Corporate VPN Using Mikrotik Cloud Feature

By SOUMIL GUPTA BHAYA
Mikrotik Certified Trainer
What is a VPN?

• A virtual private network (VPN) is a method for the extension of a private network across a public network, such as the Internet.

• It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

• A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.
Corporate VPN: The Scenario
VPN Tunnels

• PPTP- Point to Point Tunneling Protocol
• L2TP- Layer 2 Tunneling Protocol
• SSTP- Secure Socket Tunneling Protocol
• OVPN- Open VPN
Common Problems

• Router does not have static IP.

• PPTP is not working, and not very secure even if it is.

• SSTP is not compatible with Mac OS, Android, Windows XP.

• IPSEC is complicated to set up.

What Are The Solutions???
DDNS

• Dynamic Domain Name Service (DDNS) can solve the issue of absence of static ip.

• Third party DDNS services often require scripts.

• Most third party DDNS require fees.

```
:global ddnsuser "theddnsusername"
:global ddnpass "theddnspassword"
:global theinterface "interfacename"
:global ddnshost blabla.dyndns.org
:global ipdnds [:resolve $ddnshost];
:global ipfresh [:/ip address get [/ip address find interface=$theinterface ] address ]
:if ( [:typeof $ipfresh ] = nil ) do=
 :log info ("DynDNS: No ip address on $theinterface.")
} else={
 :for i from=( [:len $ipfresh] - 1) to=0 do=
 :if ( [:pick $ipfresh i] = "/") do=
 :set ipfresh [:pick $ipfresh 0 $i];
 :
 :if ($ipdnds != $ipfresh) do=
 :log info ("DynDNS: IP-DynDNS = $ipdnds")
 :log info ("DynDNS: IP-Fresh = $ipfresh")
 :log info "DynDNS: Update IP needed, Sending UPDATE...!"
 :global str
 "/nic/update?hostname=$dnshost&myip=$ipfresh&wildcard=NOCHG&mx=NOCHG&backmx=NOCHG"

/tool fetch address=members.dyndns.org src-path=$str mode=http user=$ddnsuser 

password=$ddnpass dst-path="$/DynDNS..$ddnshost"

delay 1
:global str [:/file find name="DynDNS.$ddnshost"]; 
:/file remove $str
:global ipdnds $ipfresh
:log info "DynDNS: IP updated to $ipfresh!"
} else=
 :log info "DynDNS: dont need changes";
}

/system scheduler
add interval=1m name=DynDns on-event=DynDns
policy=ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive,api start-time=startup
```
Mikrotik Cloud

• MikroTik offers a Dynamic DNS name service for RouterBOARD devices.

• Starting with RouterOS v6.14

• Your device can automatically get a working domain name.

• Useful if your IP address changes often, and you want to always connect to your router.
Mikrotik Cloud: Features

• **Currently the cloud feature only provides three services:**
  - Ddns (provide dns name for router's external IPv4 address. IPv6 not supported)
  - Approximate time (accuracy of several seconds, depends on UDP packet latency, useful when NTP is not available)
  - Time zone detection (if enabled, clock time zone will be updated even when DDNS and update time are disabled)
Mikrotik Cloud: Operation

• Router checks for outgoing IP address change: every 60 seconds
• Router waits for cloud server response: 15 seconds
• DDNS record TTL: 60 seconds
• Cloud time update: after router restart and during every ddns update (when router external IP address change or after force-ddns-update command)
• Time-zone-autodetect: The time zone is detected depending from router public IP address and our commercial database.
Mikrotik Cloud: Settings

DNS ADDRESS
PPTP With Mikrotik Cloud

• PPTP is a layer 3 tunneling protocol and uses IP routing information and addresses to bind clients to servers.

• You must permit TCP, port 1723 in the router's firewall (the PPTP server)

• Serious security vulnerabilities have been found in the protocol.

• Advantage: Compatibility with most operating systems and easy to configure.
PPTP With Mikrotik Cloud

- Server Settings

Make Sure Cloud is Enabled in the router
PPTP With Mikrotik Cloud

- **Client Settings**

- Put Cloud DDNS address in “Connect To:” box.

- Use the name and password configured in the “Secrets” tab of the server.
SSTP With Mikrotik Cloud

• SSTP is a tunnel that provides a mechanism to transport PPP or L2TP traffic through an SSL 3.0 channel.

• SSL provides transport-level security with key-negotiation, encryption and traffic integrity checking.

• The use of SSL over TCP port 443 allows SSTP to pass through virtually all firewalls and proxy servers except for authenticated web proxies.

• You can also specify a different TCP port to connect to.
SSTP With Mikrotik Cloud

- Server Settings
  - Specify a TCP port (default: 443)

Make Sure Cloud is Enabled in the router
SSTP With Mikrotik Cloud

- **Client Settings**
  - Put Cloud DDNS address in “Connect To:” box.
  - Specify TCP port used by the server
  - Use the name and password configured in the “Secrets” tab of the server.
• OpenVPN is an open-source software application that uses a custom security protocol that utilizes SSL/TLS for key exchange.

• It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

• OpenVPN has been ported and embedded to several systems.

• It is compatible with Solaris, Linux, OpenBSD, FreeBSD, NetBSD, QNX, Mac OS X, and Windows 2000/XP/Vista/7/8, Windows Mobile 6.5, iOS 3GS+, Android 4.0+. 
OVPN With Mikrotik Cloud

- Server Settings
  - Specify a port (default: 1194)
  - Specify authentication methods and ciphers

Make Sure Cloud is Enabled in the router
OVPN With Mikrotik Cloud

- **Client Settings**
  - Put Cloud DDNS address in “Connect To:” box.
  - Specify port used by the server.
  - Specify authentication methods and ciphers used by the server.
Which VPN should we use?

SSTP

• Advantages:
  • SSTP VPN makes use of TCP port 443 meaning that it can help you bypass most DNS restriction filters and firewalls on the web.
  • SSTP is largely compatible with Windows Vista, Windows 7 and above.
  • SSTP VPN has seamless security. Since SSTP uses SSL, its PPP and L2TP traffic passes over a secure https session.

• Disadvantages:
  • It is a disappointment if you’ve got an iPhone, an Xbox, an Android or any other non-Windows gadget.
  • Since SSTP VPN is not open source, it can be easily invaded by spying agencies that need to exert little effort to inject backdoors in security software
  • Typical setting for data encryption on SSTP is 256bit.
Which VPN should we use?

OVVPN

• Advantages:
  • OpenVPN is compatible with almost any device, including Windows, Mac, PC, Android, iPhone and Linux systems.
  • OpenVPN is also relatively a new encryption technology. It employs an OpenSSL library and SSLv3/TLSv1 protocols.
  • Its cryptographic algorithms take a variety of forms like 3DES, AES, RC5 and Blowfish.
  • If the ease of functional configuration is a thing to matter, then OpenVPN is definitely the right choice.

• Disadvantages:
  • No real disadvantages are known in OpenVPN. There is, however, one:
  • Unlike the Windows based SSTP, manual configuration of OpenVPN can be burdensome.
Drawbacks of Mikrotik Cloud

• Does not work if router is behind NAT.

• If router has multiple public IP addresses and/or multiple internet gateways, the exact IP used for the update may not be as expected.
To Conclude

• Mikrotik Cloud is mainly provided for ease of access if there is no static ip on the router.

• Easy to configure.

• Free of charge.

• Good feature to be used along with VPNs.
Thank You for Your Attention

Questions???