

Besnate, 24 Ottobre 2009

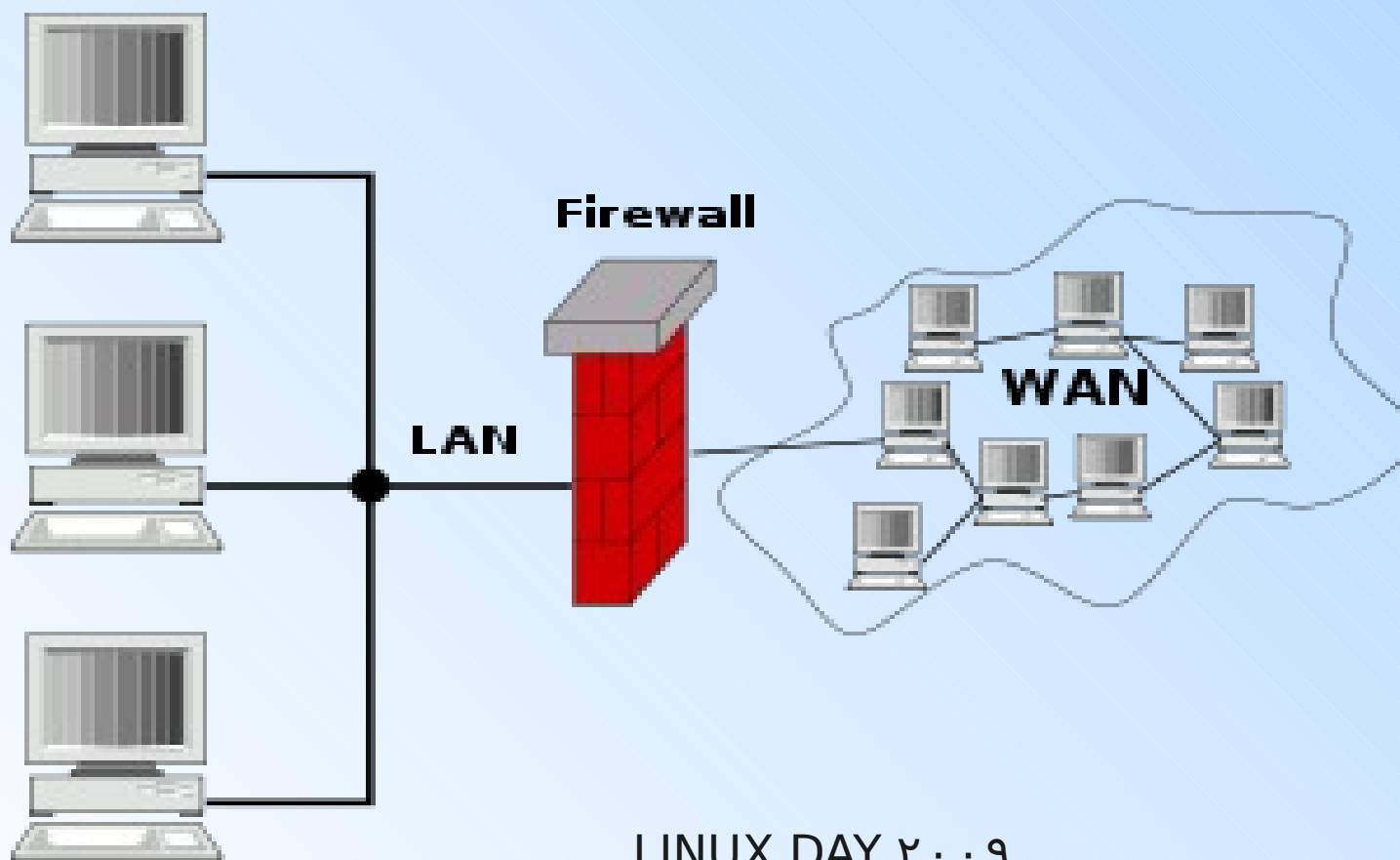


# Oltre il Firewall

Autore: Gianluca  
pipex08@gmail.com

# Cos'è un firewall

- i FIREWALL sono i semafori del traffico “di rete” del nostro PC
- Stabiliscono le regole per i pacchetti che transitano dalla rete WAN alla rete LAN e viceversa



