# ng_natを使用してみました。

Echigo BSD Users Group
神保道夫(karl@jp.freebsd.org)

## きっかけ

- 2006/02/14に、Bフレッツハイパーファミリーが開通したのに伴い、ネットワークの配線をーからやり直したら、フレッツ・スクウェアで10Mしか出ないので、チューニングの方法を探していたところ、rushaniさんから、ng_natはどうですか？ と勧められたので、使ってみた。

## ng_natとは?

- 従来の/usr/sbin/natdなどは、NAT対象のパケットを、8668番のポートにdivertして処理していた。
- それに対し、ng_natは、カーネル内部に in と out の フックを作り ipfw で対象パケットをこのフックに送るように したようだ。そして、カーネル上でNAT処理している。

## ng_natを使える環境は？

- ng_natは、FreeBSD 6.0より登場した機能なので、最新のFreeBSD 6(RELENG_6_0あるいはRELENG_6)を使う必要がある。

# どうやって使うの?(1)

- とりあえず、man ng_natしてみる。
- ng_ipfw(4)が必要と書いてある。今回は、更にローダブルカーネルモジュールを使う事にもチャレンジしたので、以下のように設定してみた。
- /boot/loader.conf
  ng_ipfw_load="YES"
  ng_nat_load="YES"

# どうやって使うの?(2)

- /etc/rc.confでは、firewallはopen状態に設定しているので、とりあえずmanに従って、/etc/rc.firewallに以下のように書いてみた。
- case ${firewall_type} in
  [Oo][Pp][Ee][Nn])
  setup_loopback
  /usr/sbin/ngctl mkpeer ipfw: nat 60 out
  /usr/sbin/ngctl name ipfw:60 nat
  /usr/sbin/ngctl connect ipfw: nat: 61 in
  /usr/sbin/ngctl msg nat: setaliasaddr 210.229.X.Y
  ${fwcmd} add 400 netgraph 61 ipv4 from any to any in via re0
  ${fwcmd} add 500 netgraph 60 ipv4 from any to any out via re0
  /sbin/sysctl net.inet.ip.fw.one_pass=0
  ${fwcmd} add 65000 pass all from any to any
  ;;

## どうやって使うの?(3)

- /etc/rc.confには、通常のNATの使い方と同じように、
  gateway_enable="YES"
  firewall_enable="YES"
  firewall_type="open"
  を書く。ただし、当然ながら、
  natd_enable="NO"
  にする。

## 注意点

- 私の家では、IPv4/IPv6を両方使っているため、netgraphの60/61に落とすパケットをIPv4だけにしないと、同一LAN上のIPv6マシンと通信できなかった。/usr/sbin/natdでも同じ問題を抱えているため、今後改善されると思われる。

## おまけ

- ipfw及びipdivertもローダブルモジュールで起動するようにしてみました。
  /boot/loader.confに、
  ipfw_load="YES"
  ipdivert_load="YES"
  を書き、カーネルはGENERICのまま使えばよい。

## natdとng_natのパフォーマンス

- Sempron 2600+,512M memory, 外側:rl0(オンボード), 内側:de0のマシンで、フレッツ・スクウェアで速度を測定してみた。
- Bフレッツの標準的なチューニング(フレッツでの推奨RWIN値)を使って測定してみたが、パフォーマンスに特に変わりはなかった。従って、100M程度のネットワークでは、どちらでも十分な速度が出る。

## ng_natでできないこと

- ng_natでは、単純なNATに関しては問題がないが、例えばnatdのredirect_portなど、natdに依存している機能は当然ながら使えない。
- マニュアルとなる資料がまだ少ないから、ng_natの本当の実力はまだ未知数である。

## まとめ

- 単純なNAT機能を使うだけであれば、natdを使っても、ng_natを使っても問題がない。ただし、凝ったことをやろうとすると、natdの方が融通が利くので便利かもしれない。
- ユーザーの用途に合わせて、選択するのが良いと思う。

## 速度激減の原因

- フレッツ・スクウェアで、10Mしか出なかったのは、使っていたケーブルが不良でした。ケーブルを変えたら、60M～80M位出るようになりました･･･
- でもまだ3Mしか出ないマシンもあります。WindowsのNode Typeの問題のようで、テーマからは外れるのでパスします。

## 参考サイト

- nyanさんのページ
  http://www.furiru.org/~nyan/unix/ng_nat.html
- 私とほぼ同じような内容のページですが、もうちょっとスマートな形で実現しているので、こちらを参照していただくとよろしいと思います。