface.

First step is to create a user

```
[admin@RemoteOffice] /ppp secret> add name=Home service=l2tp password=123
local-address=172.16.1.1 remote-address=172.16.1.2 routes="10.1.202.0/24 172.16.1.2 1"
[admin@RemoteOffice] ppp secret> print detail
Flags: X - disabled
  0   name="Home" service=l2tp caller-id="" password="123" profile=default
      local-address=172.16.1.1 remote-address=172.16.1.2 routes="10.1.202.0/24 172.16.1.2 1"

[admin@RemoteOffice] /ppp secret>
```

Notice that we set up L2TP to add route whenever client connects. If this option is not set, then you will need static routing configuration on the server to route traffic between sites through L2TP tunnel.

Next step is to enable L2TP server on the office router and configure L2TP client on the Home router.

```
[admin@RemoteOffice] /interface l2tp-server server> set enabled=yes
[admin@RemoteOffice] /interface l2tp-server server> print
            enabled: yes
            max-mtu: 1460
            max-mru: 1460
               mrru: disabled
     authentication: mschap2
    default-profile: default-encryption
[admin@RemoteOffice] /interface l2tp-server server>
```

```
[admin@Home] /interface l2tp-client> add user=Home password=123 connect-to=192.168.80.1 disabled=no
[admin@Home] /interface l2tp-client> print
Flags: X - disabled, R - running
 0 R  name="l2tp-out1" max-mtu=1460 max-mru=1460 mrru=disabled connect-to=192.168.80.1 user="Home"
       password="123" profile=default-encryption add-default-route=no dial-on-demand=no
       allow=pap,chap,mschap1,mschap2
[admin@Home] /interface l2tp-client>
```

On home router if you wish traffic for the remote office to go over tunnel you will need to add a specific static route as follows:

```
[admin@Home] /ip route> add dst-address=10.1.101.0/24 gateway=l2tp-out1
```

After tunnel is established and routes are set, you should be able to ping remote network.

Basic L2TP/IpSec setup

This example demonstrates how to easily setup L2TP/IpSec server on Mikrotik router (with installed 6.16 or newer version) for road warrior connections (works with Windows, Android And iPhones).

First step is to enable L2TP server:

```
/interface l2tp-server server
set enabled=yes use-ipsec=required ipsec-secret=mySecret default-profile=default
```

required is set to make sure that only IPSec encapsulated L2TP connections will be accepted.

Now what it does is enables L2TP server and creates dynamic ipsec peer iwth specified secret

```
[admin@MikroTik] /ip ipsec peer> print
 0  D address=0.0.0.0/0 local-address=0.0.0.0 passive=yes port=500
      auth-method=pre-shared-key secret="123" generate-policy=port-strict
      exchange-mode=main-l2tp send-initial-contact=yes nat-traversal=yes
      hash-algorithm=sha1 enc-algorithm=3des,aes-128,aes-192,aes-256
      dh-group=modp1024 lifetime=1d dpd-interval=2m dpd-maximum-failures=5
```

Note: Care must be taken if static ipsec peer configuration exists.

Next step is to create VPN pool and add some users.

```
/ip pool add name=vpn-pool range=192.168.99.2-192.168.99.100
```

```
/ppp profile
set default local-address=192.168.99.1 remote-address=vpn-pool

/ppp secret
add name=user1 password=123
add name=user2 password=234
```

If there are strict firewall policies, do not forget to add rules which accepts l2tp and ipsec.

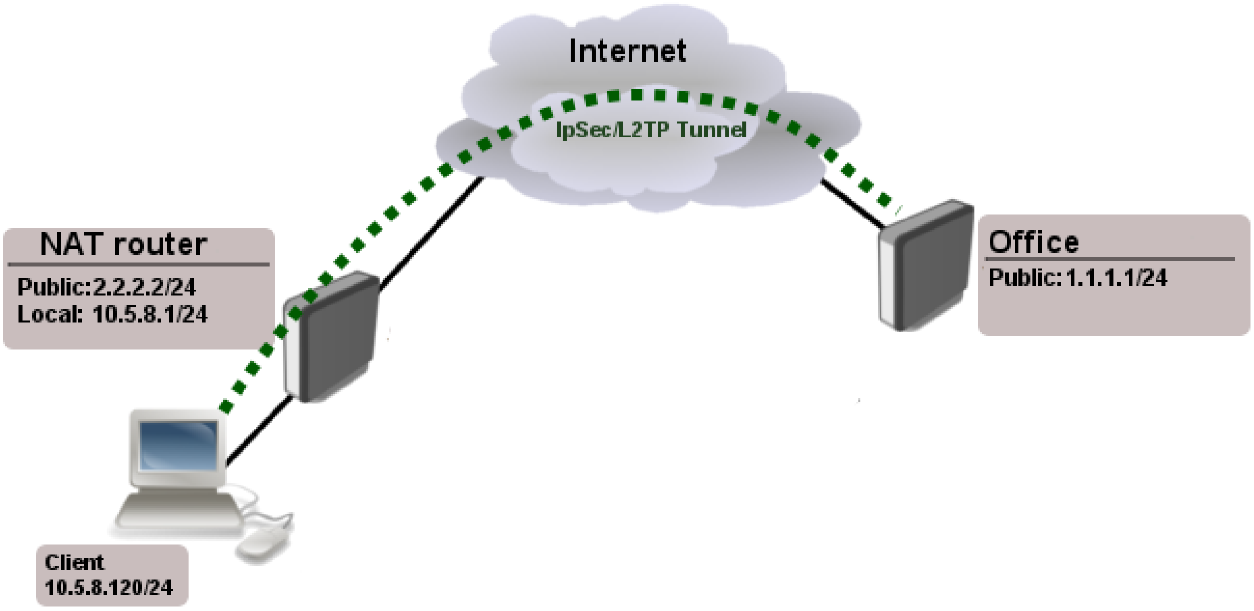
```
/ip firewall filter
add chain=input protocol=udp port=1701,500,4500
add chain=input protocol=ipsec-esp
```

