ISTITUTO NAZIONALE DI FISICA NUCLEARE

Centro Nazionale CNAF

INFN/TC-03/07
10 Giugno 2003

NOTA TECNICA SUL POSSIBILE UTILIZZO DI FIREWALL NELL' INFN

Stefano Zani[1], Riccardo Veraldi[2], Franco Brasolin[3], Angelo Veloce[4], Mario Masciarelli[4], Claudio Soprano[4], Fulvia Costa[5]

[1] *Istituto Nazionale di Fisica Nucleare C.N.A.F.*
[2] *Istituto Nazionale di Fisica Nucleare Sezione di Firenze*
[3] *Istituto Nazionale di Fisica Nucleare Sezione di Bologna*
[4] *Istituto Nazionale di Fisica Nucleare Laboratori Nazionali di Frascati*
[5] *Istituto Nazionale di Fisica Nucleare Sezione di Padova*

Abstract

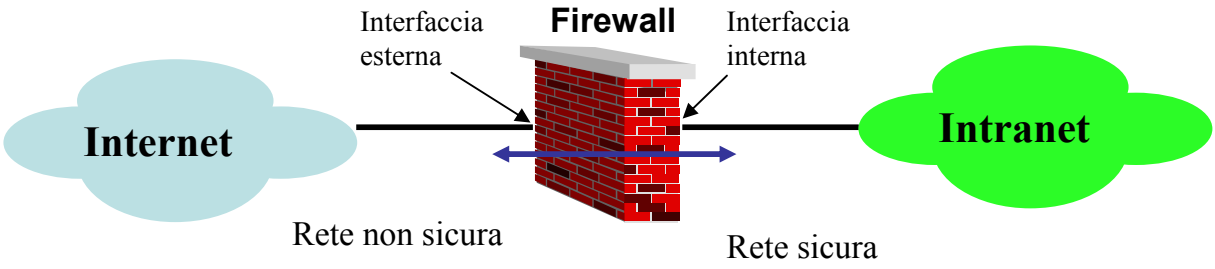
Questo documento e' una nota tecnica prodotta dal sottogruppo Firewall del Netgroup afferente alla Commissione Calcolo e Reti dell'INFN.

Il documento contiene un resoconto sui test effettuati sulle piattaforme di Firewall più diffuse e fornisce una valutazione dal punto di vista della funzionalità, gestibilità e prestazioni nell'ottica di possibili applicazioni nelle sezioni INFN.

Published by ***SIS–Pubblicazioni***
Laboratori Nazionali di Frascati

Introduzione:

Si può definire il firewall come un apparato che si pone fra una parte della rete che deve essere protetta da eventuali tentativi di intrusione ed il resto della rete svolgendo una funzione di filtro sui pacchetti che lo attraversano.
Nel corso del tempo con lo sviluppo delle tecnologie, con la parola Firewall si sono individuati device differenti sempre più complessi, la funzionalità principale e comune a tutti è quella di "Packet filter".
Il Packet filter essenzialmente decide pacchetto per pacchetto se permettergli di passare o no in base all'indirizzo di origine, alla porta di origine, all'indirizzo di destinazione o alla porta di destinazione. In alcuni casi "Stateful inspection Firewall" Può tener conto anche dello "stato" della connessione.



Per discriminare quale pacchetto può transitare attraverso al Firewall vengono definite delle ***Access Control List*** (ACL) costituite da un insieme di regole che vengono applicate alle interfacce del Firewall in ingresso o in uscita.
La funzionalità di valutazione di ACL composte da regole molto complesse richiede una notevole potenza di calcolo e questo è il motivo per cui fino a pochi anni fa questa funzionalità era riservata a macchine dedicate: I primi Firewall veri e propri.
Con l'utilizzo di CPU sempre più potenti anche all'interno dei personal computer e l'impiego di ASIC all'interno dei Router e degli Switch questa funzionalità si può realizzare anche direttamente sugli apparati di rete evoluti o mediante software su computer "Normali".
L'INFN attraverso l'operato del Netgroup ha voluto indagare su quanto è disponibile per la realizzazione di un firewall utilizzando le differenti tecnologie disponibili sul mercato.
Per quanto riguarda l'applicazione di ACL sui router sono già disponibili alcune note tecniche sul sito del gruppo che verranno referenziate in appendice B.
Il documento tratterà di implementazioni di firewall basati su piattaforme OPEN ed in particolare su OpenBSD, di firewall software e di Box proprietari.

I Componenti del sottogruppo

F.Brasolin, R.Veraldi, S.Zani, A.Veloce, S.Lusso, A.Forte, M.Masciarelli, C.Soprano.

Inoltre hanno partecipato alle prove:

O.Pinazza, D. De Girolamo.

Firewall presi in esame

Il gruppo ha preso in esame sei differenti firewall:

- **Cisco PIX 515** *(Fornito da Cisco)*
- **Box OpenBsd** *(Software gratuto, box di INFN sez. di Firenze)*
- **Infoguard IGWall** *(Fornito da Uniautomation)*
- **Symantec 5300** *(Fornito da EcoByte per Symantec)*
- **Clavister** *(Fornito da Exwai per Clavister)In uso a UniBari e Caspur*
- **Nokia + CheckPoint** *(Uniautomation per Nokia)*

A parte il Box OpenBSD che è basato appunto su OpenBSD e PF che sono gratuiti, tutti gli altri Box sono stati concessi in prova gratuita dalle ditte indicate fra parentesi.
Il firewall Clavister è un pacchetto software proprietario che è stato installato su di un Box di nostra proprietà, tutte le altre soluzioni sono costituite da harware e software proprietari.

Prove effettuate

Per provare gli apparati si è proceduto ad una installazione di base da scratch e ad alla configurazione di "Access Control List" di complessità e dimensioni differenti.
Si è anche cercato di capire se questi apparati introducessero ritardi rilevanti nel forwarding dei pacchetti o se costituissero un limite in termini di banda passante.
Durante le prove si è tenuto conto dei seguenti aspetti:

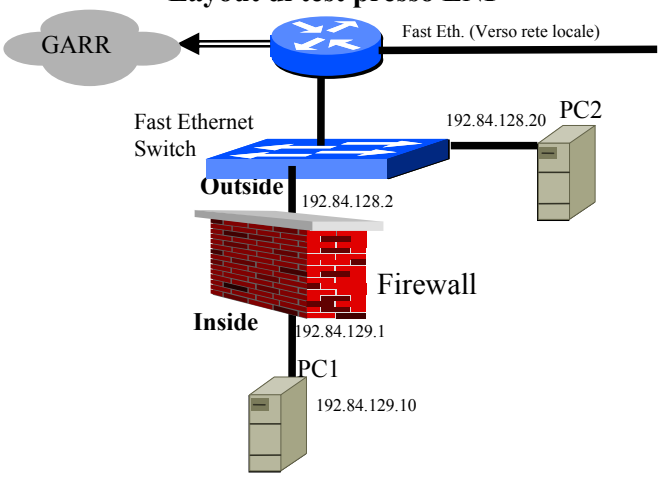
- Configurabilità dell'apparato.
- Eventuali sistemi di gestione e controllo.
- Verifica (Per quanto possibile) delle prestazioni del Box al variare della complessità delle regole applicate.

Per la misura dell'eventuale ritardo introdotto si è generalmente utilizzato il ping mentre per misure di throughput si è utilizzato Netperf 2.1pl3.

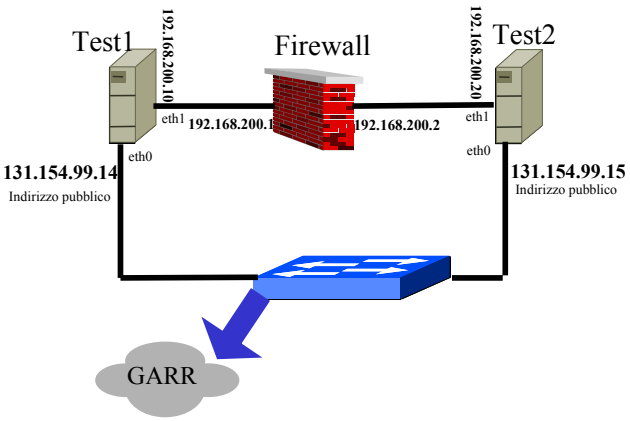
Layout ti test

Per provare gli apparati si è scelto di realizzare due layout di test uno presso i Laboratori Nazionali di Frascati e uno presso il CNAF di Bologna.

Layout di test presso LNF

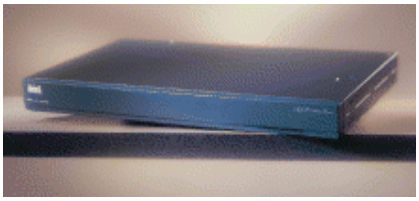


Layout di test presso il CNAF



Queste reti di test ci hanno permesso di realizzare tutte le configurazioni di prova senza impattare sul traffico di produzione.
Per provare in maniera più completa questi apparati, il modo migliore è quello di verificarne il comportamento inserendolo in una rete di produzione.
I due apparati ritenuti più interessanti sono stati inseriti sulla rete di produzione della Sezione di Bologna .

Cisco PIX 515



Test effettuati il 03/07/2002 presso:
Laboratori Nazionali di Frascati - Via E. Fermi,40 -- 00044 Frascati (RM)

Caratteristiche Firewall CISCO Testato:

Articolo	Descrizione	Quantita'	Asset Number	Serial Number
PIX-515	PIX 515 Chassis only	1	1596	44403300051
	CAB-ACI			
	SF-PIX-6.1			
	PIX-515UR-SW			
PIX-4FE	PIX Four-port 10/100 Ethernet interface, RJ45	1	25977	INV007336
PIX-VPN-ACCEL	VPN Accelerator Card (VAC) for PIX Firewall	1	58105	INV013037

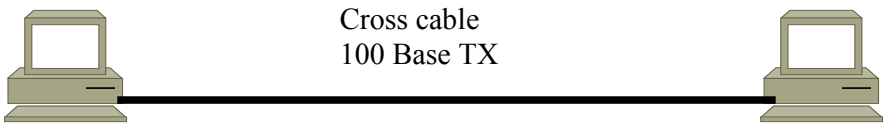
Software utilizzato:

Netperf versione 2.1pl3
Con Client e Server in comunicazione sulla porta 12865
Redhat 7.2 Kernel 2.4.9-21
ICMP Bomber

Caratteristiche dei PC utilizzati :

PC1: Duron 800 - 256MB di RAM – Fast Ethernet 3COM 3c905c
PC2 Pentium III 1.6Ghz - 256MB di RAM – Fast Ethernet on board Intel

Prove iniziali di performance tra PC1 e PC2 collegati direttamente



PC 1 (firew1)
192.84.129.10
Server Netperf in ascolto sulla porta 12865

PC 2 (firew2)
192.84.129.20
Client Netperf

Tutti i test di throughput sono stati effettuati utilizzando Netperf reiterando i test e variando i parametri di netperf (Durata dei test, dimensione del messaggio ..).

```
Per esempio:

# ./netperf -l 120 -H 192.84.129.10
# ./netperf -t UDP_STREAM -H 192.84.129.10 -- -m 50000
```

Non riporteremo in questo documento tutti i valori delle misure ma un sunto dei valori più significativi:

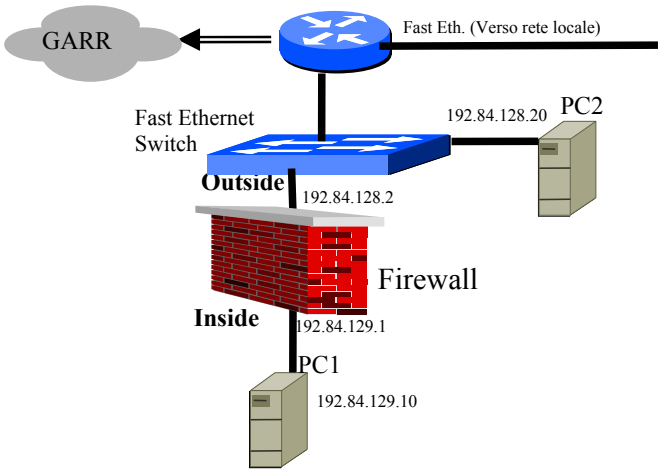
```
Throughput misurato in TCP:93.70 Mb/s
Throughput misurato in UDP:95.80 Mb/s
```

Test sulla struttura di sperimentazione

Test con access-list permit ip any any (Passante)
Throughput misurato in TCP: 93.03
Throughput misurato in UDP: 95.60
PING (Media) 356 usec

Test con firewall e acl di 84 linee
Throughput misurato in TCP: 93.20
Throughput misurato in UDP: 95.54
PING (Media) 371 usec

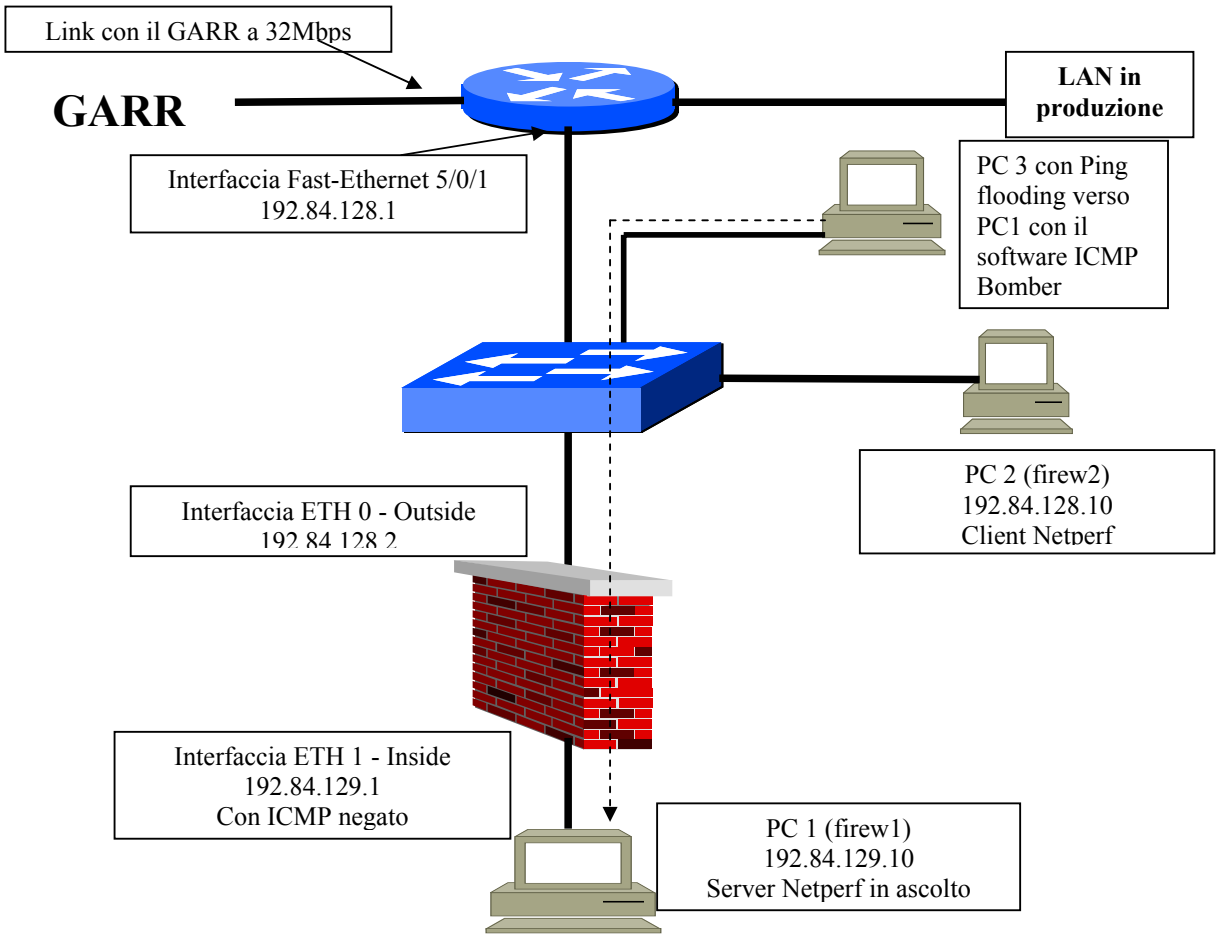
Con firewall e acl di 270 linee
Throughput misurato in TCP: 93.10
Throughput misurato in UDP: 95.39
PING (Media) Media 427 usec



Non si notano particolari differenze nel throughput passante all'aumentare delle linee di ACL applicate.

Misure con Ping Flooding

Misure fra PC1 e PC2 con icmp negato verso il PC 1 e flooding ICMP (ICMP bomber) dall'host dietro al router.



I valori di throughput ottenuti in questa configurazione sono da ritenersi nella norma considerando la banda comunque utilizzata dal Ping flooding.
Il Pix sembra non risentire a livello di funzionalità di questo tipo di attacco.

Esempio di configurazione del PIX

nameif ethernet0 outside security0 **//Interfaccia Insicura verso il router**
nameif ethernet1 inside security100 **//Interfaccia Sicura verso la LAN**
hostname pixlnf

// Access-List applicata sull'interfaccia Inside in Ingresso che permette
// qualsiasi tipo di traffico dalla LAN verso Internet
access-list acl_inside_in permit ip any any

// Access-List applicata sull'interfaccia Outside in Ingresso di 84 entry
// con match sull'ultima entry
…
access-list acl_out_test2 permit tcp any host 192.84.129.28 eq 22
access-list acl_out_test2 permit tcp any host 192.84.129.29 eq 22
access-list acl_out_test2 permit tcp any host 192.84.129.20 eq www
access-list acl_out_test2 permit tcp any host 192.84.129.21 eq www
access-list acl_out_test2 permit tcp any host 192.84.129.22 eq www
access-list acl_out_test2 permit tcp any host 192.84.129.23 eq www
access-list acl_out_test2 permit tcp any host 192.84.129.20 range 7000 7009
access-list acl_out_test2 permit tcp any host 192.84.129.21 range 7000 7009
…
icmp permit any outside **//Traffico ICMP permesso**
icmp permit any inside **//Traffico ICMP permesso**
ip address outside 192.84.128.2 255.255.255.0
ip address inside 192.84.129.1 255.255.255.0
…
//NAT Disabilitato
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 192.84.129.0 192.84.129.0 netmask 255.255.255.0 0 0

access-group acl_out_test2in interface outside
access-group acl_inside_in in interface inside

Considerazioni generali relative al PIX

Vantaggi
La piattaforma è stabile, il sistema operativo è proprietario e "IOS like".
Sono disponibili moduli VPN e moduli di interfacciamento fino alla velocità di 1 Gb/s.

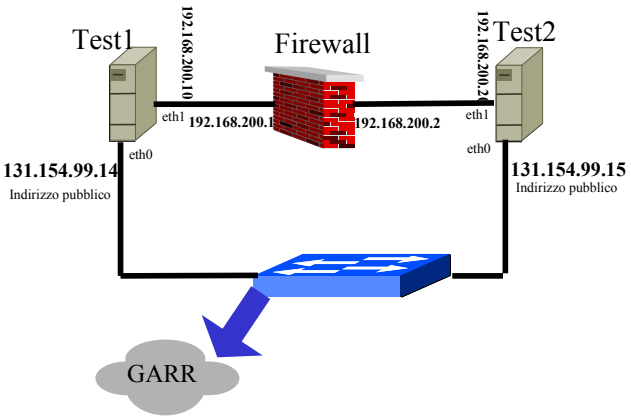
Svantaggi
L'interfaccia al sistema non è molto "User friendly".
Non sono forniti di serie strumenti di management evoluti.
Il costo del firewall risulta elevato e aggiungendo interfacce ad alta velocità e moduli di espansione aumenta in maniera importante.

Box OpenBSD

Il Firewall realizzato con OpenBSD è stato configurato su di un PC standard cosi configurato:

Processore: **Intel PIII 833 MHz**
RAM: **512 MB**
Rete: **2X Intel pro 100 (100 Mb/s)**

Sistema operativo: **OpenBSD 3.2 *Stable***
Software: ***pf*** (packet filter embedded nel sistema operativo)
Sede dei test: INFN CNAF (Bologna)



Caratteristiche dei PC di test:

PC1 e PC2 : IBM Xseries 330 Biprocessori PIII 800 512MB 2 Fast Ethernet on Board.

