



PROTEZIONE DI UNA SERVER-FARM

UTILIZZANDO LE IPTABLES DI LINUX

di Gennari Alessandro

MegaByte Sistemi Informatici – Cento (Fe)

Credo sia doveroso un ringraziamento a Fulvio Ricciardi per l'ottimo e stabile prodotto che con tanta pazienza ha creato e messo a disposizione della comunità.

In questo documento, illustro ciò che ho attuato, partendo dalla versione 1.0 beta 9, giungendo in tutta tranquillità alla attuale versione 1.0 beta 13, decisamente affidabile.

Il progetto iniziale, prevedeva di proteggere una serie di server aziendali, collocati in server-farm e collegati ad essa con rete locale a 100 mbit/s (ora siamo collegati ad 1 GB/s).

Come primo step fu acquistato un firewall hardware, di marca nota e notevolmente diffuso, con buone prestazioni (promesse) che integrasse in sé anche il controllo antispam ed antivirus a licenze rinnovabili annualmente.

Un disastro.

Le prestazioni, se attivati antispam ed antivirus erano degne di una connessione isdn, ma se disattivati, le cose miglioravano notevolmente, quindi ho optato per la disattivazione di questi comunque onerosi servizi e per questi sono andato avanti per altre strade.

Ma vi fu un momento dove il traffico web, sommato al traffico di posta si fece sentire parecchio ed anche lì (parliamo di un traffico costante di 20-30 mbit/s costanti...) il firewall andava praticamente in blocco, congelando l'accesso ai server, che diventavano "intermittenti".

Questa la goccia che mi ha fatto definitivamente "cestinare" il firewall hardware ed optare per un firewall software con hardware autocostruito.

Dopo un paio di prove, con software di larga diffusione, ma sempre rigorosamente "free" per fortuna mi sono imbattuto in ZeroShell.

Installato con soddisfazione in quanto ha riconosciuto tutto l'hardware istantaneamente e provato con altrettanta soddisfazione la configurazione via browser, ho effettuato subito un piccolo stress-test, ampiamente passato con successo.

Il software utilizzato per le prove di stress e vulnerabilità, è NSASOFT Stress Test (ora NSAuditor).

Morale : il firewall è passato immediatamente in produzione e da allora non ho fatto altro che aggiornarlo puntualmente (un mese dopo ogni rilascio).

Questa la configurazione hardware :

- Rack Supermicro 1 U, con alimentazione ridondante
- Motherboard Supermicro PDSMi - LN4+
- CPU Xeon 3040
- Ram 1 GB DDR2
- HardDisk DOM 2 GB USB 2.0
- Ethernet Gigabit x 4
- Lettore DVD
- IPMI

Come configurazione non è certamente a basso costo, perché tra un componente e l'altro, si aggira sui 900 Euro circa, se non oltre.

Posso garantire che però le prestazioni sono di tutto rispetto, visto che dopo qualche anno di onorato servizio, l'impegno della CPU difficilmente arriva a superare il 5% nonostante il traffico giornaliero sia di circa 35 GB di dati !!!

Insomma, nulla da invidiare a firewall ben più blasonati.

Il tipo di configurazione che ho voluto adottare, tutto sommato è molto semplice, ed utilizza solo le regole di IPTABLES.

Elenco qui sotto la configurazione software :

Interfaccia Lan : ETH00
Interfaccia Wan : ETH03

La lan interna è in classe A e corrisponde solo ad una porzione di essa, essendo configurata una subnet mask di tipo C, quindi LAN :

Indirizzi : 10.0.0.x Subnet : 255.255.255.0

Come Gateway ho voluto lasciare 10.0.0.1.

Su questo range di indirizzi, sono però riservati degli IP dinamici, che vanno dall'indirizzo 10.0.0.240 al 249, allo scopo di assegnare IP nel caso che si perdesse involontariamente il controllo delle schede di rete dei server, oltre a provvedere al rilascio temporaneo di IP ai vari server virtuali.

Gli indirizzi dal 10.0.0.2 al 239 sono rigorosamente fissi e corrispondono ad una decina di server "utilizzabili" ma nello stesso range, cadono i server host VMWare, le NAS, i server FTP ed alcune macchine fisiche.

Di fatto, una volta configurati i parametri essenziali, partendo dal BIOS, nel quale ho attivato l'accensione automatica una volta rilevata tensione sugli alimentatori, deciso l'unità primaria e secondaria di boot (DVD e DOM USB), installato il software come da documentazione presente sul sito www.zeroshell.net, configurata la LAN per poter accedere, sono passato a configurare correttamente su ETH03 tutti gli indirizzi IP pubblici (mi hanno assegnato una intera classe di 256 IP, quindi 253 utilizzabili per i server).

