

# Zarządzanie ruchem w sieci małego ISP



**Michał Prokopiuk**

Michał Prokopiuk, [michal@sloneczko.net](mailto:michal@sloneczko.net), <http://www.sloneczko.net>

# Trochę informacji

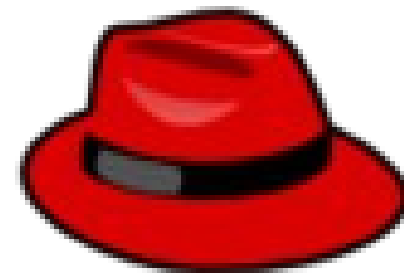
- Sloneczko.net to lokalny ISP
- działa w Krakowie na Starym Mieście i Kazimierzu
- Ilość użytkowników dobiega do 1000
- ruch dobiega do 500 Mbps

# Trochę historii



# POCZĄTKI

- łącze w dzwanianie 256 Kbps
- ośmiu użytkowników
- RedHat 5.1
- Intel Pentium 233 Mhz



# Ipchains

*ipchains -F forward*

*ipchains -P forward DENY*

*ipchains -A forward -s 192.168.0.0/24 -j MASQ*

*ipchains -A forward -i eth1 -j MASQ*

Ale tę część sobie już darujemy...

# Początki zarządzania ruchem i użytkownikami

Firewall. Tak w perlu ;)

```
package user;
BEGIN {
use Exporter();
@ISA = qw(Exporter);
@EXPORT = qw(user);
}
#modul włącza użytkowników
#drukuje znaczniki
#x - nie ma takiego użytkownika
#o - użytkownik jest oznaczony jako wyłączony
#! - przekierowanie na komunikat o braku płatności
#* - blokada za brak płatności
#. - ok, ładuje firewalle
sub user()
{
sub go
{
#należy mieć wkompiłowany modul connlimit do jądra
`$conf:::ipt_path -t filter -A FORWARD -s $ip -m mac --mac-source $mac -d 0/0 -j ACCEPT`;
`$conf:::ipt_path -t nat -A POSTROUTING -s $ip -d 0/0 -j MASQUERADE`;
}
    Michał Prokopiuk, michal@sloneczko.net, http://www.sloneczko.net
```

# Szafa serwerowa



# Przybywa użytkowników, zaczynają się problemy...

- Dwie reguły iptables per użytkownik
- Plus dodatkowe reguły jeżeli użytkownik ma więcej zarejestrowanych komputerów
- Plus dodatkowe reguły jeżeli ma publiczny adres IP
- Dwie kolejki na użytkownika
- Dodatkowo - logowanie pakietów SYN



# ... więc szukamy rozwiązania

## Hardware



**DELL 1950 2x E5345 Quad Core  
+ rozbudowa serwerowni**

**(ale o tym na końcu)**

Michał Prokopiuk, [michal@sloneczko.net](mailto:michal@sloneczko.net), <http://www.sloneczko.net>

# Nigdy nie podobało mi się IMQ...

I słusznie. Nie udało nam się przepuścić przez nie więcej niż 200 Mbps.

Więc tak szybko jak je uruchomiliśmy to się go pozbyliśmy.

# IRQBALANCE

**SOA #1**

**U mnie działa ;)**

```
          CPU0          CPU1          CPU2          CPU3          CPU4          CPU5          CPU6          CPU7
97: 3780416948 3731909947 3776701030 3731100595 3790995622 3801017819 3782469350 3774156877  PCI-MSI-edge  eth0
98: 3854191767 3752683840 3857863863 3753021885 3843597991 3833600247 3852186474 3860356090  PCI-MSI-edge  eth1
```

# Pomogło na krótko więc planujemy.

Panel administracyjny

Klient

- lista klientów
- dodaj klienta
- lista hostów
- dodaj hosta
- okazje
- dodaj lokalizację
- serwisy
- faktury
- faktury powiązania
- notowania
- statystyka
- obliczenie wpłaty
- wyloguj
- testy: firewall

Lista klientów

## PANEL ZARZĄDZAJĄCY

1 2 3 4 5 6 nazwa klienta x

słowo kluczowe:  kryterium:

pakiet:  pakiet tylko usunętych:

