



# Simple High Availability, czyli jak osiągnąłem niezawodność

Stanisław „dozzie” Klekot

V Sesja Linuksowa  
6 kwietnia 2008

# co to jest VPN?

trudne pojęcie

# co to jest VPN?

trudne pojęcie

Zwykły szyfrowany tunel.

# po \*j mi to?

do czego tego używa biznes?

## po \*j mi to?

do czego tego używa biznes?

- przezroczyste zabezpieczenie transmisji

## po \*j mi to?

### do czego tego używa biznes?

- przezroczyste zabezpieczenie transmisji
- rozszerzenie sieci lokalnej

## po \*j mi to?

### do czego tego używa biznes?

- przezroczyste zabezpieczenie transmisji
- rozszerzenie sieci lokalnej
- dostęp do intranetu spoza oddziałów

## został protokół wybrany jak (Yoda)

kilka dobrych powodów

## został protokół wybrany jak (Yoda)

### kilka dobrych powodów

- otwarty kod źródłowy daemona

## został protokół wybrany jak (Yoda)

### kilka dobrych powodów

- otwarty kod źródłowy daemona
- daemon używa standardowych bibliotek

## został protokół wybrany jak (Yoda)

### kilka dobrych powodów

- otwarty kod źródłowy daemona
- daemon używa standardowych bibliotek
- oparty o SSL

## został protokół wybrany jak (Yoda)

### kilka dobrych powodów

- otwarty kod źródłowy daemona
- daemon używa standardowych bibliotek
- oparty o SSL — podobno

## został protokół wybrany jak (Yoda)

### kilka dobrych powodów

- otwarty kod źródłowy daemona
- daemon używa standardowych bibliotek
- oparty o SSL — podobno

Niestety protokół zamknięty.

## jeszcze w pieluchach

jak zaczynała sieć?

## jeszcze w pieluchach

### jak zaczynała sieć?

- jedno łącze w centrali

## jeszcze w pieluchach

### jak zaczynała sieć?

- jedno łącze w centrali
- jeden oddział włączony w sieć

## jeszcze w pieluchach

### jak zaczynała sieć?

- jedno łącze w centrali
- jeden oddział włączony w sieć
- jeden tunel VPN

# działa, ale...

problemy

# działa, ale...

## problemy

- padające łącze

## działa, ale...

### problemy

- padające łącze
- ciągłe zmiany w okablowaniu

## działa, ale...

### problemy

- padające łącze
- ciągłe zmiany w okablowaniu
- przeciążone łącze

## zmierzyć się z problemami (gdzie jest linijka?)

### metody poprawy sytuacji

## zmierzyć się z problemami (gdzie jest linijka?)

### metody poprawy sytuacji

- 1 szersze łącze

## zmierzyć się z problemami (gdzie jest linijka?)

### metody poprawy sytuacji

- 1 szersze łącze
- 2 *service level agreement*

## zmierzyć się z problemami (gdzie jest linijka?)

### metody poprawy sytuacji

- 1 szersze łącze
- 2 *service level agreement*
- 3 łącza dzierżawione (PVC/IP VPN)

## zmierzyć się z problemami (gdzie jest linijka?)

### metody poprawy sytuacji

- 1 szersze łącze
- 2 *service level agreement*
- 3 łącza dzierżawione (PVC/IP VPN)

Wybrane zostało 3.

## łącze dzierżawione

co zrobić w przypadku awarii?

Gdy pada łącze dzierżawione. . .

## łącze dzierżawione

co zrobić w przypadku awarii?

Gdy pada łącze dzierżawione. . . może użyć łącza ze światem?

## Łącze dzierżawione

co zrobić w przypadku awarii?

Gdy pada łącze dzierżawione... może użyć łącza ze światem?

Jak?

grrr... znowu padło (admin)

ręczne przepinanie VPN-a

grrr... znowu padło (admin)

## ręczne przepinanie VPN-a

- uciążliwe dla administratora

## grrr... znowu padło (admin)

### ręczne przepinanie VPN-a

- uciążliwe dla administratora
- koszmarny czas reakcji

## grrr... znowu padło (admin)

### ręczne przepinanie VPN-a

- uciążliwe dla administratora
- koszmarny czas reakcji
- użytkownicy tracą połączenia