# Il firewall di Linux



- gestito a livello di kernel NetFilter
- l'unico firewall Linux è iptables
- Basato su
  - Regole  
definiscono le azioni da intraprendere sui pacchetti
  - Catene  
definisce come vengono trattati i pacchetti nelle diverse fasi della loro elaborazione
  - Tabelle  
definisce un tipo diverso di operazioni che è possibile effettuare sui pacchetti

# Tabelle / catene / regole



- catene
  - input
  - forward
  - output
- regole
  - accept
  - drop
  - queue
- tabelle
  - filter (prefedinita)
  - nat
  - ...

# manipolare...



Comando → iptables

- **-N** crea una nuova catena
- **-A** aggiunge una regola ad una catena
- **-i** consente, in una regola, di discriminare i pacchetti in base all'interfaccia fisica da cui sono entrati
- **-o** in base all'interfaccia fisica da cui usciranno (scelta in base alle tabelle di routing da noi impostate)
- **-j** di mandare i pacchetti ad un'altra catena
- **-X** per eliminare una catena (tutte, se non viene specificato un argomento)
- **-F** per eliminare tutte le regole di una catena (tutte, se non viene specificato un argomento)
- **-P** per impostare le politiche
  
- **-t** si specifica quale tabella manipolare



# Le applicazioni per gestire il firewall

Package and Debian package URL	Debian package description	Popularity (2008-10-07)
<a href="#">arno-iptables-firewall</a>	Single- and multi-homed firewall script with DSL/ADSL support	400
<a href="#">ferm</a>	maintain and setup complicated firewall rules	224
<a href="#">fiaif</a>	An easy to use, yet complex firewall	51
<a href="#">filtergen</a>	packet filter generator for various firewall systems	38
<a href="#">fireflie</a>	Interactive firewall rule creation tool	167
<a href="#">firehol</a>	An easy to use but powerful iptables stateful firewall	447
<a href="#">firestarter</a>	gtk program for managing and observing your firewall	1475
<a href="#">fwbuilder</a>	Firewall administration tool GUI	2416
<a href="#">guarddog</a>	firewall configuration utility for KDE	595
<a href="#">guidedog</a>	NAT/masquerading/port-forwarding configuration tool for KDE	289
<a href="#">hfl</a>	translator for firewalling rules	19
<a href="#">ipkungfu</a>	iptables-based Linux firewall	50
<a href="#">kmyfirewall</a>	iptables based firewall configuration tool for KDE	487
<a href="#">knetfilter</a>	GUI for configuring the 2.4 kernel IP Tables	267
<a href="#">lokkit</a>	basic interactive firewall configuration tool	584
<a href="#">mason</a>	Interactively creates a Linux packet filtering firewall	35
<a href="#">netscript-2.4</a>	Linux 2.4.x (and 2.6.x) router/firewall network configuration system	39
<a href="#">shorewall</a>	Shoreline Firewall (Shorewall)	2819
<a href="#">uif</a>	Advanced iptables-firewall script	30
<a href="#">uruk</a>	Wrapper for Linux iptables, for filtering rules management	64

