UTORvpn
A Cross Platform Open Source SSL VPN Implementation

Russell Sutherland
University of Toronto
2007-05-18
What is a VPN?
Virtual Private Network
Virtual
Private
(Secure)
Network
VPNs are built using tunnels
Encrypted traffic in VPN tunnel
Encapsulation is something we are already used to
Application layer
Transport layer
Network layer
Data link layer
Tunnel Information

Header

Data

Header

Data

Header

Data
Layer II encapsulations
PPTP
RFC 2637 [1999]
Point to Point Tunneling Protocol
Easy to configure
ubiquitous
but...
according to:
“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.”
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.
and finally
according to:
PPTP
Security Sucks
Moose Rocks
so maybe there is justice in the world
L2TP
Layer 2 Tunneling Protocol
RFC 2661 [1999]
L2TP v3
RFC 3931 [2005]
security added by IPsec
L2TP/IPsec
difficult to set up on M$ clients
Layer III encapsulations
IPsec
Suite of protocols
RFCs 2401–2412 [1998]
Implemented at the kernel level
key exchange daemon
OpenBSD : Kame + isakmpd
OpenBSD 4.0 : added ipsecctl
FreeBSD, NetBSD : Kame + raccoon
Linux: FreeSwan/OpenSwan + pluto
Linux v2.6x: NetKey + isakmpd/raccoon
Many commercial clients
but...
according to:
“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.”
Layer IV encapsulations
SSL/TLS
Secure Socket Layer
Transport Layer Security Protocol
RFC 2246 [1999]
TLS v1.1
RFC 4346 [2006]
OpenVPN
according to:
The OpenVPN Logo Sucks
Moose Rocks
multi-platform
economical
free*
* free as is in Dan Langille’s extra lunch boxes
tunnels either layer II or III traffic
requires TUN or TAP devices
NAT, Dynamic IP & firewall friendly
certificate based asymmetric keying
X509/PKI
static symmetric keying
UDP tunnels (standard)
TCP tunnels (optional)
road warrior
host ←→ network
branch office to central office
network ⟷ network
simple configuration
flexibility
bags & bags of options
support for 2X authentication
GUIs for Windows and Mac OS X
Rich suite of system logging
20k staff
10k grad students
Institutional Middle Ware
Authentication : Kerberos
Authorization : LDAP
Identifier : UTORid
VPN access required for remote access
staff & grad students only
> 90% clients are Windows users
Sell the technocrats
Unix + OpenVPN a preferred solution
NSIS to aid Windows install
http://nsis.sourceforge.net/
nullsoft scriptable install system
pf firewall rules!
# 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 \}"
badm_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
`Daily' Graph (10 Minute Average)

Max Sessions 31  Average Sessions 18  Current Sessions 22
Max Static 4  Average Static 2  Current Static 3

BSDCan 2007
`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
<table>
<thead>
<tr>
<th>Month</th>
<th>Num Sessions</th>
<th>Accounts</th>
<th>Total IN</th>
<th>Total OUT</th>
<th>Total Time (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>To-date</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2004-12</td>
<td>323</td>
<td>117</td>
<td>889.80 MB</td>
<td>3.49 GB</td>
<td>1603</td>
</tr>
<tr>
<td>2006-05</td>
<td>4467</td>
<td>788</td>
<td>8.09 GB</td>
<td>41.73 GB</td>
<td>7360</td>
</tr>
<tr>
<td>2006-06</td>
<td>4750</td>
<td>829</td>
<td>10.38 GB</td>
<td>53.73 GB</td>
<td>7321</td>
</tr>
<tr>
<td>2006-07</td>
<td>4889</td>
<td>868</td>
<td>10.73 GB</td>
<td>44.71 GB</td>
<td>7038</td>
</tr>
<tr>
<td>2006-08</td>
<td>4720</td>
<td>915</td>
<td>21.36 GB</td>
<td>65.35 GB</td>
<td>9199</td>
</tr>
<tr>
<td>2006-09</td>
<td>4430</td>
<td>988</td>
<td>19.93 GB</td>
<td>95.56 GB</td>
<td>9599</td>
</tr>
<tr>
<td>2006-10</td>
<td>5289</td>
<td>1031</td>
<td>27.59 GB</td>
<td>146.75 GB</td>
<td>10975</td>
</tr>
<tr>
<td>2006-11</td>
<td>5655</td>
<td>1118</td>
<td>20.54 GB</td>
<td>82.48 GB</td>
<td>13512</td>
</tr>
<tr>
<td>2006-12</td>
<td>4821</td>
<td>1153</td>
<td>29.65 GB</td>
<td>78.21 GB</td>
<td>11983</td>
</tr>
<tr>
<td>2007-01</td>
<td>5510</td>
<td>1196</td>
<td>24.69 GB</td>
<td>92.46 GB</td>
<td>14552</td>
</tr>
<tr>
<td>2007-02</td>
<td>5301</td>
<td>1247</td>
<td>36.79 GB</td>
<td>110.41 GB</td>
<td>13807</td>
</tr>
<tr>
<td>2007-03</td>
<td>6886</td>
<td>1281</td>
<td>28.64 GB</td>
<td>112.05 GB</td>
<td>16120</td>
</tr>
<tr>
<td>2007-04</td>
<td>7694</td>
<td>1328</td>
<td>107.59 GB</td>
<td>147.20 GB</td>
<td>16038</td>
</tr>
<tr>
<td>2007-05</td>
<td>2579</td>
<td>1347</td>
<td>9.69 GB</td>
<td>38.20 GB</td>
<td>5281</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>98447</strong></td>
<td><strong>1347</strong></td>
<td><strong>475.52 GB</strong></td>
<td><strong>1.44 TB</strong></td>
<td><strong>209884</strong></td>
</tr>
</tbody>
</table>
Mac OS X + Windows Install & Demo