# co jest dostępn<sup>W</sup> umiemy?

BGP

# co jest dostępn<sup>W</sup> umiemy?

## BGP

- nikt nie umiał tego postawić

# co jest dostępn<sup>W</sup> umiemy?

## BGP

- nikt nie umiał tego postawić
- dobry pomysł, gdy się już ma numer AS

## co jest dostępn<sup>W</sup> umiemy?

### BGP

- nikt nie umiał tego postawić
- dobry pomysł, gdy się już ma numer AS
- gdy brak AS, nowy tunel dopiero przy padzie starego

# co jest dostępne $\hat{W}^W$ umiemy?

## BGP

- nikt nie umiał tego postawić
- dobry pomysł, gdy się już ma numer AS
- gdy brak AS, nowy tunel dopiero przy padzie starego
  - zaleta: można użyć dowolnego protokołu

# kombinatoryka w praktyce

jak to zrobić sprytnie?

# kombinatoryka w praktyce

## jak to zrobić sprytnie?

- coś, co samo wstaje/kładzie interfejsy

# kombinatoryka w praktyce

## jak to zrobić sprytnie?

- coś, co samo wstaje/kładzie interfejsy
- VTun? PPTP? *Who uses it for sensitive data?*

# kombinatoryka w praktyce

## jak to zrobić sprytnie?

- coś, co samo wstaje/kładzie interfejsy
- VTun? PPTP? *Who uses it for sensitive data?*
- OpenVPN

# kombinatoryka w praktyce

## jak to zrobić sprytnie?

- coś, co samo wstaje/kładzie interfejsy
- VTun? PPTP? *Who uses it for sensitive data?*
- OpenVPN
- czemu nie IPsec?

# kombinatoryka w praktyce

## jak to zrobić sprytnie?

- coś, co samo wstaje/kładzie interfejsy
- VTun? PPTP? *Who uses it for sensitive data?*
- OpenVPN
- czemu nie IPsec?
  - trudne w konfiguracji(?)

# kombinatoryka w praktyce

## jak to zrobić sprytnie?

- coś, co samo wstaje/kładzie interfejsy
- VTun? PPTP? *Who uses it for sensitive data?*
- OpenVPN
- czemu nie IPsec?
  - trudne w konfiguracji(?)
  - brak TUN/TAP, nawet w KLIPS

# kombinatoryka w praktyce

## jak to zrobić sprytnie?

- coś, co samo wstaje/kładzie interfejsy
- VTun? PPTP? *Who uses it for sensitive data?*
- OpenVPN
- czemu nie IPsec?
  - trudne w konfiguracji(?)
  - brak TUN/TAP, nawet w KLIPS
  - ... i właściwie to wszystko

# coraz szybciej, coraz więcej

permanentna pajęczyna

# coraz szybciej, coraz więcej

## permanentna pajęczyna

- po dwa-trzy łącza w oddziale

# coraz szybciej, coraz więcej

## permanentna pajęczyna

- po dwa-trzy łącza w oddziale
- oddziałów kilkanaście

# coraz szybciej, coraz więcej

## permanentna pajęczyna

- po dwa-trzy łącza w oddziale
- oddziałów kilkanaście
- parędziesiąt konfigów

# coraz szybciej, coraz więcej

## permanentna pajęczyna

- po dwa-trzy łącza w oddziale
- oddziałów kilkanaście
- parędziesiąt konfigów — wszystko ręcznie?

# coraz szybciej, coraz więcej

## permanentna pajęczyna

- po dwa-trzy łącza w oddziale
- oddziałów kilkanaście
- parędziesiąt konfigów — wszystko ręcznie?

## od czego są skrypty?

DConfig — automat do dystrybucji konfiguracji.

# a jak to właściwie działa?

mechanika

# a jak to właściwie działa?

## mechanika

- pakiet *keep alive* — `--ping n`

# a jak to właściwie działa?

## mechanika

- pakiet *keep alive* — `--ping n`
- restart połączenia — `--ping-restart n`

# a jak to właściwie działa?

## mechanika

- pakiet *keep alive* — `--ping n`
- restart połączenia — `--ping-restart n`
- up/down interfejsu — `--up-restart + --up-delay`

## a jak to właściwie działa?

### mechanika

- pakiet *keep alive* — `--ping n`
- restart połączenia — `--ping-restart n`
- up/down interfejsu — `--up-restart + --up-delay`
- problemy z `--ping-restart`

# Linux itself

## mechanika Linuksa

# Linux itself

## mechanika Linuksa

- ip rule

# Linux itself

## mechanika Linuksa

- ip rule
- ip route

# Linux itself

## mechanika Linuksa

- ip rule
- ip route
- trasy z metryką

## a teraz będziemy pazerni

jak wykorzystać dwie pary łączy?

