Home, sweet $HOME

Networking casalingo con Linux

Guido Bolognesi

Network Security Manager

guido@kill-9.it

I.Net S.p.A.

Dijkstra: chi era?

Edsger Wybe Dijkstra
Rotterdam 1930 - Neunen 2002

- Laurea in fisica teorica
- 1972, ACM Turing Award
- 1982, IEEE Computer Pioneer Award

9 libri, 12 capitoli, 40 articoli
34 partecipazioni a conferenze
22 altre pubblicazioni varie
Gli EWDs, i manoscritti. Fotocopiati.

Dijkstra: perchè ricordarlo?

Perchè non l'ha fatto *nessuno*

- il concetto di sezione critica
- i semafori (la cena dei filosofi)
- programmazione strutturata (l'eliminazione del GOTO)
- il primo compilatore ALGOL
- l'algoritmo SPF (shortest-path first, OSPF)

Dijkstra: cosa diceva?

“The question of whether computers can think is like the question of whether submarines can swim”

“We must give industry not what it wants, but what it needs.”

Lo scopo del talk

La trattazione di questo setup ha alcune speranze, ma nessuna pretesa:

- fornire spunti
- dare un'idea della flessibilità
- ...e della stabilità

Il Layout fisico

A casa:

- la connessione fisica
- il firewall (Linux)
- la rete dei client (linux, Irix, Solaris, NetBSD, AIX, Win)
- varie (altre reti)

Il Layout fisico

In ufficio:

- la connessione
- il firewall (Cisco)
- la macchina (Linux)
- le altre reti

Il Layout fisico: link geografico

VTUN (vtun.sourceforge.net) Risolve il problema di nat e protocolli filtrati (TCP, UDP)

- leggero, veloce, stabile
- multipiattaforma (linux, *BSD, Solaris)
- abbastanza sicuro (preshared key, BlowFish 128, chiavi hash MD5)
- di uso intuitivo (tun*n*)
- supporta compressione (lzo,zlib) e shaping
- ...e molto altro.

Il routing

Non è difficile, basta non distrarsi :)

- rigorosamente RFC1918
- l'interfaccia in bridge (br0)
- il provider
- l'ufficio
- ...il vicino

Un minimo di sicurezza

A partire dal kernel 2.4.x è disponibile *netfilter* (iptables)

- stateful
- estremamente flessibile (packet mangling)
- rate-limiting
- plugin (h323)
- QoS

Applicativi: DNS

pdnsd (home.t-online.de/home/Moestl)
È un proxy dns server con caching permanente

- completamente RFC2181 compliant
- salva il db in uscita
- supporta record AAAA, X25, NSAP
- può utilizzare */etc/hosts*
- controlla i server con keepalive (ping, iface, script)
- leggero (4Mb di RSS su x86)

Applicativi: dhcp

Ci sono molti server dhcp disponibili.
Ho scelto il server di ISC, per svariati motivi:

- stabile
- permette di gestire più interfacce
- permette di usarlo per bootp/tftp/nfs
- c'era già pacchettizzato Debian. :)

Il dhcp permette di spegnere il portatile in ufficio, riaccenderlo a casa e continuare a lavorare.

Applicativi: il web

Squid (www.squid-cache.org)
Il più completo progetto di proxy web:

- installato sia a casa che in ufficio, come *sibling*
- gerarchico, con Cache Digests
- estremamente collaudato
- supporta SNMP
- facilmente utilizzabile con junkbuster o privoxy

Applicativi: il web (2)

Junkbuster o Privoxy, piccoli proxy “intelligenti”

- filtrano i cookie indesiderati
- possono filtrare activex, javascript, popup...
- privoxy è configurabile da web
- supportano whitelist
- possono avere un chain forwarder (tipicamente un proxy “vero”)

Applicativi: email

Postfix (www.postfix.org)

- veloce e sicuro (chroot)
- facile da amministrare (beh, più di sendmail)
- integrabile facilmente con software di content filtering, list manager
- limite ai message size
- potenti regole di filtering, in accoppiata con spamassassin

Applicativi: email - (spam)

spamassassin (www.spamassassin.org)

- utilizzato come filtro (procmail,mailfilter)
- utilizza delle regole di euristica, con uno score
- si integra con software di open relay (razor, mail-abuse.org, ordb.org)
- demonizzabile (spamc/spamd)
- fortemente personalizzabile
- ci prende :)

Monitoring: SNMP

net-snmp (www.net-snmp.org)

È una suite completa server/client SNMP.
Permette di controllare

- parametri di sistema (processi, storage, memoria, temperatura)
- parametri di rete (routing table, carico delle interfacce)
- sia locali (se installato il daemon) che remoti

Monitoring: MRTG

Multi Router Traffic Grapher (people.ee.ethz.ch)
Insieme a RRDtool è *IL* software per fare monitoring su web.