Now router is ready to accept L2TP/IpSec client connections.

L2TP/IpSec with static IPSec server setup

Ipsec/L2TP behind NAT

Consider setup as illustrated below



Client needs secure connection to the office with public address 1.1.1.1, but server does not know what will be the source address from which client connects. It is so called road-warrior setup. Our client will also be located behind the router with enabled NAT.

For the setup RouterOS router will be used as the client device behind NAT (it can be any device: Windows PC, Smartphone, Linux PC, etc.)

IP Connectivity

On the server:

```
/ip address
add address=1.1.1.1/24 interface=ether1

/ip route
add gateway=1.1.1.2
```

On the clients router:

```
/ip address
add address=2.2.2.2/24 interface=ether1
add address=10.5.8.0/24 interface=ether2

/ip route
add gateway=2.2.2.1

/ip firewall nat
add chain=srcnat action=masquerade out-interface=ether1
```

On the client:

```
/ip address
add address=10.5.8.120/24 interface=ether1
```

L2TP Config

On the server:

```
/interface l2tp-server
set enabled=yes profil=default

/ip pool
```

```
add name=l2tp-pool ranges=192.168.1.2-192.168.1.20

/ppp profile
set default local-address=192.168.1.1 remote-address=l2tp-pool

/ppp secret
add name=l2tp-test password=test123456
```

On the client:

```
/interface l2tp-client
add connect-to=1.1.1.1 disabled=no name=l2tp-out1 password=password user=l2tp-test
```

IpSec Config

On server side:

```
/ip ipsec proposal
set [ find default=yes ] enc-algorithms=3des,aes-128,aes-192,aes-256
/ip ipsec peer
add generate-policy=yes hash-algorithm=sha1 nat-traversal=yes secret=test123456
```

RouterOS as client:

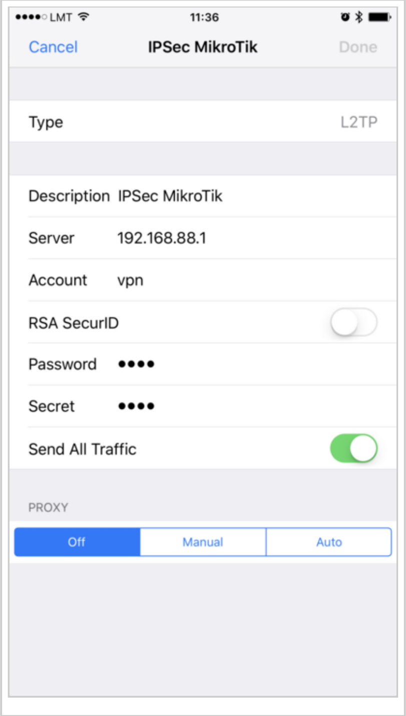
```
/ip ipsec proposal
set [ find default=yes ] enc-algorithms=aes-128
/ip ipsec peer
add address=1.1.1.1/32 hash-algorithm=sha1 nat-traversal=yes secret=test123456

/ip ipsec policy
add dst-address=1.1.1.1/32 protocol=udp sa-dst-address=1.1.1.1 \
      sa-src-address=10.5.8.120 src-address=10.5.8.120/32
```

Notice that `nat-traversal` is enabled. This option is required because Ipsec connection will be established through the NAT router otherwise Ipsec will not be able to establish phase2.

⚠ **Warning:** Only one L2TP/IpSec connection can be established through the NAT. Which means that only one client can connect to the sever located behind the same router.

Apple iOS (iPhone/iPad) Client

You must choose L2TP as VPN type in iOS to connect to the IPsec/L2TP server on RouterOS (this includes the default IPsec server created by QuickSet VPN checkbox).



IPSec MikroTik

Type L2TP

Description IPSec MikroTik

Server 192.168.88.1

Account vpn

RSA SecurID ○

Password ••••

Secret ••••

Send All Traffic ●

Read More

- BCP (Bridge Control Protocol)
- Disable IpSec used with L2TP on Windows (https://support.microsoft.com/en-us/kb/258261)
- MikroTik RouterOS and Windows XP IPSec/L2TP

[Top | Back to Content **]**

Retrieved from "https://wiki.mikrotik.com/index.php?title=Manual:Interface/L2TP&oldid=30044"

Categories: Manual | VPN | Interface

- This page was last edited on 13 November 2017, at 15:51.