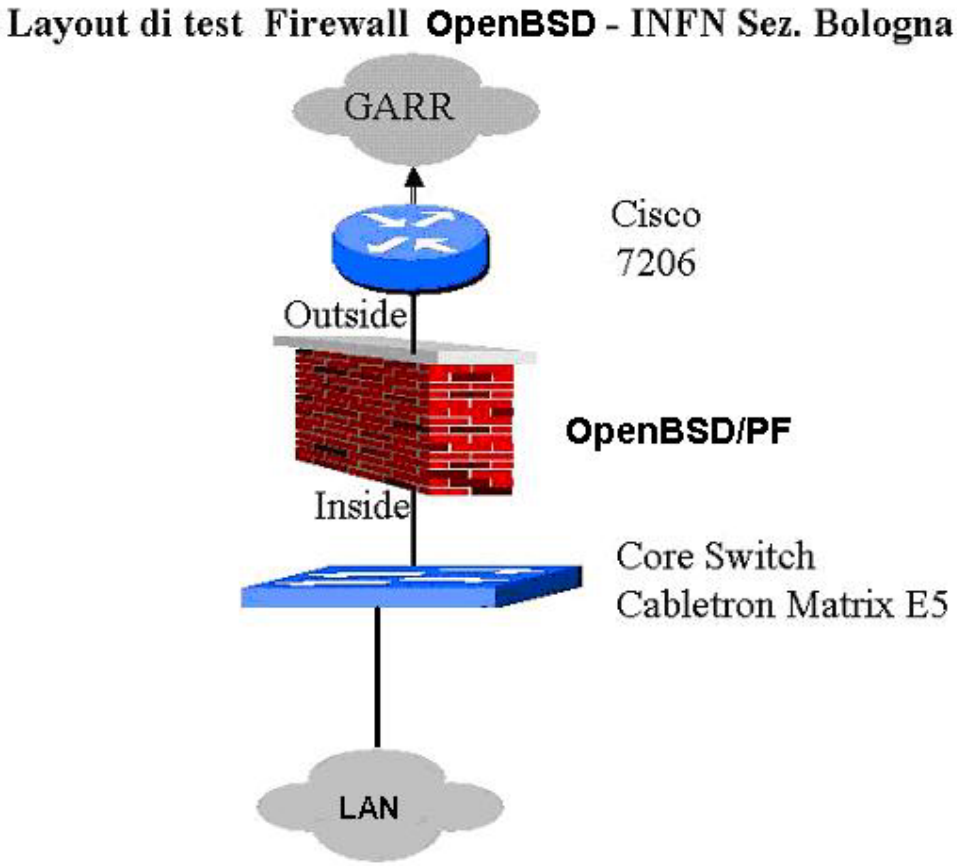
Descrizione generale

Vale la pena ricordare che sebbene OpenBSD sia un sistema operativo freeware, ha caratteristiche di sicurezza che spesso sono peculiari solo di quei sistemi di estrazione commerciale chiusi e proprietari. La prerogativa primaria degli sviluppatori di OpenBSD è quella di fornire un sistema operativo che abbia caratteristiche che lo collochino al TOP in termini di security. OpenBSD è di fatto un punto di riferimento anche per chi vende soluzioni commerciali, si veda ad esempio OpenSSH, creata come parte integrante di OpenBSD ed esportata successivamente a tutti gli altri sistemi operativi Unix. All'interno di questo environment di security si colloca anche il software di packet filtering "PF" che a differenza di altre soluzioni adottate in altri sistemi operativi, non è un add-on, ma è parte integrante del sistema stesso.
Ci sono in generale 2 modi per configurare un box OpenBSD come firewall *Bridging* e *Routing*.
La peculiarità di questo tipo di firewall è il fatto di potere "forwardare" il traffico di rete fra le due interfacce a livello OSI 2 (Data Link Layer) ed applicare le ACL a livello 2, a livello 3 (Network Layer) e a livello 4 (Transport Layer). Questo ha come conseguenza il fatto che non è assolutamente necessario assegnare al BOX OpenBSD un indirizzo IP e quindi il BOX è di fatto invisibile sulla rete dall'esterno e dall'interno poiché a livello IP non è raggiungibile.

I test di throughput hanno dato ottimi risultati e aumentando la complessità delle ACL fino a 5000 linee non si sono riscontrate riduzioni sensibili del throughput passante del firewall né si è riscontrato un aumento del round trip time.
Si può affermare che almeno fino ad una banda di 100Mb un Box così realizzato non rappresenta un collo di bottiglia per la rete.

Prova in produzione

Per potere testare l'applicabilità e le funzionalità di questo tipo di firewall in situazioni reali si è deciso di metterlo in produzione nella sezione INFN di Bologna. Il fw è stato collocato tra l'edge router e la LAN interna. Una volta attivato e configurato opportunamente non si sono riscontrati problemi a livello di connettività generale. L'utilizzo della CPU ha avuto picchi del 7% in concomitanza di un utilizzo di banda di circa 12Mbit.



Configurazione del BOX

Le interfacce di rete Intel sono due (fxp0, fxp1), occorre creare 2 file che vengono letti al boot e attivano le interfacce di rete. E' consigliato settare manualmente le opzioni a livello di data link (full duplex, 100Mbits etc.) per il tipo di interfaccia usato onde evitare problemi di auto-negoziazione.
Di seguito il carattere '#' indica un commento all'interno del file di configurazione.
Configurazione dell'interfaccia verso il router CISCO 7206

```
# /etc/hostname.fxp0
up media media 100baseTX mediaopt fdx
```

Configurazione dell'interfaccia verso la LAN interna (switch Cabletron Matrix E5)

```
# /etc/hostname.fxp1
up media media 100baseTX mediaopt fdx
```

Ora occorre configurare il bridge fra le due interfacce che consente il “forwarding” del traffico a livello 2 creando un file che viene letto al boot.

```
# /etc/bridgename.bridge0
add fxp0
add fxp1
up
```

Per abilitare l’IP forwarding bisogna editare il file /etc/sysctl.conf e aggiungere la linea:

```
# /etc/sysctl.conf
net.inet.ip.forwarding=1
```

Sono state tradotte le regole del CISCO nella sintassi di PF (circa 300 linee di ACL). La sintassi delle ACL e’ molto intuitiva e relativamente semplice da implementare.

Esempio di file pf.conf

```
#       $OpenBSD: pf.conf,v 1.3 2001/11/16 22:53:24 dhartmei Exp $
#
# See pf.conf(5) for syntax and examples

# pass all packets in and out (these are the implicit first two rules)
# pass in all
# pass out all
block in on fxp0 all
#Fa passare le connessioni ssh (Setup o syn) e permette il ritorno dei pacchetti associati
pass  in on fxp0 inet proto tcp from any to any port 22 flags S/SA keep state
#
pass in on fxp0 inet proto { tcp, udp } from any to any port 500 keep state
pass in on fxp0 inet proto { tcp, udp } from any to any port 501 keep state
..
pass in on fxp0 inet proto { tcp, udp } from any to any port > 10000 keep state
pass in on fxp0 inet proto icmp from any to any keep state
```

Una delle particolarita’ degne di nota è la possibilità di poter scegliere il comportamento del firewall in risposta nei confronti di un pacchetto che viene rigettato dalle ACL.
E’ possibile non rispondere al peer host (comportamento di default) oppure nel caso di probing TCP da parte di un peer host è possibile rispondere con un pacchetto TCP con il bit RST acceso o un pacchetto ICMP di tipo (port-unreachble). In caso di un probe UDP una risposta di tipo port-unreachable nasconde ancora di più la presenza del firewall.
Ci sono molte altre caratteristiche singolari che consentono di bloccare pacchetti che fanno parte di scan TCP atti ad identificare i sistemi operativi tramite OS fingerprint.
È possibile distinguere fra connessioni TCP,UDP e pacchetti ICMP che fanno parte di una connessione reale (che ha uno storico) pertanto possibilmente lecita e pacchetti TCP/IP che sono forgiati ad hoc per un attacco, oppure generati da stack TCP/IP difettosi.
È possibile normalizzare il traffico all’interno della propria LAN minimizzando i pacchetti frammentati a livello IP con una operazione di “Riassemblamento” effettuata dal firewall stesso.
L’utilizzo di PF in specifico è ben documentato sulla pagina di OpenBSD.

Il firewall si controlla tramite un tool che si chiama **pfctl**:

pfctl –F all	fa il flush di tutte le ACL
pfctl –f /etc/pf.conf	carica le ACL presenti nel file /etc/pf.conf
pfctl –s state	mostra lo stato delle connessioni attive
pfctl –s rules	mostra le ACL Attive del firewall ordinate cardinalmente
pfctl –s nat	mostra le ACL relative a NAT

La parte di logging relativa al firewall e' spartana ma molto efficace.
E' possibile decidere a livello di ogni singola regola il tipo di evento da "Loggare".
A questo punto quando una regola di log viene attivata le informazioni vengono inviate all'interfaccia di log che si chiama `pflog()`. Questa interfaccia è gestita da un demone `pflogd` che periodicamente scrive nel file /var/log/pflog. Per vedere i log in tempo reale occorre leggerli dall'interfaccia pflog stessa. Il formato del log è binario e leggibile tramite tcpdump che e' stato opportunamente modificato in OpenBSD per essere omologo al pacchetto PF.
Ad esempio per leggere in tempo reale i pacchetti che sono rigettati dal firewall occorre scrivere sulal linea di comando:

```
tcpdump -n -e -ttt –i pflog0
```

```
Mar 17 11:04:31.696748 rule 11/0(match): block in on fxp0:
62.211.156.40.3102 > 172.16.16.100.80: S 4112880033:4112880033(0)
win 16384 <mss 1452,nop,nop,sackOK> (DF)
```

L'output è molto dettagliato e consente di identificare l'ACL specifica (la numero 11 in questo caso) che ha "Triggerato" il log.

Per vedere lo storico del log:

```
tcpdump -n -e -ttt –r /var/log/pflog
```

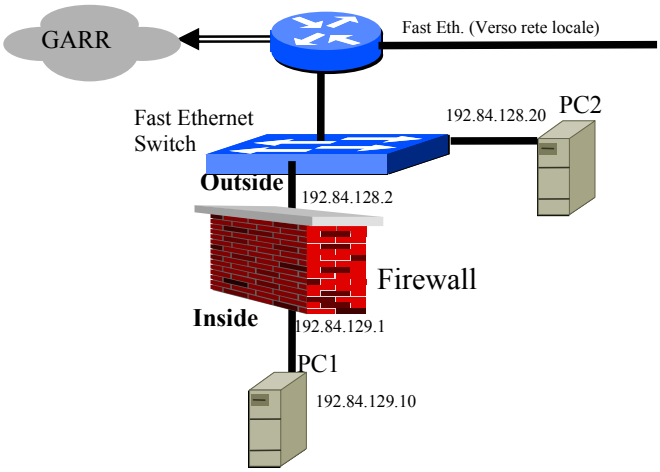
É possibile passare poi a tcpdump una serie di comandi per avere un output più granulare. (src host, dst host, src port ecc.)

Considerazioni generali relative al firewall OpenBSD

Vantaggi
Il sistema è in assoluto il più economico.
Il controllo della piattaforma è totale.
La modalità "Bridging" consente di rendere il firewall "Invisibile".
PF è molto accurato e permette si realizzare ACL anche molto complesse.

Svantaggi
È basato su di un sistema Open
Non sono disponibili interfacce grafiche di management.
Occorre dimensionare accuratamente l'hardware su cui si installa il software(anche un eccesso di RAM può penalizzare le prestazioni).

Infoguard IGWall



Caratteristiche dei PC utilizzati :

PC1: Duron 800 - 256MB di RAM – Fast Ethernet 3COM 3c905c
PC2 Pentium III 1.6Ghz - 256MB di RAM – Fast Ethernet on board Intel

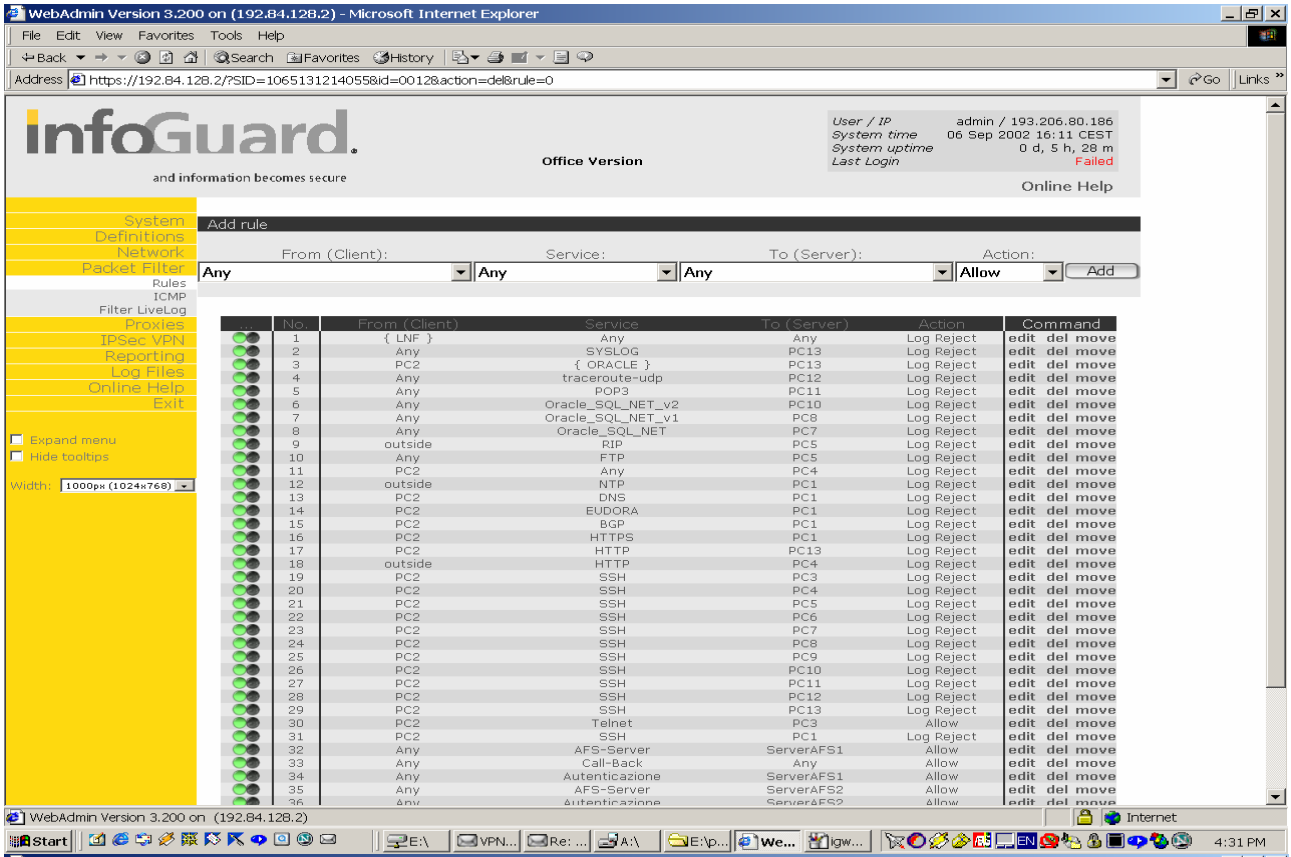
I' IGWall è un appliance che racchiude numerose funzionalità oltre a quella di Firewall.
È basato su linux e IP Tables, ha una interfaccia grafica completa e funzionale alla configurazione di base. Risulta scomoda da utilizzare in fase di definizione di ACL composte da regole numerose in quanto occorre inserirle una ad una.

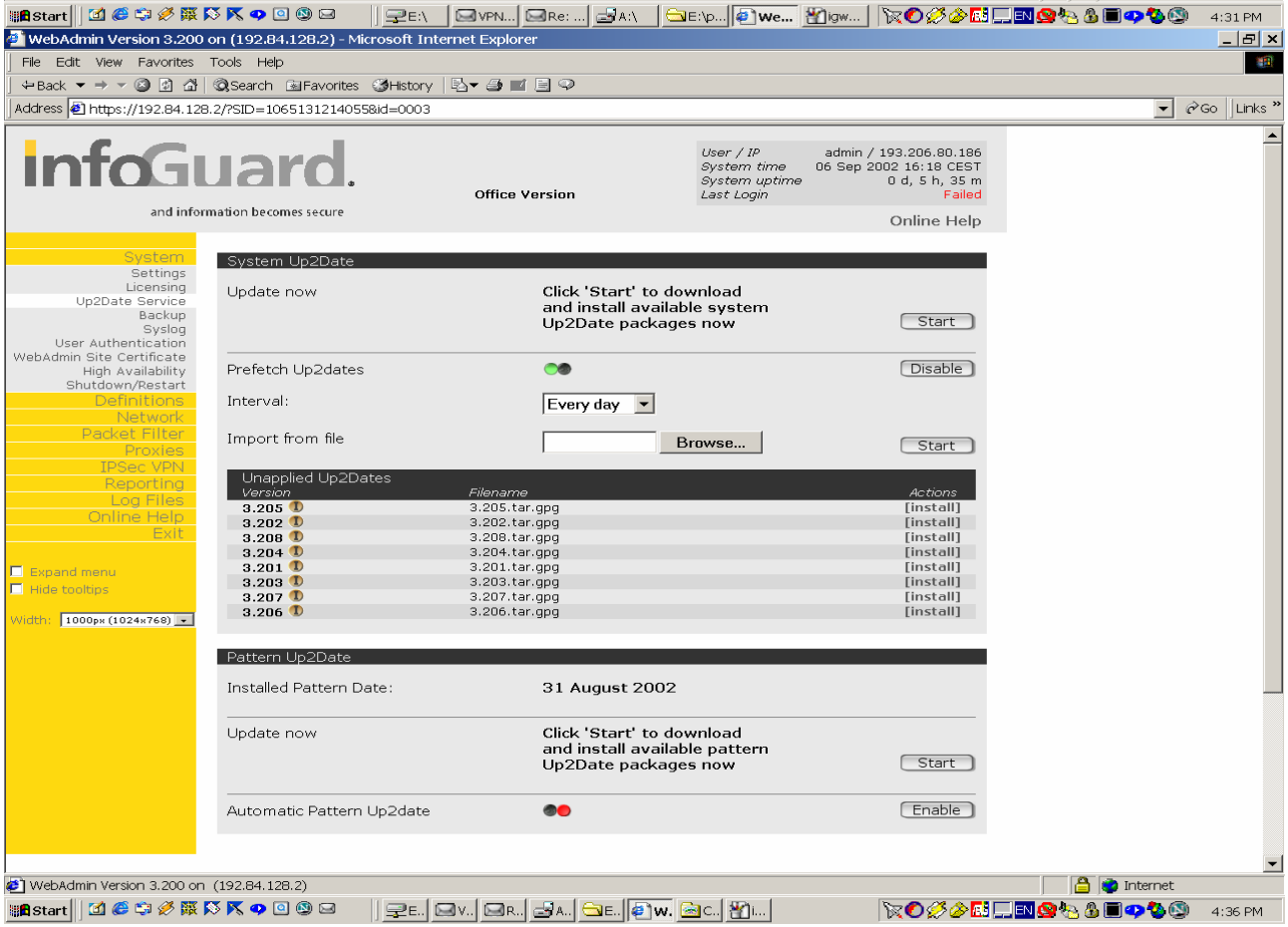
Caratteristiche di base:

- Interfaccia Web HTTPS
- S.O. Linux (IP Tables)
- NAT
- DHCP Server
- Portscan Detection
- Accounting
- VPN IPSec (Client SSH Sentinel sui client).
- Log Server
- Antispam
- Packet Filtering

I test di throughput buoni risultati anche all'aumentare della complessità delle ACL.
Non si è riscontrato un aumento del round trip time.
Si può affermare che almeno fino ad una banda di 100Mb un Box così realizzato non rappresenta un collo di bottiglia per la rete.

