Linux e software libero nella P.A.: l'esperienza dell'I.Z.S.A.M.

Daniele Zippo

Istituto Zooprofilattico Sperimentale

dell'Abruzzo e del Molise di Teramo

IZS e Apache

- Esperienze con reti e Videotel
- Ingresso in GARR
- Curiosità su software libero e gratuito
- Primo impatto con software libero
  - Server web Apache

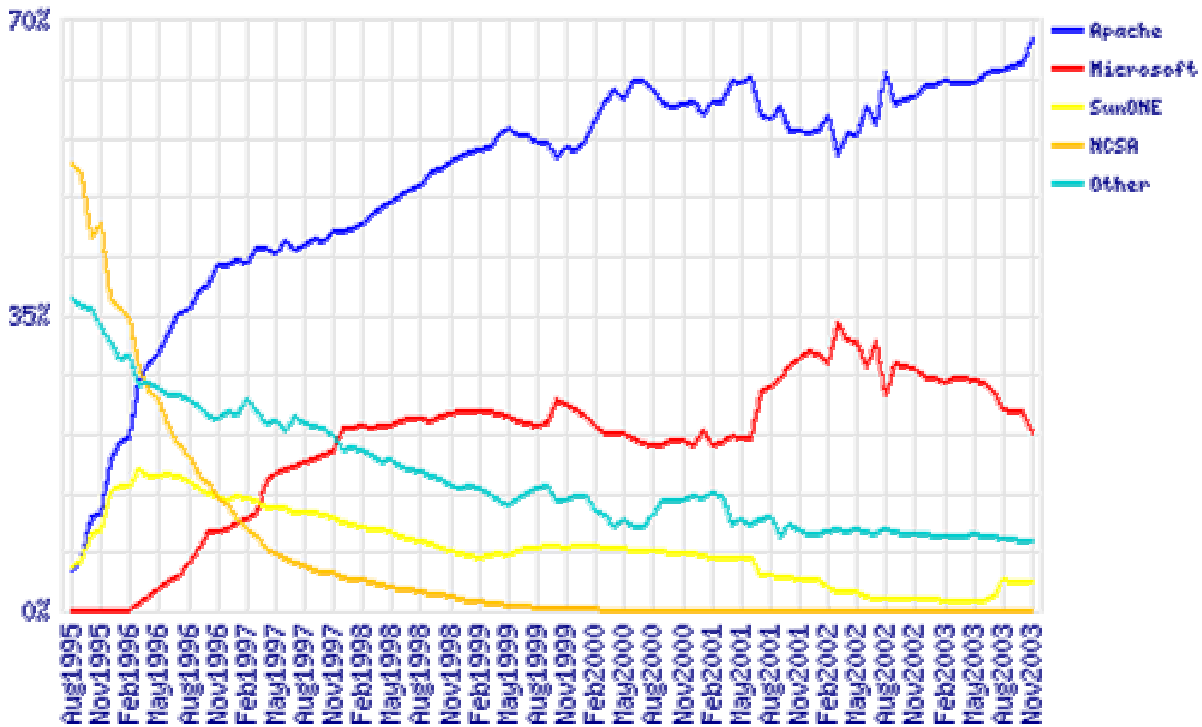
APACHE

- **Scelta del server Apache per le seguenti caratteristiche principali:**
  - **stabilità e rapido ciclo di sviluppo dovuti alla collaborazione di un folto gruppo di volontari**
  - **la disponibilità dell'intero codice sorgente in forma free (libera e gratuita)**
  - **il supporto di scripting lato server e degli scriptCGI**

Diffusione di Apache

- **Come riporta la ricerca di Netcraft, Apache rimane di gran lunga il server Web più utilizzato.**

Market Share for Top Servers Across All Domains August 1995 - November 2003



Altri software liberi in IZS

- Introduzione nella Intranet dei software liberi:
  - Squid: proxy server
  - Inn: server di feed delle new

Altri software liberi in IZS

- Passaggio dei servizi Videotel su Internet
- Naturale esigenza di fornire contenuti dinamici basati su basi dati presenti in IZS, sia su Internet sia su Intranet

Creazione di interfaccia verso DB: PERL

IZS e LINUX

- Nel 1997-98 la rete IZS diventa punto di riferimento per le informazioni veterinarie a livello nazionale.
  - Gestione del sito web del Ministero della Sanità – Dipartimento Alimenti Nutrizione e Sanità Pubblica Veterinaria
  - Connessione con tutti i distretti delle AUSL dell'Abruzzo e successivamente del Molise
- Avanzare della cultura del cracking ed il pericolo di intrusioni non desiderate