Configurato il GATEWAY con l'IP pubblico assegnatomi, sono passato alla configurazione importantissima di data ed ora, tramite i server NTP :

TimeZone : Europe/Rome
NTP : 130.60.75.60
: 209.104.4.227
: 200.144.121.33
: 193.40.133.134

Fatto ciò sono passato alla configurazione dei servizi SSH ed HTTPS, con accessibilità da ogni interfaccia, dando ovviamente dei criteri di sicurezza, soprattutto impostando su questi quale era l'indirizzo IP dal quale accedere sulle interfacce pubbliche, mentre da quelle interne è rimasto tutto aperto.

Visto l'utilizzo di una DOM USB, per evitare problemi, ho deciso di limitare i LOG, impostando un utilizzo degli stessi nella sezione Auto-Management :

Compress the oldest Log : Threshold = 40%
Delete the oldest Log : Threshold = 55%

Questo giusto per avere un minimo di LOG diagnostico.

Infine, nella sezione SCRIPTING EDITOR, in NAT and VIRTUAL SERVERS ho fatto ampio uso delle regole IPTABLES, mappando server per server le porte che voglio aprire e su quale server devono essere redirezionate.

Questo ha comportato una notevole efficienza ed una versatilità fuori dall'ordinario, di facile utilizzo ed altrettanto facile velocità di modifica e di controllo.

Unica pecca, ogni tanto, quando si creano tante regole, magari un po' complesse, si è costretti ad un riavviamento del firewall, ma è un male da poco, in quanto torna in linea in un paio di minuti.

Buon lavoro

Alessandro Gennari

REGOLE UTILIZZATE IN SCRIPTING EDITOR

NAT and VIRTUAL SERVERS

Per ovvii motivi, utilizzerò degli indirizzi interni fittizi ma realmente utilizzabili, mentre per quelli pubblici il range sarà puramente di fantasia e dovranno essere rimpiazzati da quelli reali.

Teniamo conto che se sarà assegnato un range di 8 IP, solo dal terzo al settimo saranno quelli realmente utilizzabili.

