Il FIREWALL LINUX
Basare la sicurezza della rete
su un sistema operativo
gratuito

Cosa si intende per sicurezza di rete

- Accesso a sistemi, servizi e risorse solo da e a persone autorizzate
- Evitare di essere trampolini di lancio per attacchi alla rete
- Evitare di diventare siti Warez
- Proteggere la sicurezza e la privacy delle transazioni da e verso Internet

Quando si diventa dei bersagli

- Collegamenti 24 x 24
  - Linea dedicata
  - Adsl
  - Flat
- Utenti attivi della rete
  - Fornitori di servizi
  - Siti web

Le porte di accesso al calcolatore

- Ogni software di un calcolatore che abbia necessità di comunicare con la rete apre una porta di accesso al nostro calcolatore
- Porte 1…65536
  - 1…1024
    - privilegi di sistema
    - Assegnate in modo standard a particolari servizi
      - 21 = ftp; 25 = smtp; 80 = www; 110 = pop3;
    - molto pericolose
  - Altre sono porte “non privileggiate”
    - Possono essere aperte dinamicamente da altri software o da quelli sopra citati

Come vengo sfruttati questi software

- Se il software di rete è ben costruito è quasi impossibile fare breccia attraverso esso
- Software fatti da esseri umani…quindi non esenti da errori.
- Sono gli errori dei software di rete ad essere utilizzati per l'accesso non autorizzato
- L'esigenza di un software di rete esente da errori è PRIMARIA!!!
- Gli errori si correggono solo se si hanno i sorgenti
- Microsoft non ce li da !!!
- Modello Open Source è inequivocabilmente più sicuro

Modello Open source

- Un modello filosofico di sviluppo, di diffusione e di cooperazione nel campo della I.T.
  - Libertà (0) di eseguire il programma per qualunque scopo senza vincoli sul suo utilizzo.
  - Libertà (1) di studiare il funzionamento del programma e di adattarlo alle proprie esigenze
  - Libertà (2) di ridistribuire copie del programma
  - Libertà (3) di migliorare il programma e distribuire i miglioramenti

Alcuni falsi miti sull'OS

- Tutto il software libero è gratuito. FALSO
  - La libertà non c'entra nulla con il prezzo
- Tutto il software gratuito è libero. FALSO
  - Freeware, Internet Explorer
- Tutto il software libero è senza copyright. FALSO
  - Quasi tutto l'OSS è distribuito con licenza (GPL,BSD)

Vantaggi dell'Open Source

- No costi di licenza quindi budget può prevedere costi più alti per i servizi e quindi servizi di più alto livello
- Indipendenza fornitori. Modello OS impedisce il monopolio
- Sicurezza: disposizione del codice sorgente
- Flessibilità: l'OS è ideale per personalizzazioni e adattamenti

Linux Vs. Windows: sicurezza a confronto

- Linux è OpenSource QUINDI è più sicuro!!!
- Windows è più sicuro solo perché ha usualmente attivi molti meno software di rete
  - Questo non significa che è più sicuro…
  - …significa solo che è distribuito con meno programmi !!!
- Le due regole dell'amministratore di rete
  - Mai usare Microsoft Internet Information server
  - Se proprio devi
    - preparati a passare ogni giorno per Windows Update…
    - Preparati a pregare che il problema sia già stato risolto

Cos’è un firewall

- Strumento che analizza il traffico di rete che lo attraversa applicando dei filtri
- Paragonabile ad una porta chiusa tra la rete interna e il caos di Internet
- La porta si apre solo per determinate informazioni
- Ovviamente, deve avere almeno due interfacce di rete (un ingresso ed una uscita)
- Firewall và configurato!!! NON banale.

Come è e deve essere fatto un firewall

- Può essere un macchinario pronto all'uso dal costo di svariate decine di migliaia di euro
- Può essere un vecchio 486 senza HD con sopra Linux
- Il firewall deve fare solo da firewall. Distribuzioni di default attivano molti servizi inutili e, in un firewall, dannosi.
- Non fidatevi delle configurazioni automatiche delle distribuzioni. Ok solo per utente dialup.