Seguono alcuni "Screenshot"


WebAdmin Version 3.200 on (192.84.128.2) - Microsoft Internet Explorer
https://192.84.128.2/?SID=1065131214055&id=0012&action=del&rule=0
InfoGuard
and information becomes secure
Office Version
User / IP admin / 193.206.80.186
System time 06 Sep 2002 16:11 CEST
System uptime 0 d, 5 h, 28 m
Last Login Failed
Online Help
System
Definitions
Network
Packet Filter
Rules
ICMP
Filter LiveLog
Proxies
IPSec VPN
Reporting
Log Files
Online Help
Exit
Expand menu
Hide tooltips
Width: 1000px (1024x768)
Add rule
From (Client): Service: To (Server): Action:
Any Any Any Allow Add
No. From (Client) Service To (Server) Action Command
1 { LNF } Any Any Log Reject edit del move
2 Any SYSLOG PC13 Log Reject edit del move
3 PC2 { ORACLE } PC13 Log Reject edit del move
4 Any traceroute-udp PC12 Log Reject edit del move
5 Any POP3 PC11 Log Reject edit del move
6 Any Oracle_SQL_NET_v2 PC10 Log Reject edit del move
7 Any Oracle_SQL_NET_v1 PC8 Log Reject edit del move
8 Any Oracle_SQL_NET PC7 Log Reject edit del move
9 outside RIP PC5 Log Reject edit del move
10 Any FTP PC5 Log Reject edit del move
11 PC2 Any PC4 Log Reject edit del move
12 outside NTP PC1 Log Reject edit del move
13 PC2 DNS PC1 Log Reject edit del move
14 PC2 EUDORA PC1 Log Reject edit del move
15 PC2 BGP PC1 Log Reject edit del move
16 PC2 HTTPS PC1 Log Reject edit del move
17 PC2 HTTP PC13 Log Reject edit del move
18 outside HTTP PC4 Log Reject edit del move
19 PC2 SSH PC3 Log Reject edit del move
20 PC2 SSH PC4 Log Reject edit del move
21 PC2 SSH PC5 Log Reject edit del move
22 PC2 SSH PC6 Log Reject edit del move
23 PC2 SSH PC7 Log Reject edit del move
24 PC2 SSH PC8 Log Reject edit del move
25 PC2 SSH PC9 Log Reject edit del move
26 PC2 SSH PC10 Log Reject edit del move
27 PC2 SSH PC11 Log Reject edit del move
28 PC2 SSH PC12 Log Reject edit del move
29 PC2 SSH PC13 Log Reject edit del move
30 PC2 Telnet PC3 Allow edit del move
31 PC2 SSH PC1 Log Reject edit del move
32 Any AFS-Server ServerAFS1 Allow edit del move
33 Any Call-Back Any Allow edit del move
34 Any Autenticazione ServerAFS1 Allow edit del move
35 Any AFS-Server ServerAFS2 Allow edit del move
WebAdmin Version 3.200 on (192.84.128.2)
Internet
4:31 PM


WebAdmin Version 3.200 on (192.84.128.2) - Microsoft Internet Explorer
https://192.84.128.2/?SID=1065131214055&id=0003
InfoGuard
and information becomes secure
Office Version
User / IP admin / 193.206.80.186
System time 06 Sep 2002 16:18 CEST
System uptime 0 d, 5 h, 35 m
Last Login Failed
Online Help
System
Settings
Licensing
Up2Date Service
Backup
Syslog
User Authentication
WebAdmin Site Certificate
High Availability
Shutdown/Restart
Definitions
Network
Packet Filter
Proxies
IPSec VPN
Reporting
Log Files
Online Help
Exit
Expand menu
Hide tooltips
Width: 1000px (1024x768)
System Up2Date
Update now
Click 'Start' to download and install available system Up2Date packages now
Start
Prefetch Up2dates
Disable
Interval: Every day
Import from file
Browse...
Start
Unapplied Up2Dates
Version Filename Actions
3.205 3.205.tar.gpg [install]
3.202 3.202.tar.gpg [install]
3.208 3.208.tar.gpg [install]
3.204 3.204.tar.gpg [install]
3.201 3.201.tar.gpg [install]
3.203 3.203.tar.gpg [install]
3.207 3.207.tar.gpg [install]
3.206 3.206.tar.gpg [install]
Pattern Up2Date
Installed Pattern Date: 31 August 2002
Update now
Click 'Start' to download and install available pattern Up2Date packages now
Start
Automatic Pattern Up2date
Enable
WebAdmin Version 3.200 on (192.84.128.2)
Internet
4:36 PM

Considerazioni generali relative al firewall Symantec

Vantaggi

Sistema completo e ricco di funzionalità accessorie
Buona analisi dei log

Svantaggi

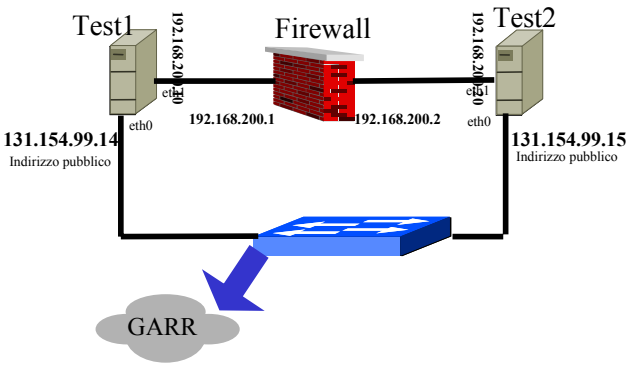
ACL confgurabili solo regola per regola.
Firewall basato su di un S.O. noto ed open
Box Gigabit costoso e non ancora disponibile

Symantech 5300

Il prodotto proposto da Symantech è un appliance basato su linux che svolge fra le altre funzioni anche quella di firewall.

Caratteristiche di base:

- Software Proprietario (Linux based)
- Management console per windows.
- NAT
- Accounting
- VPN
- Antivirus
- Packet Filtering
- IDS (Con LiveUpdate!)



Caratteristiche dei PC di test:

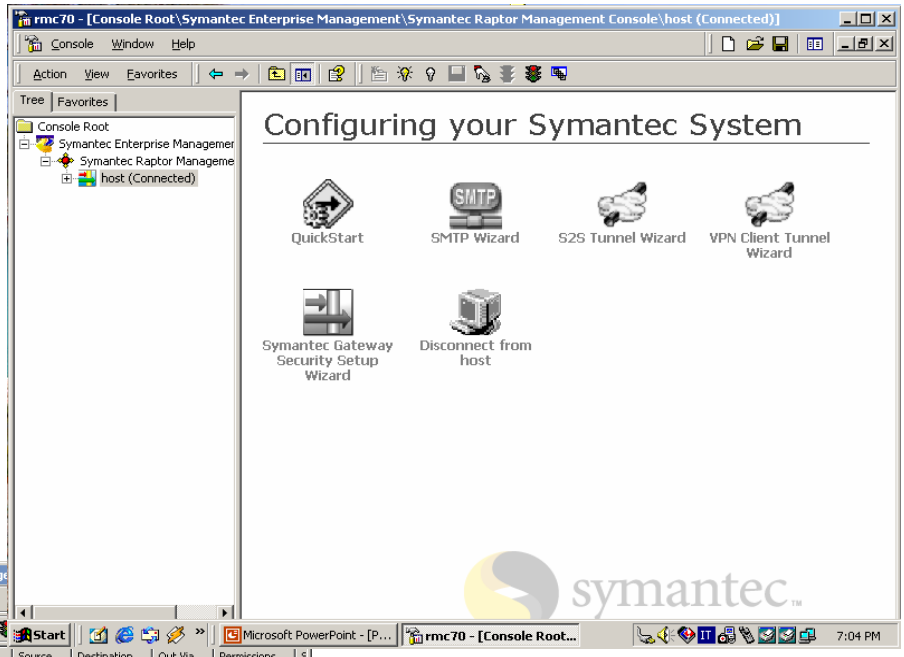
PC1 e PC2 : IBM Xseries 330 Biprocessori PIII 800 512MB 2 Fast Ethernet on Board.

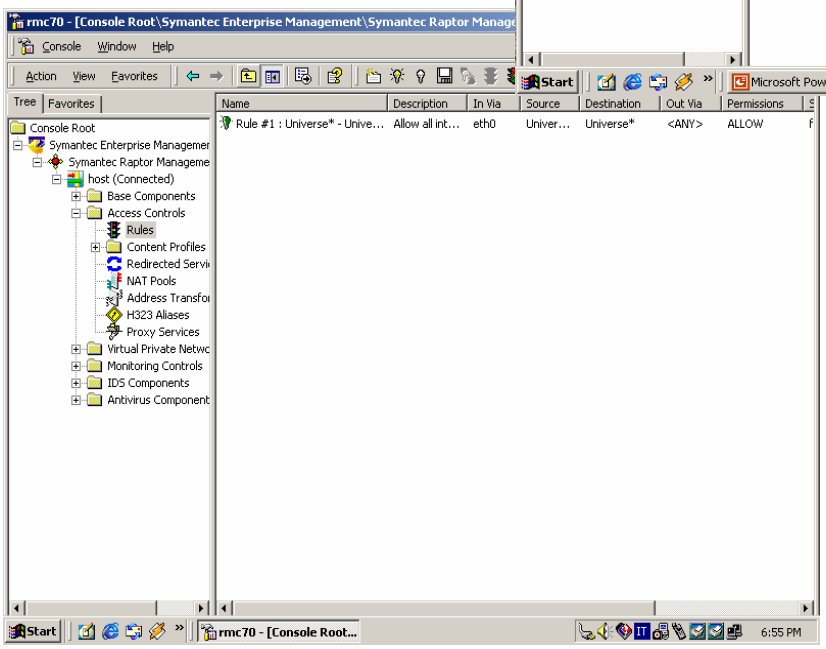
I test di throughput hanno dato buoni risultati anche aumentando la complessità delle ACL.
Non si è riscontrato un aumento del round trip time.
Si può affermare che almeno fino ad una banda di 100Mb il Symantec 5300 non rappresenta un collo di bottiglia per la rete.

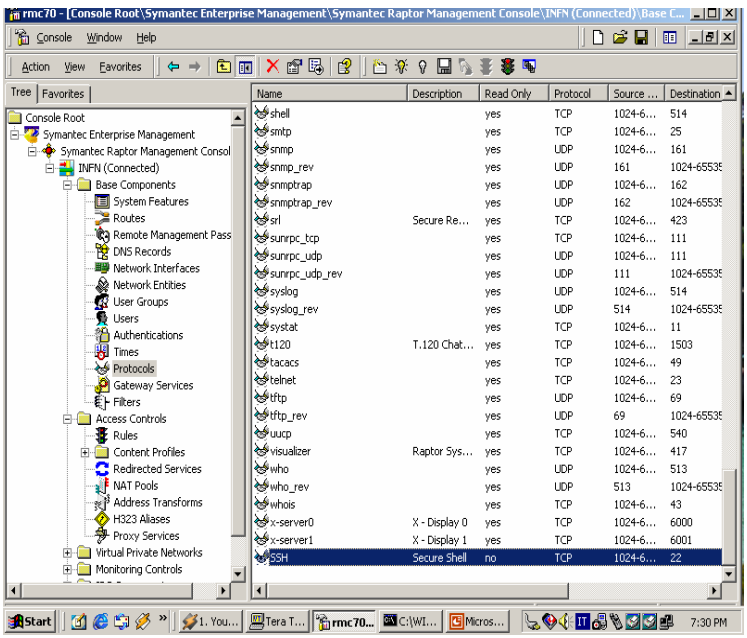
A fronte di un impatto relativamente negativo in fase di prima installazione che risulta essere un pò macchinosa, l'interfaccia grafica di gestione ed monitoring risulta efficiente e completa.
Appare chiaramente dai primi minuti che il box è decisamente complesso e si pone come soluzione integrata per tutti i problemi di sicurezza di una piccola-media azienda (VPN,IDS, Antivirus..).
La definizione di ACL è guidata e rende abbastanza semplice la composizione delle regole.
Sotto altri aspetti (IDS in modo particolare) risulta abbastanza "debole".
Per questo box come per tutti gli altri "Appliance" si ha la chiara impressione che siano stati studiati per realtà molto diverse da quella di un ente di ricerca.

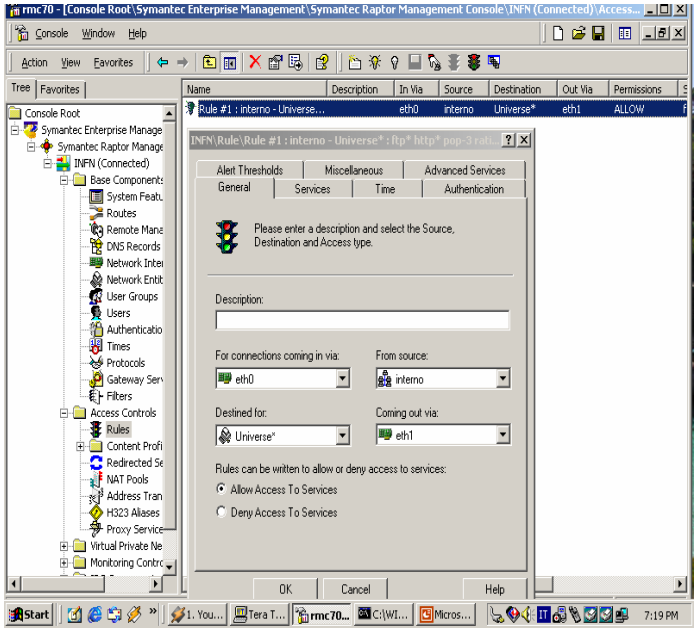
Seguono alcuni "screenshot" realtivi alla interfaccia di gestione:

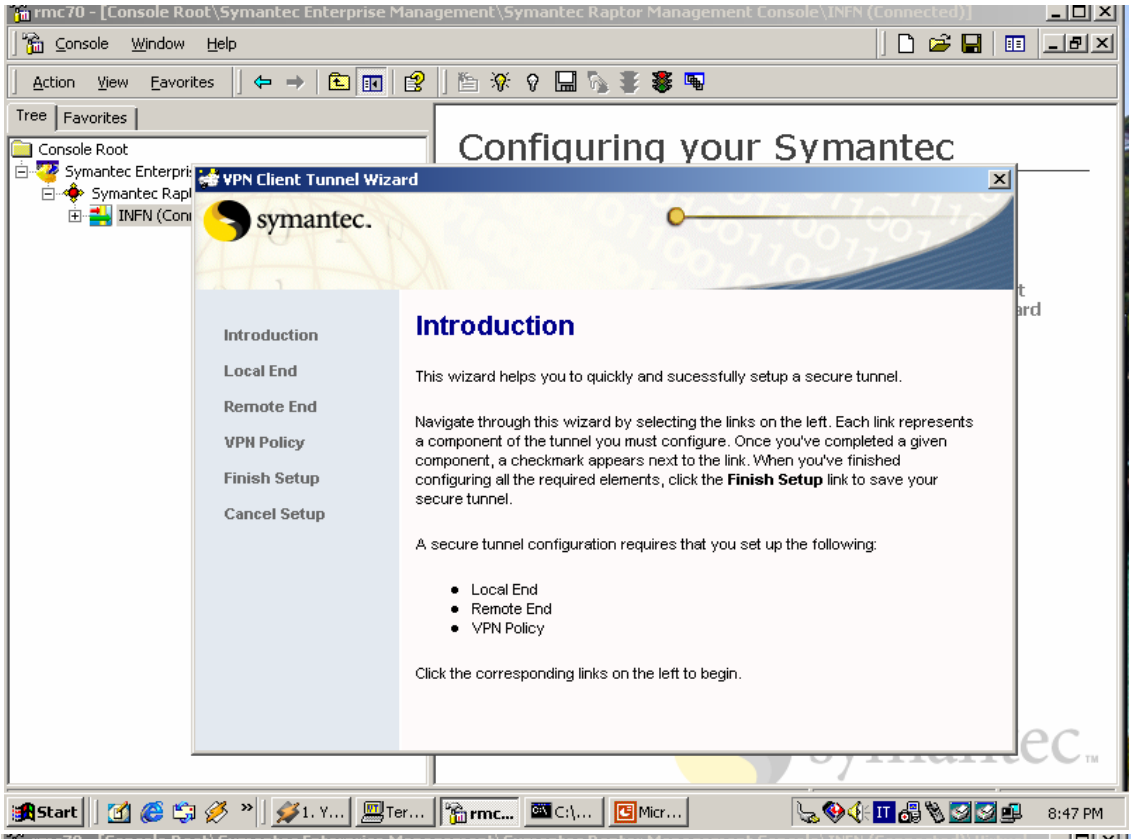
Prima configurazione e definizione delle regole.

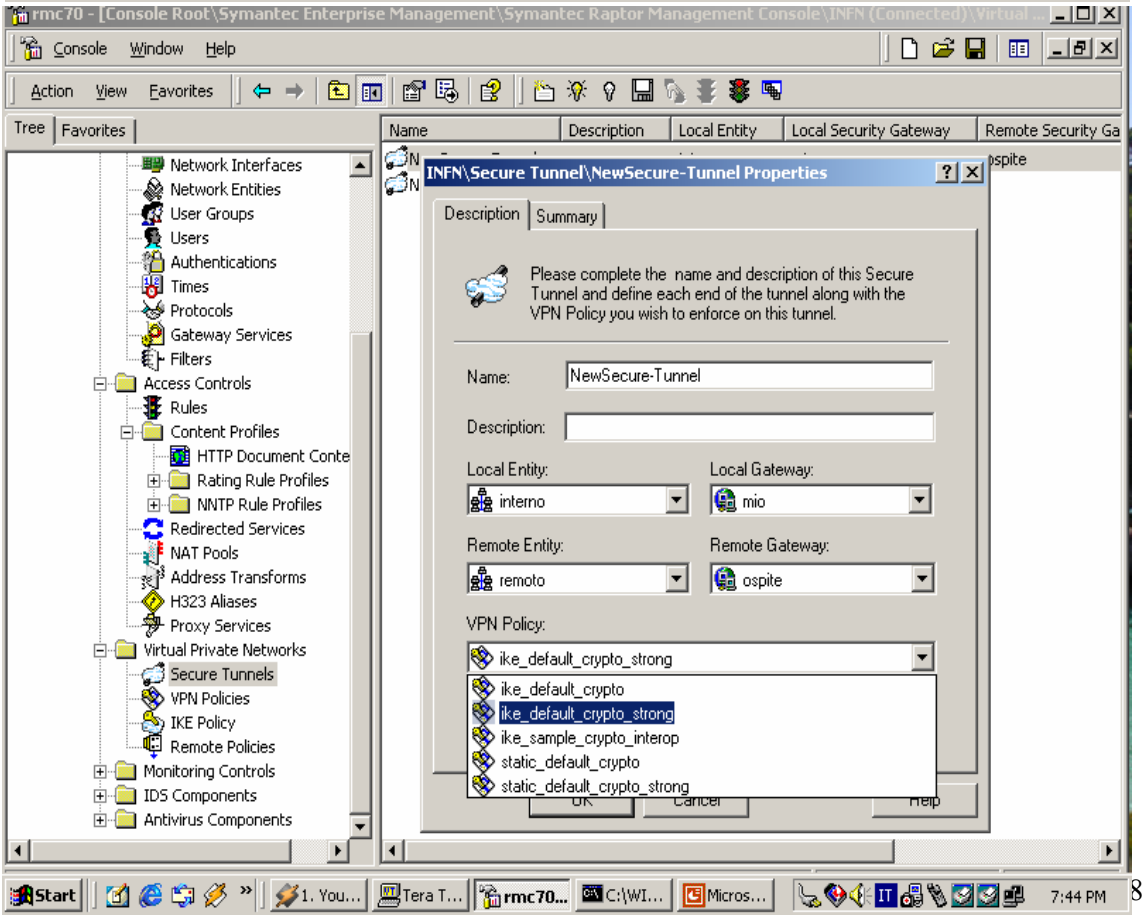









rmc70 - [Console Root\Symantec Enterprise Management\Symantec Raptor Management Console\INFN (Connected)]
Console Window Help
Action View Favorites
Tree Favorites
Console Root
Symantec Enterpri
Symantec Rapl
INFN (Con
Configuring your Symantec
VPN Client Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Introduction
This wizard helps you to quickly and sucessfully setup a secure tunnel.
Navigate through this wizard by selecting the links on the left. Each link represents a component of the tunnel you must configure. Once you've completed a given component, a checkmark appears next to the link. When you've finished configuring all the required elements, click the Finish Setup link to save your secure tunnel.
A secure tunnel configuration requires that you set up the following:
Local End
Remote End
VPN Policy
Click the corresponding links on the left to begin.
Start
8:47 PM


rmc70 - [Console Root\Symantec Enterprise Management\Symantec Raptor Management Console\INFN (Connected)\Virtual
Console Window Help
Action View Favorites
Tree Favorites
Name Description Local Entity Local Security Gateway Remote Security Ga
Network Interfaces
Network Entities
User Groups
Users
Authentications
Times
Protocols
Gateway Services
Filters
Access Controls
Rules
Content Profiles
HTTP Document Conte
Rating Rule Profiles
NNTP Rule Profiles
Redirected Services
NAT Pools
Address Transforms
H323 Aliases
Proxy Services
Virtual Private Networks
Secure Tunnels
VPN Policies
IKE Policy
Remote Policies
Monitoring Controls
IDS Components
Antivirus Components
INFN\Secure Tunnel\NewSecure-Tunnel Properties
Description Summary
Please complete the name and description of this Secure Tunnel and define each end of the tunnel along with the VPN Policy you wish to enforce on this tunnel.
Name: NewSecure-Tunnel
Description:
Local Entity: interno
Local Gateway: mio
Remote Entity: remoto
Remote Gateway: ospite
VPN Policy: ike_default_crypto_strong
ike_default_crypto
ike_default_crypto_strong
ike_sample_crypto_interop
static_default_crypto
static_default_crypto_strong
OK Cancel Help
Start
7:44 PM

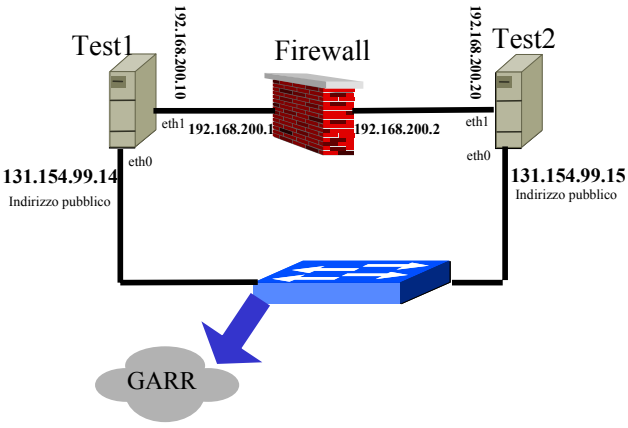
Considerazioni generali relative al firewall Symantec

Vantaggi
Dei box provati è quello che racchiude in se il maggior numero di funzioni.