Nazwa klienta	Lokalizacja	Adres świadczenia usługi	
Wacławeta Wisłakówna Tomaszowski przy ul. Słońskiej 11 w Krakowie	Skowronka 11	u Skowronka 11/7	
330 Dział Rybnik Sp. z o.o. S.A.	Karłowicza 71	Karłowicza 71/1	
Adam Filipow	Działy 29	u Działy 29/7	
Adam Tomaszek Janiec	Działy 79	Działy 79/3	
Adam Janusz Śmiech	Studzienna 71	Studzienna 18/2	
Adam Kaniażewski	Jasne 20	Bełka Jasne 20/2	
Adam Kozłowski	Działy 77	u Działy 77/12	
Adam Poczeka	Studzienna 27	u Studzienna 27/7	
Adam Poczeka	Wacławicka 11	u Wacławicka 11/7	
Adam Poczeka	Działy 27	Działy 27/4	

## STRONA WWW Z PANELEM KLIENTA

HOME O NAS USŁUGI KONTAKT SERWISY ADMINISTRACJA BLOG REZERWACJA

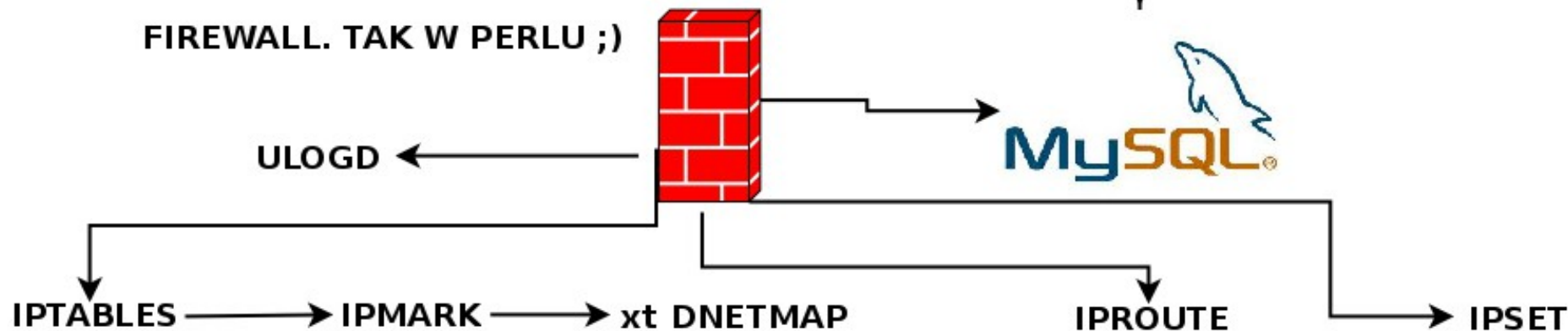
Sloneczko net

KARTA RABATOWA DLA NASZYCH KLIENTÓW!

ZOBACZ NASZE PROMOCJE

Telewizja FullHD Internet Usługi Data Center Aktualności

FileMedic Antivirus



# IPMARK

```
Iptables -t mangle -A POSTROUTING -o eth0.2 -j IPMARK --addr src --and-mask 0xffff --or-mask 0x10000  
tc filter add dev eth0.2 parent 1:0 protocol ip fw
```

Jedna reguła zastępuje nam setki reguł iptables!

▪

# xt\_DNETMAP

```
iptables. -t nat -N PUBLIC_IP
```

```
iptables. -t nat -A PUBLIC_IP -s 10.10.80.0/21 -j DNETMAP --prefix 192.166.203.0/25 --static
```

```
iptables. -t nat -I POSTROUTING -s 10.10.80.0/21 -j PUBLIC_IP
```

```
iptables. -t nat -A PREROUTING -j DNETMAP
```

```
echo 10.10.10.10:192.166.203.66 > /proc/net/xt_DNETMAP/192.166.203.0_25
```

- cztery regułki zastępują po cztery regułki na jednego klienta
- zastępuje od razu SNAT i DNAT
- obsługuje zarówno statyczne jak i dynamiczne przypisania
- loguje mapowania adresów (przydatne dla ukochanej Policji)
- niezależne od iptables modyfikowanie tablicy mapowań

# IPSET

```
ipset -F forward0
```

```
ipset -X
```

```
ipset -N forward0 macipmap --network 10.10.10.0/22
```

```
iptables -A FORWARD -m set --match-set forward0 src -j LAN_FORWARD_ACCEPT
```