Firewall di tipo packet filter

- Lavorare a livello di pacchetto
  - Livello 3 (network layer) o 4 (trasport layer)
  - Livello di intestazione del pacchetto TCP/IP
- Un pacchetto TCP/IP è fatto cosi:

Struttura di un pacchetto TCP/IP

Header IP (20 bytes)	1	2	3	4	5	6	7	8	9	10	
	Ver / TOS	DSF	Lungh. totale pacchetto		Identification		Flags / Offset		TTL	Proto (TCP)	
	11	12	13	14	15	16	17	18	19	20	
	Checksum		**Indirizzo IP sorgente (xxx.xxx.xxx.xxx)**				**Indirizzo IP destinazione (yyy.yyy.yyy.yyy)**				
Header TCP (20 bytes)	1	2	3	4	5	6	7	8	9	10	
	Porta src (aaaa)		**Porta dest (bbbb)**		Numero di sequenza del pacchetto				Ack Number		
	11	12	13	14	15	16	17	18	19	20	
	Ack Number		Offset / Flags		Windows size		Checksum		Urgent pointer		
Dati	Dati trasportati dal pacchetto										

Firewall di tipo packet filter

- Quindi le regole dei filtri possono basarsi su:
  - Indirizzo IP del mittente
  - Indirizzo IP del destinatario
  - Porta sorgente
  - Porta di destinazione
  - Flags
- Inoltre possono basarsi su
  - Interfaccia di ingresso del pacchetto
  - Interfaccia di uscita del pacchetto

Pro/contro del packet filter

- Vantaggi
  - Alta velocità nell'applicazione dei filtri
  - Degrado prestazioni della rete impercepibile
  - Basse risorse hardware
- Svantaggi
  - Non prende in considerazione gli strati successivi (Sessione,Presentazione, applicazione)
  - Non adatto quindi a filtrare virus, attacchi a server www

Firewall di tipo Application

- Lavorano sull'intero pacchetto TCP/IP
- Pro
  - Adatti a filtrare virus, attacchi web,…
- Contro
  - Degrado delle prestazioni di rete
  - Hardware potente che scala con la crescita del flusso di dati

