

# Tunnels

Abraham van der Merwe  
[abz@clug.org.za](mailto:abz@clug.org.za)

13 July 2004

# Overview

- What are tunnels?
- What are they used for?
  - Security (VPNs)
  - Abstraction (Hiding Complexity)
  - Compression
  - Routing different protocols (e.g. IPX over TCP/IP)
- Problems
  - Overhead (Wasted Traffic, TCP over TCP)
  - Complexity (Debugging, Quality of Service, Statistics)

# Requirements

- Compatibility
- Security
- Must not provide  $mtu < 1500$  bytes
  - Fragments (Dependance on ICMP)
- Low overhead
  - Throughput (packet overhead)
  - Latency (connectionless vs connection-oriented)
  - Tear down & start up time
- Robustness

# GRE and IP/IP

- Features

- Easy Configuration

- ip tunnel add demo mode gre remote 172.19.20.21 local 172.16.17.18 ttl 255
    - ip link set demo up
    - ip addr add 10.0.1.1 dev demo

- Robust

- Drawbacks

- No security

- No fragmentation (MTU Problem)

- Lack of features (Compression, Traffic Shaping)

# MPPE/PPTP

- Features
  - Compatibility (Windows, UNIX/Linux, MAC)
- Drawbacks
  - Weak Security (40-bit, 128-bit CHAP, MS-CHAPv2)
  - High overhead (PPP)
  - Microsoft Standard

# CIPE

- Features

- Low overhead (UDP)
- Public Key Cryptography (OpenSSL)
- Robust

- Drawbacks

- Lack of features (Compression, Traffic Shaping)

# IPSec

- Features
  - Standards Compliant
  - Performance, Encryption, Compression
- Drawbacks
  - Standards Compliant
  - Lack of features (Traffic Shaping)
- Linux Implementations
  - <http://www.kame.net/>
  - <http://www.freeswan.org/>
  - <http://perso.enst.fr/~beyssac/pipsec/>

# VTUN

- Features
  - Easy Configuration
  - Feature rich
- Drawbacks
  - Unmaintained
  - Not scalable
  - Buggy

# OpenVPN

- Features

- Public Key Cryptography (OpenSSL)
- Adaptive Compression (LZO)
- Traffic Shaping
- Scalable
  - Designed for frequent reconnects
  - Command-line parameters & configuration file
- Robust?

# StegTunnel

- What is it?
- How does it work?
  - TCP Sequence Number (32-bit)
  - IP Identification Number (16-bit)
  - Why not other fields?
- Further reading
  - <http://www.synacklabs.net/projects/stegtunnel/>