Esigenza di sicurezza in ambito informatico: FIREWALL

IZS e LINUX

- Introduzione nella border-line della connettività dell'IZS di un firewall:

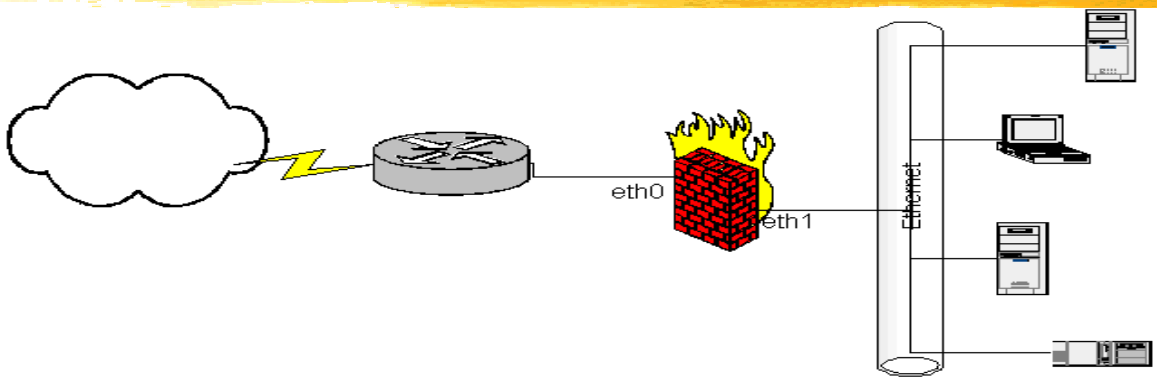
  La scelta a questo punto cade ovviamente su software libero:

  sistema operativo Linux firewall basato su ipchains

IZS e LINUX

- **L'introduzione di un firewall in una rete preesistente, soprattutto se globalmente connessa ad Internet (come era la nostra), porta al problema del trasparent bridging**
- **Il firewall seziona la rete in due sottoreti, che implicherebbe la modifica della netmask per le due sottoreti e per la sottorete interna la modifica del gateway su tutti gli host.**
- **Con il S.O. Linux che permette di affiancare un potente firewall con una soluzione di bridging, abbiamo risolto il problema rendendo "trasparente" il firewall tramite l'utilizzo del proxy ARP, senza dover effettuare nessuna modifica sul router e sugli hosts.**

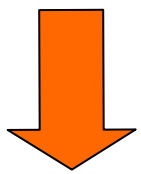
IZS e LINUX



- Il router invia un pacchetto sulla eth0 del firewall credendo che sia la scheda di rete di un host interno
- Il pacchetto entra nel firewall, che dopo avergli applicato le regole di firewall, al corretto destinatario
- Quando un host interno spedisce un pacchetto ad un host remoto, cerca di inviarlo al default gateway, il router.
- Il firewall gli fa credere di essere il router, prende il pacchetto gli applica le regole di firewall e lo invia al router.

IZS e Linux 2

- Alla fine del 2000 l'IZS spinto:
  - dalla necessità di operare un aggiornamento di banda e
  - dall'uscita, sul mercato italiano, di soluzioni di connettività di tipo xDSL a basso costo.



Acquisisce un'ulteriore linea di connettività, INTERBUSINESS, continuando ad utilizzare quella già esistente collegata alla rete universitaria italiana GARR.

IZS e Linux 2

- **PROBLEMA:** distribuire il carico sulle due linee tenendo conto della maggiore banda disponibile sul canale xDSL bilanciato però da un tetto di traffico mensile posto contrattualmente dal provider "Interbusiness" sforato il quale si passa ad una fatturazione a consumo

SOLUZIONE: aggiornamento firewall linux alla suite netfilter+iproute2 del kernel 2.4.x e l'utilizzo delle funzionalità di "statefull inspection" e "tracking connection"

IZS e Linux 2

- Le funzionalità di source-NAT assieme al marking dei pacchetti nel processo di prerouting hanno permesso la navigazione di specifici host sulla linea più veloce

- La Funzionalità di destination-NAT ha permesso ad alcuni server pubblici dell'IZS di essere visibili anche attraverso la seconda linea.

