Mały ISP w zasięgu dłoni.

Ty także możesz zostać adminem !

Borys Łącki borys@bohater.net

O mnie:

Borys Łącki

Administrator systemu Linux

ISP (Internet Service Provider)
[dostawca usług internetowych]

Dlaczego Linux ?

"Jedynym ograniczeniem jest nasza wyobraźnia..."

- otwarty (wolny !, elastyczny)
- darmowy
- bezpieczny
- wydajny
- OpenSource – każdy może coś dać...

ROUTER

Urządzenie (komputer), którego zadanie polega na kierowaniu (*route* – trasa) ruchu internetowego.

DHCP

ang. **D**ynamic **H**ost **C**onfiguration **P**rotocol

Umożliwia uzyskanie w automatyczny sposób konfiguracji sieciowej.
(np. adres IP hosta, adres IP bramy, adres serwera DNS)

http://pl.wikipedia.org/wiki/DHCP | http://www.isc.org/index.pl?/sw/dhcp/

FIREWALL (netfilter / iptables)

Potężny i rozbudowany system zarządzania sterowaniem pakietami internetowymi.

http://www.bromirski.net/docs/tlumaczenia.html

http://www.netfilter.org/ | http://www.netfilter.org/projects/iptables/

NAT

ang. **N**etwork **A**ddress **T**ranslation]

Technika polegająca na translacji adresów i umożliwiająca uzyskanie dostępu wielu komputerom w przypadku posiadania jednego zewnętrznego adresu IP.

iptables -t nat -A PREROUTING -s 192.168.10.10/32 -o eth0 -j MASQUERADE

http://www.bromirski.net/docs/translations/linux24-nat.html

MAC+IP

Zezwolenie na korzystanie z danego adresu IP wyłącznie z określonego adresu MAC karty sieciowej.

```
iptables -t nat -A PREROUTING -m mac --mac-source AA:BB:CC:DD:EE:FF \
-s 192.168.10.10 -j ACCEPT
```

ACCEPT, DROP

Akceptacja / blokada ruchu sieciowego
na podstawie zawartości oraz właściwości
pakietów internetowych.

iptables -t nat -A PREROUTING -p tcp --dport 445 -j DROP
iptables -t nat -A PREROUTING -d 123.123.123.123 -j DROP

http://www.bromirski.net/docs/translations/linux24-pf.html

PORT FORWARD

Przekierowanie portów

Specyficzne usługi wymagają aby komputer posiadał zewnętrzną adresację IP.
(serwery gier, radia internetowe,
aplikacje sieci p2p, itp.)

iptables -A PREROUTING -t nat -p tcp --dport 22 -j DNAT –to 192.168.10.20:22

DNAT,SNAT

Umożliwia stworzenie powiązania pomiędzy wewnętrznym adresem IP klienta, a zewnętrznym adresem IP operatora.

iptables -A PREROUTING -t nat -d 111.122.133.11 -j DNAT --to 192.168.10.21
iptables -A POSTROUTING -t nat -s 192.168.10.21 -j SNAT --to 111.122.133.11

Brak wpłaty, wirusy...

Moc przekierowań oraz możliwości pakietu Netfilter umożliwiają wyświetlenie w określony sposób komunikatów dla klienta:
- brak wpłaty
- zablokowany dostęp z powodu wirusów
- czasowo zablokowany

*iptables -t nat -A PREROUTING -p tcp --dport 80 -m limit --limit 30/hour *
-j DNAT --to 192.168.10.1:9999

Kolejkowanie

ang. traffic shaping

Umożliwia zaawansowane sterowanie kolejnością (priorytetami) przesyłanych pakietów na podstawie szeregu parametrów.

- ograniczanie prędkości
- wyższy priorytet dla usług interaktywnych

http://www.bromirski.net/docs/translations/lartc-pl.html
htb, cbq, wrr, red, sfq, hfsc, **tcng**

MONITORING

Simple **N**etwork **M**anagement **P**rotocol

Umożliwia zarządzanie i nadzór szeregu urządzeń takich jak router, switch, AP.

Systemy monitorujące - informujące o zachodzących zdarzeniach.

Nagios / Zabbix / Cacti / Mrtg / RRDtool

www.net-snmp.org | www.nagios.org | www.cacti.net
www.zabbix.com | http://oss.oetiker.ch/

PROXY

Serwer Proxy odpowiada za przechowywanie części podręcznych dokumentów (głównie stron WWW), a co za tym idzie umożliwia zaoszczędzenie pasma łącza internetowego.

www.squid-cache.org
http://pl.wikipedia.org/wiki/Squid_(oprogramowanie)

NARZĘDZIA

Zaplecze pomocnych narzędzi wykorzystywanych w trakcie pracy:

ping, mtr, iperf, iftop, iptraf, tcpdump, tcpflow, tcptrack, ngrep, nmap, wget, curl itp.

www.google.com :]

DANE

1. Pliki

2. Baza danych (typu SQL)

Umożliwia łatwe, szybkie i wydajne przeglądanie, modyfikowanie, usuwanie oraz dodawanie danych.

Zarządzanie ze strony WWW.

HOSTING

- strony WWW (Apache + PHP)
- poczta (Postfix, Exim, Sendmail)
- spam (SpamAssassin)
- ftp (Proftpd, Vsftpd)
- inne (IMAP, POP3, SSL)

BACKUP

Protokół RSYNC, który charakteryzuje się tym, iż umożliwia przesyłanie jedynie danych, które na prawdę zostały zmienione.

- przesyłamy jak najmniej
- w jak najkrótszym czasie
- możliwość tworzenia przyrostowych backupów (oszczędność miejsca)

http://backuppc.sourceforge.net/ | www.samba.org/rsync/ | www.bacula.org

WSPÓLNE DANE

Serwer plików - umożliwia wymianę plików w warstwie sieciowej (także z systemami MS Windows).

www.samba.org

TELEFONIA

Centrala telefoniczna

Wykonywanie połączeń telefonicznych oraz VoIP, przekierowania grupowe lub indywidualne, automatyczna sekretarka, menu głosowe, billing połączeń itp.

ROUTING

Protokoły routingu używane są do wymiany informacji o trasach pomiędzy sieciami komputerowymi.

Quagga – Aplikacja odpowiedzialna za protokoły routingu: BGP, OSPF, RiP

www.quagga.net

BEZPIECZEŃSTWO

- IDS (snort)
- honeypot (nepenthes)
- skanery sieciowe (nmap, nessus)
- integralność danych (aide, tripwire)
- spam (spamdetector, AntiSpamProxy)

Dziękuję za uwagę...

borys@bohater.net