はじめに

いわゆる ipf のメモ。

日本語の情報

みんな探すと思うんだけど、悲しいことに ipf-howto の日本語訳はない。

ipf のソースをとってきて展開すると、その中に IPF.KANJI(IP filter ショートガイド) というドキュメントがあり、これがまとまった日本語の情報としては唯一といっていいものだった。

最近では、あちこちの Web にちらほらみかけるが、まとまったものとしては、稚内北星学園大学のサマースクールのテキストらしい「フィルタリング」が、よくできていると思うので、上記 IPF.KANJI と一緒に読もう。

てっとりばやく、NAT 環境をつくる

- 下記、NAT の中の環境を、10.1.2.0/24 とする。
- 下記、外側のインターフェースを re0 とする。
- 下記、内側のインターフェースを re1 とする。

NetBSD の場合

パケットフォワードがデフォルトでは有効になっていないので、有効にしよう。

```
net.inet.ip.forwarding=1
```

を /etc/sysctl.conf に書く。

つぎに、NAT とパケットフィルタの設定。ipf で関係するのは /etc/defaults/rc.conf のこの部分。

```
ipfilter=NO             ipfilter_flags=""       # uses /etc/ipf.conf
ipnat=NO                                        # uses /etc/ipnat.conf
ipfs=NO                 ipfs_flags=""           # save/load ipnat and ipf states
ipmon=NO                ipmon_flags="-Dns"      # syslog ipfilter messages
```

とりあえず使いたかったら、上二つを YES にする。/etc/rc.conf に、書く。

```
ipfilter=YES
ipnet=YES
```

フィルターを /etc/ipf.conf に書く。別になにも書かなくてもよいけど、最低限のサンプルをつくる perl スクリプトがあるので、それを使ってもよい。(perl をインストールしていない場合は、まずインストールしてから。)

```
# perl /usr/share/examples/ipf/mkfilters | grep -v inet6 | tee /etc/ipf.conf
block in log quick from any to any with ipopts
block in log quick proto tcp from any to any with short
pass out on re0 all head 150
block out from 127.0.0.0/8 to any group 150
block out from any to 127.0.0.0/8 group 150
pass in on re0 all head 100
block in from 127.0.0.0/8 to any group 100
pass out on re1 all head 250
block out from 127.0.0.0/8 to any group 250
```

```
block out from any to 127.0.0.0/8 group 250
pass in on re1 all head 200
block in from 127.0.0.0/8 to any group 200
```

NAT の設定を /etc/ipnat.conf に書く。

```
map re0 10.1.2.0/24 -> 0.0.0.0/32 proxy port ftp ftp/tcp
map re0 10.1.2.0/24 -> 0.0.0.0/32 portmap tcp/udp 40000:60000
map re0 10.1.2.0/24 -> 0.0.0.0/32
```

再起動したら、使えるようになっているはず。

もうちょっとちゃんとした情報が欲しい人は、こっちも読んでみてね。

- NetBSD Guide Configuring IPFILTER.
- NetBSD Guide Configuring IPNAT.
- /usr/share/examples/ipf の下にあるサンプル（BASIC-NAT と nat-setup をまずどうぞ）

FreeBSD の場合

パケットフォワードがデフォルトでは有効になっていないので、有効にしよう。

```
gateway_enable="YES"
```

を /etc/rc.conf に書く。

つぎに、NAT とパケットフィルタの設定。ipf で関係するのは /etc/defaults/rc.conf のこの部分。

```
ipfilter_enable="NO"            # Set to YES to enable ipfilter functionality
ipnat_enable="NO"               # Set to YES to enable ipnat functionality
ipmon_enable="NO"               # Set to YES for ipmon; needs ipfilter or ipnat
ipfs_enable="NO"                # Set to YES to enable saving and restoring
```

とりあえず使いたかったら、上二つを YES にする。/etc/rc.conf に、書く。

```
ipfilter_enable="YES"
ipnat_enable="YES"
```

フィルターを /etc/ipf.rules に書く。別になにも書かなくてもよいけど、最低限のサンプルをつくる perl スクリプトがあるので、それを使ってもよい。（perl をインストールしていない場合は、まずインストールしてから。）

```
# perl /usr/share/examples/ipfilter/mkfilters | grep -v inet6 > /etc/ipf.rules
```

NAT の設定を /etc/ipnat.rules に書く。

```
map re0 10.1.2.0/24 -> 0.0.0.0/32 proxy port ftp ftp/tcp
map re0 10.1.2.0/24 -> 0.0.0.0/32 portmap tcp/udp 40000:60000
map re0 10.1.2.0/24 -> 0.0.0.0/32
```

再起動したら、使えるようになっているはず。

もうちょっとちゃんとした情報が欲しい人は、こっちも読んでみてね。

- FreeBSD Handbook The IPFILTER (IPF) Firewall.
- /usr/share/examples/ipfilter の下にあるサンプル（BASIC-NAT と nat-setup をまずどうぞ）

OpenBSD の場合

ipf はなくなりました。

DragonFly BSD の場合

ipf はなくなりました。