Ehi Tu! Si tu con quel computer sotto braccio.. Dove pensi di andare? ...E` ovvio a installare il Firewall!

Giuseppe Marocchio
Giuseppe@irmos.it
http://www.giuseppe-marocchio.com
GPG Key ID 0XB905E35B

$ whois lan

-Socio di LUGVR, Metro Olografix, Ush.it

-Gioca e lavora regolarmente con PHP / Apache / iptables / Linux e OpenBSD in genere

Finalità

-Prendere coscienza dei pericoli di internet

-capire perchè è importante proteggersi

-capire cosa fa e cosa non fa un firewall

Firewall?

Firewall viene letteralmente tradotto in **“muro di fuoco”**. Questo muro virtuale ha il compito di proteggerci da eventuali malintenzionati che vogliano sfruttare i nostri sistemi informatici

Perché proteggerci?

-È un vostro diritto

-Molte persone sono maliziose

-La sicurezza non è mai troppa

-I vostri dati sono importanti

-Risparmiarsi problemi evitabili

ma... è la Panacea?

NO

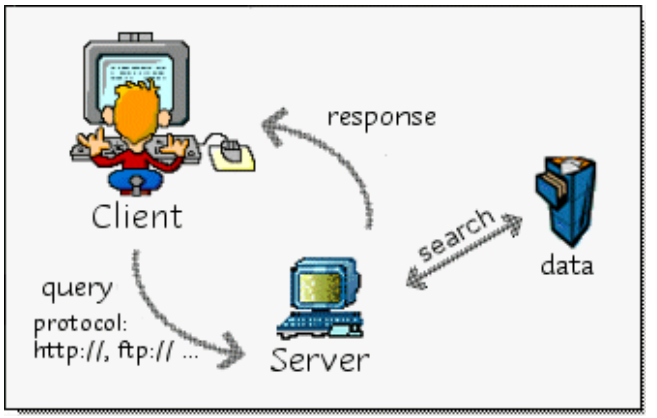
Un firewall non protegge da tutti i pericoli che possiamo incontrare su internet: ad esempio lo SPAM e i Virus non sono materia da firewall

E.. a cosa servirebbe?

Un firewall lavora solitamente ai livelli 2/3/4 della pila ISO/OSI, in pratica FILTRA le connessioni che ci arrivano o partono dal nostro PC

Cosa sono i servizi?

Un servizio è un applicazione che resta in ascolto su una determinata porta, ad ogni richiesta posta viene quindi generata una risposta inviata via rete.



Es: www, ftp, smtp, pop3

Chi offre i servizi?

Tutti i computers offrono servizi, chi più chi meno. Anche solo per trasferire file da un pc a un altro viene utilizzato un servizio. Diventa quindi **Importantissimo** definire **CHI** può accedevi. E questa è materia da **Firewall.**

Proteggere solo i servizi?

No! esistono molti tipi di attacco che non comportano un intrusione ma provocano **SOLO** una congestione sulle vostre connessioni. Si chiamano **DOS** e possono mettere **fuori uso la vostra rete anche per giorni.!**

ho bisogno di un Firewall!

CERTO!

Tutti hanno bisogno di un firewall
è nel vostro interesse averlo,
tutti abbiamo qualche servizio da
proteggere.

ma... Quale Firewall?

Eistono molti strumenti che fanno
da firewall, e c'è chi lo fa meglio
e chi lo fa peggio.

Quale scelgo??

Scegliere il firewall

Le alternative sono veramente molte
ma il consiglio è quello di
affidarsi a strumenti **OpenSource**
dove si è veramente **SICURI** che non
ci siano sorprese.

Si all'opensource!

Miglia di persone che leggono il codice sorgente in tutto il mondo sono una vera **GARANZIA** per la qualità, il numero di bachi si riduce drasticamente, e si ha la certezza che non ci siano Backdoor nel applicativo.

Qualcuno si ribellerebbe di sicuro!

Ho deciso, OpenSource!

L'opensource è bella perchè è **varia**, infatti sono molte le soluzioni che ci vengono messe a disposizione, alcune si equivalgono, altre si diversificano.

È quasi una giungla!

Le soluzioni

Ecco alcune soluzioni disponibili:

Linux: iptables / ipchains (OLD)
FreeBSD: pf / ipwf
OpenBSD: pf

E.. Windows?

Windows!?! come potete affidare la sicurezza dei vostri dati a un sistema operativo di cui non possiamo conoscere l'implementazione? Potrebbe succedere di TUTTO.

NO, IO non voglio rischiare... e VOI ?

Ma io ho il router!

NON importa! un router (da supermercato) solitamente fa banalmente NAT e come ci ha spiegato Alessio in un altra occasiona NAT non è una sicurezza!

“Un router è una scatoletta elettrica che talvolta riesce a connettersi a internet”
cit: A. L.R. P.

E.. il Fw hardware?

Il firewall hardware non è un vero firewall, spesso è una scatoletta elettrica con qualche lucetta che talvolta riesce fa fare da firewall, solitamente sono prodotti proprietari che si possono equiparare a windows... (per configurazione e amministrazione)
ma.. qualcuno si salva!

Chi? Quale Vendor?

Svariati vendor (non più di 5 o 6) rilasciano i sorgenti del proprio prodotto... un esempio? **Linksys**! I suoi router/firewall Linux based sono **OpenSource**! SI di questi possiamo fidarci!

Distribuzioni Dedicate

Esistono distribuzioni linux di facile uso pensate apposta per i fungere da firewall sono tutte OpenSource e spesso sono anche gratuite. Dotate di interfaccia web permettono anche ai meno esperti di effettuare piccole modifiche in caso di necessità

Ora ho capito!

Ora so di chi mi posso fidare ma in pratica... cosa si fa quando si configura un firewall? È semplice! Si scrivono delle **REGOLE** in base alle quali decidiamo COSA far **passare**, cosa **bloccare** e di cosa **tener traccia**

Un esempio

Ho un server linux, voglio bloccare tutte le richieste in arrivo sulla porta 22 da parte sistemi diversi dal mio!

Iptables -A INPUT -p tcp –dport 22 -s ! 10.80.2.4 -j DROP

Altri Esempi

pass in on dc1 proto tcp all keep state
(pf)

iptables -A LANINT -p tcp -s 10.1.1.0/24 gateway.messenger.hotmail.com -j DROP

ad esempio la seconda regola blocca MSN messanger da una rete locale

È complicato!

Si è vero scrivere le regole di un firewall è tuttaltro che semplice, fortuamente ci sono delle aziende che possono fare questo lavoro per voi! Ma ricordate sempre di chidere una soluzione OpenSource!

Il pericolo è **ovunque**

Il pericolo è ovunque su internet non centra la vostra connessione, il vostro provider, siete **SEMPRE** sotto attacco. Bisogna **PROTEGGERSI**, anche la rete wireless di casa va protetta!

Paranoid is a Virtue!

Siate **paranoici**! E non dimenticate che la sicurezza è un cammino non una meta, bisogna tenere aggiornati costantemente i propri sistemi non si arriva **MAI**.

A chi non fa almeno una
domanda, che alzandosi
si strappi una mutanda!

Bibliografia

- www.openbsd.org
- www.isc.org
- www.kernel.org
- www.netfilter.org
- $ man && google :)

Licenza

Grazie della partecipazione.

Sono a vostra disposizione per qualsiasi chiarimento o precisazione.