## a teraz będziemy pazerni

jak wykorzystać dwie pary łącz?

Jedną parą łącz SSH, drugą parą poczta.

## a teraz będziemy pazerni

### jak wykorzystać dwie pary łącz?

Jedną parą łącz SSH, drugą parą poczta.

- druga tablica routingu

## a teraz będziemy pazerni

### jak wykorzystać dwie pary łącz?

Jedną parą łącz SSH, drugą parą poczta.

- druga tablica routingu
- iptables -j MARK

## a teraz będziemy pazerni

### jak wykorzystać dwie pary łącz?

Jedną parą łącz SSH, drugą parą poczta.

- druga tablica routingu
- iptables -j MARK
- ip rule fwmark

# nasza pazerność nie zna granic

## nasza pazerność nie zna granic

co można zrobić firewallowi?

```
iptables -o tpnet -j SNAT --to $tpnet_addr
```

## nasza pazerność nie zna granic

co można zrobić firewallowi?

```
iptables -o tpnet -j SNAT --to $tpnet_addr
```

default gateway

```
ip route add default via X.X.X.X metric 5  
ip route add default via Y.Y.Y.Y metric 10  
ip route add default via Z.Z.Z.Z metric 15
```

## nasza pazerność nie zna granic

co można zrobić firewallowi?

```
iptables -o tpnet -j SNAT --to $tpnet_addr
```

default gateway

```
ip route add default via X.X.X.X metric 5  
ip route add default via Y.Y.Y.Y metric 10  
ip route add default via Z.Z.Z.Z metric 15
```

Bezkarne kasowanie wpisów z main.

```
ssh primary-router /sbin/shutdown -h now
```

VRRP

```
ssh primary-router /sbin/shutdown -h now
```

VRRP

WTF?

```
ssh primary-router /sbin/shutdown -h now
```

## VRRP

WTF?

Co to daje?

```
ssh primary-router /sbin/shutdown -h now
```

## VRRP

WTF?

Co to daje?

Jak to działa?

```
ssh primary-router /sbin/shutdown -h now
```

## VRRP

WTF?

Co to daje?

Jak to działa?

- router *standby*

```
ssh primary-router /sbin/shutdown -h now
```

## VRRP

WTF?

Co to daje?

Jak to działa?

- router *standby*
- *standby* OpenVPN

```
ssh primary-router /sbin/shutdown -h now
```

## VRRP

WTF?

Co to daje?

Jak to działa?

- router *standby*
- *standby* OpenVPN
- routing między sieciami w oddziale

```
ssh primary-router /sbin/shutdown -h now
```

## VRRP

WTF?

Co to daje?

Jak to działa?

- router *standby*
- *standby* OpenVPN
- routing między sieciami w oddziale
- DHCP?

```
ssh primary-router /sbin/shutdown -h now
```

## VRRP

WTF?

Co to daje?

Jak to działa?

- router *standby*
- *standby* OpenVPN
- routing między sieciami w oddziale
- DHCP? IP przybite do MAC

## 255 sieciówek

802.1Q

## 255 sieciówek

### 802.1Q

- porty nietagowane

## 255 sieciówek

### 802.1Q

- porty nietagowane, porty tagowane

## 255 sieciówek

### 802.1Q

- porty nietagowane, porty tagowane
- interfejsów więcej niż portów w sieciówkach

## 255 sieciówek

### 802.1Q

- porty nietagowane, porty tagowane
- interfejsów więcej niż portów w sieciówkach
- likwidacja wiązek kabli

## 255 sieciówek

### 802.1Q

- porty nietagowane, porty tagowane
- interfejsów więcej niż portów w sieciówkach
- likwidacja wiązek kabli
- do montażu nie trzeba rebootu

# ten kabelek jest niepotrzebny? oops!...

bonding

# ten kabelek jest niepotrzebny? oops!...

## bonding

- padnięta sieciówka

## ten kabelek jest niepotrzebny? oops!...

### bonding

- padnięta sieciówka
- można przepinać kable

## ten kabelek jest niepotrzebny? oops!...

### bonding

- padnięta sieciówka
- można przepinać kable
- uszkodzony switch

## ten kabelek jest niepotrzebny? oops!...

### bonding

- padnięta sieciówka
- można przepinać kable
- uszkodzony switch
- różne metody

# Pytania?



## Dziękuję za uwagę