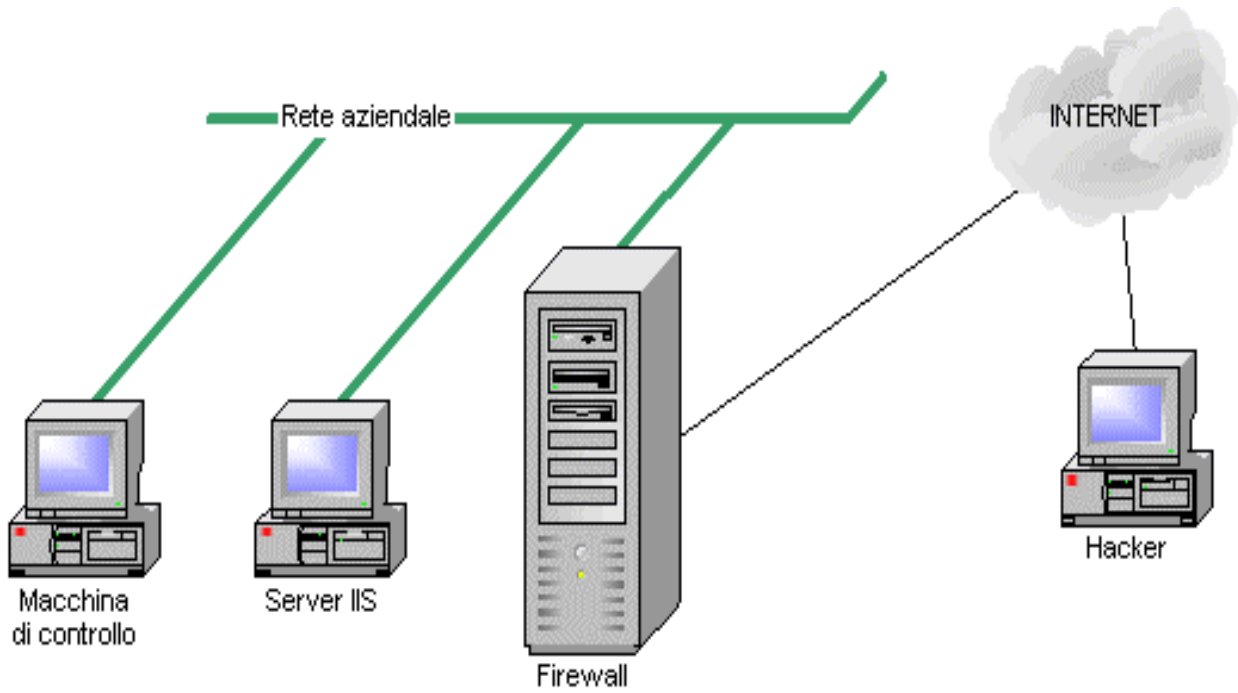
Il vantaggio di avere un firewall

- Si chiudono tutti i servizi che si sa non sono attivi sulla rete
- Server pubblici NON possono essere chiusi…vanno amministrati…con competenza!!!
- Servizi/macchine interne possono essere invisibili dall'esterno
- Altri servizi "non amministrati" eventualmente presenti sulle macchine aziendali non sono comunque visibili dall'esterno

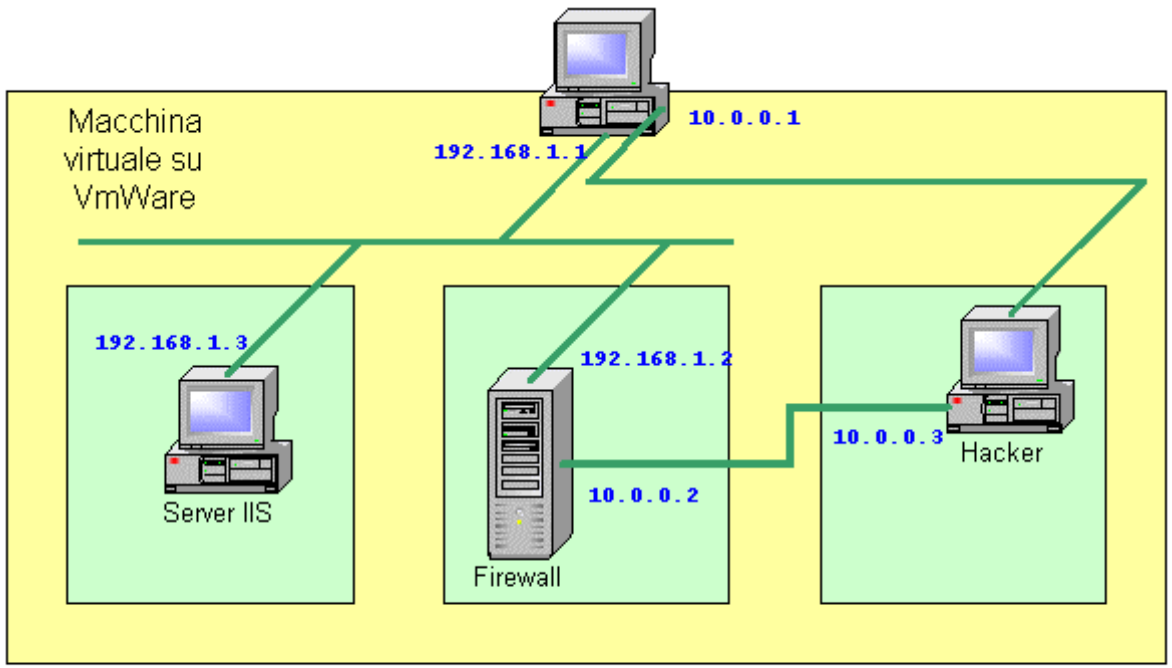
Altre funzionalità del firewall

- Attivazione di VPN con/per sedi remote
- Monitoraggio dell'utilizzo della rete da parte dei vostri utenti interni
- Accesso a determinati host/servizi solo da determinati range di indirizzi IP (sedi distaccate…)
- Blocco di determinate macchine alla navigazione verso determinati siti o verso tutta l'INTERNET (utenti che pensano a navigare invece che a lavorare, siti porno…)
- Blocco di determinati servizi INTERNET (file sharing, chat, download file,…)
- Modifica dei pacchetti TCP/IP