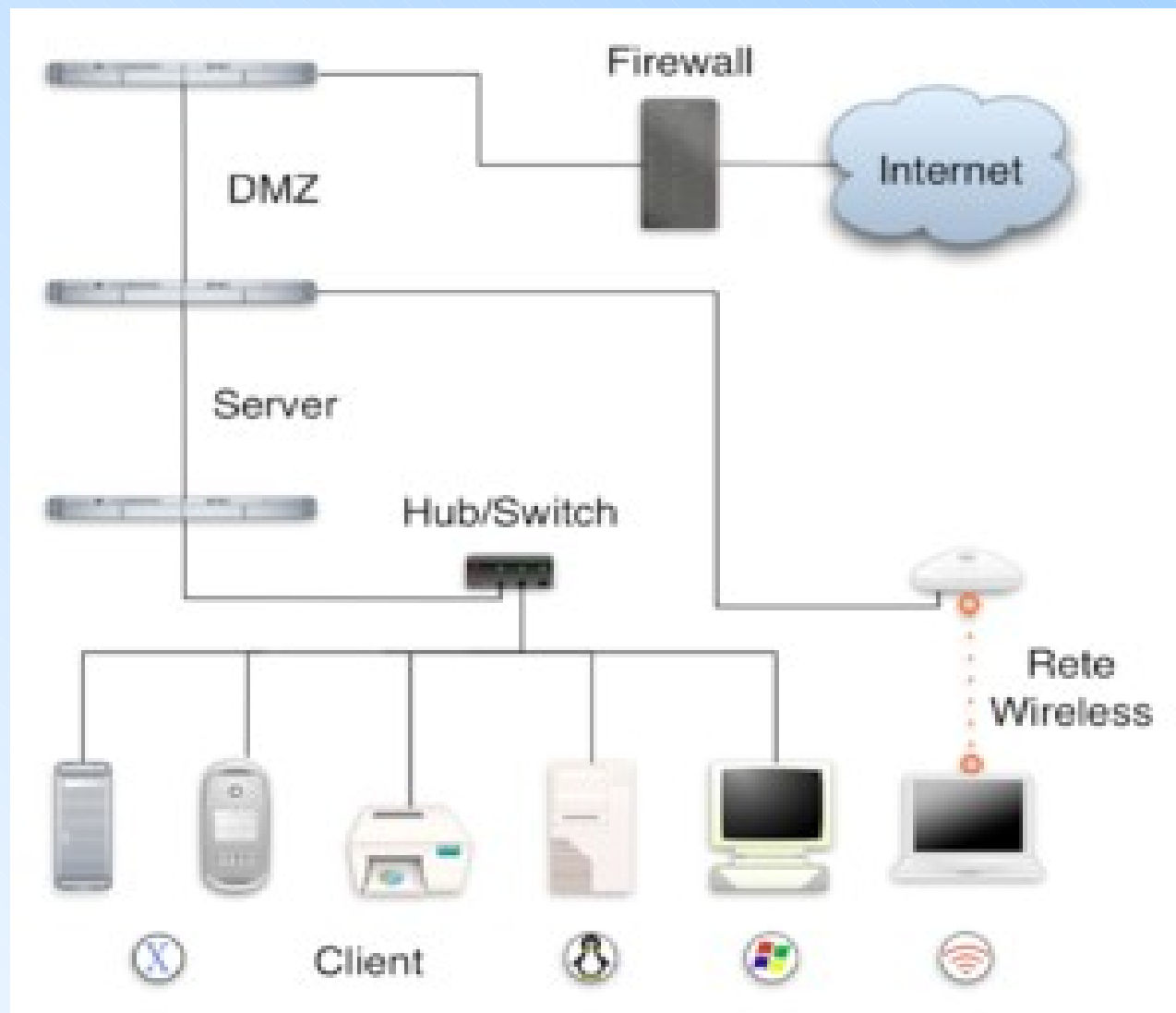
# Demo 1



- firestarter
- Script iptables semplici
  - Firewall con solo DROP policy
  - Nat

# Reti “articolate”

- DMZ
- WLAN
- LAN



# Demo 2



- Iptables con 2 schede di rete
- Iptables “complesso” (fonera Fon Spot)

# limiti dei firewall



- non in grado di gestire il contenuto dei pacchetti
- è statico
- non in grado di riconoscere attacchi
- una delle vulnerabilità più conosciute di un firewall di fascia media è l'HTTP tunneling, che consente di bypassare le restrizioni Internet utilizzando comunicazioni HTTPS solitamente concesse dai firewall

# in-sicurezza



- LAN → autenticazione di un account di posta con uno sniffer attivo con firewall attivo ;)
- Wlan non protetta dal firewall!
- Porte aperte: possono subire attacchi
  - Brute force
  - DoS denial of service
  - Hack zero day
  - ...

