@branch.dreaminfo.biz 방화벽 설정

echo “201 mark1” >> /etc/iproute2/rt_tables

vim /etc/rc.local

```
14 ip rule add fwmark 1 table mark1
15 ip route add default via 10.0.0.1 table mark1
16 iptables -t mangle -A PREROUTING -s 192.168.1.0/24 -j MARK --set-mark 1
17
```

@hq.dreaminfo.biz 방화벽 설정

```
 2 iptables -F
 3 iptables -t nat -F
 4 iptables -P INPUT DROP
 5 iptables -P FORWARD DROP
 6 #########   NAT   ############
 7 iptables -t nat -A POSTROUTING -s 172.16.0.1/32 -j SNAT --to 108.96.58.1
 8 iptables -t nat -A POSTROUTING -s 172.16.0.2/32 -j SNAT --to 108.96.58.2
 9 iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o eth0 -j MASQUERADE
10 iptables -t nat -A PREROUTING -d 108.96.58.1/32 -j DNAT --to 172.16.0.1
11 iptables -t nat -A PREROUTING -d 108.96.58.2/32 -j DNAT --to 172.16.0.2
12 ######## INPUT ########
13 iptables -A INPUT -s 10.0.0.0/30,192.168.0.0/16,172.16.0.0/24,108.96.58.0/24 -j ACCEPT
14 iptables -A INPUT -p gre -j ACCEPT
15 iptables -A INPUT -p esp -j ACCEPT
16 iptables -A INPUT -p ospf -j ACCEPT
17 ######### 192.168.1.0/24 <-> 172.16.0.0/24 <-> 192.168.0.0/24 #########
18 iptables -A FORWARD -s 172.16.0.0/24,192.168.1.0/24 -d 192.168.0.0/24 -m state --state ESTABLISH
   ED,RELATED -j ACCEPT
19 ###############     ICMP    ##################################################
20 iptables -A FORWARD -s 172.16.0.0/24,192.168.0.0/16 -p icmp --icmp-type 8 -j ACCEPT
21 iptables -A FORWARD -s 95.201.100.0/24,108.96.58.0/24,114.204.56.0/24 -p icmp --icmp-type 0 -j A
   CCEPT
22 ###################   IN <-> OUT  ####################################
23 iptables -A FORWARD -s 192.168.1.0/24,172.16.0.0/24 -j ACCEPT
24 iptables -A FORWARD -s 95.201.100.0/24,114.204.56.1/32 ! -p icmp -j ACCEPT
25 ###################   MAIL RELAY  ############
26 iptables -A FORWARD -d 108.96.58.2 -p tcp -m multiport --dport 465 -j ACCEPT
27 iptables -A FORWARD -d 108.96.58.2 -p udp -m multiport --dport 465 -j ACCEPT
```

_____ 위에 껒 여 하지마 하지마 위에 하지;마----------

아래가 진리

```
#!/bin/sh -e
iptables -F
iptables -t nat -F
iptables -P INPUT DROP
iptables -P FORWARD DROP
#########   NAT   #############
iptables -t nat -A POSTROUTING -s 172.16.0.1/32 -j SNAT --to 108.96.58.1
iptables -t nat -A POSTROUTING -s 172.16.0.2/32 -j SNAT --to 108.96.58.2
iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o eth0 -j MASQUERADE
iptables -t nat -A PREROUTING -d 108.96.58.1/32 -j DNAT --to 172.16.0.1
iptables -t nat -A PREROUTING -d 108.96.58.2/32 -j DNAT --to 172.16.0.2


iptables -A FORWARD -s 95.201.100.0/24,114.204.56.0/24,108.96.58.0/24 -p icmp -j DROP
iptables -A INPUT -p ospf -j ACCEPT
iptables -A FORWARD -s 172.16.0.0/24,192.168.0.0/16,10.0.0.0/30,95.201.100.0/24,108.96.58.0/24,1
14.204.56.0/24 -j ACCEPT

iptables -A INPUT -s 172.16.0.0/24,192.168.0.0/16,10.0.0.0/30,95.201.100.0/24,108.96.58.0/24,114
.204.56.0/24 -j ACCEPT

```

간단하다