Per gli IP pubblici utilizzerò il range 82.10.20.1 – 50 (facendo corrispondere la parte finale degli IP pubblici con quelli interni)

```
# Tabella IP dei Server Interni
#
# FIREWALL      =      10.0.0.1      (HTTPS, SSH)
# WEBSERVER    =      10.0.0.10     (SSH, HTTP, HTTPS, FTP)
# MYSQLSERVER  =      10.0.0.20     (SSH, HTTP, HTTPS, MYSQL)
# FTPSERVER    =      10.0.0.30     (SSH, FTP, SFTP, HTTP, HTTPS)
# MAILSERVER   =      10.0.0.40     (SSH, SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS, HTTP, HTTPS, MYSQL)
# TERMSERVER   =      10.0.0.50     (RDP)
# -----
#
# Il firewall ZeroShell viene configurato via HTTPS o SSH, e volutamente non fa parte di nessuna regola qui sotto elencata

# Server : WEBSERVER
#
iptables -t nat -A PREROUTING -p tcp --dport 20 -d 82.10.20.10 -i ETH03 -j DNAT --to-destination 10.0.0.10:20
iptables -t nat -A PREROUTING -p tcp --dport 21 -d 82.10.20.10 -i ETH03 -j DNAT --to-destination 10.0.0.10:21
iptables -t nat -A PREROUTING -p tcp --dport 22 -d 82.10.20.10 -i ETH03 -j DNAT --to-destination 10.0.0.10:22
iptables -t nat -A PREROUTING -p tcp --dport 80 -d 82.10.20.10 -i ETH03 -j DNAT --to-destination 10.0.0.10:80
iptables -t nat -A PREROUTING -p tcp --dport 443 -d 82.10.20.10 -i ETH03 -j DNAT --to-destination 10.0.0.10:443

# Server : MYSQLSERVER
#
iptables -t nat -A PREROUTING -p tcp --dport 22 -d 82.10.20.20 -i ETH03 -j DNAT --to-destination 10.0.0.20:22
iptables -t nat -A PREROUTING -p tcp --dport 80 -d 82.10.20.20 -i ETH03 -j DNAT --to-destination 10.0.0.20:80
iptables -t nat -A PREROUTING -p tcp --dport 443 -d 82.10.20.20 -i ETH03 -j DNAT --to-destination 10.0.0.20:443
iptables -t nat -A PREROUTING -p tcp --dport 3306 -d 82.10.20.20 -i ETH03 -j DNAT --to-destination 10.0.0.20:3306

# Server : FTPSERVER
#
iptables -t nat -A PREROUTING -p tcp --dport 20 -d 82.10.20.30 -i ETH03 -j DNAT --to-destination 10.0.0.30:20
iptables -t nat -A PREROUTING -p tcp --dport 21 -d 82.10.20.30 -i ETH03 -j DNAT --to-destination 10.0.0.30:21
iptables -t nat -A PREROUTING -p tcp --dport 22 -d 82.10.20.30 -i ETH03 -j DNAT --to-destination 10.0.0.30:22
iptables -t nat -A PREROUTING -p tcp --dport 80 -d 82.10.20.30 -i ETH03 -j DNAT --to-destination 10.0.0.30:80
iptables -t nat -A PREROUTING -p tcp --dport 443 -d 82.10.20.30 -i ETH03 -j DNAT --to-destination 10.0.0.30:443

# Server : MAILSERVER
#
iptables -t nat -A PREROUTING -p tcp --dport 22 -d 82.10.20.40 -i ETH03 -j DNAT --to-destination 10.0.0.40:22
iptables -t nat -A PREROUTING -p tcp --dport 25 -d 82.10.20.40 -i ETH03 -j DNAT --to-destination 10.0.0.40:25
iptables -t nat -A PREROUTING -p tcp --dport 80 -d 82.10.20.40 -i ETH03 -j DNAT --to-destination 10.0.0.40:80
iptables -t nat -A PREROUTING -p tcp --dport 110 -d 82.10.20.40 -i ETH03 -j DNAT --to-destination 10.0.0.40:110
iptables -t nat -A PREROUTING -p tcp --dport 143 -d 82.10.20.40 -i ETH03 -j DNAT --to-destination 10.0.0.40:143
iptables -t nat -A PREROUTING -p tcp --dport 443 -d 82.10.20.40 -i ETH03 -j DNAT --to-destination 10.0.0.40:443
iptables -t nat -A PREROUTING -p tcp --dport 465 -d 82.10.20.40 -i ETH03 -j DNAT --to-destination 10.0.0.40:465
iptables -t nat -A PREROUTING -p tcp --dport 587 -d 82.10.20.40 -i ETH03 -j DNAT --to-destination 10.0.0.40:587
iptables -t nat -A PREROUTING -p tcp --dport 993 -d 82.10.20.40 -i ETH03 -j DNAT --to-destination 10.0.0.40:993
iptables -t nat -A PREROUTING -p tcp --dport 995 -d 82.10.20.40 -i ETH03 -j DNAT --to-destination 10.0.0.40:995
iptables -t nat -A PREROUTING -p tcp --dport 3306 -d 82.10.20.40 -i ETH03 -j DNAT --to-destination 10.0.0.40:3306

# Server : TERMSERVER
#
iptables -t nat -A PREROUTING -p tcp --dport 3389 -d 82.10.20.50 -i ETH03 -j DNAT --to-destination 10.0.0.50:3389

# REGOLE PER PORTE UDP
# Nel caso servisse attivare una regola per porte UDP, inserire la seguente riga (debitamente configurata)
# iptables -t nat -A PREROUTING -p udp -i ETH03 -d 82.10.20.xx --dport 1234 -j DNAT --to-destination 10.0.0.xx:1234

# Regole di POSTROUTING (ASSOLUTAMENTE DA NON DIMENTICARE !!!)
iptables -t nat -I POSTROUTING 1 -s 10.0.0.10 -o ETH03 -j SNAT --to 82.10.20.10
iptables -t nat -I POSTROUTING 1 -s 10.0.0.20 -o ETH03 -j SNAT --to 82.10.20.20
iptables -t nat -I POSTROUTING 1 -s 10.0.0.30 -o ETH03 -j SNAT --to 82.10.20.30
iptables -t nat -I POSTROUTING 1 -s 10.0.0.40 -o ETH03 -j SNAT --to 82.10.20.40
iptables -t nat -I POSTROUTING 1 -s 10.0.0.50 -o ETH03 -j SNAT --to 82.10.20.50
```

P.S.: Avendo ritrascritto una parte della configurazione da me funzionante, spero di non avere commesso errori.
Nel caso, non abbiate problemi a contattarmi all'indirizzo : itc@datarack.it