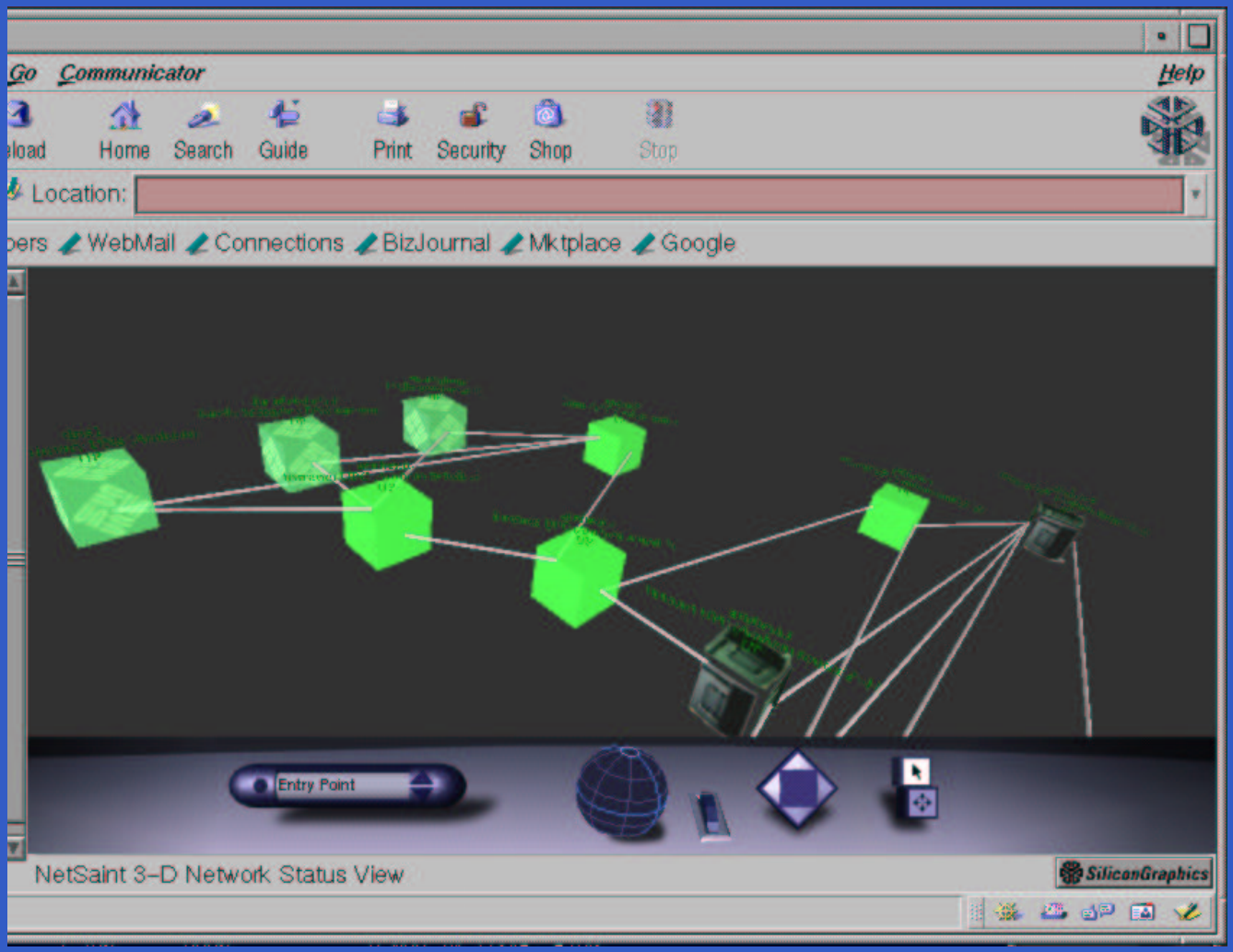
- fa nativamente grafici di tutto ciò che parla SNMP
- facilmente scriptabile
- robusto e scalabile
- estremamente personalizzabile

Monitoring: Nagios

Nagios (www.nagios.org) è il successore di NetSaint

- controlla servizi di rete e di host
- è facile scrivere plugin (shell, C, perl, awk, ...)
- configurazione di rete gerarchica
- volendo, è attivo
- renderizza la struttura di rete in VRML :)

Monitoring: VRML view



La “gestione documenti”

Tutti i documenti che non sono legati ad una macchina specifica sono su un file server che monta

- NFSv3
- Samba
- Unison
- ...e un DDS-2. :)

Un piccolo progetto6

Ormai è ora di giocare con IPv6! ...ma il mio provider di connettività non lo trasporta. Quindi:

- un piccolo tunnel IPv6 over PPP over ssh :)
- una rete di tunnel IPv6 in IPv4 per altre macchine interne
- routing IPv6 con ospf6d di zebra

...e abbiamo tutti una modesta /64 pubblica (circa 4 milioni di indirizzi)

Per concludere

La parte audio? :)

- Apache+Edna
- ohphone

Possibili sviluppi futuri:

- backup (amanda?)
- reportistica (domotica)
- antifurto (O2 cam)

Fatti, non pugnette!

Dicevamo all’inizio “stabile”:

01:18:15 up 293 days, 13:37, 3 users,
load average: 0.48, 0.40, 0.36

Q&A, Ringraziamenti

Grazie a...

- Laura
- Linux
- vi, LaTeX, Prosper (prosper.sourceforge.net)
- Google
- la comunità OpenSource
- erlug e gli amici