Anagrafe Bovina

- Nel 2002 esigenza di gestire in tempo reale l'anagrafe nazionale degli allevamenti e dei capi bovini e bufalini, che ha comportato una revisione integrale dell'architettura hardware e software.
- L'attenzione si è focalizzata in modo specifico sui seguenti elementi:
  - la sicurezza dell'intero sistema
  - il livello delle prestazioni da garantire al cliente
  - l'affidabilità del nuovo applicativo gestionale
  - garantire una scalabilità dell'architettura

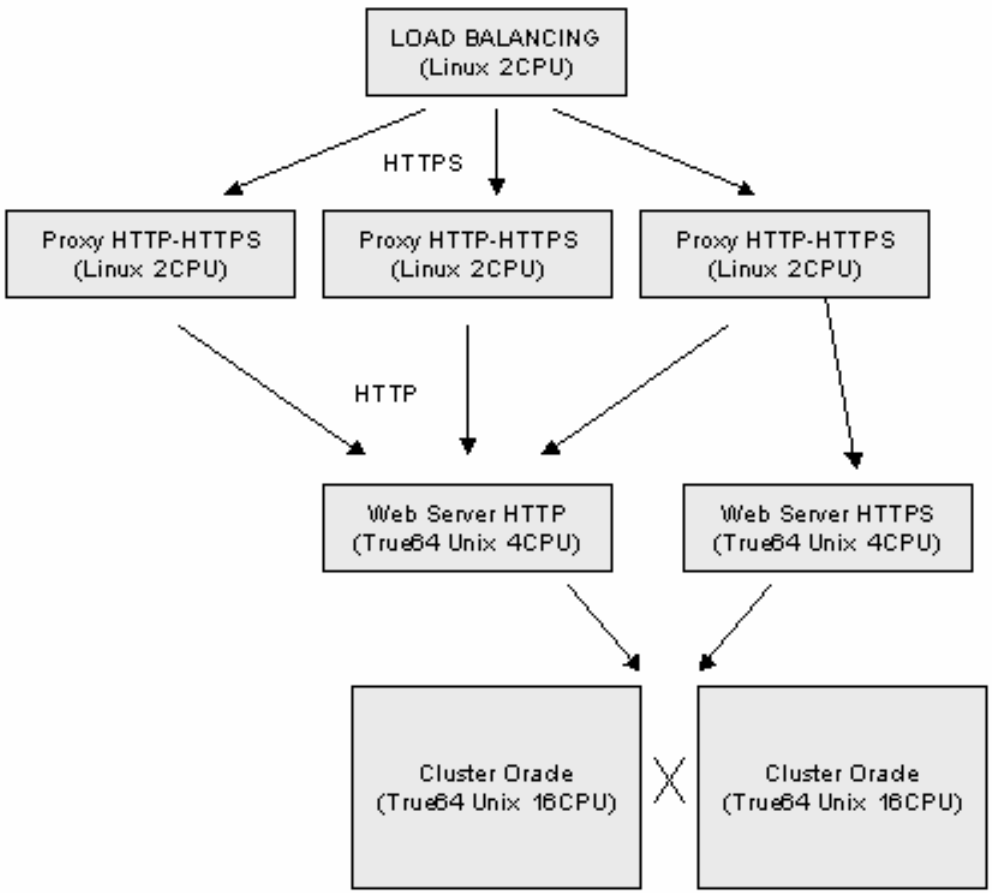
Anagrafe - Sicurezza

- Separazione tra la rete dell'IZS e quella dell'Anagrafe
- Protezione della rete dell'anagrafe con firewall Linux con l'adozione della suite netfilter+iproute2
- Collegamento tra le reti dell'anagrafe e dell'IZS tramite politiche di firewall e regole di routing tra i due firewall

- Crittografia dei dati utilizzando il protocollo sicuro HTTPS tramite l'utilizzo di Apache e dei moduli opensource OpenSSL e mod_ssl

Anagrafe - Scalabilità

- Per attuare la scalabilità si è deciso di costruire una infrastruttura a 4 livelli



Anagrafe - Scalabilità

- Un livello di bilanciatore
- Un livello di server HTTPS
- Un livello di server HTTP

- Un livello per i server con le base dati

Anagrafe - Scalabilità

- Separazione in due livelli tra lo strato di connessione TCP/IP e quello applicativo HTTPS
  - Dover apparire all'esterno come un unico server web (indirizzo www univoco)
  - Necessità di dover scalare l'infrastruttura al crescere delle richieste, distribuendole su più server