Attacco ad un server Web – Struttura logica della rete d'esempio



Attacco ad un server Web – Struttura reale



Analisi delle strategie di difesa

- Bloccare i servizi che non esistono sulla propria rete
- Quello che conosci lo elimini ☺
- Far passare tutto e bloccare determinati host/servizi è una scelta sbagliata
- Va scelta la filosofia inversa
- Si blocca tutto e si lascia passare solo quei pacchetti diretti verso servizi pubblici
- Configurazione più complessa e rischiosa (si può dimenticare di aprire qualcosa o qualcosa che sembra funzionare poi in realtà non funziona), ma l'unica accettabile

Come si configura un firewall

- Conoscenze non superficiali di
  - TCP/IP
  - Protocolli di rete
  - Routing
- Fare un elenco completo dei servizi che devono essere accessibili dalla rete
- Fare un elenco di situazioni particolare

Configurazione 0

- Tutto quello proveniente dall'esterno o dall'interno per il firewall va bloccato
- Tutto quello proveniente dal firewall va accettato
- Tutto quello proveniente dall'esterno verso l'interno va bloccato
- Tutto quello proveniente dall'interno per l'esterno passa indisturbato

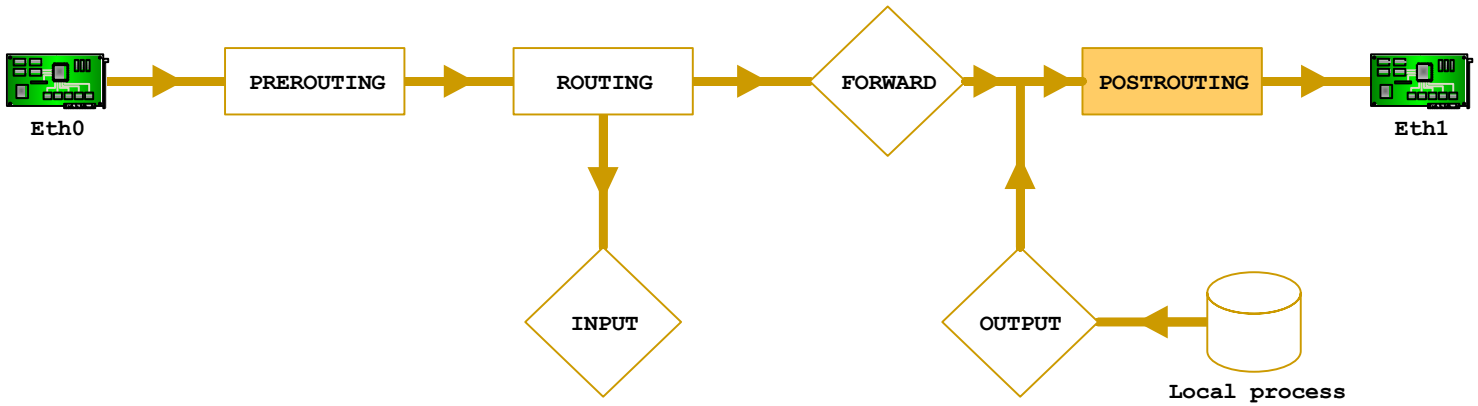
Introduzione a Iptables

- Soluzione completa di firewall su Linux
- Implementata a livello di kernel dalla versione 2.4.0

