Setup a L2TP over IPSec VPN Server on Linux

Lawrence Chiu@2007/08/30

前言:
在VPN還沒有被提出之前，公司與分公司之間要傳送資料時只能透過專線或是其它的方法來解決，但這花費不是一般公司能負荷的。又或者公司的員工出差時，萬一想連回公司存取資料時，那怎麼辦呢？傳統的作法是可透過modem撥回公司，但這電話費也太貴了些，如果在國內還可接受，但萬一人在國外呢？

所以有人就提出了VPN的方法來解決這樣的情況，VPN最主要的目的就是透過公眾網路（Internet)來傳遞相隔兩地的區域網路之間的資料，使用者一但透過VPN連回公司，他就好像人在公司中工作非常的方便，但因為公眾網路是open的，所以在這上面所傳遞的資料必需經過authentication，encryption與data integrity。

VPN連線的方法有很多種，比如: PPTP，IPSec，L2TP/IPSec與L2TP without IPSec，其中PPTP與L2TP主要是給User透過撥接的方法連回公司的網路存取資料，就好比在家透過modem撥接上Internet一般，而IPSec呢？主要是應用在LAN to LAN模式的VPN架構，也就是公司對分公司。

這篇文章主要是在說明架設L2TP/IPSec VPN Server讓遠端的使用者，可以透過這台機器連回公司的網路，但由於環境的原因我只有提供兩台電腦互接上後，L2TP Client是否可以撥接上L2TP/IPSec Server並順利取得IP address，為何要採取L2TP/IPSec呢? 主要的原因是L2TP本身並沒有資料加密，並不安全，所以我們可以透過IPSec來做資料加密以補L2TP本身的不足，事實上如果要應用在真實的環境中，您必需要有一張以上的網卡，並透過iptables來做後續的控管，要考慮到的問題很多，很抱歉這篇文章沒有提供這樣的資訊，這篇文章的主要目的是要讓大家能順利架設起L2TP/IPSec Server，因為筆者在實作時遇到了很多問題，最後終於把安裝與架設的過程精簡到這樣，其中如果有遺漏或不清楚的地方請多多賜教，筆者的Blog在: http://go-linux.blogspot.com/

您可以到這個Blog留下您寶貴的意見，非常感謝！

Test Environment:

L2TP Client ---------- L2TP Server

L2TP Client: Windows XP SP2
L2TP Server: CentOS 5.0

IP address of L2TP Client: 10.5.30.200
IP address of L2TP Server: 10.5.30.3

必要套件:
xl2tpd-1.1.09-1.fc5.src.rpm
openswan-2.4.9-31.el5.i386.rpm

ipsec-tools* (預設已安裝)
ppp* (預設已安裝)

Setup Procedure:

1.Install RPM:
rpm –ivh openswan*
rpm –ivh xl2tpd* (That's source rpm you must rebuild it)

2.Configure L2TP Server:
2.1 設定帳號與密碼:
vi /etc/ppp/chap-secrets
lawrence * "redhat" *

2.2 設定xl2tpd設定檔:
[global]
; listen-addr = 192.168.1.98
;
;requires openswan-3.1
;ipsec saref = yes
;
;debug tunnel = yes
auth file = /etc/ppp/chap-secrets #指定透過這個檔案做身份確認
[lns default]
ip range = 192.168.1.128-192.168.1.254 #L2TP/IPSec Server會發出的IP scope
local ip = 192.168.1.99 #L2TP/IPSec Server的IP address
require chap = yes #採取CHAP來作身份確認
refuse pap = yes #不採取PAP，因為是明文傳送不安全
require authentication = yes
name = LinuxVPNserver
ppp debug = yes
pppoptfile = /etc/ppp/options.xl2tpd #這邊可以設定當使用者撥接成功後的一些參數，比如DNS Server IP
length bit = yes

2.3 設定/etc/ppp/options.xl2tpd
ipcp-accept-local
ipcp-accept-remote
ms-dns 192.168.1.1
ms-dns 192.168.1.3
ms-wins 192.168.1.2
ms-wins 192.168.1.4
noccp
auth
crtscts
idle 1800
#mtu 1410
#mru 1410
nodefaultroute

debug
lock
proxyarp
connect-delay 5000
logfile /var/log/xl2tpd.log #新增一個L2TP log file以利除錯用

2.4 啟動L2TP Server
service xl2tpd start; chkconfig xl2tpd on

3. 設定IPSec
3.1 PSK setting:
vi /etc/ipsec.secrets
include /etc/ipsec.d/*.secrets
10.5.30.3 %any : PSK "1234567890"

10.5.30.3 -> Server IP address
%any -> allow all machines
格式要一模一樣，不然會出錯

3.2 設定l2tp-psk.conf
套用範例即可:
cp /etc/ipsec.d/examples/l2tp-psk.conf /etc/ipsec.d/
chmod 755 l2tp-psk.conf

3.3 啟動IPSec
service ipsec start; chkconfig ipsec on

3.4 Check IPSec status
ipsec verify
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path [OK]
Linux Openswan Uopenswan-2.4.9-31.el5/K2.6.18-8.1.8.el5 (netkey)
Checking for IPsec support in kernel [OK]
NETKEY detected, testing for disabled ICMP send_redirects [OK]
NETKEY detected, testing for disabled ICMP accept_redirects [OK]
Checking for RSA private key (/etc/ipsec.d/hostkey.secrets) [OK]
Checking that pluto is running [OK]
Two or more interfaces found, checking IP forwarding [OK]
Checking NAT and MASQUERADEing [N/A]
Checking for 'ip' command [OK]
Checking for 'iptables' command [OK]
Opportunistic Encryption Support [DISABLED]

這麼一來L2TP over IPSec**就成功架設起來了，如果有問題的話可查看以下的**log file
/var/log/message
/var/log/secure
/var/log/xl2tpd.log

4. L2TP Client setting:
4.1新增連線

1. 開始->設定->網路連線->新增連線精靈
2. 選擇連線到公司網路(使用指定撥號或是vpn)
3. 選擇虛擬私人網路連線
4. 輸入名稱(可以隨意選)
5. 輸入VPN server IP (10.5.30.3)

4.2 修改設定

1.在安全性的分頁中->選擇進階->只勾選CHAP->可省加密

2. 點選"ipsec 設定"選項,輸入PSK(pre-shared key)

成功撥接上的圖: