UTORvpn
A Cross Platform Open Source SSL VPN Implementation

Russell Sutherland
University of Toronto
2007-05-18

What is a VPN?

BSDCan 2007

Virtual Private Network

BSDCan 2007

Virtual

BSDCan 2007

Private

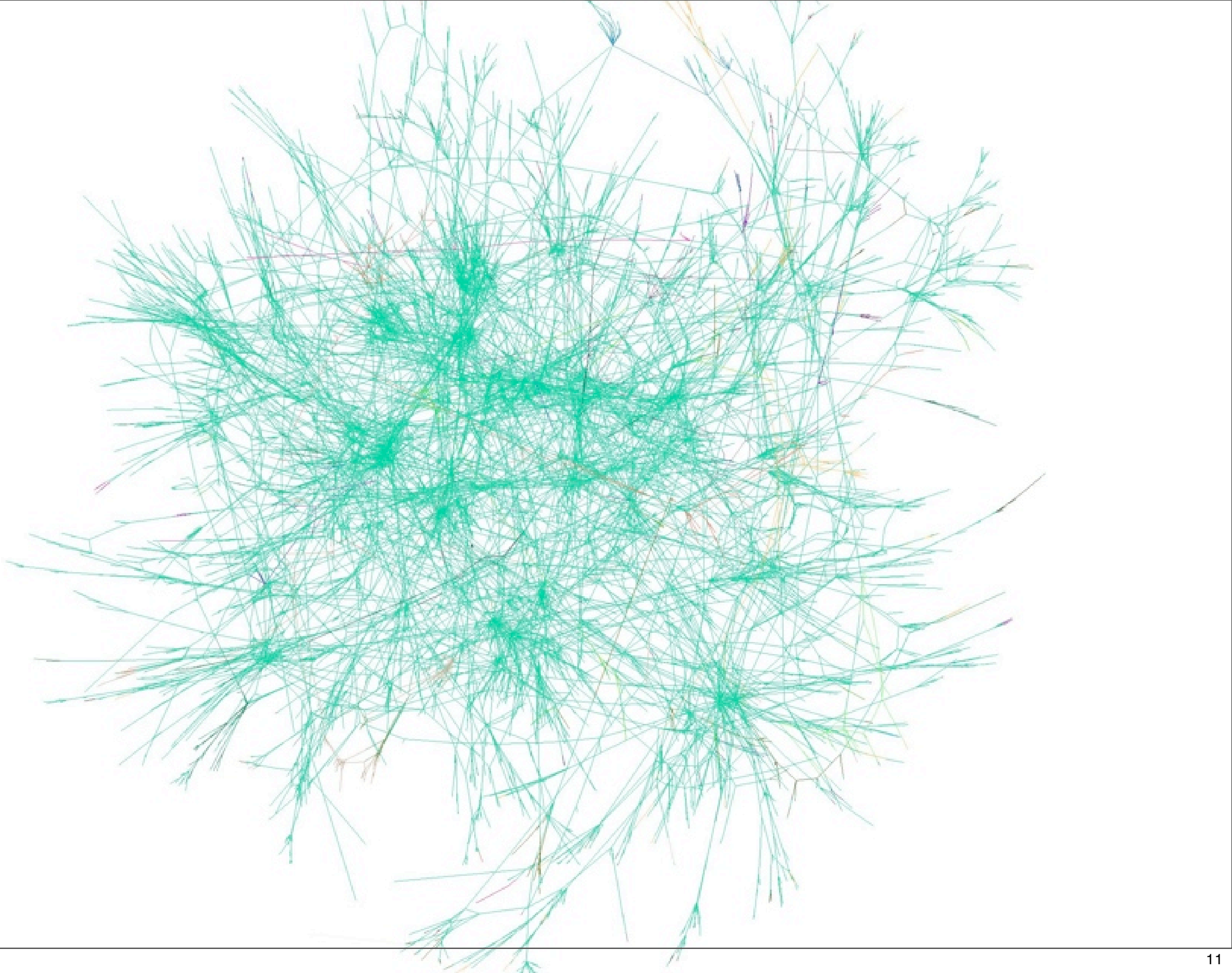
BSDCan 2007

(Secure)

BSDCan 2007

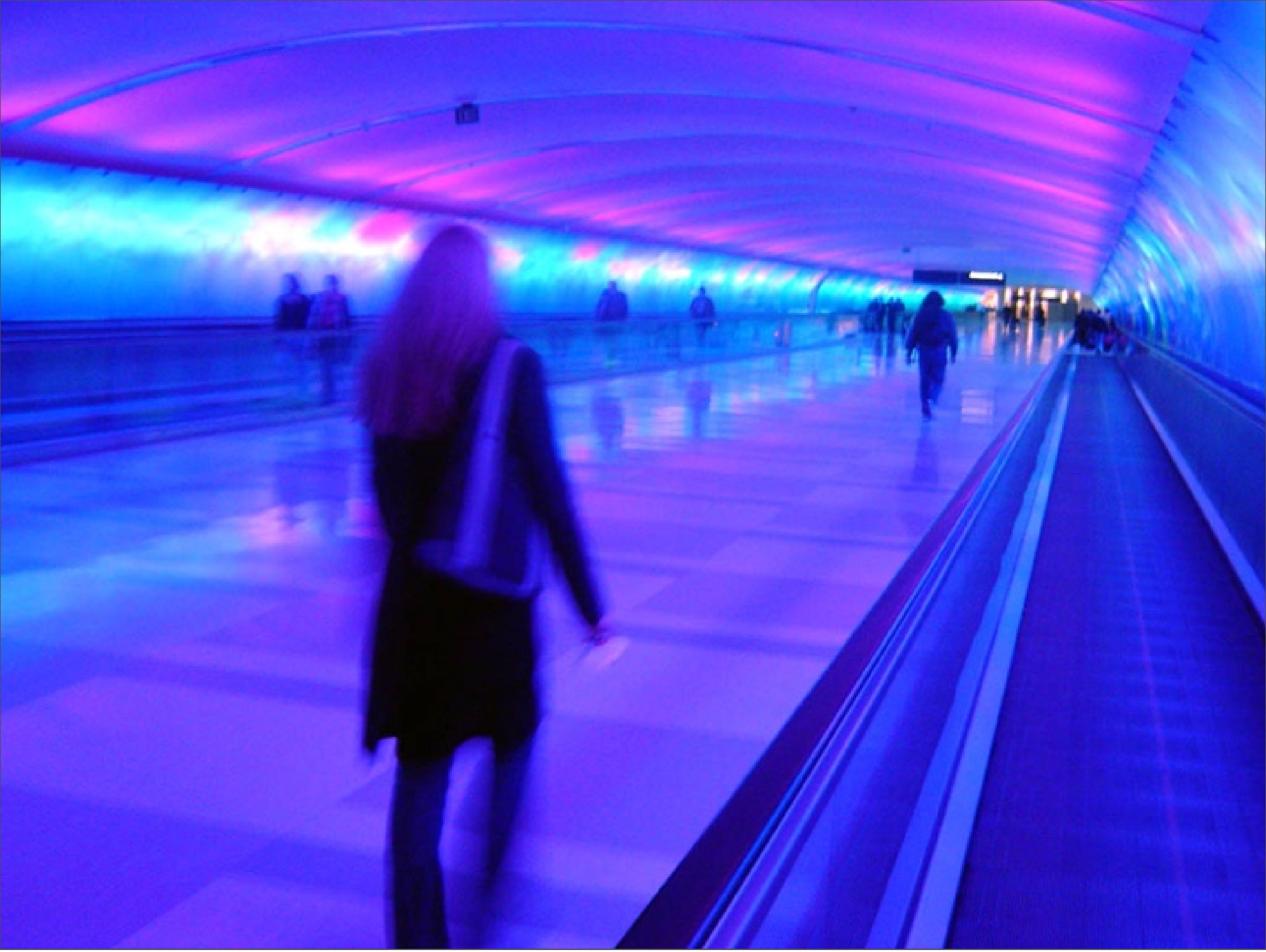
Network

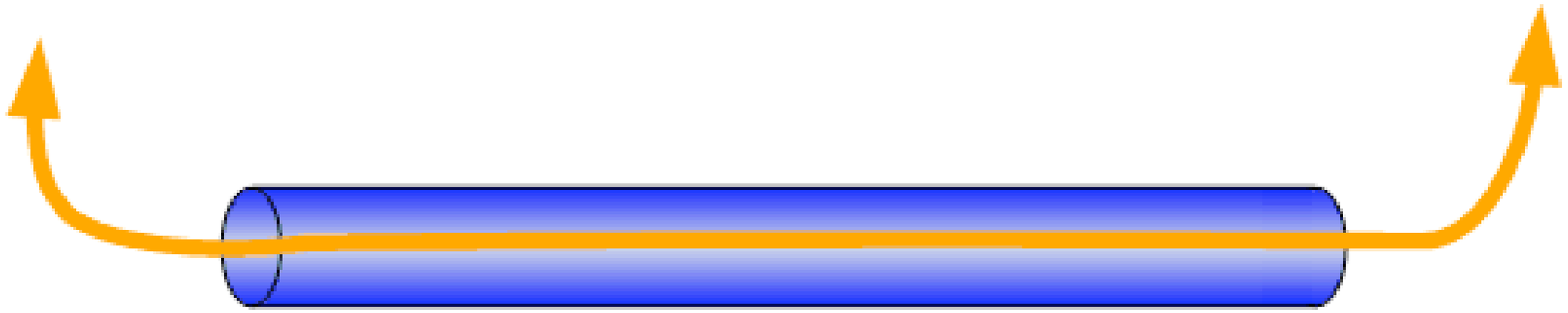
BSDCan 2007



VPNs are built using tunnels

BSDCan 2007



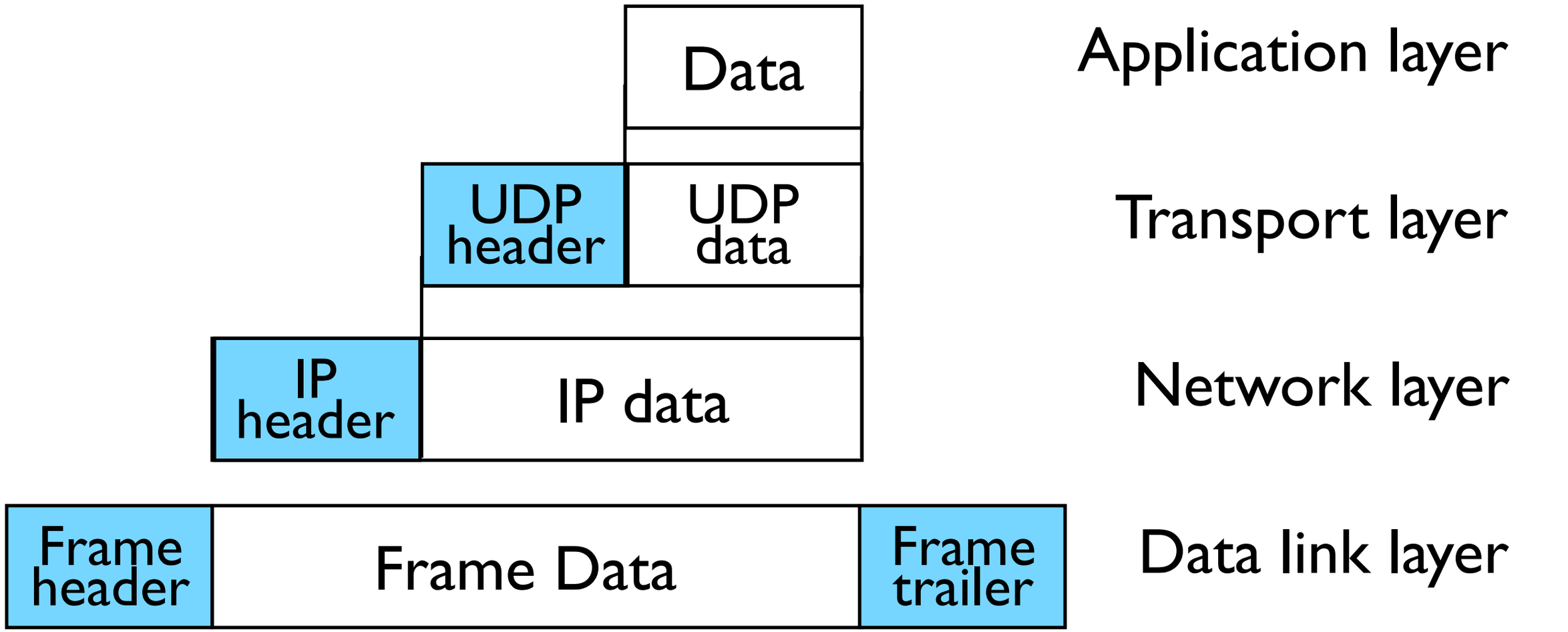


Encrypted traffic in VPN tunnel

BSDCan 2007

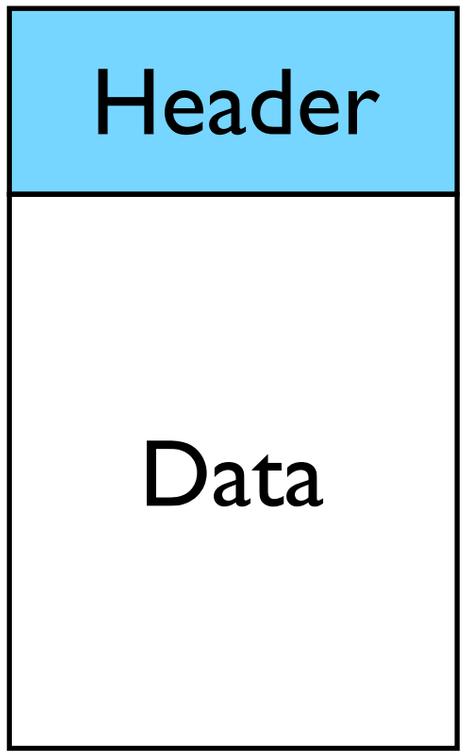
Encapsulation is something we are already used to

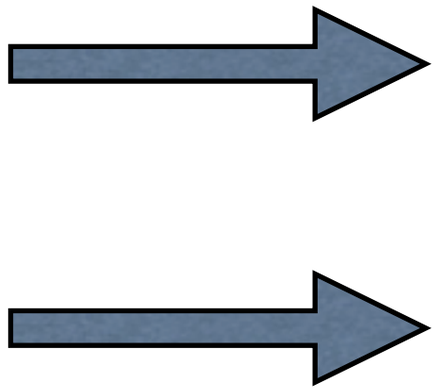
BSDCan 2007

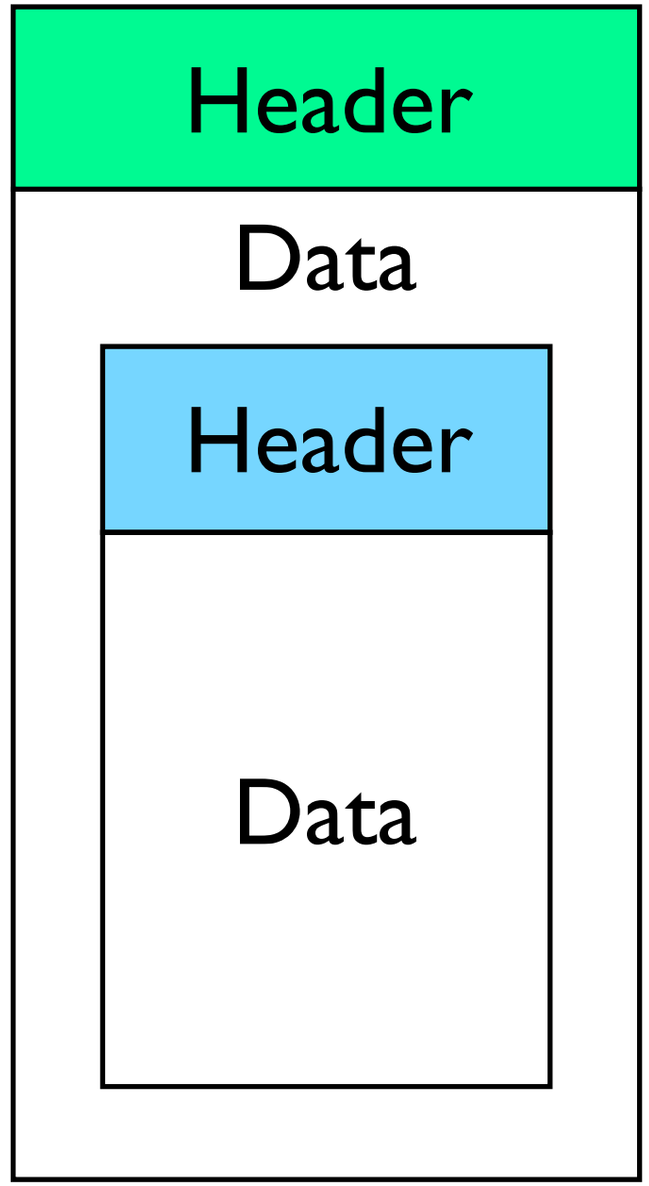

Data
UDP header
UDP data
IP header
IP data
Frame header
Frame Data
Frame trailer
Application layer
Transport layer
Network layer
Data link layer


BSDCan 2007

Tunnel Information







BSDCan 2007

Layer II encapsulations

PPTP

BSDCan 2007

RFC 2637 [1999]

BSDCan 2007

Point to **P**oint **T**unneling **P**rotocol

BSDCan 2007

BSDCan 2007

BSDCan 2007

Easy to configure

BSDCan 2007

ubiquitous

BSDCan 2007

but...

BSDCan 2007

according to:

BSDCan 2007


BSDCan 2007

“Microsoft PPTP is very broken, and there's no real way to fix it without taking the whole thing down and starting over. This isn't just one problem, but six different problems, any one of which breaks the protocol.”

BSDCan 2007

and according to Peter Mueller:

PPTP is known to be a faulty protocol. The designers of the protocol, Microsoft, recommend not to use it due to the inherent risks. Lots of people use PPTP anyway due to ease of use, but that doesn't mean it is any less hazardous. The maintainers of PPTP Client and Poptop recommend using OpenVPN (SSL based) or IPSec instead.

BSDCan 2007

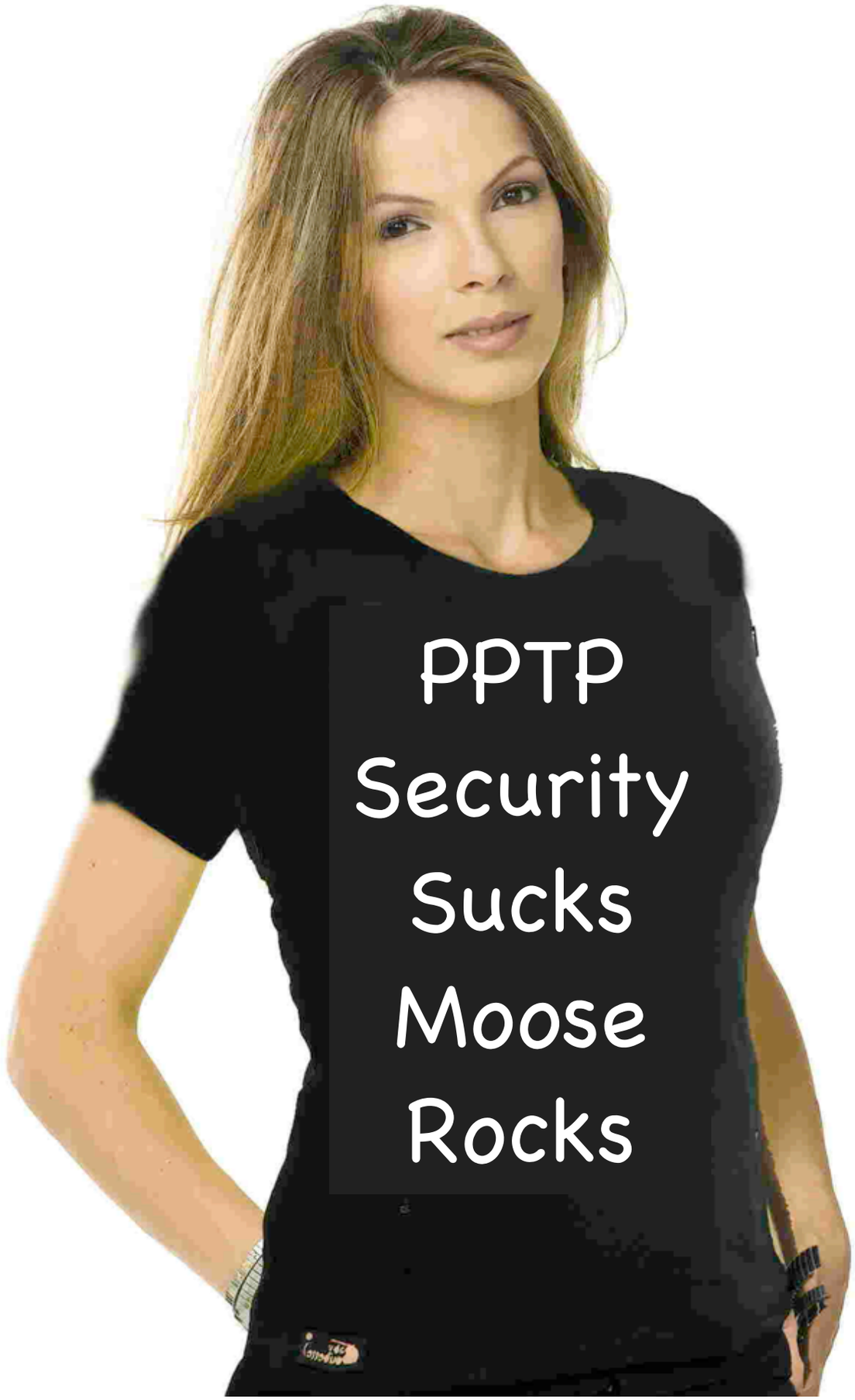
and finally

BSDCan 2007

according to:

BSDCan 2007

BSDCan 2007



BSDCan 2007

so maybe there is justice in the world

BSDCan 2007

L2TP

BSDCan 2007

Layer **2** **T**unneling **P**rotocol

BSDCan 2007

RFC 2661 [1999]

BSDCan 2007

L2TP v3

BSDCan 2007

RFC 3931 [2005]

BSDCan 2007

security added by IPsec

BSDCan 2007

L2TP/IPsec

BSDCan 2007

RFC 3193 [2001]

BSDCan 2007

difficult to set up on M$ clients

BSDCan 2007

Layer III encapsulations

BSDCan 2007

IPsec

BSDCan 2007

Suite of protocols

BSDCan 2007

RFCs 2401-2412 [1998]

BSDCan 2007

Implemented at the kernel level

BSDCan 2007

key exchange daemon

BSDCan 2007

OpenBSD : Kame + isakmpd

BSDCan 2007

OpenBSD 4.0 : added ipsecctl

BSDCan 2007

BSDCan 2007

FreeBSD, NetBSD : Kame + raccoon

BSDCan 2007

Linux : FreeSwan/OpenSwan + pluto

BSDCan 2007

Linux v2.6x: NetKey + isakmpd/raccoon

BSDCan 2007

Many commercial clients

BSDCan 2007

but...

BSDCan 2007

according to:

BSDCan 2007

BSDCan 2007

“Even though the protocol is a disappointment -- our primary complaint is with its complexity -- it is the best IP security protocol available at the moment.”

BSDCan 2007

Layer IV encapsulations

BSDCan 2007

SSL/TLS

BSDCan 2007

Secure **S**ocket **L**ayer

BSDCan 2007

Transport **L**ayer **S**ecurity Protocol

BSDCan 2007

RFC 2246 [1999]

BSDCan 2007

TLS v1.1

BSDCan 2007

RFC 4346 [2006]

BSDCan 2007

BSDCan 2007

BSDCan 2007

BSDCan 2007

BSDCan 2007

OpenVPN

BSDCan 2007

BSDCan 2007

according to:

BSDCan 2007

BSDCan 2007

BSDCan 2007

http://www.openvpn.net/

BSDCan 2007

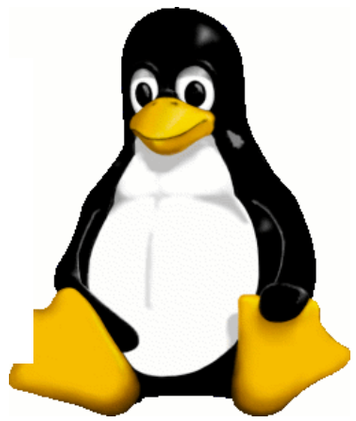
multi-platform

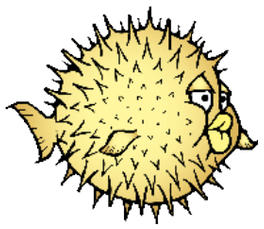
BSDCan 2007


NetBSD


Microsoft
Windows 2000


FreeBSD






OpenBSD


Microsoft
Windows xp


solaris


BSDCan 2007

economical

BSDCan 2007

free*

BSDCan 2007

* free as is in Dan Langille's extra lunch boxes

BSDCan 2007

tunnels either layer II or III traffic

BSDCan 2007

requires TUN or TAP devices

BSDCan 2007

NAT, Dynamic IP & firewall friendly

BSDCan 2007

certificate based asymmetric keying

BSDCan 2007

X509/PKI

BSDCan 2007

static symmetric keying

BSDCan 2007

UDP tunnels (standard)

BSDCan 2007

TCP tunnels (optional)

BSDCan 2007

road warrior

BSDCan 2007

host ⟷ network

BSDCan 2007

branch office to central office

BSDCan 2007

network ⟷ network

BSDCan 2007

simple configuration

BSDCan 2007

flexibility

BSDCan 2007

bags & bags of options

BSDCan 2007

support for 2X authentication

BSDCan 2007

GUIs for Windows and Mac OS X

BSDCan 2007

Rich suite of system logging

BSDCan 2007

BSDCan 2007

20k staff

BSDCan 2007

10k grad students

BSDCan 2007

Institutional Middle Ware

BSDCan 2007

Authentication : Kerberos

BSDCan 2007

Authorization : LDAP

BSDCan 2007

Identifier : UTORid

BSDCan 2007

VPN access required for remote access

BSDCan 2007

staff & grad students only

BSDCan 2007

> 90% clients are Windows users

BSDCan 2007

Sell the technocrats

BSDCan 2007

Unix + OpenVPN a preferred solution

BSDCan 2007

NSIS to aid Windows install

http://nsis.sourceforge.net/

BSDCan 2007


nullsoft scriptable install system


BSDCan 2007

pf firewall rules!

BSDCan 2007

```
# pf.conf for vpn.utoronto.ca - UTORvpn server
#
# $Id: pf.conf,v 1.1 2007/05/09 16:51:26 matt Exp matt $

int_if                  = bge0
ext_if                  = bge0
vpn_if                  = tun
internal_net            = "10.11.12.0/24"
protos                  = "{ tcp, udp }"
bad_ports               = "{ 42, 67:69, 135, 137:139,\
                             161:162, 445, 593,\
                             4444 }"
# table to hold dynamic list of hosts allowed to bypass #
windows port blocking
table <blessed> persist
table <vpn_net> { 10.11.12.192/29 }
set skip on lo0
scrub in all
```

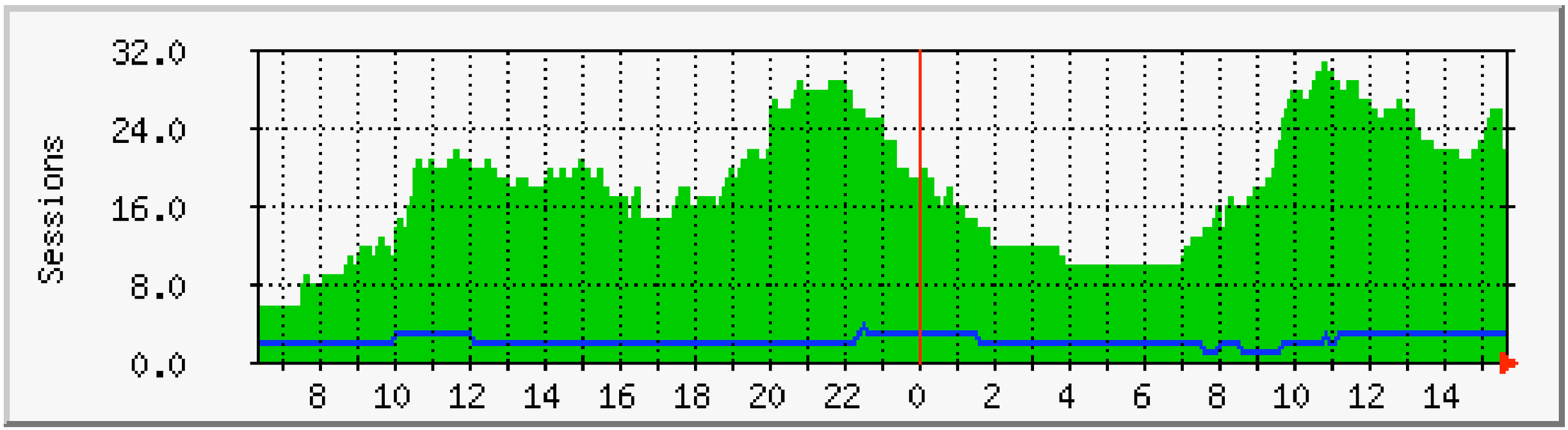
```
# Default is to block everything
block in log all

# Allow HTTP and HTTPS access from all hosts
pass  in quick on $ext_if proto tcp \
      from any to $ext_if port http keep state
pass  in quick on $ext_if proto tcp \
      from any to $ext_if port https keep state

# allow all UDP traffic coming in on UTORvpn ports
pass  in quick on $ext_if proto udp \
     from any to $ext_if port 1194:1196 keep state
pass  in quick on $ext_if proto udp \
     from any to $ext_if port 5000:5001 keep state
```

```
# Only allow VPN traffic from good ports or special addresses
# allow hosts in <blessed> table to use "bad" ports
pass  in quick on $vpn_if proto $protos \
     from <blessed> to any keep state

# block the bad ports on the tun interfaces
# but let everything else through
block in quick on $vpn_if proto $protos \
     from <vpn_net> port $bad_ports to any
block in quick on $vpn_if proto $protos \
     from <vpn_net> to any port $bad_ports
pass  in on $vpn_if proto $protos \
     from <vpn_net> to any keep state

# Allow all outgoing traffic
pass  out on $ext_if proto $protos \
     from $ext_if to any keep state
pass  out on $ext_if proto $protos \
     from <vpn_net> to any keep state
```

Logging tools

BSDCan 2007

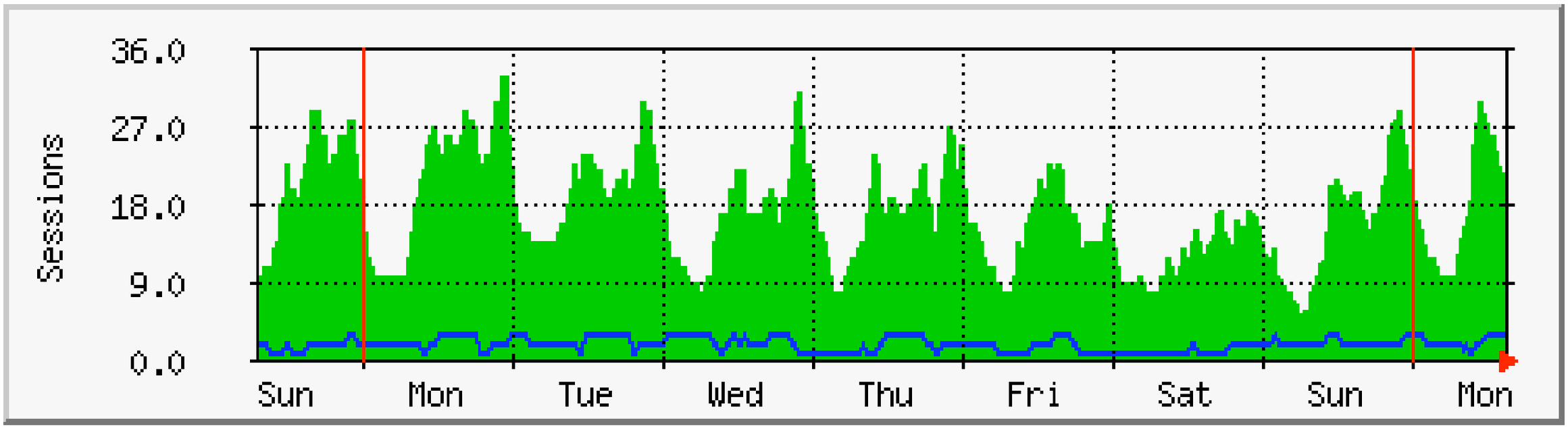
`Daily' Graph (10 Minute Average)



Max Sessions 31 Average Sessions 18 Current Sessions 22

Max Static 4 Average Static 2 Current Static 3

`Weekly' Graph (30 Minute Average)

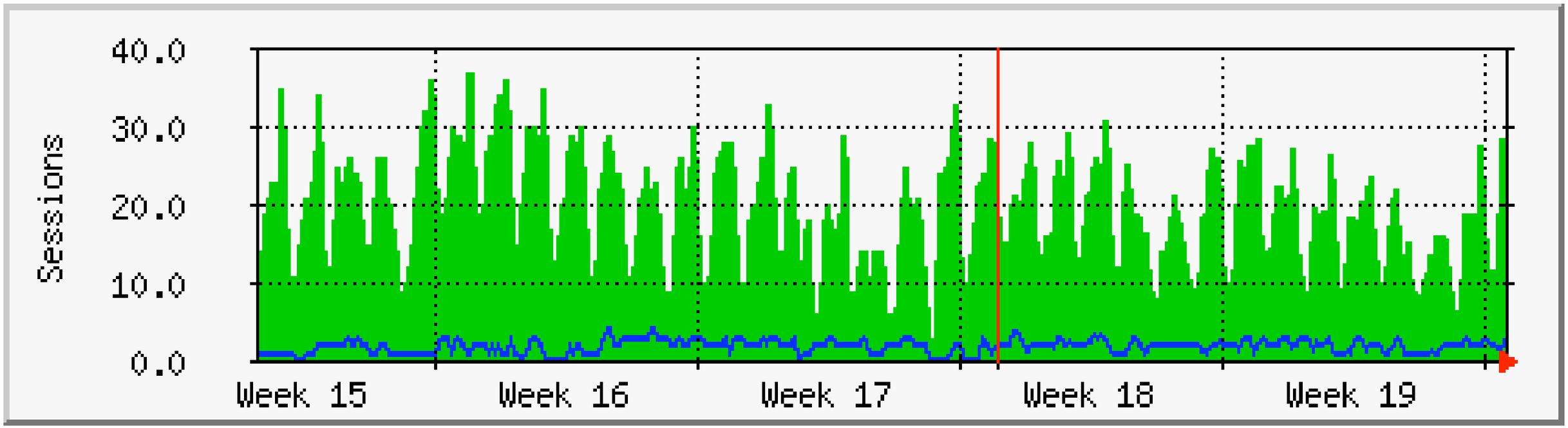


Max Sessions 33 Average Sessions 17 Current Sessions 22

Max Static 3 Average Static 2 Current Static 3

BSDCan 2007

`Monthly' Graph (2 Hour Average)

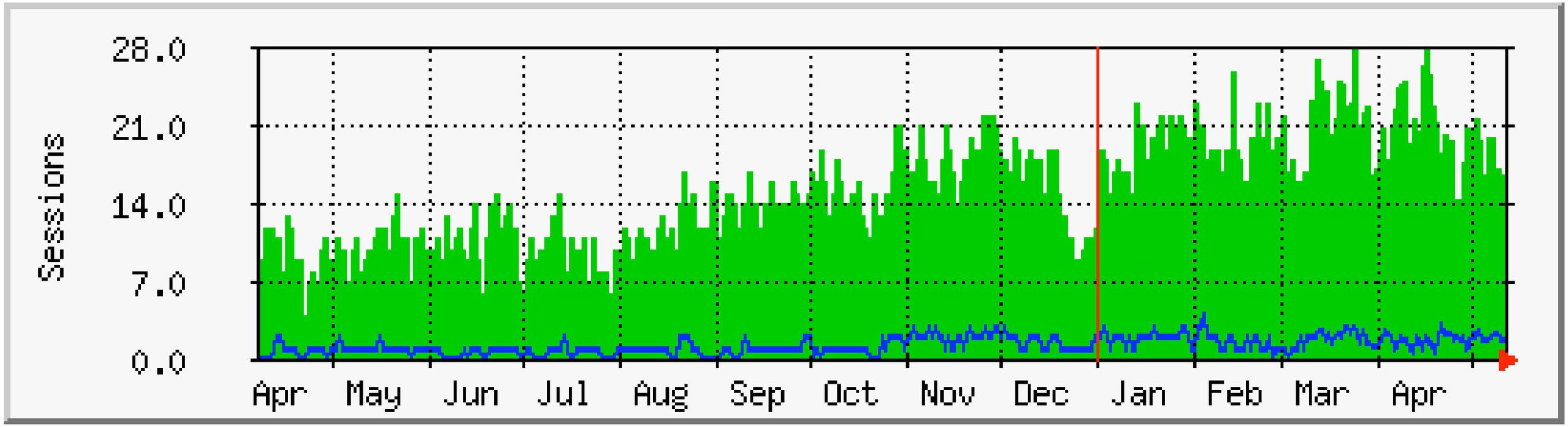


Max Sessions 37 Average Sessions 19 Current Sessions 25

Max Static 4 Average Static 2 Current Static 3

BSDCan 2007

`Yearly' Graph (1 Day Average)



Max Sessions 28 Average Sessions 15 Current Sessions 12

Max Static 4 Average Static 1 Current Static 1

BSDCan 2007

	Month	Num Sessions	Accounts		Total IN	Total OUT	Total Time
			To-date	Monthly			(hours)
	2004-12	323	117	117	889.80 MB	3.49 GB	1603
	2006-05	4467	788	29	8.09 GB	41.73 GB	7360
	2006-06	4750	829	41	10.38 GB	53.73 GB	7321
	2006-07	4889	868	39	10.73 GB	44.71 GB	7038
	2006-08	4720	915	47	21.36 GB	65.35 GB	9199
	2006-09	4430	988	73	19.93 GB	95.56 GB	9599
	2006-10	5289	1031	43	27.59 GB	146.75 GB	10975
	2006-11	5655	1118	87	20.54 GB	82.48 GB	13512
	2006-12	4821	1153	35	29.65 GB	78.21 GB	11983
	2007-01	5510	1196	43	24.69 GB	92.46 GB	14552
	2007-02	5301	1247	51	36.79 GB	110.41 GB	13807
	2007-03	6886	1281	34	28.64 GB	112.05 GB	16120
	2007-04	7694	1328	47	107.59 GB	147.20 GB	16038
	2007-05	2579	1347	19	9.69 GB	38.20 GB	5281
		98447	**1347**		**475.52 GB**	**1.44 TB**	**209884**

BSDCan 2007

Mac OS X + Windows Install & Demo

BSDCan 2007