Svantaggi
IDS di scarsa qualità
Firewall basato su di un S.O. noto ed Open
Manca la versione Gigabit
Il prezzo della versione presa in esame è decisamente elevato.

Firewall Clavister

La soluzione presa in esame è un firewall software**.**



Caratteristiche del PC su cui è stato installato Clavister:
IBM Xseries 330 Biprocessore PIII 800 512MB 2 Fast Ethernet on Board.

Caratteristiche dei PC di test:

PC1 e PC2 : IBM Xseries 330 Biprocessori PIII 800 512MB 2 Fast Ethernet on Board.

Caratteristiche di base:

- S.O.+Software Proprietari (<1MB)
- Management console per windows in grado di gestire più firewall anche geograficamente distribuiti.
- Supporto Vlan 802.1q!
- Packet Filter
- Traffic Shaping
- NAT
- VPN
- Tool di Analisi dei Log

Il pacchetto software proposto è proprietario, non si appoggia ad alcun sistema operativo noto ed è stato sviluppato interamente in Ansi C ed assembler dalla casa produttrice.
Tutto il software (sistema operativo incluso) occupa circa 1MB (Sta su un floppy).
Le prestazioni dichiarate dalla casa madre sono notevolmente elevate (fino a 4Gb/s su macchine dotate di PCIX).
Chiaramente le performance sono legate all'hardware utilizzato.
Esistono tabelle in cui vengono indicati i valori di throughput sostenuti dal firewall in funzione dei vari parametri quali CPU, BUS e schede di rete.
In generale il supporto è garantito per tutti i maggiori produttori di schede madri e di schede di rete per cui si può utilizzare hardware "Commodity".

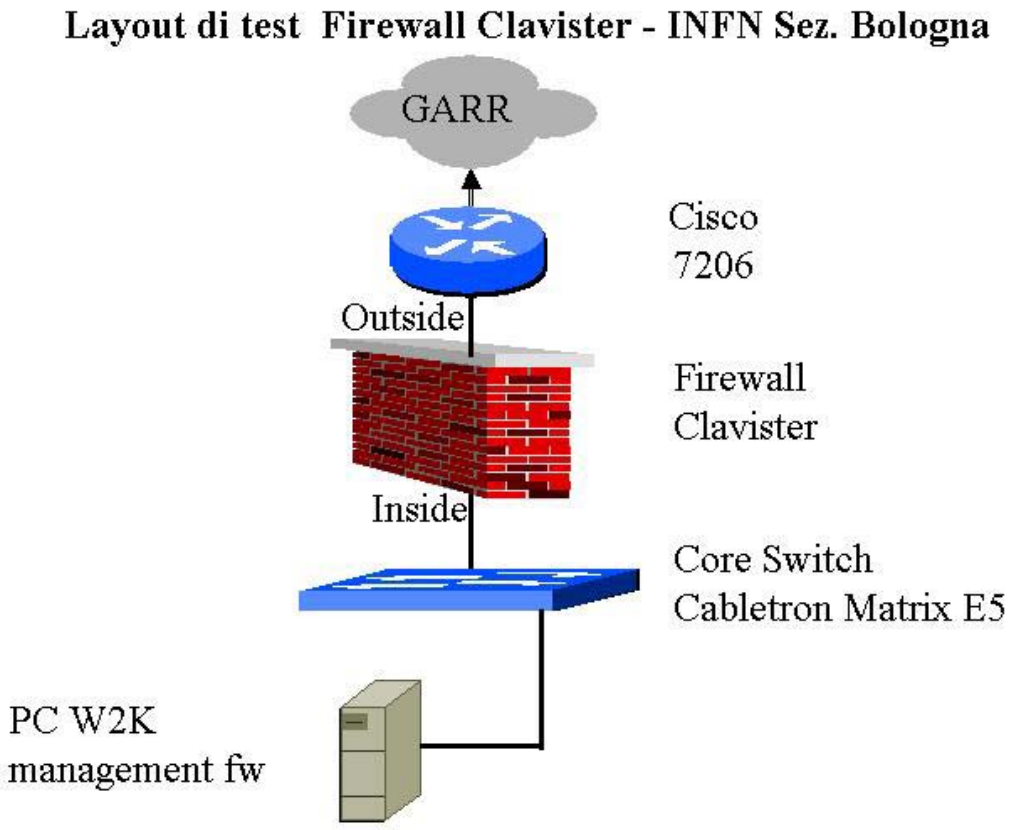
Per quanto riguarda la parte di management e monitoring viene fornito un pacchetto di gestione che "Gira"su piattaforma Windows e che permette un ottimo controllo dell'apparato via rete (Tramite una sessione crittografata).

Test preliminari di throughput con netperf

Anche per questo firewall i test di throughput all'aumentare della complessità delle ACL hanno dato ottimi risultati e non si è riscontrato un aumento del round trip time.
Un traffico di 100 Mb/s non condiziona in alcun modo le prestazioni del firewall.

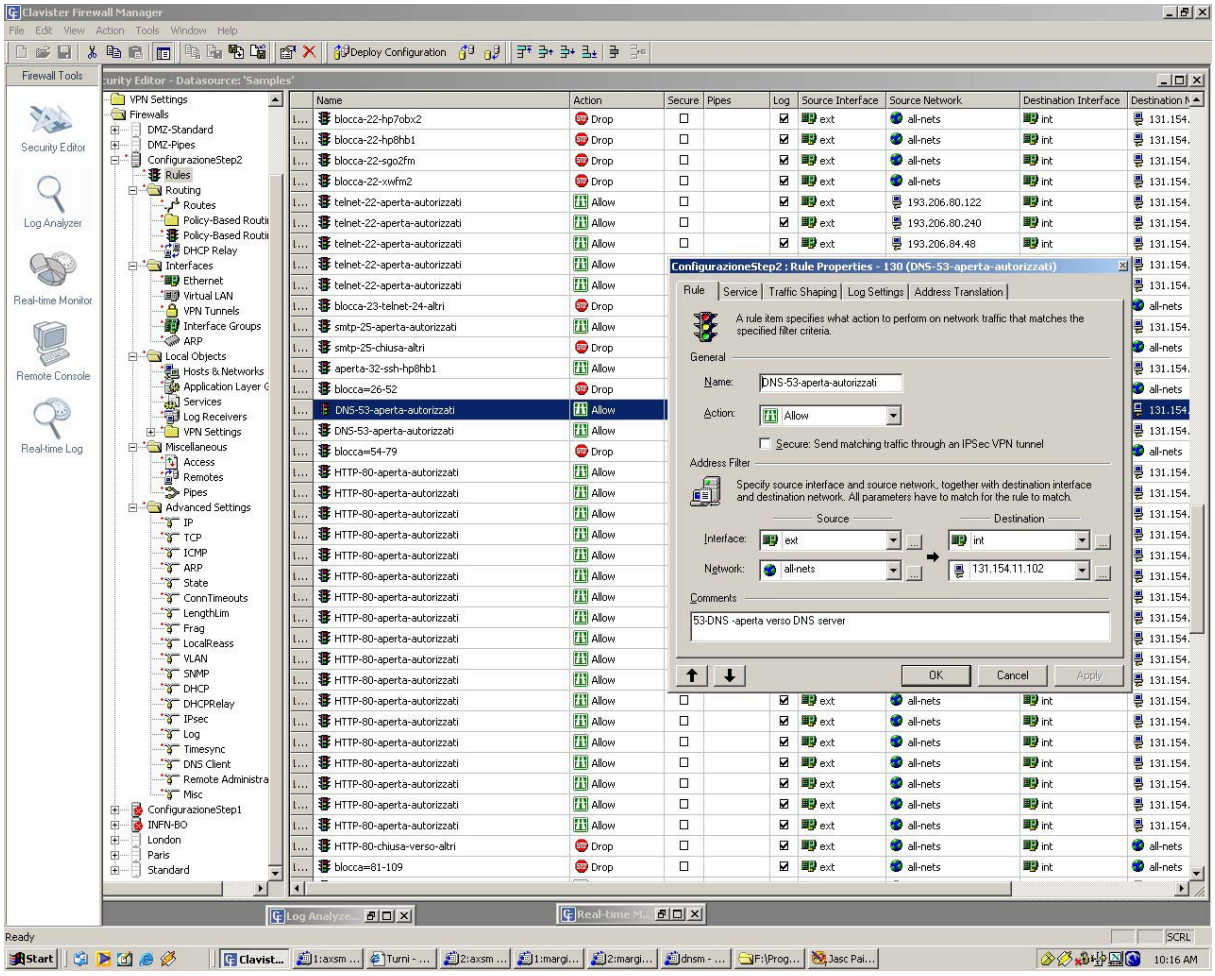
Prova in produzione

Per poter effettuare test più significativi con queste apparecchiature, si è deciso di provare il fw Clavister in produzione presso la sezione INFN di Bologna. Nel test il fw è stato inserito tra il router perimetrale e la LAN:

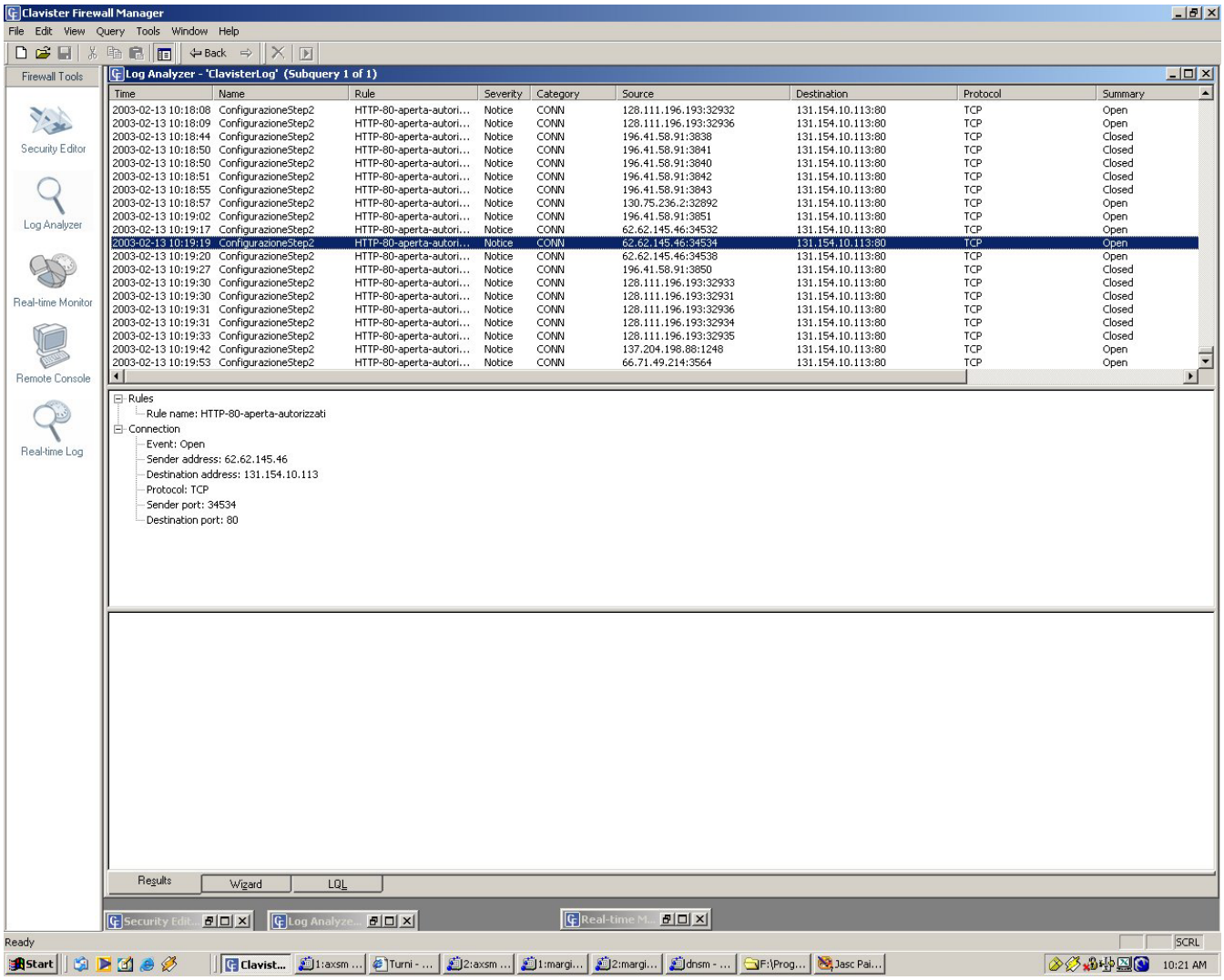


Sono state configurate sul FW le stesse ACL presenti sul Router Cisco (circa 300 righe) per poterne verificare le prestazioni in condizioni di traffico normale (traffico medio della sezione nel periodo è di circa 10-15 Mb/s e l'occupazione di cpu del Router Cisco non va mai oltre il 10%).
Il firewall Clavister è stato perfettamente in grado di sopportare il carico di lavoro dato dalle ACL, non superando mai il 5% di occupazione CPU.

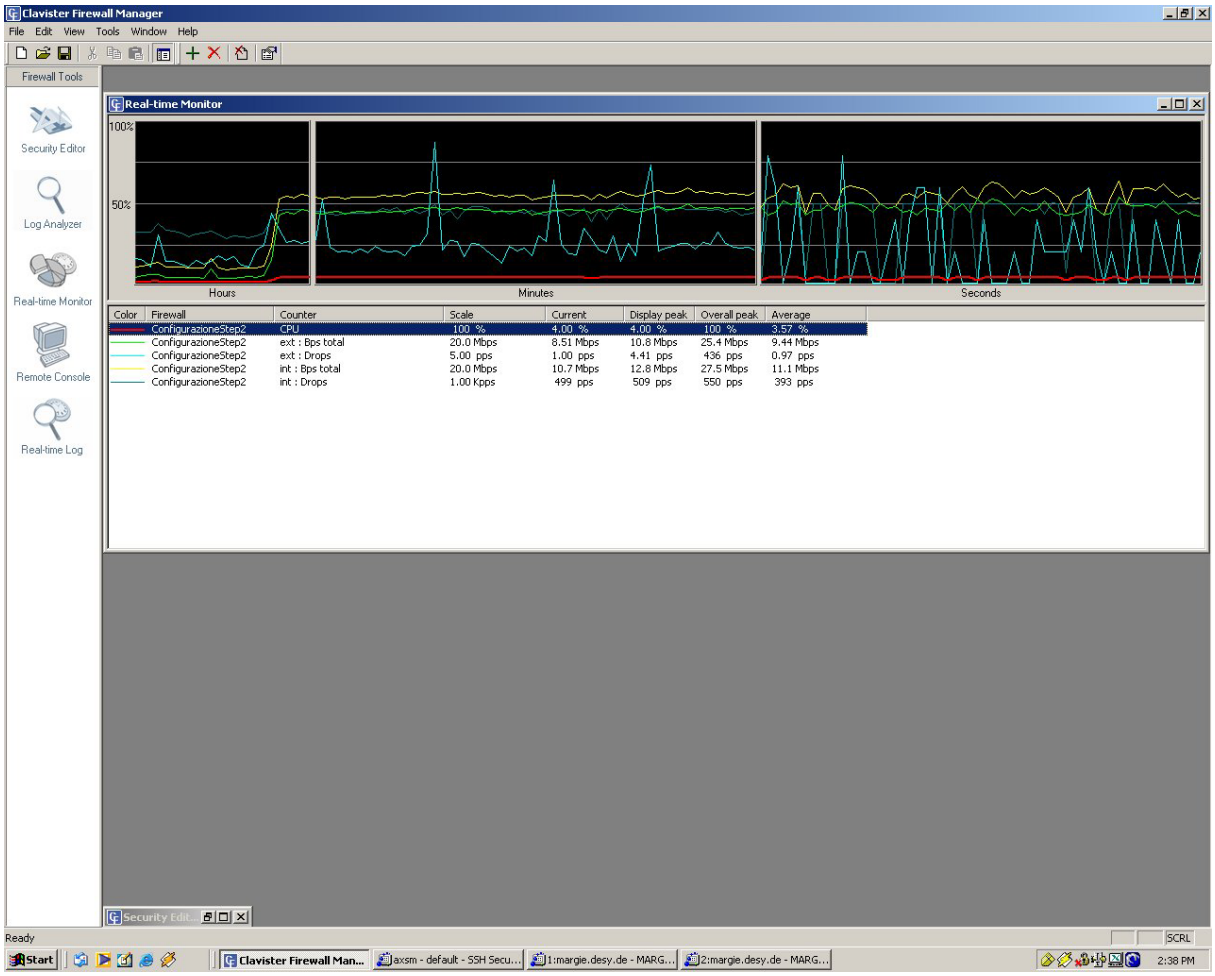
Per quanto riguarda la configurazione, il software di management (per Windows) si è rivelato molto efficace e intuitivo. Riportiamo alcune schermate relative alla configurazione generale, riguardanti le ACL e il Logging:


Clavister Firewall Manager
File Edit View Action Tools Window Help
Deploy Configuration
Firewall Tools
Security Editor
Log Analyzer
Real-time Monitor
Remote Console
Real-time Log
VPN Settings
Firewalls
DMZ-Standard
DMZ-Pipes
ConfigurazioneStep2
Rules
Routing
Routes
DHCP Relay
Interfaces
Ethernet
Virtual LAN
VPN Tunnels
Interface Groups
ARP
Local Objects
Hosts & Networks
Services
Log Receivers
VPN Settings
Miscellaneous
Access
Remotes
Pipes
Advanced Settings
IP
TCP
ICMP
ARP
State
ConnTimeouts
LengthLim
Frag
LocalReass
VLAN
SNMP
DHCP
DHCPRelay
IPsec
Log
Timesync
DNS Client
Misc
ConfigurazioneStep1
INFN-BO
London
Paris
Standard
Name
Action
Secure
Pipes
Log
Source Interface
Source Network
Destination Interface
blocca-22-hp7obx2
blocca-22-hp8hb1
blocca-22-sgo2fm
blocca-22-xwfm2
telnet-22-aperta-autorizzati
blocca-23-telnet-24-altri
smtp-25-aperta-autorizzati
smtp-25-chiusa-altri
aperta-32-ssh-hp8hb1
blocca=26-52
DNS-53-aperta-autorizzati
blocca=54-79
HTTP-80-aperta-autorizzati
HTTP-80-chiusa-verso-altri
blocca=81-109
Drop
Allow
ext
int
all-nets
193.206.80.122
193.206.80.240
193.206.84.48
131.154.
ConfigurazioneStep2 : Rule Properties - 130 (DNS-53-aperta-autorizzati)
Rule
Service
Traffic Shaping
Log Settings
Address Translation
A rule item specifies what action to perform on network traffic that matches the specified filter criteria.
General
Name:
DNS-53-aperta-autorizzati
Action:
Allow
Secure: Send matching traffic through an IPSec VPN tunnel
Address Filter
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.
Source
Destination
Interface:
Network:
131.154.11.102
Comments
53-DNS -aperta verso DNS server
OK
Cancel
Apply
Log Analyze...
Real-time M...
Ready
SCRL
Start
Clavist...
10:16 AM

Per ogni ACL è possibile definire il livello di logging.
Esiste inoltre la possibilità di visualizzare i singoli eventi che interessano (per esempio in caso di debugging).
E' anche possibile inviare in formato testo i log ad un PC per gestirli separatamente.