# Tools



- Fail2ban  
specifico per servizio: ssh, apache, ...  
analizzatore dei log di iptables  
ban IP
- denyhosts
- Port Knocking  
aprire le porte a richiesta
- One Time Password (hot-spot)  
generatori di accessi/password one-time
- Incapsulamento dei servizi in "canali protetti"

# xIDS



- NIDS Network Intrusion Detection System
  - i sistemi NIDS Network Intrusion Detection System, sono strumenti dediti ad analizzare il traffico di uno o più segmenti di una LAN al fine di individuare anomalie nei flussi o probabili intrusioni informatiche
  - Snort: strumento open source

# Glossario 1/3



Fonte: <http://www.wikipedia.org>

- **Porta**

le porte sono lo strumento utilizzato per realizzare la multiplazione delle connessioni a livello di trasporto, ovvero per permettere ad un calcolatore di effettuare più connessioni contemporanee verso altri calcolatori, facendo in modo che i dati contenuti nei pacchetti in arrivo vengano indirizzati al processo che li sta aspettando.

- **Pacchetto**

Nel gergo informatico si chiama pacchetto ciascuna sequenza di dati distinta trasmessa su una rete o in generale su una linea di comunicazione (ad esempio su una linea seriale) che utilizzi la commutazione di pacchetto.

- **IP**

L'Internet Protocol (IP) è un protocollo di rete a pacchetto, non connesso; secondo la classificazione ISO/OSI è di livello rete (3)

La versione correntemente usata del protocollo IP è detta anche IPv4 per distinguerla dalla più recente IPv6, nata dall'esigenza di gestire meglio il crescente numero di computer connessi ad Internet.

IP è un protocollo di interconnessione di reti (Inter-Networking Protocol), nato per interconnettere reti eterogenee per tecnologia, prestazioni, gestione

I protocolli di trasporto utilizzati su IP sono soprattutto TCP e UDP.

# Glossario 2/3



Fonte: <http://www.wikipedia.org>

- **TCP**

Transmission Control Protocol (TCP) è un protocollo di livello di trasporto della suite di protocolli Internet. È definito nella RFC 793, e su di esso si appoggiano gran parte delle applicazioni Internet.

Il TCP può essere classificato al livello trasporto (OSI level 4) del modello di riferimento OSI, e di solito è usato in combinazione con il protocollo di livello rete (OSI level 3) IP

- **UDP**

Lo User Datagram Protocol (UDP) è uno dei principali protocolli della suite di protocolli Internet. È un protocollo di trasporto a pacchetto, usato di solito in combinazione con il protocollo IP.

# Glossario 3/3



- **LAN**

Una Local Area Network (LAN) (rete in area locale o più semplicemente rete locale in italiano) è una tipologia di rete informatica contraddistinta da un'estensione territoriale non superiore a qualche chilometro.

L'implementazione classica di LAN è quella che serve un'abitazione o un'azienda all'interno di un edificio, o al massimo più edifici adiacenti fra loro.

- **WLAN**

wireless local area network, termine inglese abbreviato in WLAN, indica una rete locale senza fili che sfrutta la tecnologia wireless.

- **WAN**

La rete in area geografica, in sigla WAN (del corrispondente termine inglese "wide area network"), spesso abbreviata anche in rete geografica, è una tipologia di rete informatica contraddistinta da un'estensione territoriale pari ad una regione geografica, quindi superiore sia alla rete locale che alla rete metropolitana.

# Riferimenti e approfondimenti



- <http://www.wikipedia.org>
- Iptable for Fun - C. Contavalli (socio LinuxVar) - <http://www.mod-xslt2.com/people/ccontavalli/docs-it/ip/ip4dummies/>
- Video cracking WEP - <http://www.youtube.com/watch?v=STHbFwsNcVo>