FreeBSDでProxyServer

Echigo BSD Users Group(EBUG)
神保道夫(@karl0204)

HTTP Proxy Serverとは？

- 改めて紹介するほどでもないかもしれませんが、Webサイトをアクセスする際に、自ホストから直接アクセスするのではなく、代理でアクセスしてくれるサーバーの事。
- NATがない時代に、Firewallサーバーの上で動かしたり、コンテンツキャッシュを目的として使ってみたり。
- 某所では、まだ学校向けにフィルタリングサービスとして使っていたりするのかな？

なんで今更Proxy Server？

- なんとなく、です(笑)
- squid って、まだ生き残っているのかなぁ、とか、新しいProxy Serverってあるのかなぁ、と、ほとんどネタ的調査です。
- 今回は、squidと、trafficserverを取り上げてみます。

squid(1)

- 10年ほど前に使ってみたことがあり。
- transparent proxy(透過Proxy)機能ってのがあり、ユーザーにProxyを利用していることを意識せずに、コンテンツキャッシュを行うことができる機能があります。
- ルーターの設定で、任意の80番ポートへのアクセスをハイジャックしてsquidのポート(3128とか)に転送すると、squidが代わりにサイトにアクセスし、結果をクライアントに戻します。
- CISCOのルーターの機能を使ったり、FreeBSDならpf / IPFilterを使うのがお手軽。

squid(2)

- squid 3.1.19がportsに入っているので、「Enable transparent proxying with PF」もしくは「Enable transp. proxying with IPFilter」にチェックをつけてコンパイルすると、transparent proxyが有効になります。
- /etc/pf.conf に、以下のような行を追記しておけば、port 80へのアクセスをハイジャックしてsquidに転送してくれます。
  記載の際は、オープンプロキシにならないように注意！

```
nat on re0 from 192.168.0.0/16 to any -> re0
rdr on re1 proto tcp from 192.168.0.0/16  to any port 80 -> 210.229.xx.xxx port 3128
block in quick on re0 proto tcp from any to 210.229.xx.xxx port 3128
```

- ちなみに、rdrの行を、localhost 3128と書くとダメみたいですね・・・。

squid(3)

- /usr/local/etc/squid/squid.conf に、transparent proxyや、通常のproxyの設定を記述します。

  http_port 3128 intercept
  cache_mem 1024 MB
  cache_dir diskd /var/squid/cache 2048 16 256

- transparent proxyの設定は、squid 3.1から”intercept”に名称変更されたみたいですね。ネット上には、古い資料が一杯あるので注意です。

squid(4)

- squidは、/dev/pfをアクセスしますが、/usr/local/sbin/squidは、owner squid, group squidで動いているので、/dev/pfにアクセスできません。
- よって、
  /etc/groupの、operatorにsquidを加える
  /dev/devfs.confに
  own　pf root:operator
  perm pf 0640
  を記述し、/etc/rc.d/devfs restart を実行
  の様な対応が必要かも。
- 動き出したら、適宜、/usr/local/sbin/squid –k rotateを実行し、ログをローテートしましょう。

squid(5)

- これで動くと思いきや、全く実用にならない・・・。/var/log/messagesに、
  Squid Parent: child process 26610 started
  Squid Parent: child process 26610 exited due to signal 6 with status 0
  pid 26610 (squid), uid 100: exited on signal 6 (core dumped)
  が大量に。/var/log/squid/cache.logにも、
  storeDiskdSend: msgsnd: (35) Resource temporarily unavailable
  storeDiskdSend CREATE: (35) Resource temporarily unavailable
  storeDiskdSend: msgsnd: (35) Resource temporarily unavailable
  が大量に。調べてみると、おまじないで、/boot/loader.conf に以下の記述をしろ、と。
  kern.ipc.msgmnb=8192
  kern.ipc.msgmni=40
  kern.ipc.msgseg=512
  kern.ipc.msgssz=64
  kern.ipc.msgtql=2048
- sysctl -a とかで見て、必要な設定を加えましょう。うちはこれで安定稼働しました。

TrafficServer(1)

- 現在公開されているTrafficServerは、Yahoo!で使用していたProxy Serverの機能をオープンソース化して公開したもの。
- 元々は、Inktomi社によって開発されたが、のちにYahoo! 社が買収して利用。
- 現在は、ApacheのサイトにSVNリポジトリが置かれ、ソースコードを取得できる。
- FreeBSDのportsから、trafficserver 3.0.2がインストールできる(2012/02/11現在)

TrafficServer(2)

- portsからインストールして、以下の設定をすれば、使えるようになります。
- /usr/local/etc/trafficserver/records.config
  LOCAL proxy.local.incoming_ip_to_bind STRING 192.168.4.2
  CONFIG proxy.config.url_remap.remap_required INT 0
  CONFIG proxy.config.reverse_proxy.enabled INT 0
- 元々のTrafficServerは、Reverse Proxyとして動作するようになっています。通常の利用形態では、ReverseProxyはないと思われますので、OFFにしてください(そうしないと、サイトが見つからない旨のエラーが表示される)。
- 更に、以下の設定に変更すると便利かもしれないです(ログをASCII形式で出力する)。
  CONFIG proxy.config.log.squid_log_is_ascii INT 1
  CONFIG proxy.config.log.common_log_is_ascii INT 1
  CONFIG proxy.config.log.extended_log_is_ascii INT 1
  CONFIG proxy.config.log.extended2_log_is_ascii INT 1
- TrafficServerは、Transparent Proxyではないので、ブラウザのProxyの設定を変更するか、proxy.pac を自動配布するように設定してください。

TrafficServer(3)

- もしかして、
  WARNING: connection throttle too high, 30000 (throttle) + 192 (internal use) > 16384 (file descriptor limit), using throttle of 16192
  のようなメッセージが出るかもしれません。
- その場合、
  sysctl –w kern.maxfilesperproc=32000
  を実行してください。

細かい設定は・・・

- squidは、以下のサイトを参考に。
  http://www.squid-cache.org/
  http://wiki.squid-cache.org/
- TrafficServerは、以下のサイトを参考に。
  http://trafficserver.apache.org/
  https://cwiki.apache.org/confluence/display/TS/Traffic+Server