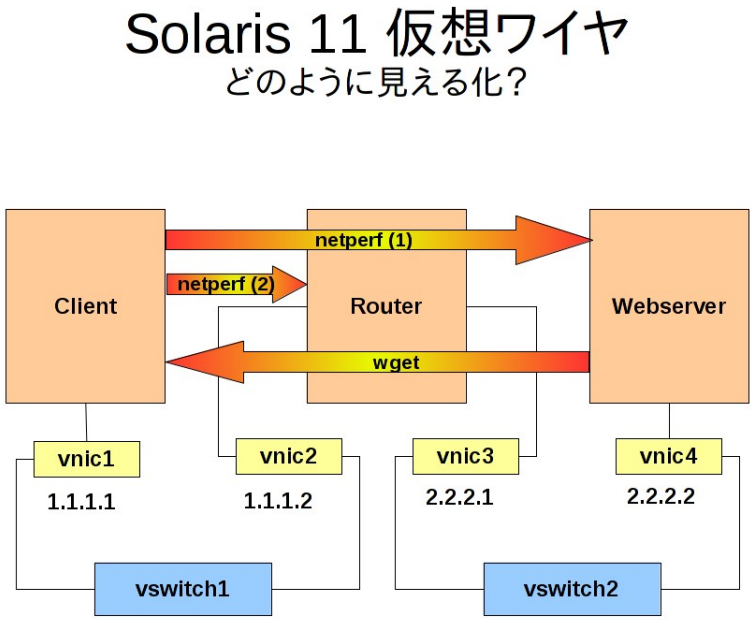
Solaris 3 分クッキング: レシピ 第 21 巻　仮想ワイヤ で ipfilter のデモ

更新日	2012/06/15　shoji.haraguchi@oracle.com
難易度/危険度	★☆☆☆☆/★★★☆☆
root 権限の必要性	有り

<仕込み>
　第 20 巻仮想ワイヤどのように見える化？の環境をそのまま利用します



<デモ>

```
$ sudo zlogin router ipadm show-addr
$ sudo zlogin router svcs ipfilter:default
```

デフォルトでは /etc/ipf/ipf.conf には何も記述されておりません。

```
$ sudo zlogin router cat /etc/ipf/ipf.conf
$ sudo zlogin router ipfstat -io
```

Router の /etc/ipf/ipf.conf に下記を追記する。

```
# Allow in/out Loopback
pass out quick on lo0
pass in quick on lo0

# Allow port 80(http)
pass out quick proto tcp from any to any port = 80 keep state
pass out quick proto udp from any to any port = 80

# Deny out on vnic3 all
block out log on vnic3 all
#block in log on vnic3 all
```

Ipfilter サービスの設定　/etc/ipf/ipf.conf の内容を取り込むように設定

```
$ sudo zlogin router svccfg -s ipfilter:default listprop
$ sudo zlogin router svccfg -s ipfilter:default setprop
firewall_config_default/policy = astring: "custom"
$ sudo zlogin router svccfg -s ipfilter:default setprop
firewall_config_default/custom_policy_file = astring:
"/etc/ipf/ipf.conf"
```

ipfilter サービスの有効化

```
$ sudo zlogin router svcadm refresh ipfilter:default
$ sudo zlogin router svcadm enable ipfilter:default
$ sudo zlogin router ipfstat -io
```

Netperf 1.1.1.1 → 2.2.2.2 のすべてのパケットは全てブロックされますが、http のパケット 2.2.2.2 → 1.1.1.1 はパスされていること確認することができます。

<参考資料>
Oracle Solaris の管理 (IP フィルタ)
http://docs.oracle.com/cd/E26924_01/html/E25872/ipfilter-admin-1.html