Npppd: easy vpn with OpenBSD

Giovanni Bechis
giovanni@openbsd.org

Institute of Biostructures and Bioimaging,
Napoli, Italy
Apr 6, 2013
A little presentation

- sysadmin and web developer at SnB, my own software house
- developer for OpenBSD
- every now and then, developer for some other open source software
The initial problem

- two offices and some people with their laptop who wish to use their main software remotely
The proposed solution

- the two offices has been connected to a Windows Server in a web farm with the terminal server connections protected by a vpn
Vpn software

- Vpn software that could be used for this setup on our OpenBSD firewall:
  - iked(8)
  - openvpn
  - poptop
  - npppd(8)
npppd(8) main features

- it is a PPP and tunneling daemon which supports PPTP, L2TP and PPPoE
- it can authenticate using a local file or a remote radius server
- it can use pipex(4) to accelerate ip packets forwarding
- it can use tun(4) or pppx(4) interfaces to tunnel packets
npppd(8) short story

- npppd(8) has been initially developed by IIJ
- it first appeared in OpenBSD 5.3
npppd(8) configuration

- the configuration file is /etc/npppd/npppd.conf
- the configuration file format has changed a lot during development
"Basic" npppd(8) configuration

authentication LOCAL type local {
    users-file "/etc/npppd/npppd-users"
}

tunnel PPTP_ipv4 protocol pptp {
    listen on 0.0.0.0
}

ipcp IPCP {
    pool-address 10.0.0.2-10.0.0.100
    dns-servers 192.168.0.254
}

interface pppx0 address 10.0.0.1 ipcp IPCP
bind tunnel from PPTP_ipv4 authenticated by LOCAL to pppx0
npppd-users(5) file format

alex:\n  :password=alex’s password:\n  :framed-ip-address=10.0.0.33:

john:\n  :password=John’s password:
"Advanced" npppd(8) configuration

```
authentication RADIUS type radius {
    authentication-server {
        address 192.168.0.1 secret "hoge hoge"
    }
}

tunnel L2TP_ipv4 protocol l2tp {
    listen on 0.0.0.0
}
 ipcp IPCP {
    pool-address 10.0.0.2-10.0.0.100
dns-servers 192.168.0.254
}

interface pppx0 address 10.0.0.1 ipcp IPCP
bind tunnel from L2TP_ipv4 authenticated by RADIUS to pppx0
```
l2tp setup

- to setup an l2tp tunnel you have to configure both npppd.conf and ipsec.conf
- your pf.conf setup should be changed accordingly
Ipsec setup for l2tp tunnels

public_ip = "1.2.3.4"
ike passive esp transport \
    proto udp from $public_ip to any port 1701 \
    main auth "hmac-sha1" enc "aes" group modp2048 \
    quick auth "hmac-sha1" enc "3des" \
    psk "mysecret"
Pf setup for l2tp tunnels

pass quick proto { esp, ah } from any to any
pass in quick on egress proto udp from any to any \
   port {500, 4500, 1701} keep state
pass on enc0 from any to any keep state (if-bound)
npppd monitoring

To monitor npppd vpn sessions you can use npppctl

```
# npppctl session all
Ppp Id = 18

  Ppp Id : 18
  Username : giovanni
  Realm Name : radius
  Concentrated Interface : tun1
  Assigned IPv4 Address : 192.168.255.205
  Tunnel Protocol : PPTP
  Tunnel From : 151.71.144.16:31342
  Start Time : 2013/02/04 11:35:24
  Elapsed Time : 131 sec (2 minutes)
  Input Bytes : 11256 (11.0 KB)
  Input Packets : 130
  Input Errors : 0 (0.0%)
  Output Bytes : 19241 (18.8 KB)
  Output Packets : 160
  Output Errors : 17 (9.6%)
```
npppd monitoring

If you use pppx(4) interfaces you can have some info from the ifconfig command too

# ifconfig pppx0
pppx0: flags=8051<UP,POINTOPOINT,_RUNNING,MULTICAST> mtu 1360
    description: giovanni
    priority: 0
    groups: pppx
    inet 192.168.255.1 --> 192.168.255.205 \ netmask 0xffffffff
npppd monitoring

As usual, with ipsec, ipsecctl is your friend

# ipsecctl -s all
FLOWS:
flow esp in proto udp from 9.2.71.195 port l2tp \
  to 192.168.2.250 port l2tp peer 9.2.71.195 \
  srcid 192.168.2.250/32 dstid 192.168.1.101/32 type use
flow esp out proto udp from 192.168.2.250 port l2tp \
  to 9.2.71.195 port l2tp peer 9.2.71.195 \
  srcid 192.168.2.250/32 dstid 192.168.1.101/32 type require

SAD:
esp transport from 192.168.2.250 to 9.2.71.195 \
  spi 0x41f46e6a auth hmac-sha1 enc aes
esp transport from 9.2.71.195 to 192.168.2.250 \
  spi 0x6d7d8716 auth hmac-sha1 enc aes
Vpn gui interface
Vpn gui interface

Wednesday, 20 February 2013, 18:45:10 CET

<table>
<thead>
<tr>
<th>#</th>
<th>user</th>
<th>ip address</th>
<th>callerid</th>
<th>name</th>
<th>duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>giovanni</td>
<td>192.368.255.205</td>
<td>-</td>
<td>Giovanni Bechis</td>
<td>00:11:06</td>
</tr>
</tbody>
</table>
Vpn gui interface
Microsoft tips and Microsoft bugs

Microsoft, dns, kerberos and mtu
Microsoft tips and bugs

ipsec nat-t support

Windows Registry Editor Version 5.00

[HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent]
"AssumeUDPEncapsulationContextOnSendRule"=dword:00000002
npppd future

- fixing bugs
- better integration with pf
- arp cache support
Thank you for your attention!

Questions?