È possibile visualizzare il carico di CPU, il traffico, i pacchetti scartati etc.
Si possono selezionare i dati di maggior interesse per avere a colpo d'occhio l'andamento del funzionamento del firewall.
È possibile visualizzare anche il numero di volte che una singola ACL viene applicata; questa funzione risulta molto utile in fase di debugging o in caso di attacchi alla rete.

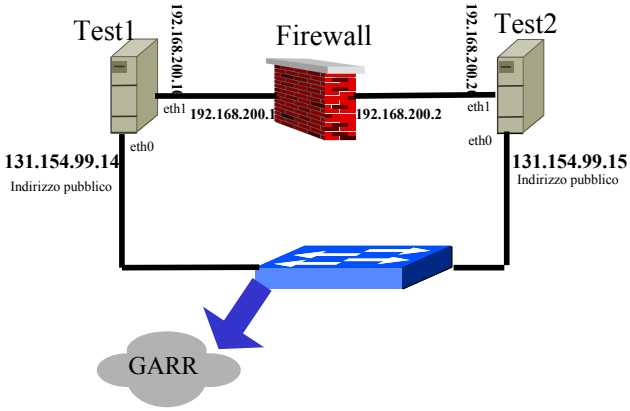


Considerazioni generali relative al firewall Clavister

Vantaggi
Software proprietario non basato su sistemi operativi noti
Codice snello e molto efficiente
Elevate prestazioni e scalabilità relativamente economica (il solo costo di un PC più performante)
Sistema di management e "Monitoring" completo e disaccoppiato dal firewall stesso (Gira su un PC esterno)
Possibilità di creare e gestire un cluster di firewall tramite una unica stazione di controllo.
Supporto "Trunking" '802.1q (Configurandolo anche su vlan differenti).

Svantaggi
La configurazione iniziale non è banale.
Al prezzo del software va aggiunto il costo del pc su cui deve essere installato.

Firewall Nokia



Caratteristiche dei PC di test:

PC1 e PC2 : IBM Xseries 330 Biprocessori PIII 800 512MB 2 Fast Ethernet on Board.

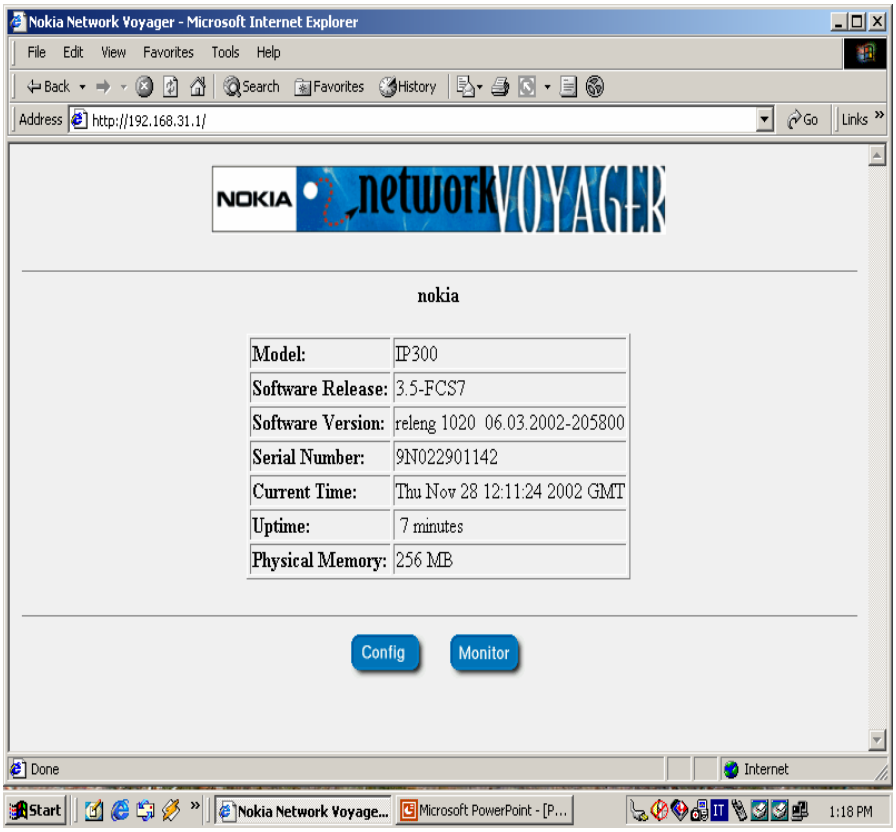
Il firewall Nokia è una soluzione di tipo appliance e si propone come apparato unico di accesso e messa in sicurezza della rete.
Questo oggetto può sostituire egregiamente un piccolo router di accesso alla WAN.

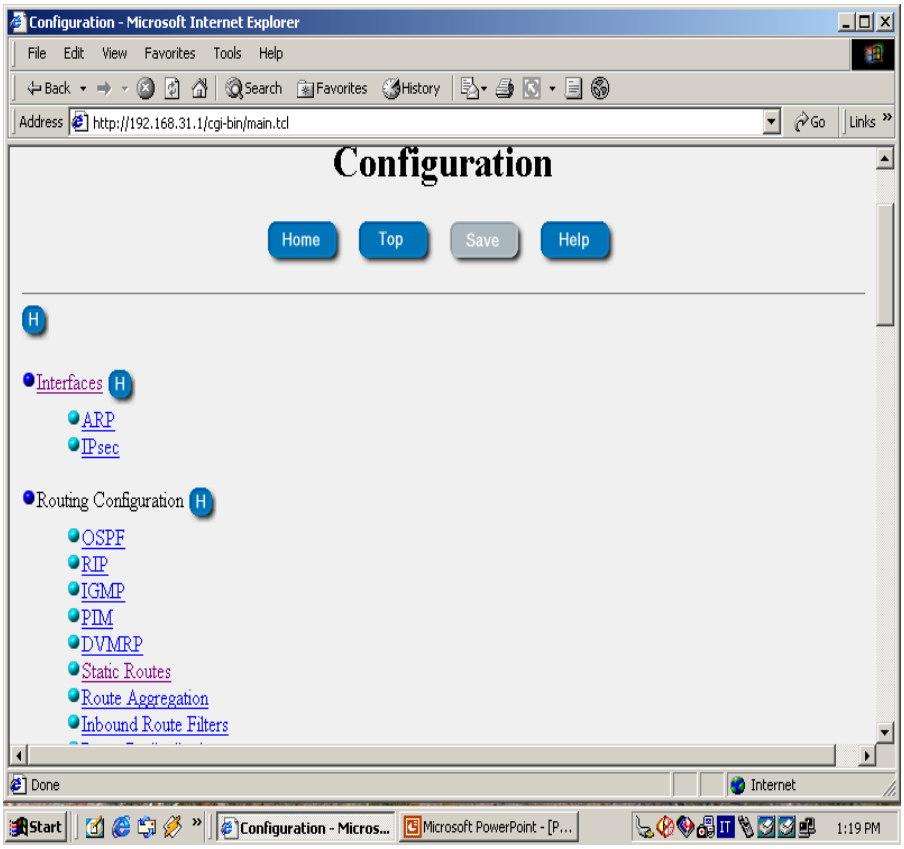
Caratteristiche di base:

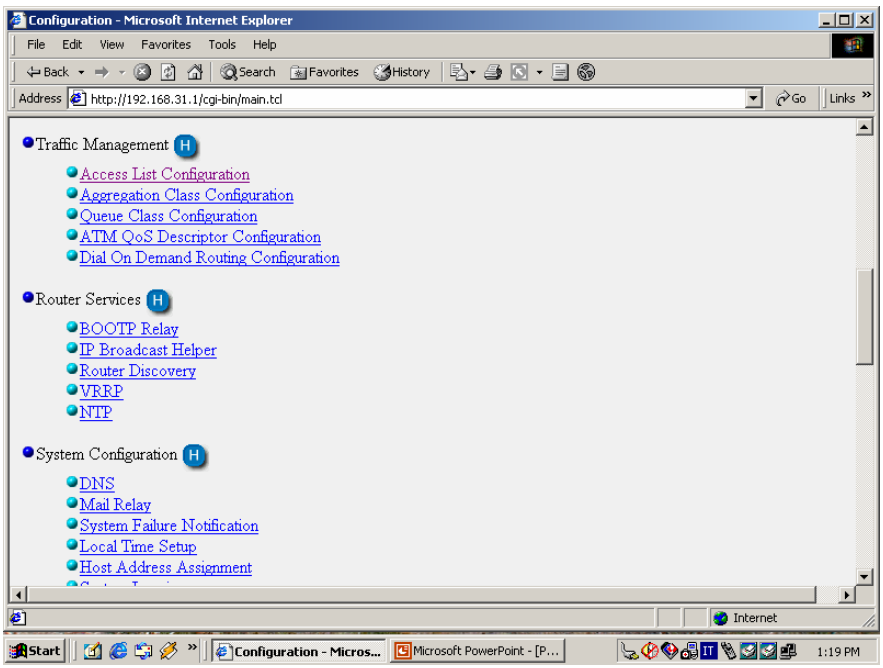
- Interfaccia Web
- Supporto di interfacce WAN V35 T1/E1
- Funziuonalità di routing (RIP,OSPF,BGP)
- Firewall (Firewall1)
- VPN IPSec .
- IDS

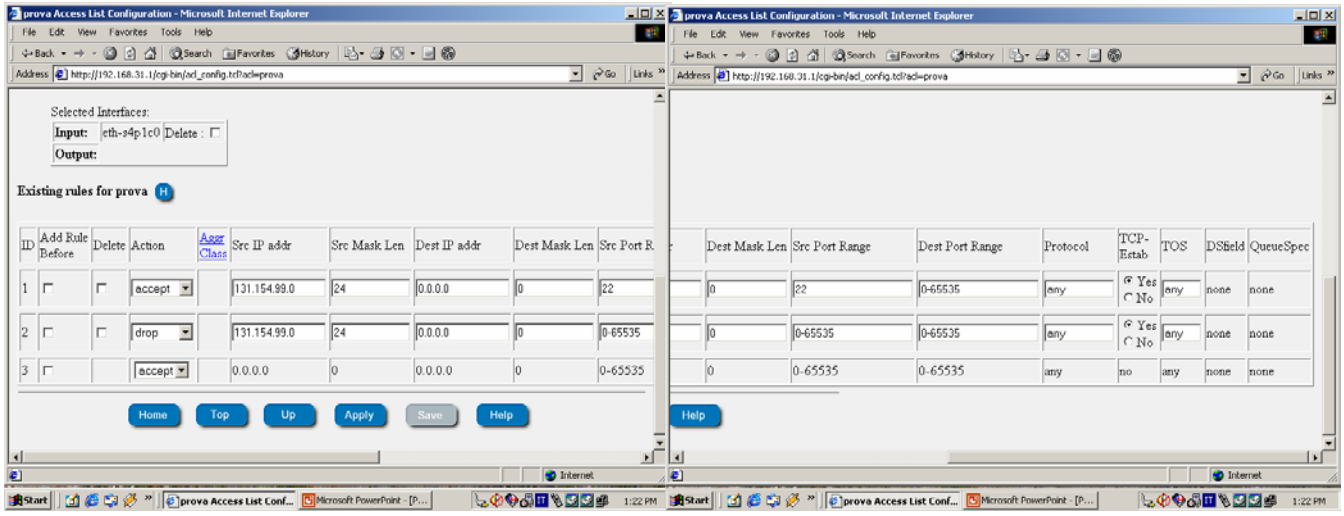
Il test di questo apparato si è concluso con la parte di configurazione di base e di alcune regole per motivi legati alla scarsa disponibilità di tempo per la prova e per lo scarso supporto fornito dal rivenditore che lo ha reso disponibile (gratuitamente).
Le prime impressioni sono state positive in quanto la parte di installazione è rapida e l'interfaccia di configurazione dei parametri di base è molto buona.
Per quanto riguarda la impostazione di ACL, l'interfaccia Web si è dimostrata farraginosa e poco funzionale per un consistente numero di regole.

A seguire alcuni "screenshot" relativi alla interfaccia grafica.

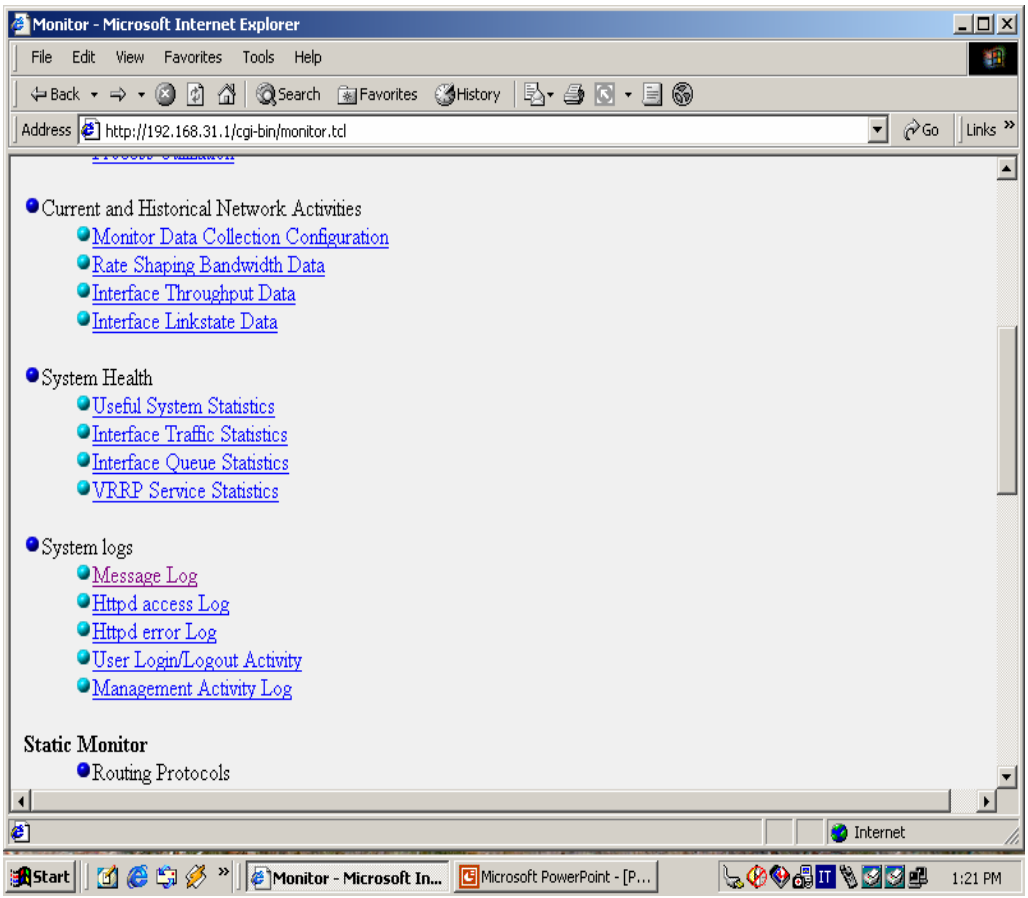

Nokia Network Voyager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.31.1/
Go Links
NOKIA networkVOYAGER
nokia
Model: IP300
Software Release: 3.5-FCS7
Software Version: releng 1020 06.03.2002-205800
Serial Number: 9N022901142
Current Time: Thu Nov 28 12:11:24 2002 GMT
Uptime: 7 minutes
Physical Memory: 256 MB
Config
Monitor
Done
Internet
Start
Nokia Network Voyage...
Microsoft PowerPoint - [P...
1:18 PM


Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.31.1/cgi-bin/main.tcl
Go Links
Configuration
Home
Top
Save
Help
H
Interfaces H
ARP
IPsec
Routing Configuration H
OSPF
RIP
IGMP
PIM
DVMRP
Static Routes
Route Aggregation
Inbound Route Filters
Done
Internet
Start
Configuration - Micros...
Microsoft PowerPoint - [P...
1:19 PM


Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.31.1/cgi-bin/main.tcl
Go Links
Traffic Management
Access List Configuration
Aggregation Class Configuration
Queue Class Configuration
ATM QoS Descriptor Configuration
Dial On Demand Routing Configuration
Router Services
BOOTP Relay
IP Broadcast Helper
Router Discovery
VRRP
NTP
System Configuration
DNS
Mail Relay
System Failure Notification
Local Time Setup
Host Address Assignment
Internet
Start
Configuration - Micros...
Microsoft PowerPoint - [P...
1:19 PM


prova Access List Configuration - Microsoft Internet Explorer
Selected Interfaces:
Input: eth-s4p1c0 Delete :
Output:
Existing rules for prova
ID Add Rule Before Delete Action Aggr Class Src IP addr Src Mask Len Dest IP addr Dest Mask Len Src Port R
Dest Mask Len Src Port Range Dest Port Range Protocol TCP-Estab TOS DSfield QueueSpec
1 accept 131.154.99.0 24 0.0.0.0 0 22 0 22 0-65535 any Yes No any none none
2 drop 131.154.99.0 24 0.0.0.0 0 0-65535 0 0-65535 0-65535 any Yes No any none none
3 accept 0.0.0.0 0 0.0.0.0 0 0-65535 0 0-65535 0-65535 any no any none none
Home Top Up Apply Save Help
Help
Internet
Start
prova Access List Conf...
Microsoft PowerPoint - [P...
1:22 PM


Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.31.1/cgi-bin/monitor.tcl
Go Links
Monitor
Home Top Help
H
Dynamic Monitor
System Utilization
CPU and Memory Utilization
Disk and Swap Space Utilization
Process Utilization
Current and Historical Network Activities
Monitor Data Collection Configuration
Rate Shaping Bandwidth Data
Interface Throughput Data
Interface Linkstate Data
System Health
Useful System Statistics
Done
Internet
Start
Monitor - Microsoft In...
Microsoft PowerPoint - [P...
1:20 PM


Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.31.1/cgi-bin/monitor.tcl
Go Links
Current and Historical Network Activities
Monitor Data Collection Configuration
Rate Shaping Bandwidth Data
Interface Throughput Data
Interface Linkstate Data
System Health
Useful System Statistics
Interface Traffic Statistics
Interface Queue Statistics
VRRP Service Statistics
System logs
Message Log
Httpd access Log
Httpd error Log
User Login/Logout Activity
Management Activity Log
Static Monitor
Routing Protocols
Internet
Start
Monitor - Microsoft In...
Microsoft PowerPoint - [P...
1:21 PM

Considerazioni generali relative al firewall Nokia

Vantaggi
Sistema completo di numerose funzioni
Può sostituire anche il router d'accesso

Svantaggi

Configurazione delle regole macchinosa anche se guidata da una buona interfaccia grafica.
Firewall basato su di un SO. noto ed Open.
Prezzo elevato

Tabella comparativa dei prezzi "Novembre 2002"

Ovviamente i prezzi sono stati "Fotografati" nello stesso istante.
Vista la rapida evoluzione degli apparati presi in considerazione i prezzi indicati valgono solo come metro comparativo in quanto alla data di pubblicazione del documento, se considerati nel loro valore assoluto non saranno aggiornati.

Firewall	ACL	IDS	VPN	Gigabit	Prezzo
Cisco PIX 515	Si	No	Disponibile(Vpn Accelerator Card)	Disponibile da 525 in poi (+3000€ ad interfaccia)	~8.000€
Nokia IP330	Si	Si (Realsecure Nokia)	Si (Check Point-1)	Non disponibile per ora	26.500 €(Unlimited)
Symantec SGS 5300	Si	Si	Si	Non disponibile per ora	17.300€ (256 users) 34.173€ (Unlimited)
Infoguard IGWALL	Si	No	Si	Disponibile Come opzione	5.907€ (Unlimited)
Box BSD	Si (pf)	No (SNORT configurabile a parte)	Configurabile	Disponibile (Performance dipendenti dall'hardware)	~0€ (+il PC)
Clavister	Si	No	Si	Fino a 2Gb su PCIX	~7200€ (Illimitata +2 anni upgrade e certificazione per 2 persone)

Altre soluzioni potenzialmente interessanti che non sono state ancora provate sono:
I firewall della ***Netscreen*** (www.netscreen.com) che utilizzano degli ASIC per la valutazione delle ACL e dovrebbero avere prezzi relativamente conteunti.