Plus dell'IpTables

- Gira da un 486 in su
- File di configurazione testuale
- Manipolazione dei pacchetti in diversi momenti del processo di trasferimento del pacchetto da una scheda ad un'altra
- Catene
- Marcatura dei pacchetti IP
- Valido contro i DOS (Rate limiting)
- Passaggio del pacchetto ad una procedura esterna
- Plug-ins

Funzionamento di Iptables



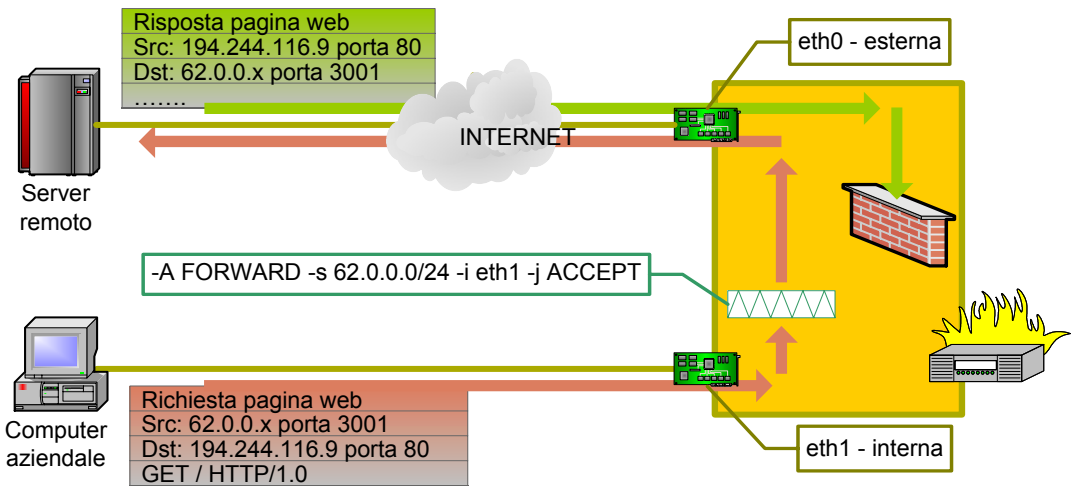
- Durante i vari processi di trasferimento del pacchetto si possono impostare dei filtri decisionali
- Analogia flusso di liquido in un tubo. Questi hook sono fori di ispezione nel tubo da cui è possibile pescare o anche solo osservare il flusso
- ACCEPT – DROP - REJECT

Configurazione di Iptables

- Le prime tre condizioni della configurazione 0 si traduce in
  - `-P INPUT DROP`
    `-P OUTPUT ACCEPT`
    `-P FORWARD DROP`
- La quarta si traduce così
  - `-A FORWARD -s  x.x.x.x/n –i eth1 –j ACCEPT`
- Gli utenti interni non riescono ancora a navigare…pacchetti di risposta non arrivano.

La risposta a richieste interne

- Come mai i pacchetti di risposta non entrano?
  - Sono bloccati dalla regola -P FORWARD DENY!
- Tipica connessione di tipo HTTP



Soluzione standard (no iptables)

- Aprire all'esterno le porte non privilegiate
- Ci si basa sulla assunzione che queste porte
  - Sono aperte per brevi intervalli di tempo (richieste client)
  - Non hanno privilegi di sistema elevati
  - Vengono aperti da sistemi client e non da sistemi server
- Non si tiene conto del fatto che
  - Va contro la filosofia di base di configurazione del firewall
  - Alcuni servizi leciti sono attivi su queste porte (proxy su 3180/8080)
  - Backdoor/trojan si attivano proprio su queste porte

Modulo ip_conntrack (Stateful Inspection)

- Apertura delle porte non privilegiate fa da palliativo all'impossibilità pratica di capire, dal solo pacchetto in ingresso, se sia correlato ad una richiesta interna
- Soluzione di ipTables: tenere traccia delle richieste interne
- Analisi che confronta il pacchetto in ingresso con tutti quelli transitati in uscita
- Questa analisi ritorna un eventuale stato del pacchetto relativamente a pacchetti usciti in precedenza

