How to Homebrew VPNs from Ingredients Found in Your Own Kitchen

1

Building a VPN

- You can build a VPN with scrap systems for under $450 a site!
  - Capable of handling T1+ speeds
  - Uses imported/exported encryption (SSH)
  - FREE except for the hardware
    - P200mmx w/1gb disk
    - Linux/BSDI/OpenBSD/FreeBSD/whatever
    - Network card

2

Building a VPN *(cont)*

- This idea appears to have origiinated with Olaf Titz
  - Subsequent enhancements by Steve Berry and Thor Simon
- This is a simple refinement over early VPNs (ca 1992) that used tunnel IP drivers

3

Building a VPN* *(cont)*

Pentium 233 running LINUX (appears not to be CPU bound)

Throughput Mb/S		
Cypher		Mean
3des[4]		1.43
des	2.38	2.31
blowfish	2.87	2.78
none		3.25
non-VPN		7.90

	Percent of non-VPN Throughput
Cypher	
3des	18.1
des	30.1
blowfish	36.3
none	41.1
non-VPN	100

*Performance measures courtesy Steve Berry

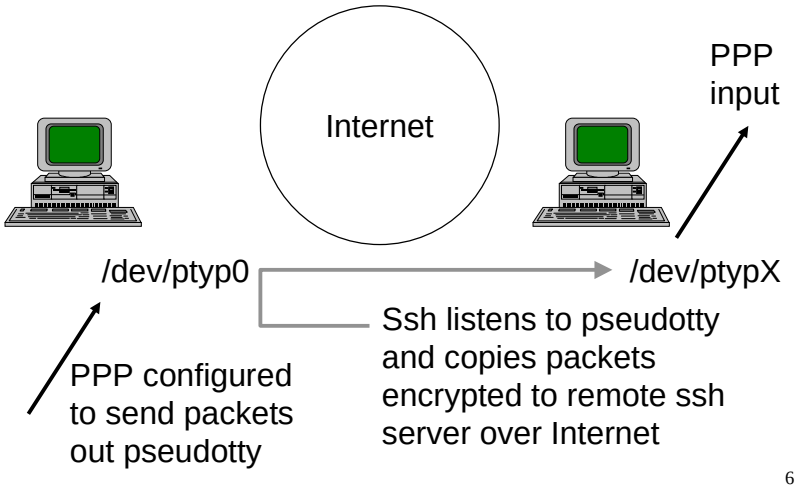
4

Building a VPN *(cont)*

- The hack:
  - Allocate a pseudoterminal
  - Have a point-to-point crypto program listen to it on one side
  - Run pppd on the other side
  - Then set routing up to make the traffic go through the point-to-point tunnel

5

Homebrew VPN



6

Building a VPN *(cont)*

- Sample scripts for LINUX on:
  - www.clark.net/pub/mjr/vpn/
- Sample implementation is in perl
  - Most of the code deals with allocating pseudottys
- Should interoperate transparently between any UNIX systems that run PPP (!)

7