Ciscco Firewall Service Module per Cisco Catalyst 6500 che è un firewall integrato su di una scheda che si inserisce direttamente sulla matrice di switch di un Catalyst 6500 (consumando 1 slot) e permette di operare in modalità non bloccante fino a 4-5 Gb/s. Ovviamente questa soluzione è indicata per realtà che gestiscono un traffico passante molto sostenuto.

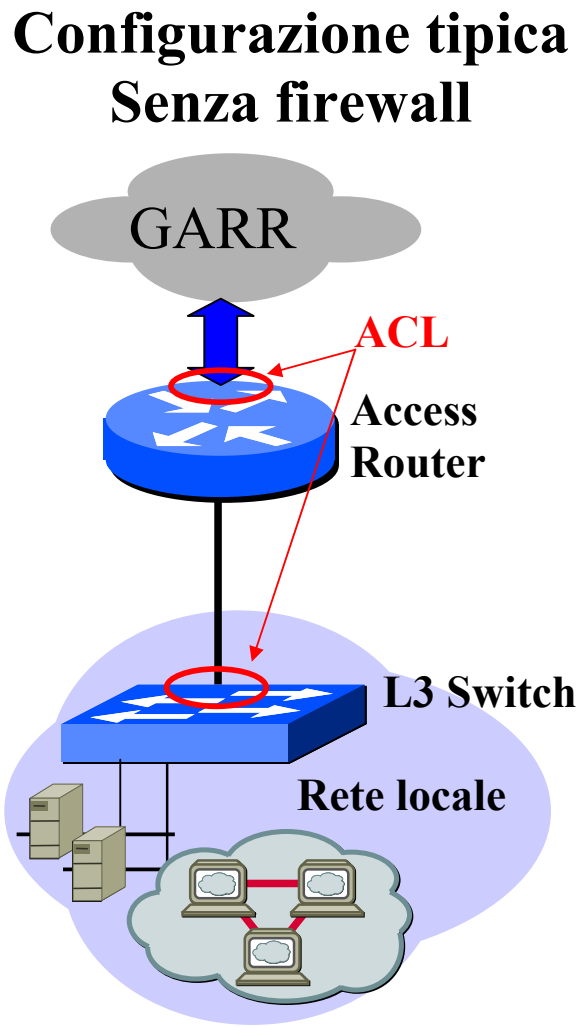
Utilizzo dei Firewall nelle sezioni dell'INFN

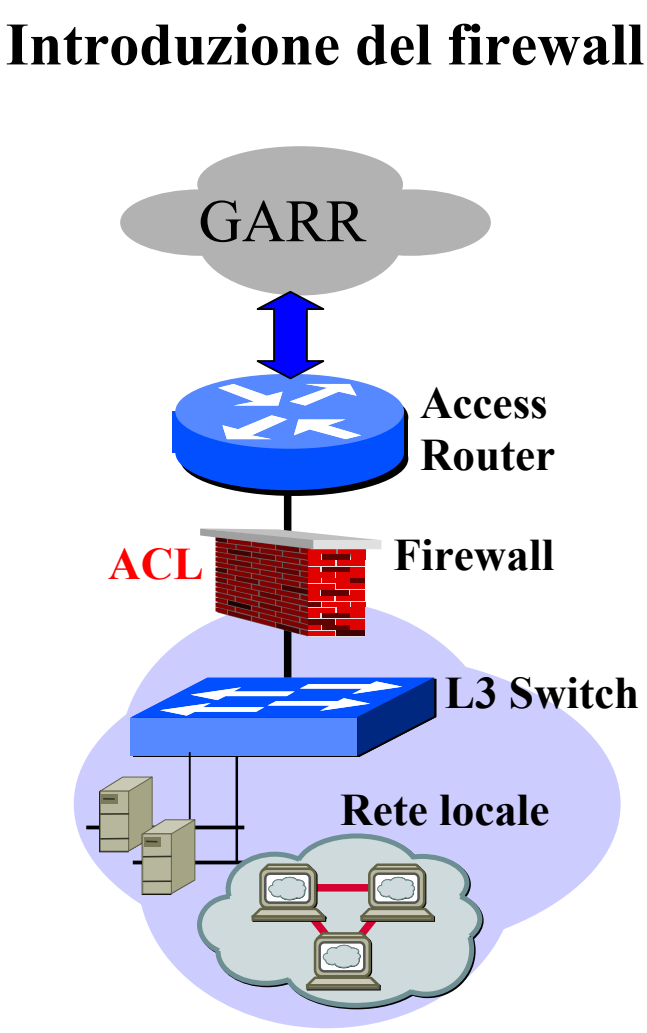
In generale nell'INFN per il tipo di applicazioni e per il tipo di dati da "Muovere" sulla rete non si ricorre a configurazioni particolarmente complesse come DMZ .
Sarebbe buona norma separare le reti ospitanti i server "Esterni" da quelle destinate ad uso interno in modo da gestire meglio e con politiche differenziate il flusso di traffico fra reti adibite ad utilizzi differenti. Questo punto è diventato di attualità con l'introduzione massiccia di apparati wireless che dovrebbero essere inseriti su rami di rete da considerarsi "Insicuri".

L'introduzione di un firewall scarica la CPU del Router o dello switch dalla valutazione delle ACL.

Se Router o Switch gestiscono ACL in Hardware (a wire speed) l'unico vantaggio nell'introduzione di un firewall esterno è nella eventuale semplicità di gestione e monitoring delle funzionalità legate alla sicurezza.

Un firewall di fascia medio bassa può essere la giusta soluzione qualora fosse necessario mettere in sicurezza un ramo particolare della LAN, oppure nel caso in cui il soggetto adibito alla gestione delle politiche di sicurezza del centro non fosse anche il gestore del router di frontiera.





Conclusioni

Anche se dal punto di vista delle performance non siamo riusciti con i mezzi utilizzati a verificare effettimavente quali fossero i limiti degli oggetti in test, possiamo affermare che le soluzioni di tipo Appliance (PIX, Nokia, Symanyec, Infoguard) non sono state ritenute particolarmente interessanti sia per fattori economici sia perchè non introducono particolari benefici in termini di prestazioni. In generale spesso sono risultati oggetti molto validi per realtà differenti dalla nostra come piccole-medie aziende o provider commerciali.

I due firewall che ci sono parsi più interessanti sono Clavister e OpenBSD+PF.
Questi due firewall sono stati impiegati in ambiente di produzione con buoni risultati.

Le seguenti righe riassumono ciò che ci è piaciuto delle due soluzioni:

OpenBSD

- E` la soluzione più economica
- E' facilmente adottabile da chi non deve gestire bande molto elevate
- PF e' un ottimo packet filter.
- La possibilità di funzionare in modalità Bridging è notevolmente interessante

Clavister

- Sicurezza legata alla accuratezza (e riservatezza) del codice
- Ottime performance legate alla compattezza del codice e scalabilità delle performace a basso costo (Non occorre acquistare nuove licenze per poter scalare a bande superiori al Gigabit).
- Ottimo sistema di Management e monitoring remoto.
- Possibilità di gestione in cluster.

NOTA: Tutti i test sono stati effettuati considerando traffico di tipo IP.
Nel caso si debbano gestire in maniera nativa (non in tunnel su IP) altri protocolli quali per esempio AppleTalk, occorrerà verificare che sia specificata la gestine di tali protocolli.

Appendice A

Riferimenti:

Questa nota , le presentazioni ed eventuali aggiornamenti saranno disponibili all'interno del sito del Netgroup: http://www.infn.it/netgroup

Questi sono i link dei produrttori dei firewall provati.

Cisco: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/
Symantec: http://www.symantec.com
Clavister: http://www.clavister.com
Infoguard: http://www.infoguard.com/
Nokia: http://www.nokia.com (Networks)
OpenBSD (PF): http://www.openbsd.com/faq/faq6.html#PF

Appendice B

Esempi di configurazione di ACL su varie piattaforme:

Filtri per router Enterasys .

La sintassi è:

acl <nome> permit/deny <protocollo> src-addr/mask dest-addr/mask src-port dest-port [options].

<nome> è una stringa qualsiasi, può essere anche un numero, sceglierò d'ora in avanti il nome *103*
<protocollo> può essere ip, udp, tcp, icmp, igmp, oltre ai protocolli legati a ipx.

Tra le opzioni posso specificare *established* e *log*.

Due cose sono sempre da tenere presenti:

- L'ordine è essenziale perché al primo match soddisfatto il router interrompe la scansione delle access-list. Per applicare delle modifiche è quindi necessario annullare tutte le access-list precedenti. Il primo comando da dare sarà:
  *no acl 103 **

- Il deny è implicito, devo quindi ricordarmi di permettere tutto ciò che non ho proibito:
  acl 103 permit ip

La lista che segue riguarda le access-list che è consigliato applicare:

AntiSpoofing

Blocca il traffico proveniente da network riservate:

acl 103 deny ip 0.0.0.0/32 any any any log
acl 103 deny ip 127.0.0.0/8 any any any log
acl 103 deny ip 10.0.0.0/8 any any any log
acl 103 deny ip 172.16.0.0/12 any any any log
acl 103 deny ip 192.168/16 any any any log

e proveniente da network locali:

acl 103 deny ip XXX.YYY.ZZZ.0/24 any any any log

NB: inserire una riga per ognuna delle network del proprio dominio

Blocco di eventuali host indesiderati

Se volete bloccare l'ingresso di host specifici:

acl 103 deny ip xxx.yyy.zzz.kkk/32 any any any log

Blocco di eventuali network indesiderate

Se volete bloccare l'ingresso di network specifiche:

acl 103 deny ip xxx.yyy.zzz.0/24 any any any log
Blocca tutto dalla porta 1 alla porta 20

Le porte dalla 1 alla 20 non sono normalmente necessarie

acl 103 deny udp any any any 1-20 log
acl 103 deny tcp any any any 1-20 log
Filtra porta 21 - FTP
acl 103 permit tcp xxx.yyy.zzz.kkk/32 sss.ddd.fff.ggg/32 any 21 <<< host to host
acl 103 permit tcp xxx.yyy.zzz.0/24 sss.ddd.fff.ggg/32 any 21 <<< network to host
acl 103 deny tcp any any any 21 log
acl 103 deny udp any any any 21 log
Blocca porta 22 - SSH

Se avete host con versioni SSH non sicure:

acl 103 deny tcp any xxx.yyy.zzz.kkk/32 any 22
acl 103 deny udp any xxx.yyy.zzz.kkk/32 any 22
Filtra porta 23 - Telnet
acl 103 permit tcp xxx.yyy.zzz.kkk/32 sss.ddd.fff.ggg/32 any 23 <<< host to host
acl 103 permit tcp xxx.yyy.zzz.0/24 sss.ddd.fff.ggg/32 any 23 <<< network to host
acl 103 deny tcp any any any 23 log
acl 103 deny udp any any any 23 log
Blocca porta 24 - any private mail system

La porta 24 non è normalmente necessaria

acl 103 deny tcp any any any 24 log
acl 103 deny udp any any any 24 log
Filtra porta 25 - SMTP

La porta 25 deve essere aperta solo verso il(i) mailserver xxx.yyy.zzz.kkk:

acl 103 permit tcp any xxx.yyy.zzz.kkk/32 any 25
acl 103 deny tcp any any any 25 log
acl 103 deny udp any any any 25 log
Blocca tutto dalla porta 26 alla porta 52

Le porte dalla 26 alla 52 non sono normalmente necessarie

acl 103 deny udp any any any 26-52 log
acl 103 deny tcp any any any 26-52 log
Filtra porta 53 - DNS

La porta 53 deve essere aperta solo verso il(i) DNS Nameserver locali xxx.yyy.zzz.kkk in udp; in tcp solo da macchine DNS server esterne autorizzate al zone-transfer:

acl 103 permit udp any xxx.yyy.zzz.kkk/32 any 53 <<< per ogni server
acl 103 permit tcp ddd.fff.ggg.hhh/32 xxx.yyy.zzz.kkk/32 any 53 <<< per ogni server
acl 103 deny tcp any any any domain log
acl 103 deny udp any any any domain log
Blocca tutto dalla porta 54 alla porta 79

Le porte dalla 54 alla 79 non sono normalmente necessarie

acl 103 deny udp any any any 54-79 log
acl 103 deny tcp any any any 54-79 log
Filtra porta 80 - HTTP

La porta 80 deve essere aperta solo verso il(i) WWW-http Server xxx.yyy.zzz.kkk:

acl 103 permit tcp any xxx.yyy.zzz.kkk/32 any 80 <<< per ogni server
acl 103 deny tcp any any any 80 log
acl 103 deny udp any any any 80 log
Blocca tutto dalla porta 81 alla porta 109

Le porte dalla 81 alla 109 non sono normalmente necessarie

acl 103 deny udp any any any 81-109 log
acl 103 deny tcp any any any 81-109 log
Filtra porta 110 - POP3

La porta 110 deve essere aperta solo verso il(i) POP3 Server xxx.yyy.zzz.kkk, se ce ne sono:

acl 103 permit tcp any xxx.yyy.zzz.kkk32 any 110 <<< per ogni server
acl 103 deny tcp any any any 110 log
acl 103 deny udp any any any 110 log
Blocca tutto dalla porta 111 alla porta 122

Le porte dalla 111 alla 122 non sono normalmente necessarie

acl 103 deny udp any any any 111-122 log
acl 103 deny tcp any any any 111-122 log
Filtra porta 123 - NTP

La porta 123 deve essere aperta solo verso il(i) NTP (Time syncronization) Server xxx.yyy.zzz.kkk, se ce ne sono:

acl 103 permit udp any xxx.yyy.zzz.kkk/32 any 123 <<< per ogni server
acl 103 deny tcp any any any 123 log
acl 103 deny udp any any any 123 log
Blocca tutto dalla porta 124 alla porta 136

Le porte dalla 124 alla 136 non sono normalmente necessarie

acl 103 deny udp any any any 124-136 log
acl 103 deny tcp any any any 124-136 log
Filtra porte 137 138 139 - NetBios

La porte 137, 138, 139 devono essere aperte solo se necessario o richiesto (p.e. Server NICE) xxx.yyy.zzz.kkk (verificate anche se serve aperta la porta 445 - Microsoft DS):

all to host:

acl 103 permit tcp any xxx.yyy.zzz.kkk/32 any 137-139
acl 103 permit udp any xxx.yyy.zzz.kkk/32 any 137-139
acl 103 deny tcp any any any 137-139 log
acl 103 deny udp any any any 137-139 log
oppure host to host:
acl 103 permit tcp sss.ddd.fff.ggg/32 xxx.yyy.zzz.kkk/32 any 137-139
acl 103 permit udp sss.ddd.fff.ggg/32 xxx.yyy.zzz.kkk/32 any 137-139
acl 103 deny tcp any any any 137-139 log
acl 103 deny udp any any any 137-139 log
Blocca tutto dalla porta 140 alla porta 142

Le porte dalla 140 alla 142 non sono normalmente necessarie

acl 103 deny udp any any any 140-142 log
acl 103 deny tcp any any any 140-142 log
Filtra porta 143 - IMAP

La porta 143 deve essere aperta solo verso il(i) IMAP Server xxx.yyy.zzz.kkk:

acl 103 permit tcp any xxx.yyy.zzz.kkk/32 any 143 <<< per ogni server
acl 103 deny tcp any any any 143 log
acl 103 deny udp any any any 143 log
Blocca tutto dalla porta 144 alla porta 169

Le porte dalla 144 alla 169 non sono normalmente necessarie

acl 103 deny udp any any any 144-169 log
acl 103 deny tcp any any any 144-169 log
Filtra porta 170 - PRINT-SRV

Se volete permettere l'accesso alla stampante xxx.yyy.zzz.kkk da altri domini presenti sulla vostra LAN, p.e. network sss.ddd.fff.0 del Dipartimento di Fisica (vedere anche porta 515):

acl 103 permit tcp sss.ddd.fff.0/24 xxx.yyy.zzz.kkk/32 any 170 <<<per ogni stampante
acl 103 deny tcp any any any 170 log
acl 103 deny udp any any any 170 log
Blocca tutto dalla porta 171 alla porta 442

Le porte dalla 171 alla 442 non sono normalmente necessarie

acl 103 deny udp any any any 171-442 log
acl 103 deny tcp any any any 171-442 log
Filtra porta 443 - HTTPS

La porta 443 deve essere aperta solo verso il(i) WWW-HTTPS e/o WebMail Server, xxx.yyy.zzz.kkk:

acl 103 permit tcp any xxx.yyy.zzz.kkk/32 any 443 <<< per ogni server
acl 103 deny tcp any any any 443 log
acl 103 deny udp any any any 443 log
Blocca tutto dalla porta 444 alla porta 448

Le porte dalla 444 alla 448 non sono normalmente necessarie

acl 103 deny udp any any any 444-448 log
acl 103 deny tcp any any any 444-448 log
Filtra porta 449 - AS Server Mapper

Alcuni Java script utilizzati dall' Amministrazione INFN a Frascati sull'host sss.ddd.fff.ggg potrebbero avere la necessità di questa porta aperta verso il sistema AS400 locale xxx.yyy.zzz.kkk:

acl 103 permit tcp sss.ddd.fff.ggg/32 xxx.yyy.zzz.kkk/32 any 449
acl 103 deny tcp any any any 449 log
acl 103 deny udp any any any 449 log
Blocca tutto dalla porta 450 alla porta 514

Le porte dalla 450 alla 514 non sono normalmente necessarie

acl 103 deny udp any any any 450-514 log
acl 103 deny tcp any any any 450-514 log
Filtra porta 515 - SPOOLER

Se volete permettere l'accesso alla stampante xxx.yyy.zzz.kkk da altri domini presenti sulla vostra LAN, p.e. network sss.ddd.fff.0 del Dipartimento di Fisica (vedere anche porta 170):

acl 103 permit tcp sss.ddd.fff.0/24 xxx.yyy.zzz.kkk/32 any 515 <<<per ogni stampante
acl 103 deny tcp any any any 515 log
acl 103 deny udp any any any 515 log
Blocca tutto dalla porta 516 alla porta 960

Le porte dalla 516 alla 960 non sono normalmente necessarie

acl 103 deny udp any any any 516-960 log
acl 103 deny tcp any any any 516-960 log
Porte da 961 a 990 aperte per ssh

Filtra porta 993 - IMAP4 (IMAP SSL)

La porta 993 deve essere aperta solo verso il(i) IMAP-SSL server xxx.yyy.zzz.kkk:

acl 103 permit tcp any xxx.yyy.zzz.kkk/32 any 993 <<< per ogni server
acl 103 deny tcp any any any 993 log
acl 103 deny udp any any any 993 log
Porte da 994 a 1022 aperte per ssh

Alcune altre porte da chiudere:

```
!
! 1080 chiusa per IRC
!

acl 103 deny tcp any any any 1080 log
acl 103 deny udp any any any 1080 log
!
! 1993 UDP chiusa per sicurezza SNMP CISCO
!
acl 103 deny udp any any any 1993 log
!
! 2049 NFS
!
acl 103 deny tcp any any any 2049 log
acl 103 deny udp any any any 2049 log
!
! 6667 chiusa per IRC
!
acl 103 deny tcp any any any 6667 log
acl 103 deny udp any any any 6667 log
!
! 27374 chiusa per worm ramen
!
acl 103 deny tcp any any any 27374 log
acl 103 deny udp any any any 27374 log
```

Nelle ultime istruzioni del file inserisco il permesso di passaggio a tutto quello che non è stato filtrato e l'applicazione dell'access list all'interfaccia:

```
acl 103 permit ip
acl 103 apply interface <nome dell'interfaccia> input logging deny-only
```

Nell'esempio l'access lista viene abilitata sui pacchetti in ingresso e per default è stato abilitato il logging di tutti i pacchetti filtrati, in questo caso non serve specificare l'opzione log nelle istruzioni di deny.