Stati ritornati da ip_conntrack

- NEW
  - Pacchetto non correlato. Nuova connessione dall'esterno
- ESTABLISHED
  - Pacchetto appartenente ad una connessione esistente (caso richiesta www)
- RELATED
  - Pacchetto correlato ma non appartenente ad una connessione (caso richiesta FTP-FTP data)
- INVALID
  - Errore nel processo di ricerca
- La regola che completa la configurazione 0 e' quindi
  - `-A FORWARD -d x.x.x.x/n -m state \`
    `--state ESTABLISHED,RELATED -j ACCEPT`

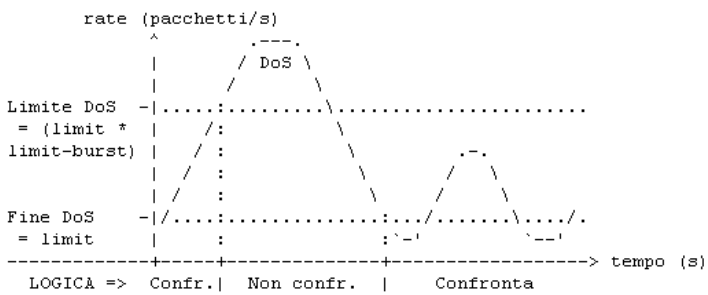
Aprire un servizio pubblico

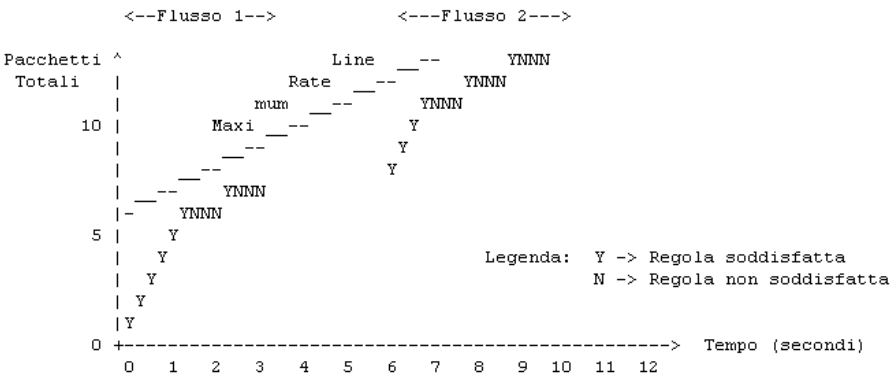
- Server web interno
  - `-A FORWARD -p tcp -d y.y.y.y \`
    `--dport web -j ACCEPT`

Limit Bursting e porte istericheche

- Limitare i ping in ingresso

```
-t FILTER \
  -A FORWARD \
  -p icmp \
  -icmp-type \
   echo-request \
  -m limit \
  -limit 1/s \
  -j ACCEPT
```





SNAT e il masquerade

- `-t nat -A POSTROUTING -o ppp0 -j MASQUERADE`
- `-t nat -A POSTROUTING -o eth0 -j SNAT \`
  `-to xxx.xxx.xxx.xxx`

Destination Nat

- `-t nat -A PREROUTING -p tcp -d y.y.y.y \`
  `-dport web -j DNAT -to z.z.z.z`

Routing avanzato

- `-A PREROUTING -i eth0 -t mangle -p tcp \`
  `-dport web -j MARK --set-mark 1`
- `ip rule add from x.x.x.x table linkFast`
- `Ip route add default via y.y.y.y dev eth1 \`
  `table linkFast`
- `Ip rule add fwmark 1 lookup linkFast`

Riferimenti

- Linux Networking HowTo
- Linux 2.4 Packet Filtering HowTo
- Linux 2.4 Nat HowTo
- IpRoute2 Utility Suite HowTo
- Linux 2.4 Advanced Routing HowTo
- MonMotha’a Firewall configuration files
- Linux firewall: metti una marchia in più nella tua rete
  - http://www.ebruni.it/it/???