- **tworzy mapę reguł, alokując (tu 8 bitów) na mapowanie mac:ip i odwołuje się bezpośrednio do niego, nie przetwarza reguł liniowo jak iptables**
- **pozwała na tworzenie różnego rodzaju mapowań (bitmap, hash) i przyporządkowań (ip, ip:mac, port, ip:port, net i kilka innych)**
- **pozwała na niezależne od iptables modyfikowanie mapowań**

# Obowiązki wobec naszego państwa...

- Każdy ISP ma obowiązek przez 2 lata przechowywać logi połączeń swoich użytkowników
- Obowiązek ten spełnia logowanie pakietów SYN. Syslog zabierał nam cały procesor.
- Odkąd zaczęliśmy używać ulogd problem logów sprowadza się do zapewnienia miejsca na archiwa :)



# Efekty naszych prac

- 200 regułek iptables na utrzymanie wszystkich użytkowników (blokady, komunikaty itp.)
- dwie kolejki na użytkownika
- znikome obciążenie routera
- łatwość zarządzania siecią
- niemal pełna automatyzacja obsługi płatności, faktur i wszelkich operacji klienckich
- brak awarii związanych z głównym węzłem sieci od bardzo dawna
- ogólna radość i szczęście :)

**Nie obyło się bez inwestycji w infrastrukturę.**

**BYŁO**

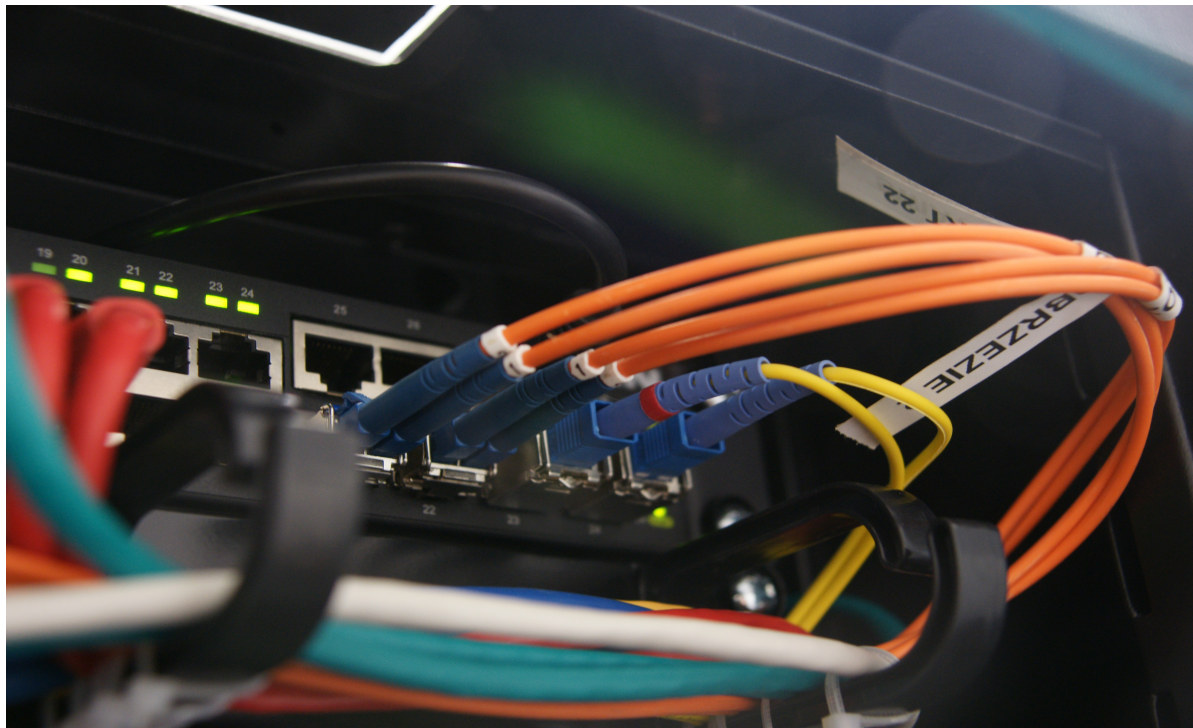


**JEST**



Michał Prokopiuk, [michal@sloneczko.net](mailto:michal@sloneczko.net), <http://www.sloneczko.net>

## SZKIELET SIECI I GŁÓWNE WĘZŁY OPARTE SĄ NA SWIATŁOWODACH



# Moja ulubiona zabawka :)

Generator Diesel 10 kV z systemem ATS



**PYTANIA?**