Filtro in uscita

Esempio analogo al precedente ma applicato ai pacchetti in uscita.

```
!
! ********************************
! filtro per wan in uscita
! ********************************
!

acl 104 deny tcp xxx.yyy.kkk.zzz/32 any any any log
acl 104 deny udp xxx.yyy.kkk.zzz/32 any any any log
!
! 27374 chiusa per worm ramen
!
```

```
acl 104 deny tcp any any any 27374 log
acl 104 deny udp any any any 27374 log
!
! antispoofing dalle network locali
!
acl 104 permit ip xxx.yyy.kkk.0/24 any any any
acl 104 permit ip xxx.yyy.hhh.0/24 any any any
!
! tutto il resto viene bloccato
!
acl 104 deny ip any any any any log
acl apply interface wan0 output
!
```

Attivazione filtri

I file con i filtri devono risiedere su una macchina che abbia TFTP attivo in una directory autorizzata al TFTP (vedi /etc/inetd.conf o equivalente). Le protezioni dei file devono essere: -rwxr-xr-x (chmod 775).

Dalla console del router, in modalità enable, bisogna dare i seguenti comandi per caricare le access list:

```
# no acl 103 *

# save active

# copy tftf-server to scratchpad
TFTP server?
Source filename?

# save active
```

Ricordate di salvare le modifiche:
copy active to startup
Per salvare la configurazione sul server tftp
copy startup to tftp-server
Le access list possono essere modificate anche da console; in modo enable e dopo essere entrati in configure, si usa
acl-edit <nome acl>
Le access list compaiono in ordine e precedute da un numero. È possibile cancellarle:

```
(acl-edit)> delete <numero>
```

oppure inserirle nel modo standard:

```
(acl-edit)> acl 103 permit …….
```

e poi posizionarle
(acl-edit)> move <numero posizione attuale> after <numero posizione acl precedente>

con il comando
(acl-edit)> exit
si esce e si salva

Filtri per router Cisco

Questa è una guida per creare un filtro ACL-based su router Cisco per bloccare in ingresso le porte più vulnerabili, permettendone l'accesso solo verso le macchine autorizzate (e protette) a fornire i servizi. Le indicazioni riportate non possono ovviamente coprire tutte le possibilità, ma permettono di poter implentare una protezione minimale.
Viene riportato anche un esempio di filtro in uscita (Antispoofing).
Per una descrizione completa delle porte controllate il sito: iana (Internet Assigned Numbers Authority)
NB: questo filtro va applicato per il traffico in **ingresso** sull'interfaccia di collegamento verso il GARR.
Onde evitare interruzioni nei servizi di rete, è consigliabile implementare le ACL un po' per volta e non tutte contemporaneamente: a mano a mano controllate il logging e verificate con i vostri utenti se compaiono inconvenienti.
Le access-list sono solitamente lunghe e complesse: editate un file con un nome mnemonico dove scrivere tutte le regole che verrà poi caricato sul router via tftp. Inserite nel file dei commenti (carattere ! in prima colonna): vi serviranno in futuro come riferimento.
Le ACL verranno poi interpretate nell'ordine in cui sono scritte; fate attenzione perché il router uscirà dal filtro al primo match che incontra, ignorando le righe successive.
Nell' esempio che segue viene utilizzata l'access-list numero 103 (questo numero può essere scelto tra 100 e 199). Vedremo in seguito come verrà attivata sul router.

Tutte le righe di access-list terminano con "log": in questo modo ogni volta che un pacchetto viene scartato, viene loggato sul router, ed eventualmente anche su una macchina che raccoglie i log, per analisi successive (anche per questo vedremo in seguito come fare).

- Prima e ultima riga del filtro

  Il filtro deve DEVE SEMPRE avere come prima riga:

  ```
  no access-list 103
  ```

  questo perché altrimenti le nuove regole con le ACL verranno aggiunte alla access-list 103 già attiva sul router. Non è possibile infatti aggiungere ACL in mezzo ad un filtro: bisogna cancellarlo e poi ricrearlo.

  Inoltre DEVE SEMPRE avere come ultime righe:

  ```
  access-list 103 permit ip any any
  end
  ```

  La prima serve per fare passare tutto quello che non viene bloccato dalle ACL (senza questa riga il default sarebbe **deny any any** implicito);
  la seconda termina il filtro.

- Permette le connessioni già aperte

I pacchetti che hanno già superato la fase di setup (p.e. connessioni dall'interno della LAN) non vengono controllati.

```
access-list 103 permit tcp any any established
```

- AntiSpoofing

  Blocca il traffico proveniente da network riservate:

```
access-list 103 deny ip host 0.0.0.0             any log
access-list 103 deny ip 127.0.0.0   0.255.255.255 any log
access-list 103 deny ip 10.0.0.0    0.255.255.255 any log
access-list 103 deny ip 172.16.0.0  0.15.255.255  any log
access-list 103 deny ip 192.168.0.0 0.0.255.255   any log
```

  e proveniente da network locali:

```
access-list 103 deny ip XXX.YYY.ZZZ.0  0.0.0.255 any log
```

  NB: inserire una riga per ognuna delle network del proprio dominio

- Blocco di eventuali host indesiderati

  Se volete bloccare l'ingresso di host specifici:

```
access-list 103 deny   ip  host xxx.yyy.zzz.kkk  any  log
```

- Blocco di eventuali network indesiderate

  Se volete bloccare l'ingresso di network specifiche:

```
access-list 103 deny   ip  xxx.yyy.zzz.0 0.0.0.255  any  log
```

- Blocca tutto dalla porta 1 alla porta 20

  Le porte dalla 1 alla 20 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 1 20 log
access-list 103 deny   tcp any any range 1 20 log
```

- Filtra porta 21 - FTP

  FTP trasmette la password in chiaro per cui è potenzialmente pericoloso, a volte però è necessario tenerlo aperto verso alcune macchine (p.e. macchine amministrazione). Se dovete lasciarlo aperto, fatelo solo network to host o (meglio) host to host e bloccate FTP verso le altre macchine:

```
access-list 103 permit tcp xxx.yyy.zzz.kkk host sss.ddd.fff.ggg eq 21
<<< host to host
access-list 103 permit tcp xxx.yyy.zzz.0 0.0.0.255 host sss.ddd.fff.ggg eq
21       <<< network to host
access-list 103 deny   tcp any any eq 21 log
access-list 103 deny   udp any any eq 21 log
```

- Blocca porta 22 - SSH

  Se avete host con versioni SSH non sicure:

```
access-list 103 deny tcp any host xxx.yyy.zzz.kkk  eq 22
access-list 103 deny udp any host xxx.yyy.zzz.kkk  eq 22
```

- Filtra porta 23 - Telnet

  Telnet trasmette la passowrd in chiaro come FTP ma a volte è necessario tenerlo aperto:

```
access-list 103 permit tcp xxx.yyy.zzz.kkk host sss.ddd.fff.ggg eq 23
<<< host to host
access-list 103 permit tcp xxx.yyy.zzz.0 0.0.0.255 host sss.ddd.fff.ggg eq
23       <<< network to host
access-list 103 deny   tcp any any eq 23 log
access-list 103 deny   udp any any eq 23 log
```

- Blocca porta 24 - any private mail system

  La porta 24 non è normalmente necessaria(iana)

```
access-list 103 deny   tcp any any eq 24 log
access-list 103 deny   udp any any eq 24 log
```

- Filtra porta 25 - SMTP

  La porta 25 deve essere aperta solo verso il(i) mailserver xxx.yyy.zzz.kkk:

```
access-list 103 permit tcp any host xxx.yyy.zzz.kkk   eq smtp
access-list 103 deny   tcp any any eq smtp log
access-list 103 deny   udp any any eq 25   log
```

- Blocca tutto dalla porta 26 alla porta 52

  Le porte dalla 26 alla 52 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 26 52 log
access-list 103 deny   tcp any any range 26 52 log
```

- Filtra porta 53 - DNS

  La porta 53 deve essere aperta solo verso il(i) DNS Nameserver locali xxx.yyy.zzz.kkk in udp;
  in tcp solo da macchine DNS server esterne autorizzate al zone-transfer:

```
access-list 103 permit udp any host xxx.yyy.zzz.kkk eq domain  <<<
aggiungere più righe per più server
access-list 103 permit tcp host ddd.fff.ggg.hhh host xxx.yyy.zzz.kkk eq
domain  <<< aggiungere più righe per più server
access-list 103 deny   tcp any any eq domain log
access-list 103 deny   udp any any eq domain log
```

- Blocca tutto dalla porta 54 alla porta 79

Le porte dalla 54 alla 79 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 54 79 log
access-list 103 deny   tcp any any range 54 79 log
```

- Filtra porta 80 - HTTP

  La porta 80 deve essere aperta solo verso il(i) WWW-http Server xxx.yyy.zzz.kkk:

```
access-list 103 permit tcp any host xxx.yyy.zzz.kkk eq www     <<<
aggiungere più righe per più server
access-list 103 deny   tcp any any eq www log
access-list 103 deny   udp any any eq 80  log
```

- Blocca tutto dalla porta 81 alla porta 109

  Le porte dalla 81 alla 109 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 81 109 log
access-list 103 deny   tcp any any range 81 109 log
```

- Filtra porta 110 - POP3

  La porta 110 deve essere aperta solo verso il(i) POP3 Server xxx.yyy.zzz.kkk, se ce ne sono:

```
access-list 103 permit tcp any host xxx.yyy.zzz.kkk eq pop3     <<<
aggiungere più righe per più server
access-list 103 deny   tcp any any eq pop3 log
access-list 103 deny   udp any any eq 110  log
```

- Blocca tutto dalla porta 111 alla porta 122

  Le porte dalla 111 alla 122 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 111 122 log
access-list 103 deny   tcp any any range 111 122 log
```

- Filtra porta 123 - NTP

  La porta 123 deve essere aperta solo verso il(i) NTP (Time syncronization) Server xxx.yyy.zzz.kkk, se ce ne sono:

```
access-list 103 permit udp any host xxx.yyy.zzz.kkk eq 123     <<<
aggiungere più righe per più server
access-list 103 deny   tcp any any eq 123  log
access-list 103 deny   udp any any eq 123  log
```

- Blocca tutto dalla porta 124 alla porta 136

  Le porte dalla 124 alla 136 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 124 136  log
access-list 103 deny   tcp any any range 124 136  log
```

- Filtra porte 137 138 139 - NetBios

La porte 137, 138, 139 devono essere aperte solo se necessario o richiesto (p.e. Server NICE) xxx.yyy.zzz.kkk (verificate anche se serve aperta la porta 445 - Microsoft DS):

all to host:

```
access-list 103 permit tcp any host xxx.yyy.zzz.kkk  range 137 139
access-list 103 permit udp any host xxx.yyy.zzz.kkk  range 137 139
access-list 103 deny   tcp any any range 137 139 log
access-list 103 deny   udp any any range 137 139 log
```

oppure host to host:

```
access-list 103 permit tcp host sss.ddd.fff.ggg host xxx.yyy.zzz.kkk
range 137 139
access-list 103 permit udp host sss.ddd.fff.ggg host xxx.yyy.zzz.kkk
range 137 139
access-list 103 deny   tcp any any range 137 139 log
access-list 103 deny   udp any any range 137 139 log
```

- Blocca tutto dalla porta 140 alla porta 142

  Le porte dalla 140 alla 142 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 140 142  log
access-list 103 deny   tcp any any range 140 142  log
```

- Filtra porta 143 - IMAP

  La porta 143 deve essere aperta solo verso il(i) IMAP Server xxx.yyy.zzz.kkk:

```
access-list 103 permit tcp any host xxx.yyy.zzz.kkk eq 143     <<<
aggiungere più righe per più server
access-list 103 deny   tcp any any eq 143  log
access-list 103 deny   udp any any eq 143  log
```

- Blocca tutto dalla porta 144 alla porta 169

  Le porte dalla 144 alla 169 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 144 169  log
access-list 103 deny   tcp any any range 144 169  log
```

- Filtra porta 170 - PRINT-SRV

  Se volete permettere l'accesso alla stampante xxx.yyy.zzz.kkk da altri domini presenti sulla vostra LAN, p.e. network sss.ddd.fff.0 del Dipartimento di Fisica (vedere anche porta 515):

```
access-list 103 permit tcp sss.ddd.fff.0 0.0.0.255 host xxx.yyy.zzz.kkk eq
170     <<< aggiungere più righe per più stampanti
access-list 103 deny   tcp any any eq 170  log
access-list 103 deny   udp any any eq 170  log
```

- Blocca tutto dalla porta 171 alla porta 442

  Le porte dalla 171 alla 442 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 171 442  log
access-list 103 deny   tcp any any range 171 442  log
```

- Filtra porta 443 - HTTPS

  La porta 443 deve essere aperta solo verso il(i) WWW-HTTPS e/o WebMail Server, xxx.yyy.zzz.kkk:

```
access-list 103 permit tcp any host xxx.yyy.zzz.kkk eq 443     <<<
aggiungere più righe per più server
access-list 103 deny   tcp any any eq 443  log
access-list 103 deny   udp any any eq 443  log
```

- Blocca tutto dalla porta 444 alla porta 448

  Le porte dalla 444 alla 448 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 444 448  log
access-list 103 deny   tcp any any range 444 448  log
```

- Filtra porta 449 - AS Server Mapper

  Alcuni Java script utilizzati dall' Amministrazione INFN a Frascati sull'host sss.ddd.fff.ggg potrebbero avere la necessità di questa porta aperta verso il sistema AS400 locale xxx.yyy.zzz.kkk:

```
access-list 103 permit tcp host sss.ddd.fff.ggg host xxx.yyy.zzz.kkk eq
449
access-list 103 deny   tcp any any eq 449  log
access-list 103 deny   udp any any eq 449  log
```

- Blocca tutto dalla porta 450 alla porta 514

  Le porte dalla 450 alla 514 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 450 514  log
access-list 103 deny   tcp any any range 450 514  log
```

- Filtra porta 515 - SPOOLER

  Se volete permettere l'accesso alla stampante xxx.yyy.zzz.kkk da altri domini presenti sulla vostra LAN, p.e. network sss.ddd.fff.0 del Dipartimento di Fisica (vedere anche porta 170):

```
access-list 103 permit tcp sss.ddd.fff.0 0.0.0.255 host xxx.yyy.zzz.kkk eq
515     <<< aggiungere più righe per più stampanti
access-list 103 deny   tcp any any eq 515  log
access-list 103 deny   udp any any eq 515  log
```

- Blocca tutto dalla porta 516 alla porta 960

  Le porte dalla 516 alla 960 non sono normalmente necessarie(iana)

```
access-list 103 deny   udp any any range 516 960  log
access-list 103 deny   tcp any any range 516 960  log
```

- Porte da 961 a 990 aperte per ssh
- Filtra porta 993 - IMAP4 (IMAP SSL)

  La porta 993 deve essere aperta solo verso il(i) IMAP-SSL server xxx.yyy.zzz.kkk:

```
access-list 103 permit tcp any host xxx.yyy.zzz.kkk   eq 993   <<<
aggiungere più righe per più server
access-list 103 deny   tcp any any eq 993 log
access-list 103 deny   udp any any eq 993 log
```

- Porte da 994 a 1022 aperte per ssh
- Con questo abbiamo terminato le porte definite **Well Known**. Per le porte superiori, ecco alcuni esempi di porte da filtrare:

```
!
! 1080 chiusa per IRC
!
access-list 103 deny   tcp any any eq 1080 log
access-list 103 deny   udp any any eq 1080 log
!
! 1993 UDP chiusa per sicurezza SNMP CISCO
!
access-list 103 deny   udp any any eq 1993 log
!
! 2049 NFS
!
access-list 103 deny   tcp any any eq 2049 log
access-list 103 deny   udp any any eq 2049 log
!
!  6667 chiusa per IRC
!
access-list 103 deny   tcp any any eq 6667 log
access-list 103 deny   udp any any eq 6667 log
!
! 27374 chiusa per worm ramen
!
access-list 103 deny   tcp any any eq 27374 log
access-list 103 deny   udp any any eq 27374 log
```

- Chiusura del file

  Come già riportato all'inizio, chiudete il file con:

```
access-list 103 permit any any
end
```

- Filtro in uscita

  In questo esempio viene creato un filtro (access-list 104 in questo caso) in **uscita** per l'interfaccia verso la rete esterna.
  Queste ACL servono per:

  - bloccare host del vostro dominio (p.e. host compromessi in attesa di bonifica).
  - bloccare porte in uscita utilizzate da virus.

- Antispoofing delle network locali: permette l'uscita solo dei pacchetti che abbiano come source address indirizzi delle network locali.
- tutto il resto viene bloccato

```
no access-list 104
!
! ********************************
! filtro per wan in uscita
! ********************************
!
access-list 104 deny   tcp host xxx.yyy.kkk.zzz any log
access-list 104 deny   udp host xxx.yyy.kkk.zzz any log
!
! 27374 chiusa per worm ramen
!
access-list 104 deny   tcp any any eq 27374 log
access-list 104 deny   udp any any eq 27374 log
!
! antispoofing dalle network locali
!
access-list 104 permit ip xxx.yyy.kkk.0 0.255.255.255 any
access-list 104 permit ip xxx.yyy.hhh.0 0.255.255.255 any
!
! tutto il resto viene bloccato
!
access-list 104 deny ip any any log
!
end
```

- Attivazione filtri

I file con i filtri devono risiedere su una macchina che abbia TFTP attivo in una directory autorizzata al TFTP (vedi **/etc/inetd.conf** o equivalente). Le protezioni dei file devono essere: **-rwxr-xr-x** (chmod 775).
Dalla console del Cisco, in enable, individuate (**show interface**) l'interfaccia di accesso alla rete esterna (p.e. ATM2/0.1) ed eseguite i seguenti comandi per caricare il file con il filtro e associare l'access-list 103 al traffico entrante ed eventualmente l'access-list 104 al traffico uscente dell'interfaccia verso il GARR.

```
# copy tftp run
host ? [return]
Address of remote host? host-con-tftp
Name of configuration file? /drectory-tftp/filtro.103
```

Il router carica il filtro, segnalando se ci sono errori di sintassi o se l'operazione viene completata con successo.
Se lo avete implementato, ripete l'operazione per il filtro in uscita (access-list 104).
Ora associamo i filtri all'interfaccia:

```
# conf t
interface ATM2/0.1
```

```
 ip access-group 103 in
 ip access-group 104 out     << solo se implementato
control Z
```

Ricordate di salvare le modifiche:

```
# copy run startup
# copy run tftp
```

per salavare la configurazione su host con tftp deve esistere nella directory abilitata al tftp un file vuoto con protezione:
-rwxrwxrwx (chmod 777).

Logging

Dalla console del Cisco è possibile monitorare i pacchetti scartati con il comando:

```
# show logging
```

in testa alla videata vengono visualizzati gli eventi più recenti. Questo sistema non è però molto comodo: visualizza solo gli eventi più recenti. Per inviare i messaggi di log su un host, eseguite i seguenti comandi sul router:

```
# conf t
logging buffered 16384                  << dimensioni buffer
no logging console                      << disabilita i messaggi su
console
logging trap debugging                  << livello dei messaggi generati
logging facility local6                 << definisce su quale facility il
syslog della macchina riceve i messaggi
logging xxx.yyy.kkk.hhh                 << host di destinazione
```

Sull'host di destinazione, nel file **/etc/syslog.conf** (o equivalente) inserire una riga:

```
local6.debug
/directory/cisco.log
```

Su questi log file si possono utilizzare tool automatici per verificare eventuali scan, compromissioni, etc.
A seconda della quantità e complessità delle ACL, questo file può crescere di dimensioni rapidamente: utilizzate tool come logrotate per ruotarli, comprimerli e archiviarli.

Con il comando **show process** è possibile visualizzare il carico della cpu del Cisco per verificare l'impatto dei filtri sulle performance del router.

Filtri per BOX Open BSD (pf.conf).

