IPsec L2TP

Version: 3538

Table of Contents

IPsec L2TP

Introduction

This document describes how to setup an ImageStream router to terminate IPsec L2tp tunnels.

Requirements

- The router must be running at least 4.4.0-100 or newer
- A IPSec L2tp client(Windows 7 or Mac OS X Lion have built-in clients)

Method of Operation

This type of Vpn actually relies on two different technologies to function correctly. First an IpSec connection is established between the ImageStream router and the Vpn client. In this example we show how to do this with a pre-shared key. Then after the IPsec SA is established, an L2tp tunnel is initiated to the ImageStream router from the client. The L2tp subsystem in the ImageStream router then handles the connection. In this example user authentication is handled via usernames and passwords stored in the Network Interface configuration(wan.conf) but it is possible to use external radius servers. Consult the L2tp documentation for more information.

Configuration

Below is the /etc/ipsec.conf configuration.

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
version 2.0
# basic configuration - auto generated on Sat Nov 26 15:20:02 EST 2005
config setup
       interfaces=%defaultroute
       klipsdebug=none
       plutodebug=none
       uniqueids=yes
       nat_traversal=yes
conn L2TP-PSK
       authby=secret
       pfs=no
       rekey=no
       keyingtries=3
       #
       # ------------------------------------------------------------
       # The VPN server.
       #
       # Allow incoming connections on the external network interface.
       # If you want to use a different interface or if there is no
       # defaultroute, you can use:   left=your.ip.addr.ess
       #
       left=%defaultroute
```

```
        #
        leftprotoport=17/1701
        # If you insist on supporting clients that use non-standard ports
        # you can use:    leftprotoport=17/%any
        #
        # ------------------------------------------------------------
        # The remote user(s).
        #
        # Allow incoming connections only from this IP address.
        right=%any
        # If you want to allow multiple connections from any IP address,
        # you can use:    right=%any
        #
        rightprotoport=17/%any
        auto=add
```

Below is an example /etc/ipsec.secrets file. In this example the ip address is the address of the ImageStream routers internet facing connection. In this case the IPsec pre-shared key is "testingipsec". This will need to be configured in IPsec L2tp client. Other configurations using X.509 and RSA certs are possible.

```
# This file holds shared secrets or RSA private keys for inter-Pluto
# authentication.  See ipsec_pluto(8) manpage, and HTML documentation.
18.54.23.30 %any : PSK "testingipsec"
```

Below is the Network Interface Configuration. Please note that this configuration stores the username and password information for the L2tp configuration in clear text in the wan.conf. It is possible to use an external radius server for the authentication consult the L2tp documentation if you require that.

This example creates a Virtual-Template that will assign address from the 192.168.88.0/24 network to connecting clients. This configuration is fully self-contained and requires no other services outside of the router to function correctly. Since these are private addresses, you may require Nat configuration on the router to give them connectivity to the Internet.

```
!
version 2.00
!
interface Loopback0
 ip address 18.54.23.30 255.255.255.255
!
interface Ethernet0
 ip address 18.54.23.30 255.255.255.0
 ipv6 address 2001:470:c325:1::30/64
!
user josh password testing1
!
interface Tunnel500
 tunnel mode l2tp
 tunnel peer name default
 tunnel local name ipsec-l2tp
 tunnel virtual-template 1
!
interface Virtual-Template1
 ip address 192.168.88.1 255.255.255.0
 peer default ip pool pool1
 ppp authentication pap
```

```
 mtu 1500
!
ip name-server 8.8.8.8
ip local pool pool1 192.168.88.10 192.168.88.100
!
ip route 0.0.0.0 0.0.0.0 18.54.23.1
!
```