

Npppd: easy vpn with OpenBSD

Giovanni Bechis
giovanni@openbsd.org



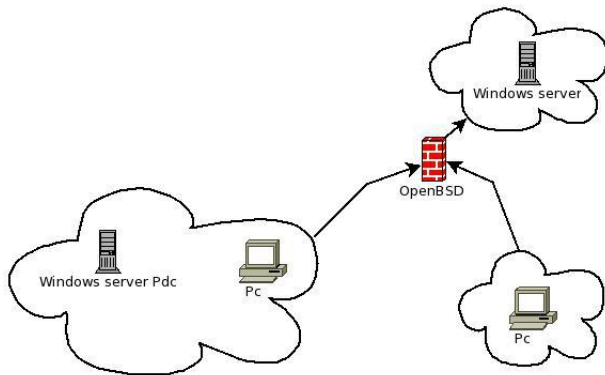
Institute of Biostructures and Bioimaging,
Napoli, Italy
Apr 6, 2013

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 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 IJ
- ▶ 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

npppd.conf(5)

"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)

npppd-users(5) file format

```
alex:\
    :password=alex's password:\
    :framed-ip-address=10.0.0.33:
john:\
    :password=john's password:
```

npppd.conf(5)

"Advanced" npppd(8) configuration

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

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
```

I2tp setup

- ▶ to setup an I2tp tunnel you have to configure both npppd.conf and ipsec.conf
- ▶ your pf.conf setup should be changed accordingly

ipsec.conf(5)

Ipssec 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.conf(5)

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 nppctl

```
# nppctl 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
```

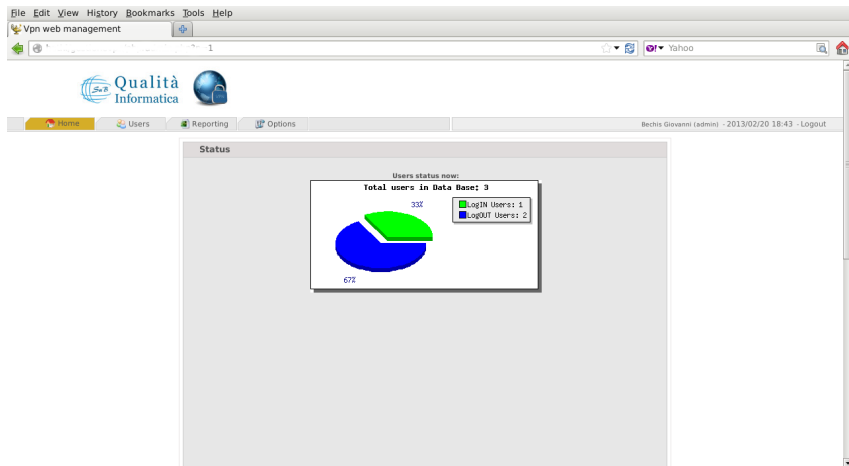
```
FLAWS:
```

```
flow esp in proto udp from 9.2.71.195 port 12tp \  
  to 192.168.2.250 port 12tp 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 12tp \  
  to 9.2.71.195 port 12tp 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

File Edit View History Bookmarks Tools Help

Vpn web management

Qualità Informatica

Home Users Reporting Options

Bechis Giovanni (admin) - 2013/02/20 18:45 - Logout

Reporting
Online users
Accounting
Global Stats
User Stats

Online Users

localhost
localhost

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

1 users connected unknown free lines

#	user	ip address	callerid	name	duration
1	giovanni	192.168.255.205	-	Giovanni Bechis	00:11:06

Vpn gui interface

The screenshot displays the Vpn web management interface. At the top, there is a menu bar with 'File', 'Edit', 'View', 'History', 'Bookmarks', 'Tools', and 'Help'. Below the menu is a search bar containing 'Vpn web management'. The browser's address bar shows 'http://localhost:8080/'. The page header includes the 'Qualità Informatica' logo and a navigation bar with 'Home', 'Users', 'Reporting', and 'Options'. The user is identified as 'Bechis Giovanni (admin) - 2013/02/20 18:48 - Logout'.

On the left side, there are two sidebar menus: 'Users' (Add, Find, Edit, Failed logins, Bad users) and 'Groups' (Add, Edit).

The main content area features a 'Subscription Analysis for giovanni' section. It contains a table with columns: #, logged in, session time, upload, download, server, terminate cause, and callerid. The table lists five sessions from 2013-02-20 to 2013-02-21. A summary row at the bottom of the table shows a total session time of 24 minutes and 8 seconds, with a total upload of 109.23 KBs and a total download of 52.22 KBs.

Below the table, there are search filters for 'user' (giovanni), 'from date' (2013-02-13), 'to date' (2013-02-21), 'pagesize' (10), and 'order' (recent first). A 'show' button is also present. A note explains that the 'from date' matches any login after the 00:00 of that day, and the 'to date' any login before the 23:59 of that day.

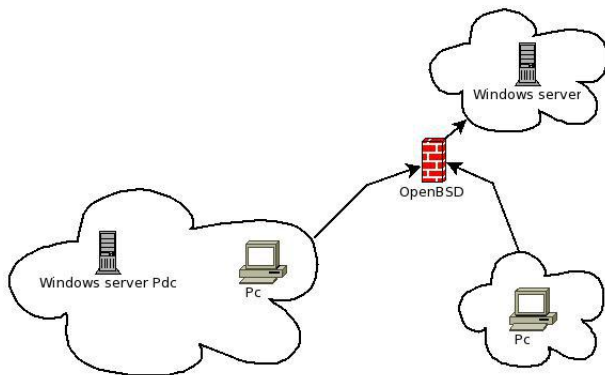
	SHOW	EDIT	USER INFO				
	ACCOUNTING	BADUSERS	DELETE	TEST			
	OPEN SESSIONS						
2013-02-13 up to 2013-02-21							
#	logged in	session time	upload	download	server	terminate cause	callerid
1	2013-02-20 18:34:04	14 minutes, 30 seconds	28.74 KBs	3.63 KBs	localhost:0	User-Request	-
2	2013-02-15 13:35:25	2 minutes, 46 seconds	26.16 KBs	43.53 KBs	localhost:0	User-Request	-
3	2013-02-13 18:13:49	1 minutes, 25 seconds	21.18 KBs	1.51 KBs	localhost:2	User-Request	-
4	2013-02-13 18:06:21	14 seconds	11.65 KBs	1.09 KBs	localhost:1	User-Request	-
5	2013-02-13 17:59:33	5 minutes, 13 seconds	21.51 KBs	2.46 KBs	localhost:0	User-Request	-
Page Total		24 minutes, 8 seconds	109.23 KBs	52.22 KBs			

user: giovanni from date: 2013-02-13 to date: 2013-02-21 pagesize: 10 order: recent first show

the from date matches any login after the 00:00 that day, and the to date any login before the 23:59 that day. the default values shown are the current week.

Microsoft tips and Microsoft bugs

Microsoft, dns, kerberos and mtu



Microsoft tips and bugs

ipsec nat-t support

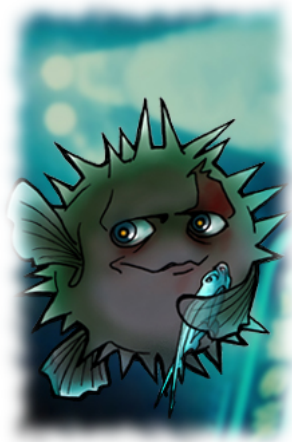
Windows Registry Editor Version 5.00

```
[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?