```
# definitions
ExtIF="fxp0"
NoRouteIPs="{ 127.0.0.0/8, xzy.YYY.0.0/16, XXX.16.0.0/12, XX.0.0.0/8 }"
IntNet="{ XYZ.ZYX.10.0/24, XYZ.ZYX.11.0/24, XYZ.ZYX.12.0/24, XYZ.ZYX.102.0/24 }"

# default deny stance
block in all
block out all

# allow established connections
pass in on $ExtIF inet proto tcp all flags S/SA keep state
pass in on $ExtIF inet proto udp all keep state
pass in on $ExtIF inet proto icmp all keep state

# don't allow anyone to spoof non-routeable addresses
block in log  quick on $ExtIF from $NoRouteIPs to any
block out log quick on $ExtIF from any to $NoRouteIPs

# antispoofing on local network
block in log  quick on $ExtIF from $IntNet to any
pass out quick on $ExtIF inet proto tcp from $IntNet to any flags S/SA keep state
pass out quick on $ExtIF inet proto udp from $IntNet to any keep state
pass out quick on $ExtIF inet proto icmp from $IntNet to any keep state
block out log quick on $ExtIF from any to any

# blocca gnutella 27.6/02
block in log  quick on $ExtIF inet proto { tcp, udp } from any to any port 6346

# chiude in ingresso
#
# chiudi i seguenti host
# host pcopax2 (bonaventura)  9/7/02
# host pcze05  (margotti) 7.10.02
# host pcrossim (rossi m.-casali) 5.1/03
#
block in log  quick on $ExtIF from any to { XYZ.ZYX.11.212, XYZ.ZYX.12.35, XYZ.ZYX.102.12 }

# host chiusi 27/6/02 - Labe A
# serverXXX.colonIER.com  XXX.XX.YYY.130
# pcblade XYZ.ZYX.11.252
# Server Active Directory - chiusi su richiesta GP 130103
#
block in log  quick on $ExtIF from any to { XYZ.ZYX.12.198, XYZ.ZYX.12.202 }

# Host esterni chiusi dopo vari attacchi e segnalazioni
#
#
# FB 20.11/2002 from Lan
#
block in log  quick on $ExtIF from any to xzy.XYZ.128.98

# FB 20.8/2002 from www.incidents.org
#
block in log  quick on $ExtIF from { 160.28.214.170, 61.144.129.82, 155.210.92.35, 203.116.40.34,
130.88.153.201, 209.186.21.3, 209.186.21.3, 147.52.98.222, 24.198.97.198, 212.62.233.98 } to any
#
block in log  quick on $ExtIF from 216.15.251.130 to any
#
block in log  quick on $ExtIF from any to XYZ.ZYX.11.252
```

```
#
#

# shitlist: host chiusi dopo accessi di pcopXXX(bonaventura) 9.7.02
#
block in log  quick on $ExtIF from { 206.132.249.170, 208.48.234.214, 208.51.236.61, 209.244.160.169,
209.247.11.165, 209.247.11.186, 64.159.17.162, 64.214.196.241 } to any

# host chiusi dopo scan 21.6/2002
#
block in log  quick on $ExtIF from { 205.155.87.8, 80.62.57.109 } to any

# host chiusi dopo attacchi su pcmar - 17.07/02
#
block in log  quick on $ExtIF from { 213.20.65.85, 195.239.154.86, 62.163.169.53, 213.215.167.98,
211.64.xzy.1, 217.229.198.31 } to any

# name: sul.e.kth.se - attacchi su porta 7001 verso server AFS
#
block in log  quick on $ExtIF from 130.237.48.109 to any

# name: chi-qbu-nvc-vty41.as.wcom.net
#
block in log  quick on $ExtIF from 216.xzy.163.41 to any

# amigo.dps.digex.net
#
block in log  quick on $ExtIF from 165.117.241.90 to any

# name: kinneret.kinneret.co.il
#
block in log  quick on $ExtIF from 207.232.16.1 to any

# name: rub004.ud00.ne.interbusiness.it
#
block in log  quick on $ExtIF from 195.120.36.4 to any

# h213-10-138.BO1.albacom.net
#
block in log quick on $ExtIF from 213.213.10.138 to any

# irc.mindspring.com
#
block in log quick on $ExtIF from 207.69.200.132 to any

# Name:    fun.ircd.it
#
block in log quick on $ExtIF from 194.183.2.245 to any

# Name:    tiscali.ircd.it
#
block in log quick on $ExtIF from 195.130.233.45 to any

# irc.stealth.net
#
block in log quick on $ExtIF from 206.252.xzy.195 to any

# Name:    us.undernet.org
#
block in log quick on $ExtIF from { 207.173.16.33, 207.96.122.250,  205.252.46.98, 207.110.0.52,
205.188.149.3, 207.69.200.131, 207.114.4.35, 204.127.145.17, 216.24.134.10, 208.51.158.10, 199.170.91.114
} to any
```

```
# Sconosciuto che accedeva a pcort (sottorete .hkt.net):
#
block in log quick on $ExtIF from 203.100.64.77 to any

# Sottorete iinet.net.au
block in log quick on $ExtIF from 203.59.145.149 to any

# info-services-3.sunderland.ac.uk
#
block in log quick on $ExtIF from 157.228.35.30 to any

# nic-163-c220-020.mw.mediaone.net
block in log quick on $ExtIF from 24.163.220.20 to any

# 130.frogspace.net
#
block in log quick on $ExtIF from 216.65.12.130 to any

# attacchi su sgi max gaze
#
block in log quick on $ExtIF from { 157.228.35.30, 212.64.110.129 } to any

# robert.coria.fr
#
block in log quick on $ExtIF from 195.103.87.7 to any

# voyager.co.nz
block in log quick on $ExtIF from 202.2.96.3  to any

# ftptunnel.ztx.compaq.com
#
block in log quick on $ExtIF from 161.114.3.105 to any

# ntt.net
#
block in log quick on $ExtIF from 155.69.177.18 to any

# df.unibo.it
#
block in log quick on $ExtIF from XYZ.ZYX.48.108 to any

#  alternet NS
#
block in log quick on $ExtIF from 211.39.21.253 to any

# sakura.ad.jp
#
block in log quick on $ExtIF from 210.188.232.12 to any

# galactica.it
#
block in log quick on $ExtIF from 213.167.213.235 to any

# roxybar
#
block in log quick on $ExtIF from 194.20.52.213 to any

# raf.forobit.it
#
block in log quick on $ExtIF from 195.216.128.98 to any
```

```
# paolo.lan.it
#
block in log quick on $ExtIF from 195.250.1.59 to any

# mail.ats.it
#
block in log quick on $ExtIF from 195.62.227.25 to any

# righi.df.unibo.it
#
block in log quick on $ExtIF from XYZ.ZYX.49.17 to any

# iunet.it
#
block in log quick on $ExtIF from 193.70.128.6 to any

# linux.mediaservice.net
#
block in log quick on $ExtIF from 195.103.87.15 to any

#########################################################
# network bloccate                                      #
#########################################################
#
# FB 20/8/2002
block in log quick on $ExtIF from 211.62.0.0/16 to any

# technotronics
#
block in log quick on $ExtIF from 209.100.46.0/24 to any

# alternet
#
block in log quick on $ExtIF from { 212.177.240.0/24, 212.177.241.0/24 } to any

# dip.t-dialin.net
#
block in log quick on $ExtIF from 212.185.212.0/24 to any

# AsianWork
#
block in log quick on $ExtIF from 210.106.255.0/24 to any

# PCPLUTO9 XYZ.ZYX.11.133
# pcxxxx.bo.infn.it XYZ.ZYX.10.87
# pcxxxxxx.bo.infn.it XYZ.ZYX.102.84 - FB 9.6/02
# adsl-195-184-238-122.mistral-uk.net  195.184.238.122
#
pass in quick on $ExtIF inet proto tcp from 134.158.105.0/24 to XYZ.ZYX.102.84 port 6000><6003 flags
S/SA keep state
#
block in log quick on $ExtIF inet proto { tcp, udp } from any to { XYZ.ZYX.11.133, XYZ.ZYX.10.87,
XYZ.ZYX.102.84, 195.184.238.122 }

# chiude da porta 1 a 20
#
block in log quick on $ExtIF inet proto { tcp, udp } from any to any port 1><20

# 21 FTP    aperto solo per autorizzati:
# Amministrazione da fuxxx.lnf.infn.it
# xzy.XYZ.84.48  a ammbo XYZ.ZYX.11.26
# Amministrazione da Tarazed.lnf.infn.it
```

```
# xzy.XYZ.84.208 a ammbo XYZ.ZYX.11.26
#
pass in quick on $ExtIF inet proto tcp from { xzy.XYZ.84.48, xzy.XYZ.84.208 } to XYZ.ZYX.11.26 port 21
flags S/SA keep state
#
block in log quick on $ExtIF inet proto tcp from any to any port 21

# ! 22    SSH    chiuso verso ssh versione non sicure:
#
#                 sunvlXXX       XYZ.ZYX.11.44          paperoga
#                 sunvlXXX       XYZ.ZYX.11.78          paperoga
#                 pccmXXX         XYZ.ZYX.102.64         grandi
#                 pchXXX          XYZ.ZYX.10.87          dolce-gabbana
#                 hp7XXX         XYZ.ZYX.10.135         dolce-gabbana
#                 hp7XXX         XYZ.ZYX.10.175         dolce-gabbana
#                 hp8XXX          XYZ.ZYX.10.180         dolce-gabbana (s
# shd gira su porta 32)
#                 xwfm2          XYZ.ZYX.11.46          archimede
#                 sgoYYY          XYZ.ZYX.11.89          max gaze
#                 PCPLxc      XYZ.ZYX.11.133         paperinik
#
#  TCP porta 22 ssh
#
block in log quick on $ExtIF inet proto { tcp, udp } from any to { XYZ.ZYX.11.44, XYZ.ZYX.11.78,
XYZ.ZYX.102.64, XYZ.ZYX.10.87, XYZ.ZYX.10.135, XYZ.ZYX.10.175, XYZ.ZYX.10.180,
XYZ.ZYX.11.46, XYZ.ZYX.11.89, XYZ.ZYX.11.133 }

# 23    Telnet  24 any private mail system
#
# aperto telnet solo per autorizzati Amministrazione a AMMBO XYZ.ZYX.11.26
#
#             pctxxxx.lnf.infn.it            xzy.XYZ.80.122
#             pcanxxxxxx.lnf.infn.it         xzy.XYZ.80.240
#             funxxx.lnf.infn.it             xzy.XYZ.84.48
#             tarxxxxx.lnf.infn.it           xzy.XYZ.84.208
#             pcxxxx.lnf.infn.it             xzy.XYZ.80.213
#
pass in quick on $ExtIF inet proto tcp from { xzy.XYZ.80.122, xzy.XYZ.80.240, xzy.XYZ.84.48,
xzy.XYZ.84.208, xzy.XYZ.80.213 } to XYZ.ZYX.11.26 port 23 flags S/SA keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any

# 25    SMTP   aperto lnxm & mail
#
pass in quick on $ExtIF inet proto tcp from any to { XYZ.ZYX.12.200, XYZ.ZYX.102.70 } port 25 flags
S/SA keep state

# 32    SSH    aperto per hpxxxx Salli
#
pass in quick on $ExtIF inet proto tcp from any to XYZ.ZYX.10.180 port 32 flags S/SA keep state
pass in quick on $ExtIF inet proto udp from any to XYZ.ZYX.10.180 port 32 keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 26><52

# 53   DNS     aperto solo dnsm dnsi
#
pass in quick on $ExtIF inet proto { tcp, udp } from any to { XYZ.ZYX.11.102, XYZ.ZYX.10.4,
XYZ.ZYX.11.102, XYZ.ZYX.10.4 } port 53 keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 54><79

# 80   http WWW     aperto ai servers
```

```
#
pass in quick on $ExtIF inet proto tcp from any to { XYZ.ZYX.10.84, XYZ.ZYX.10.99, XYZ.ZYX.10.113,
XYZ.ZYX.10.143, XYZ.ZYX.10.180, XYZ.ZYX.10.184, XYZ.ZYX.10.xzy, XYZ.ZYX.11.26,
XYZ.ZYX.11.66, XYZ.ZYX.11.74, XYZ.ZYX.11.119, XYZ.ZYX.11.173, XYZ.ZYX.11.238,
XYZ.ZYX.12.98, XYZ.ZYX.102.66, XYZ.ZYX.102.79 } port 80 flags S/SA keep state
#
pass in quick on $ExtIF inet proto tcp from yyy.xxx.43.242 to XYZ.ZYX.10.248 port 80 flags S/SA keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 80

# 81-109 chiuso tutto
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 81><109

# 110   POP3 aperto ai server
#
pass in quick on $ExtIF inet proto tcp from any to XYZ.ZYX.10.180 port 110 flags S/SA keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 110

# 111  SunRPC chiuso a tutti in attesa di notizie
# 112-122 chiuso tutto
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 111><122

# 123 NTP aperta in udp
#
block in quick log on $ExtIF inet proto tcp from any to any port 123

# 124-136 chiuso tutto
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 124><136

#  137-138-139 Netbios su Ip  solo verso:
#  server Nice     XYZ.ZYX.11.110 - XYZ.ZYX.11.95
#  CDF from fnal   XYZ.ZYX.10.77  - XYZ.ZYX.12.22
#  CMS (ben) XYZ.ZYX.102.15
#  PCPLUTO4       XYZ.ZYX.11.173
#  infn-bo-oplà (pippo) da pcpippo1 XXZ.XYZ.187.189 e pcpippo2 xxz.xyz.187.1
#  90 (Cern)
#
pass in quick on $ExtIF inet proto tcp from any to { XYZ.ZYX.11.110, XYZ.ZYX.11.95, XYZ.ZYX.11.173 }
port 137><139 flags S/SA keep state
pass in quick on $ExtIF inet proto tcp from XYZ.ZXY.236.130 to XYZ.ZYX.10.77 port 137><139 flags S/SA
keep state
pass in quick on $ExtIF inet proto tcp from XYZ.ZXY.232.171 to XYZ.ZYX.10.77 port 137><139 flags S/SA
keep state
pass in quick on $ExtIF inet proto tcp from XYZ.ZXY.236.130 to XYZ.ZYX.12.22 port 137><139 flags S/SA
keep state
pass in quick on $ExtIF inet proto tcp from XYZ.ZXY.232.171 to XYZ.ZYX.12.22 port 137><139 flags S/SA
keep state
pass in quick on $ExtIF inet proto tcp from 194.190.162.45 to XYZ.ZYX.102.15  port 137><139 flags S/SA
keep state
pass in quick on $ExtIF inet proto tcp from XXZ.XYZ.187.189 to XYZ.ZYX.11.141 port 137><139 flags
S/SA keep state
pass in quick on $ExtIF inet proto tcp from XXZ.XYZ.187.190 to XYZ.ZYX.11.141 port 137><139 flags
S/SA keep state
pass in quick on $ExtIF inet proto tcp from XXZ.XYZ.187.167 to XYZ.ZYX.11.141 port 137><139 flags
S/SA keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 137><139
```

```
# 140-142 chiuso tutto
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 140><142

#  143 IMAP aperto solo ai server
#
pass in quick on $ExtIF inet proto tcp from any to { XYZ.ZYX.10.180, XYZ.ZYX.11.78, XYZ.ZYX.10.223 }
port 143 flags S/SA keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 143

# 144-169 chiuso tutto
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 144><169

# 170 print-srv aperta da dipartimento a printserver Morassutti
#
pass in quick on $ExtIF inet proto tcp from XYZ.ZYX.xx.0/24 to { XYZ.ZYX.yy.50, XYZ.ZYX.yy.82 } port
170 flags S/SA keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 170

# 171-177 chiuso tutto
# 177 Xdmcp UDP/TCP chiuso
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 171><177

# 178-442 chiuso tutto
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 178><442

# 443 https - solo server wwwxxx lnxxx mx my mail
#
pass in quick on $ExtIF inet proto tcp from any to { XYZ.ZYX.10.84, Xxy.ZYX.10.113, XYZ.ZYX.102.70,
XYZ.Zxx.12.196, XYZ.ZYX.12.197, XYZ.Zyx.12.200 } port 443 flags S/SA keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 443

# 444 chiuso tutto
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 444

# 445 aperto per pippo da Cern:
# infn-bo-oplà (pippo) da pcpippo1 XXZ.XYZ.187.189 e pcpippo2 xxz.xyz.187.190
# (Cern)
#
pass in quick on $ExtIF inet proto tcp from { XXZ.XYZ.187.189, XXZ.XYZ.187.190, XXZ.XYZ.187.167,
XXZ.XYZ.187.189, XXZ.XYZ.187.190, XXZ.XYZ.187.167 } to XYZ.ZYX.11.141 port 445 flags S/SA keep
state
pass in quick on $ExtIF inet proto udp from { XXZ.XYZ.187.189, XXZ.XYZ.187.190, XXZ.XYZ.187.167,
XXZ.XYZ.187.189, XXZ.XYZ.187.190, XXZ.XYZ.187.167 } to XYZ.ZYX.11.141 port 445 keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 445

# 446-448 chiuso tutto
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 446><448

# 449 Per java script aperto verso ammbo da xzy.XYZ.80.122
#                                    xzy.XYZ.80.240
#
```

```
pass in quick on $ExtIF inet proto tcp from { xzy.XYZ.80.122, xzy.XYZ.80.240 } to XYZ.ZYX.11.26 port
449 flags S/SA keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 449

# 450-499 chiuso tutto
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 450><499

# 500 aperto UDP per PCMINNIE.bo.infn.it XYZ.ZYX.10.69
#                 infn-bo-opal2     XYZ.ZYX.11.141
# test VPN 29/10/2002
#
pass in quick on $ExtIF inet proto tcp from any to { XYZ.ZYX.10.69, XYZ.ZYX.11.141 } port 500 flags
S/SA keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 500

# 501-514 chiuso tutto
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 501><514

# 515 printer aperta da dipartimento a lpsccl,laserps-1,axpbo7,prserver
#
pass in quick on $ExtIF inet proto tcp from XYZ.ZYX.48.0/24 to { XYZ.ZYX.11.50, XYZ.ZYX.10.84,
XYZ.ZYX.11.82, XYZ.ZYX.11.61, XYZ.ZYX.10.172 } port 515 flags S/SA keep state
pass in quick on $ExtIF inet proto tcp from { XYZ.ZYX.49.0/24, XYZ.ZYX.50.0/24 } to XYZ.ZYX.10.172
port 515 flags S/SA keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 515

# 516-634 chiuso tutto
# 635 Mountd tutto chiuso
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 516><634

# 636-960 chiuso tutto
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 636><960

# 961 - 992 aperto per ssh
#
# 993 - IMAP SSL
#
pass in quick on $ExtIF inet proto tcp from any to { XYZ.ZYX.10.68, XYZ.ZYX.10.227, XYZ.ZYX.11.61,
XYZ.ZYX.12.200, XYZ.ZYX.102.70 } port 993 flags S/SA keep state
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 993

#  994-1022 aperto per ssh
#
#
# 1080 chiusa per IRC
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 1080

# 1115 chiusa per ardus-transfer
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 1115

# 1214 chiusa per Kazaa e Morpheous (mp3)
#
```

```
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 1214

# 1433-1434 chiusa per  MS-SQL udp/tcp
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 1433><1434

# 1993 UDP chiusa per sicurezza SNMP CISCO
#
block in quick log on $ExtIF inet proto udp from any to any port 1993

# 2002 sicurezza SSL (in & out)
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 2002

# 2049 NFS
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 2049

# 2773-2774 Sub-Seven trojan - 5/1/2003
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 2773><2774

# 6346-6347 - Gnutella 6.11.2002
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 6346><6347

# 6667 chiusa per IRC
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 6347

# 27374 chiusa per worm ramen
#
block in quick log on $ExtIF inet proto { tcp, udp } from any to any port 27374

# 43981 Netware - solo udp
#
block in quick log on $ExtIF inet proto udp from any to any port 43981


#############################################################################
# deny macchine in uscita                                                   #
#############################################################################
#
# PCPLUTO9 XYZ.ZYX.11.133
# pcxx XYZ.ZYX.10.87
#
block out quick log on $ExtIF from { XYZ.ZYX.11.133, XYZ.ZYX.10.87, XYZ.ZYX.12.35 } to any

# 1214 chiusa per Morpheus
#
block out quick log on $ExtIF inet proto { tcp, udp } from any to any port 1214

# 1433-1434 chiusa per  MS-SQL udp/tcp
#
block out quick log on $ExtIF inet proto { tcp, udp } from any to any port 1433><1434

# 2002 vulnerabilita' SSL
#
block out quick log on $ExtIF inet proto { tcp, udp } from any to any port 2002

# 6346-6347 porta Gnutella
#
```

```
block out quick log on $ExtIF inet proto { tcp, udp } from any to any port 6346><6347

# 6667 trojan Sendmail - 9.10.02
#
block out quick log on $ExtIF inet proto { tcp, udp } from any to any port 6667

# 27374 chiusa per worm ramen
#
block out quick log on $ExtIF inet proto { tcp, udp } from any to any port 27374
```